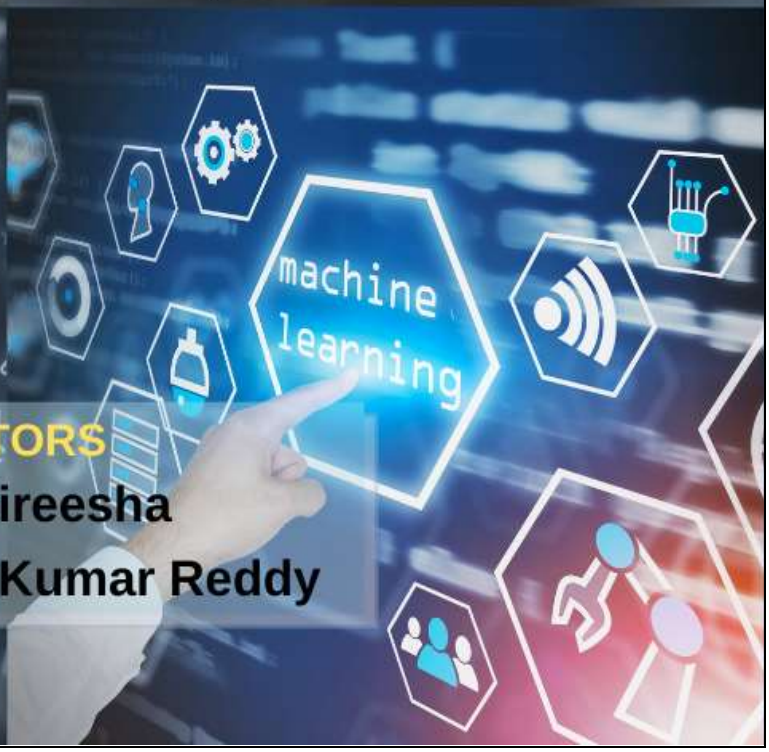
ADVANCED TRENDS IN COMPUTER SCIENCE AND INFORMATION TECHNOLOGY



EDITORS

Dr. V. Sireesha

Dr. Y. Pavan Kumar Reddy

Advanced Trends in Computer Science and Information Technology

EDITORS:

Dr. V.Sireesha
Dr.Y.Pavan Kumar Reddy

First Edition: July 2021

ISBN: 978-93-91303-04-04

Price: 500/-

Published By:

Jupiter Publications Consortium
(Promulgating Your Prudence in Publishing)
Chennai – 600 092.
Mobile: 9790911374 / 9962578190
E-Mail: director@jpc.in.net

Imprint:

Jupiter Publications Consortium

Geethanjali
Institute of Science and Technology

NATIONAL CONFERENCE ON ADVANCED TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (NCATCSIT' 2021)

On 03rd JULY, 2021

EDITORS
Dr. V.Sireesha
Dr.Y.Pavan Kumar Reddy

ORGANISED BY
Geethanjali Institute of Science and Technology, Kovur, Nellore, Andhra Pradesh
(Accredited by NAAC with "A" Grade)
Affiliated to JNTUA, Anantapuram
URL: WWW.gist.edu.in

PUBLISHED BY
Jupiter Publications Consortium
Chennai, Tamil Nadu, India.
www.jpc.in.net

Geethanjali
Institute of Science and Technology

NCATCSIT-

NATIONAL CONFERENCE ON ADVANCED TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY

Department of Computer Science and Technology
Geethanjali Institute of Science and Technology
Accredited with NAAC "A" Grade
Kovur, Nellore, Andhra Pradesh

From Correspondent's Desk

Shri.N.Sudhakar Reddy
Secretary & Correspondant,
Geethanjali Institute of Science and Technology,
Accriated with NAAC "A" Grade
Kovur,Nelllore,Andhra Pradesh

I feel delighted and gratified that the department of CSE is organizing a national level conference on the theme "Advanced trends in CSE and I.T." with a great sense of achievement in the time of the pandemic situation.

I sincerely hope that this event will serve the purpose of providing the students with greater access to the emerging trends in the ever-evolving technology. It is an established truth that society is witnessing rapid strides in computer and information technology, boosting the nation's economy, besides paving the way for social development. On this momentous occasion, I am proudly stating that this institution is the unquestionable pioneer amidst its peer institutions in organizing numerous virtual events, such as workshops, seminars, symposiums, and conferences, thus contributing to the cause of engineering education as part of its corporate social responsibility initiative during these turbulent covid pandemic times it is a common knowledge that such professional events as symposium and conferences will go a long way in expanding the scope of expertise potential and understanding of the engineering aspirants in their respective fields of specialization. In this connection, I am pleased to state that the institution has always been in the forefoot of launching such dynamic initiatives in the best interests of the students by giving them a foretaste of the evolving trends in technology in the 21st century.

I heartily congratulate and compliment the organizers, who are the propelling forces behind the successful conduct of the event.

Shri.N.Sudhakar Reddy

Secretary & Correspondent.

From Secretary's Desk

Shri.P.Sreenivasulu Reddy
Joint Secretary,
Geethanjali Institute of Science and Technology,
Accriated with NAAC "A" Grade
Kovur,Nelllore,Andhra Pradesh

I am happy and proud to note that the department of CSE of holding a National Level Symposium highlighting the theme "Advanced Trends in CSE and I.T.," aiming at the student stakeholders and faculty about the emerging trends in a contemporary technological scenario. None can deny that technology provides a solid foundation on which the edifice of a country's progress rests. If the current generation of engineering students were to stay relevant in the constantly evolving job market scenario, such professional events play a vital role in harvesting their potential while ensuring them brighter, provisioning employment prospects.

I express my profound optimism that this national-level event will eventually benefit budding engineering by igniting the spark of curiosity inherent in their standard frame of mind. Also, in this context, I express my firm belief that this academic and professional event will raise curtains on exciting exchange of ideas, informative deliberations, and enlightening interactions among the young minds and faculty, further enriching and revitalizing their technical expertise and capabilities.

I am delighted to extend my best wishes and compliments to the HOD, CONVENOR, ORGANISING COMMITTEE, and OTHER faculty, whose contribution to the event's successful conduct deserves rich compliments appreciations.

Shri.P.Sreenivasulu Reddy
Joint Secretary

From Principal's Desk

Prof.Dr.G.Subba Rao
Principal,
Geethanjali Institute of Science and Technology,
Accriated with NAAC "A" Grade,
Kovur,Nelllore,Andhra Pradesh.

It gives me great delight to note that the department of CSE is organizing a national level conference on "ADVANCED TRENDS IN CSE AND IT," with the chief objective of keeping the engineering aspirants abreast of the advanced trends in computer science and engineering and I.T. in the emerging technology scenario. It is a refutable fact that seminars, workshops, symposiums, and conferences are dynamic initiatives that form the core of engineering education, facilitating the cross-pollination of innovative ideas and knowledge transfer. These academic initiatives provide a vibrant platform for accelerating society's technological progress by enriching young brains through mutual exchange of knowledge and transformation about their domains of specialization. It is sincerely hoped that the recent national-level conference will focus on the contemporary trends in CSE and I.T.

I very strongly believe that this event will facilitate the confluence of the best trains and provide exposure to the emerging technologies such as ARTIFICIAL INTELLIGENCE, MACHINES LEARNING, ROBOTICS AND DATA SCIENCES and equip the students with adequate awareness and knowledge to match with the requirements of industry thus playing a pivotal role in taking forward the country o the path to technological development on this momentous occasion.

I appreciate the collective dedicated Endeavour put in by the organizers in the successful conduct of this glories event.

Prof.Dr.G.Subba Rao
Principal,
GIST, Nellore

From Convener's Desk

Dr. V.Sireesha,
Professor & Head of Department, CSE
Geethanjali Institute of Science and Technology, Kovur,
Andhra Pradesh

With each passing day, technology is proliferating and evolving rapidly, which calls for special skills, competencies, and capabilities on the students' part to reach the heights of professional excellence in the rapidly changing technology scenario. There is a mounting demand for A.I., Machine Learning, and Data Science Specializations apart from the traditional computer science & Engineering domain. It is really a matter of great pride and privilege to play a lead role as the Head of the Department of Computer Science and Engineering to conduct a National Level Conference on the theme "ADVANCED TRENDS IN CSE AND IT "for the benefit of Engineering aspirants, with the chief objective of facilitating and enlightening interaction and informative deliberations between the students and industry experts which pave the way for this cross-flow of innovative ideas and exchange of knowledge.

On this Auspicious Occasion, I express my firm hope and belief that the national event would serve the intended purpose of providing new thoughts and inputs about the emerging technologies and prepare the students to effectively handle the complex challenges in a broad range of computer-centered domains and usher in technological growth and advancement of the nation.

It gives me great pleasure and pride to state on this glorious occasion that this virtual national level event is unfolding itself with the outstanding team spirit, unwavering commitment, and collaborative effort of the faculty member, technical and non-technical staff of the CSE department. It gives a great pleasure to state that this national event would be successfully conducted with the blessings of our beloved principal and patronage cooperation and support from the management in all aspects.

I express my fond hope that this event would evoke an overwhelming response from the students coming from engineering institutions in various states across the country.

Dr.V.Sireesha,
Head of Department, CSE

Chief Guest's Profile

Dr.Hanumanthappa M
Professor & Chairman,
Department of Computer Science & Applications,
Bangalore University, Bangalore 56.

BIOGRAPHY

Dr. Hanumanthappa.M received his post-graduate degree from Bangalore University and M.Phil in Data Mining. He was bestowed with a Ph.D. degree in Data Mining from Bangalore University in 2009. He is currently offering his excellent services as a professor in the Department of Computer Science and Applications, Bangalore University.

He has gained 15 Years of Research & Teaching Experiences in Data Mining, particularly in Parallel Query Optimization, Application in Computational Fluid Dynamics, Data Mining techniques for software reliability. To his credit Dr.Hanumanthappa.M has published over 115 Technical Papers at various National and International Conferences. He donned the role of a resource person, delivered numerous enlightening technical talks in various reputed Engineering Colleges, and promoted the cause of Computer Science and Engineering. He played a significant role as session chair and keynote speaker at National and International Conferences held across the country and contributed to the enrichment of technical competencies and relevant skills among the engineering aspirants.

Dr.Hanumanthappa.M has supervised 10 Ph.D. students. He authored three monographs. He adjusted nearly 50 Ph.D. and M.Phil Computer Science Thesis of various universities and conducted 18 Viva voice examinations for Ph.D., M.Phil candidates. He published five books related to Computer Science and Fundamentals, Data Warehousing, and Business intelligence. He was a member of, Review Committee for various International Journals, including Springers, ACM. He is a founder of MIAE, IEEE, SWAK, and Indian Science Congress, and his academic and professional caliber and credentials are outstanding.

I am sure that Engineers from the Industry and Academic Institution will go a long way in knowledge sharing to help engineering students grow and compete globally. The conference will provide a dynamic platform to facilitate the exchange of innovative ideas and create networks for R & the development of R&D.

I convey my warm greetings & best wishes to all the participants and wish the event a grand success.

DR. HANUMANTHAPPA M

NCATCSIT-2021

NATIONAL CONFERENCE ON ADVANCED TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY

Keynote Speakers

Keynote Speaker Profile

Dr. M.V.P. Chandra Sekhara Rao,
Professor, Dept. of CSE,
RVR & JC College of Engineering
Guntur, Andhra Pradesh

BIOGRAPHY

Dr. M.V.P Chandrasekhara Rao received his Engineering Degree from Gulbarga University, M.S in Computer System from BITS, Pilani, and M.Tech from JNTU Kakinada in 2003. He was awarded the Ph.D. Degree in Computer Science and Engineering from JNTU Hyderabad in 2012. In 1995, he started his career as a Programmer and gained his Professional Experience step by step and currently offering his valuable services as a Professor in the Department of Computer Science and Engineering at RVR & J.C. College of Engineering Guntur.

He has over 25 years of Teaching Experience in Computer Science and Engineering, particularly in Data Warehousing and Data Mining. He has published over 35 papers in Reputed Journals like **SCOPUS.** He has three patents issued by the Government of India in Deep learning and Deep Neural Networks, Image Classification. He has guided 7 Ph. D Scholars under his Guidance.

To his credit, he notched up best performing SPOC awards for achieving "A.A." Rating in NPTEL Local Chapters. He eminently discharged multiple responsibilities as a coordinator at the college level. He has a Life Membership in the Indian Society for Technical Education, Computer Society of India, and IAENG. He has delivered his enlightening lectures on the major domains of Computer Science and Engineering at various Engineering colleges, thus widening the scope of knowledge and expertise of the engineering aspirants.

Through this conference, I am delighted that our teachers and students will get an opportunity to interact with Research Scholars and renowned experts from engineering institutions of national and global repute and standing.

On this glorious occasion, I am pleased to convey my warm compliments and best wishes to all the participants and wish the event a grand success.

DR. M.V.P. CHANDRASEKHARA RAO

Keynote Speaker Profile

Dr. Kesavan
Principal
Bangalore College of Engineering and Technology
Bangalore

BIOGRAPHY

Area of Research Interest:

- Mobile Communication
- Antennas and Radiation
- Microwave Strip Antennas
- Digital & Analog Communication

Dr.Kesavan received his B.E Degree in Electronics and Communication Engineering from NIT, Trichy. He received his M.E in Analog Communications from Anna University, Chennai.

Dr.Kesavan received his Doctoral Degree in Mobile Communication from Anna University Chennai.

Dr. Kesavan has over 21 years of Teaching Experience with three years of PRINCIPAL as a desk at Bangalore College of Engineering and Technology, Bangalore. He has published over 23 Research Papers in the Field of Communication Engineering in various Reputed National and International Journals.

I convey my warm greetings and best wishes to all the participants and a great success.

Dr. KESAVAN

Keynote Speaker Profile

Dr. Saleti Sumalatha
Assistant Professor
Department of Computer Science and Engineering
SRM University
Andhra Pradesh

BIOGRAPHY

Area of Research Interest:

- To implement a learning management system and study the navigational patterns to enhance students learning.
- To develop incremental mining algorithms

Awards & Fellowships:

Ph.D. Fellowship – Ministry of Human Resource Development

Dr. Saleti Sumalatha completed her B.Tech graduation in Computer Science and Engineering from Narayana Engineering College, JNTU Hyderabad, in 2004. She pursued her M.Tech in Computer Science and Engineering from Annamacharya Institute of Science and Technology, JNTU Anantapur. She was awarded her Doctoral Degree from the National Institute of Technology, Warangal.

It speaks volumes of the technical excellence she has achieved as Dr. SaletiSumalatha published several Technical Papers in National and International Proceedings and Journals. Her current Research Interest includes Big Data, Data Mining, and Machine Learning.

I convey my warm greetings and best wishes to all the participants and wishing the grand event success.

Dr.S.SUMALATHA

NCATCSIT-2021
Geethanjali Institute of Science and Technology, Kovur, Nellore, Andhra Pradesh

NATIONAL CONFERENCE ON ADVANCED TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY

Organizing Committee Members:

- Dr.P.Nagendra Kumar
- Dr.M.Mathan Kumar
- Mrs.V.Gayatri
- Mrs.V.Bharathi,
- Mrs.N.Siva Nagamani
- Mr.Sk.Asiff
- Mr.Y.V.Ramesh,
- Mrs.K.Sukeerthi,
- Mr.Sd.Hyder,
- Mr.K.Chiranjeevi,
- Ms.K.Sreelakshmi,
- Mr.T.Prasanth,
- Mrs.P.Chandrakala,
- Mrs.N.Divya Sruthi,
- Mr.Muralidharan

Table of Contents

This Page Intentionally Left Blank

ADAPTIVE BEAMFORMING BY USING LMS ALGORITHM FOR SMART ANTENNA

P.Sree Lakshmi[1], V.Meghana[2] M.Mahitha[3], L.Sasidhar Reddy[4], B.Pavan Kumar[5],
Assoc.Professor[1], UG Scholar[2,3,4,5] Department of ECE, Audisankara institute of technology
SPSR Nellore, Andhra Pradesh, India-524101

Abstract:

The smart antennas are widely used for wireless communication, because it has a ability to increase the coverage and capacity of a communication system. Smart antenna performs two main functions such as direction of arrival estimation (DOA) and beamforming. Using beamforming algorithm. smart antenna is able to form main beam towards desired user and null in the direction of interfering signals. This paper evaluate the performance of LMS (Least Mean Square) beamforming algorithm in the form of normalized array factor (NAF) and mean square error(MSE) by varying the number of elements in the array and the placing between the sensor elements. The simulations are carried out using MATLAB.

Keywords:

DOA (direction of arrival), LMS (least mean square),AF (array factor)

1. Introduction

Adaptive beamforming is a technique in which an array of antennas are used to achieve maximum reception in the direction of desired user while signals of same frequency from other directions are rejected. This is achieved by varying the weights of the each of antennas used in the array. A smart antenna system combines multiple antenna elements with a signal- processing capability to optimize its radiation and or reception pattern automatically in response to the signal environment. Multiple antennas have ability to enhance the capacity and performance without the need of of additional power or spectrum. In adaptive beamforming the optimum weights are iteratively computed using complex algorithms based upon different criteria. The criteria for choosing the adaptive beamforming algorithm is depends on it's performance and convergence rate.

Adaptive beamforming algorithm can be classified in to two main categories such as Non blind and blind adaptive algorithms. Non blind adaptive algorithms require the statistical knowledge of the transmitted signal in order to converge to a weight solution. This is achieved by using a pilot training sequence sent over the channel to receiver to help to identify the desired user. Whereas, blind algorithms do not need any training sequence, hence the term 'blind'. They attempt to restore some characteristic of the transmitted signal in order to separate it from the other users in the surrounding environment. This paper focus on the implementation of Least Mean Square(LMS) algorithm which is a type of non blind algorithm.

Types of Beamforming

Beamforming is customarily categorized into switched beamforming or adaptive beamforming. The following are distinctions between the two major categories of Beamforming regarding the choices in transmit strategy.

Switched Beamforming

Switched beamforming from multiple fixed beams with heightened sensitivity in particular directions. These antenna systems detect signal strength, choose from one of several predetermined, fixed beams and switch from one beam to another as the mobile moves throughout the sector. Instead of shaping the directional antenna pattern with the metallic properties and physical design of a single element (like a sectorized antenna), switched beam systems combine the outputs of multiple antennas in such a way as to form finely sectorized (directional) beams with more spatial selectivity than can be achieved with conventional, single-element approaches as shown in figure 1.1

ISBN: 978-93-91303-04-04

Figure 1.1 Switched Beamforming Coverage Pattern.

Adaptive beamforming

Adaptive beamforming represents the most advanced smart antenna approach to date. Using a variety of new signal-processing algorithms, the adaptive system takes advantage of its ability to effectively locate and track various types of signals to dynamically minimize interference and maximize intended signal reception. Both systems attempt to increase gain according to the location of the user. However, only the adaptive system provides optimal gain while simultaneously identifying, tracking, and minimizing interfering signals.

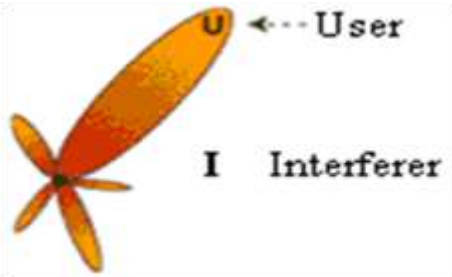


Figure 1.2: Adaptive Array Coverage.

The figure 1.2 shows, Omni directional antennas are obviously distinguished from their intelligent counterparts by the number of antennas (or antenna elements) employed. Switched beamforming and adaptive beamforming however, share many hardware characteristics and are distinguished primarily by their adaptive intelligence. To process information that is directionally sensitive requires an array of antenna elements (typically 4 to 12), the inputs from which are combined to control signal transmission adaptively. Antenna elements can be arranged in linear, circular, or planar configurations and are most often installed at the base station, although they may also be used in mobile phones or laptops.

ADAPTIVE ALGORITHMS:

The adaptive algorithm used in the signal processing has a profoundeffect on the performance of a Smart Antenna system. Although thesmart antenna system is sometimes called the Space DivisionMultiple Access, it is not the antenna that is smart. The function of an antenna is to convert electrical signals into electromagnetic waves or vice versa but nothing else. The adaptive algorithm is the one that gives a smart antenna system its intelligence. Without an adaptive algorithm, the original signals can no longer be extracted. Adaptive beam forming algorithms are classified as either DOA-based, temporal-reference based, or signal-structure-based. In DOA-based beam forming, the direction-of-arrival algorithm passes the DOA information to the beam former. The beam forming algorithm is used to design a radiation pattern with the main beam directed towards the signal of interest, and with nulls in the directions of the interferers. On the other hand, temporal-reference beam formers use a known training sequence to adjust the weights, and to form a radiation pattern with a maximum towards the signal of interest and nulls towards the signals not of interest.

LMS Algorithm

The Least Mean Square (LMS) algorithm, introduced by Windrow and Hoff in 1959 is an adaptive algorithm, which uses a gradient-based method of steepest decent. LMS algorithm uses the estimates of the gradient vector from the available data. LMS incorporates an iterative procedure that makes successive corrections to the weight vector in the direction of the negative of the gradient vector which eventually leads to the minimum mean square error. Compared to other algorithms LMS algorithm is relatively simple. The LMS algorithm is based on the principle of the steepest descend and is applied to the MSE performance measurement.

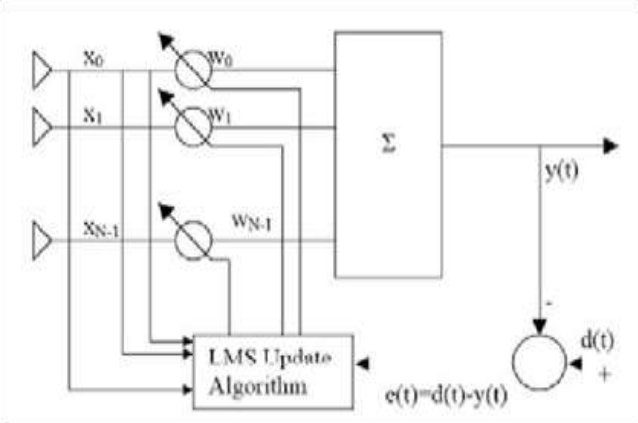


Figure 1.3:- Block diagram of LMS algorithm.

ISBN: 978-93-91303-04-04

2. RESULTS AND DISCUSSION:

For simulation purposes the uniform linear array with M number of element and input signal is modulated by using BPSK modulation is considered. simulation of LMS algorithm is carried out using MATLAB to illustrate how various parameters such as number of antenna element, inter element spacing ,number of interferes and variation in SNR parameter affect the beam formation and convergence of the algorithm.

Consider that the desired users is arriving at an angle of 30 degree and an interfere user at an angle of -50 degree. The spacing between the individual element is half wavelength and the signal to noise ratio(SNR) is 30db. The array factor for 8 element antenna antenna array is computed.

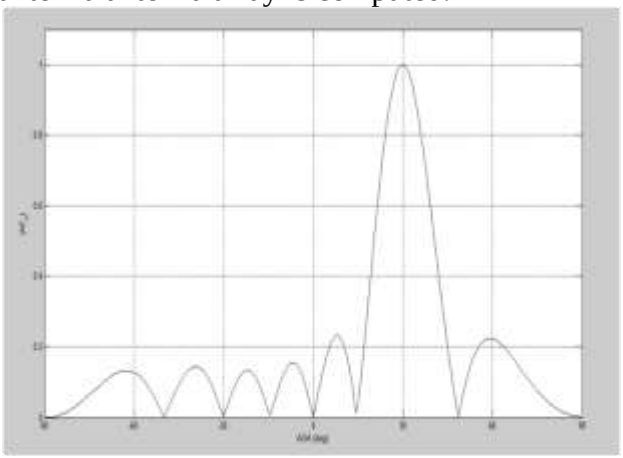


Figure 1.4:- Array Factor plot when user is in 30 degrees and interference is in -50 degrees.

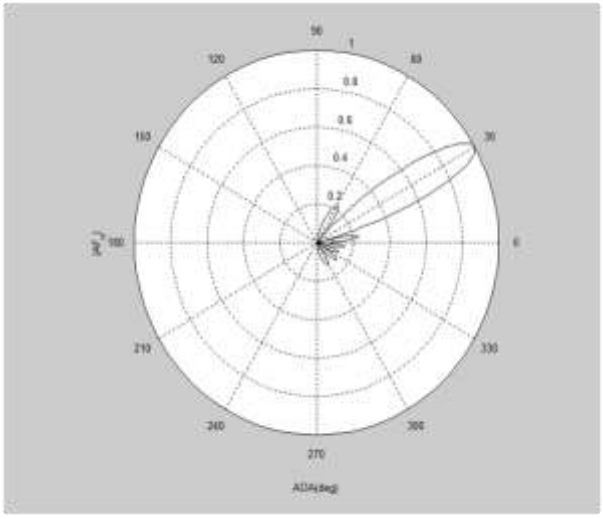


Figure 1.5:- Polar Array Factor plot when user is in 30 degrees interference is in -50 degrees.

The optimum complex weights in the case for which the algorithm converges is as follows.

The weights for the N = 8 ULA are:

w1 = 1
w2 = 0.039282+0.96946i
w3 = -1.0191+0.035592i
w4 = -0.0012587-0.98307i
w5 = 0.98175-0.050995i
w6 = 0.018624+1.0195i
w7 = -0.97018+0.012303i
w8 = -0.053152-0.99859i

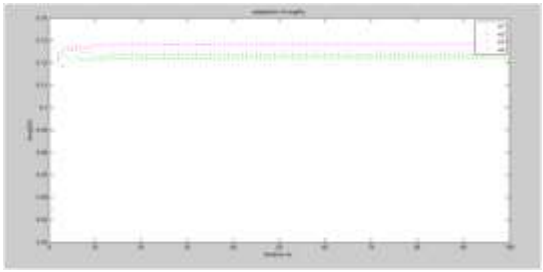


Figure 1.5:- magnitude of weights when no. of array elements is 8.

Another simulation result is describes the algorithmic changing the weighting in each iteration. From figure 6.3, it is observed that this algorithm converge after 50 iterations. As number of iterations increases the weights remains constant.

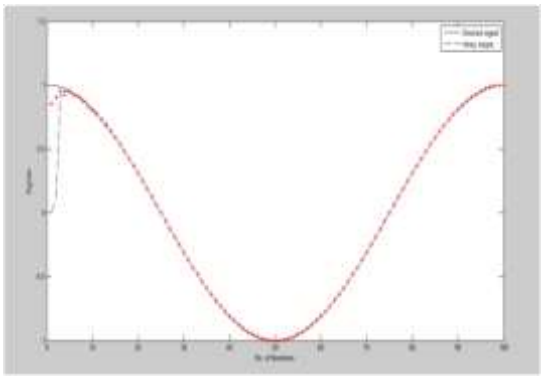


Figure 1.6:- **Acquisition and tracking of desired signal and actual array output.**

Another simulation is as shown in figure. 6.4it is observe that the array output acquires and tracks the desired signal after 50 iterations. If the signal characteristics are rapidly changing, the LMS algorithm may not allow tracking of the desired signal in a satisfactory manner.

ISBN: 978-93-91303-04-04

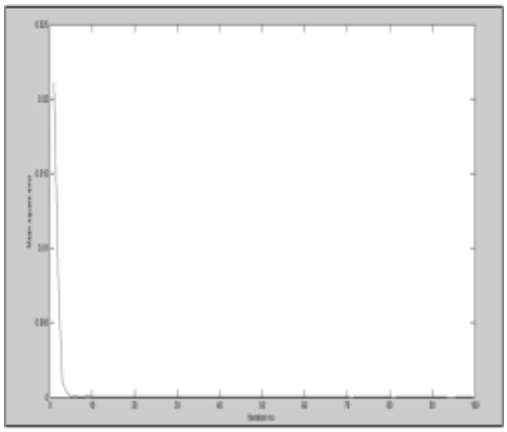


Figure 1.7:- Mean square error Vs iteration number.

Finally, we simulated the MSE error in each iteration. From figure 6.5, it is observed that MSE is decreases each iteration and it is converge after 50 iterations. By increasing the number of iterations the mean square error value decreases and tracking of desired signal is improved.

3. CONCLUSION:

In this work , we analysis the performance of adaptive LMS algorithm for smart antenna systems which very important for smart antenna design. The performance of LMS algorithm is compared on the basis of normalized array factor and mean square error (MSE) for SA systems. It is observed that an LMS algorithm is converging after 50 iteration. The attractive quality of LMS algorithm is less computational complexity. Our findings are explained in details in the above result and analysis section with graphs.In this, adaptive beamforming techniques such as Least Mean Square Algorithm and is used to achieve the minimum mean squared error, convergence rate and coverage area. This algorithms is used in smart/adaptive antenna array system in coded form, to enhance mobile communication system performance. It is confirmed from the results that narrow beam of beam of smart antenna can be steered towards the desired direction by steering beam angle, keeping element spacing 0.5λ , number of elements n and altering weights w(n) adaptively. In The Least mean square algorithm by increasing the number of iterations mean square error is reduced and tracking of desired Signal is improved. Convergence rate and coverage area is also improved in LMS algorithm.

BIBLIOGRAPHY:

1. M. Yasin, Dr. Pervez Akhtar and Dr. Valiuddin "Performance Analysis of LMS and NLMSAlgorithms for a Smart Antenna System" Published in International journal of Computer Applications, Volume 4-No. 9, August 2010.

2. U.Chalva.,Dr.P.V.Humgund., "Performance Study of a Non-blind Algorithm for Smart Antenna System", International Journal of Electronics and Communication Engineering", Vol.5,Issue 4,pp.447-455,2012.

3. D.M.M.Rahaman., Md.M.Hossair, "Least Mean Square (LMS) For Smart Antenna", Universal Journal of Communications and Network",pp-16-21,2013.

4. M.Jain.,V.Gupta., "Performance Analysis of MUSIC LMS Algorithm for Smart Antenna", International Journal of Scientific Engineering and Technology,Vol.2,Issue 10,pp1004-1007,2013.

5.V.Kumar.,Dr.Rajouria., "Performance Analysis of LMS Adaptive Beamforming Algorithm", International Journal of Engineering and Communication Technology,Vol.4,Issue 5,July-Sept-2013.

6..RevatiJoshi,Ashwinikumar Dhande "ADAPTIVE BEAMFORMING USING LMS ALGORITHM" International Journal of Research in Engineering and Technology (IJRET)eISSN: 2319-1163 | pISSN: 2321-7308,2014.

PAPR Reduction in OFDM systems using Selective Mapping

N.Bhargavi[1], Ch.Venkata Saraswathi[2], G.Yaswanth[3], K.Dileep Kumari[4], , Syed Aleem[5]
[1,2,3,4,5] Department of ECE, Audisankara Institute Of Technology, Gudur, Andhrapradesh.

Abstract: To eliminate this high PAPR, many techniques have been proposed, among which SLM (Selective Mapping) technique is considered to be the best PAPR reduction techniques. In this technique we first generate a number of alternate OFDM signals from the original data block. These are then transmitted to the OFDM signal having minimum PAPR (peak-to-average power ratio). SLM (Selective Mapping) system use the sample powers of sub blocks to generate cost functions for selecting samples to estimate the peak power of each candidate signal, thus reducing the computational complexity of the system. The data rate and complexity at the transmitter side is one of the best advantages for this technique when compared to the other techniques for PAPR (peak-to-average power ratio) reduction.

Keywords: PAPR, OFDM, data block, Selective mapping, power

1. Introduction:

Communication is one of the important aspects of life. Signals were initially sent in the analog domain , are being sent more and more in the digital domain. For better transmission, even single carrier waves are being replaced by multi carriers. Multi carrier systems like CDMA and OFDM are now a day's being implemented commonly. In the OFDM system, orthogonally placed sub carriers are used to carry the data from the transmitter end to the receiver end. Presence of guard band in this system deals with the problem of ISI. But the large Peak to Average Power Ratio(PAPR) of these signal have some effects on the communication systems. The major drawback of orthogonal frequency-division multiplexing(OFDM) is its high Peak-to-average power ratio(PAPR).

The demand of high data rate services has been increasing very rapidly and there is no slowdown in sight. We know that the data transmission includes both wired and wireless medium. Often, these services require very reliable data transmission over very harsh environment. Most of these transmission systems experience much degradation such as large attenuation, noise, multipath, interference, time variance, nonlinearities and must meet the finite constraints like power limitation and cost factor. One physical layer technique that has gained a lot of popularities due to its robustness in dealing with these impairments is multi-carrier modulation technique. In multi-carrier modulation, the most commonly used technique is Orthogonal Frequency Division Multiplexing (OFDM); it has recently become very popular in wireless communication.

Unfortunately the major drawback of OFDM transmission is its large envelope fluctuation which is quantified as Peak to Average Power Ratio (PAPR). Since power amplifier is used at the transmitter, so as to operate in a perfectly linear region the operating power must lies below the available power. For reduction of this PAPR lot of algorithms have been developed. All of the techniques has some sort of advantages and disadvantages [1]. Clipping and Filtering is one of the basic technique in which some part of transmitted signal undergoes into distortion. Also the Coding scheme reduces the data rate which is undesirable. If we consider Tone Reservation (TR) technique it also allows the data rate loss with more probable of increasing power. Again the techniques like Tone Injection (TI) and the Active Constellation Extension (ACE) having a criteria of increasing power will be undesirable in case of power constraint environment. If we go for the Partial Transmit Sequence (PTS) and Selected Mapping (SLM) technique, the PTS technique has more complexity than that of SLM technique.

Digital Communication System

The A/D converter being used to convert the analog source to the digital i.e in the form of binary sequences. The source encoding takes place to compress the transmitted digital data up to an extent such that it can be received without any loss. There are some basic source coding techniques are available like the Hoffman coding and Shannon-

ISBN: 978-93-91303-04-04

Fano coding. The objective of source encoding is to remove redundancy from the source. The sequence of binary digits from the source encoder also known as information sequence, is passed to the channel encoder. The channel encoder add redundant bits to the information sequence from the received signal for the reliable communication. The channel encoder maps k information bits into a unique n bit sequence called codeword. The ratio n k is a measure of the redundancy introduced by the channel encoder and the reciprocal of this ratio is called code rate. The output of the channel encoder is passed to the digital modulator.

The digital modulator maps the binary information sequence into signal waveforms. The modulation may be binary or m−ary. In binary modulation two distinct waveforms are used to represent the binary digits 0 and 1 whereas in m−ary modulation m = 2b distinct waveforms are used to represent a binary word of b bits. The modulated wave form is being transmitted from the transmitter to the receiver through channel. In the channel due to addition of noise the transmitted signal becomes corrupted.

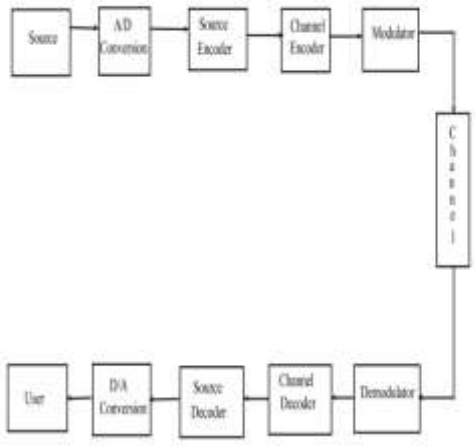


Figure 1-1: Block Diagram a General Digital Communication System

Multipath Channels

The sources of noise are thermal noise, atmospheric noise, manmade noise etc., which are random in nature and generally unpredictable. At the receiving end the digital demodulator consists of matched filter type detector or correlator type detector converts the received signal waveforms into binary sequence, which represent the estimated word. The output from the demodulator is passed to the channel decoder, that recovers the information sequence from the knowledge of the code.

The transmitted signal faces various obstacles and surfaces of reflection, as a result of which the received signals from the same source reach at different times. This gives rise to the formation of echoes which affect the other incoming signals. Dielectric constants, permeability, conductivity and thickness are the main factors affecting the system. Multipath channel propagation is devised in such a manner that there will be a minimized effect of the echoes in the system in an indoor environment. Measures are needed to be taken in order to minimize echo in order to avoid ISI (Inter Symbol Interference). The figure 1.2 shows the scenario for multipath propagation.

Muticarrier Transmission Schemes

In a single carrier system, a single fade causes the whole data stream to under go into the distortion i.e known as the frequency selective fading. To overcome the frequency selectivity of the wideband channel experienced by single-carrier transmission, multiple carriers can be used for high rate data transmission. In multicarrier transmission [4], a single data stream is transmitted over a number of lower rate subcarriers. The figure 1.3 shows the basic structure and concept of a multicarrier transmission system

Figure 1-2 Multipath Propagation

ISBN: 978-93-91303-04-04

Using this multicarrier transmission the frequency-selective wideband channel can be approximated by multiple frequency-flat narrowband channels. Let the wideband be divided into N narrowband subchannels, which have the subcarrier frequency of fk, k = 0, 1, ..., N − 1. Orthogonality among the subchannels should be maintained to suppress the ICI (Inter Carrier Interference) which leads to the distortionless transmission. So in this transmission scheme the different symbols are transmitted with orthogonal subchannels in parallel form[6]. If the oscillators are being used to generate the subcarriers for each subchannel, the implementation of this transmission scheme becomes complex. To avoid this complexity one important transmission scheme comes into picture that is the OFDM (Orthogonal Frequency Division Multiplexing).

Inter Symbol Interference

Inter symbol interference (ISI) is a form of distortion of a signal in which one symbol interferes with subsequent symbols. This is an unwanted phenomenon as the previous symbols have similar effect as noise, which makes the communication as some sort of unreliable. It is usually caused by multipath propagation or the inherent nonlinear frequency response of a channel causing successive symbols to blur together. The presence of ISI in the system introduces error in the decision device at the receiver output. Therefore, in the design of the transmitting and receiving filters, the objective is to minimize the effects of ISI and thereby deliver the digital data to its destination with the smallest error rate possible[5].

Inter Carrier Interference

Presence of Doppler shifts and frequency and phase offsets in an OFDM system causes loss in orthogonality of the sub-carriers. As a result, interference is observed between sub-carriers. This phenomenon is known as inter - carrier interference (ICI)[7].

Cyclic Prefix

The Cyclic Prefix or Guard Interval is a periodic extension of the last part of an OFDM symbol that is added to the front of the symbol in the transmitter, and is removed at the receiver before demodulation[8]. According to the figure 1.5 the addition of Cyclic Prefix (CP) takes place after the parallel to serial conversion and being removed at the receiver side before the DFT operation. The OFDM symbol with considering the Cyclic Prefix is shown in figure 1.3.

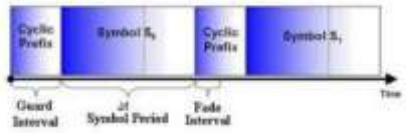


Figure 1.3: Cyclic Prefix

2. RESULTS AND DISCUSSIONS:

Complexity analysis of STBC MC-CDMA and SISO MC-CDMA

T he complexities associated in both SISO and STBC schemes are summarized in table 3.1 .STBC scheme employing two transmitting antennas and one receiver antenna performs better than SISO schema.

Table1: Complexity analysis associated with STBC MC-CDMA and SISO MC-CDMA in terms of PAPR and BER performance

System Type	SNR in Db at BER of 10^{-3}	PAPR in dBA at PAPR of 10^{-3}
STBC	8.9	6.8
SISO	18	6.5

DF plot for Selective Mapping scheme

The figure shows the CCDF plot for selective mapping scheme. As the number of antennas are increased on the either side of the transmitter or receiver , the PAPR will increase but at the same time diversity order will increase which in turn will improve the BER performance. So there is always a trade-off when going for higher number of antennas to achieve minimum PAPR and better BER performance.

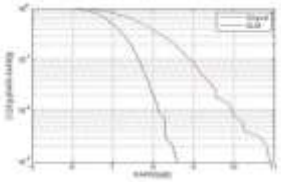


Figure 1.4: CCDF plot for the Selective Mapping scheme.

ISBN: 978-93-91303-04-04

3. CONCLUSION

The proposed STBC MCCDMA with SLM technique is compared with SISO MC-CDMA with SLM technique in terms of CCDF and BER performance. CCDF plots show that SISO MC-CDMA with SLM scheme performs marginally better than STBC MC-CDMA with SLM scheme at a huge BER degradation. CCDF and BER plots for multiple users have also been plotted and it can be concluded that as the no of users increase the CCDF performance improves and BER performance degrades.

BIBILOGRAPHY

1. M. D. Hassib, M. Singh, M. Ismail and R. Nordin, "Efficient and low complexity STBCOFDM scheme over fading channel," in Communications (APCC), 2012 18th Asia-Pacific Conference on, 2012

2. S. H. Han and J. H. Lee, "An overview of peak-to-average power ratio reduction techniques for multicarrier transmission," Wireless Communications, IEEE, vol. 12 no. 2, pp. 56-65, 2005.

3. V. Tarokh, H. Jafarkhani and A. R. Calderbank, "Space-time block codes from orthogonal designs," Information Theory, IEEE Transactions on, vol. 45, no. 5, pp. 1456-1467, 1999.

4. S. Alamouti, "A simple transmit diversity technique for wireless communications," Selected Areas in Communications, IEEE Journal on, vol. 16, no. 8, pp. 1451-1458, 1998

5. Shah, A. M. Haimovich, M. K. Simon, and M.-S. Alouini, et al, (2000)

6. V. Tarokh, H. Jafarkhani and A. R. Calderbank, "Space-time block codes from orthogonal designs," Information Theory, IEEE Transactions on, vol. 45, no. 5, pp. 1456-1467, 1999

7. S. Alamouti, "A simple transmit diversity technique for wireless communications," Selected Areas in Communications

8.Bauml, R., Fischer, R., and Huber, J,"R Guangyue Lu1, Ping Wu and Catharina CarlemalmLogothetis," Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping" IEE Electronics Letters, vol. 32,pp. 2056-2057, 1996. 9.Pankaj Kumar Sharma," Power Efficiency Improvement in OFDM System using SLM with Adaptive Nonlinear Estimator" World Applied Sciences .

Parallel Decoding For Burst Error Detection And Correcting

K.Shashi Kumar , thilak.d ,sushma.k, dhamini.c , venkata sai ramya.v
Department of ECE ,Srinivasa Ramanujan Institute OfTechnology ,Anantapuramu,515701,
Andhra Pradesh, India

ABSTRACT: With growing technologies, burst mistakes or cluster mistakes in various memory types are getting more and more prevalent. Some of the processes that create clustered mistakes include multiple bit upset caused by particle hits, write trouble errors and magnetic field coupling. A novel class of single burst error codes was introduced throughout this project that corrects an explosion of any magnitude in such a codeword. A code-building process is described that allows us to create an existing scheme, e.g. Hamming codes. The novel approach for decoding that suggested class of codes, particularly allows quicker decoding, also was described. Different Hamming code constructs and BCH codes have indeed been proposed for this project as well as the decoding difficulty and duplication are compared with current techniques. The approach described reduces the decoder complexity throughout all circumstances, especially for larger burst error sizes, to little or no increased data redundancy. Throughout this research, a parallel decoding system is demonstrated using a novel family of single explosive error correction codes. The suggested parallel decoding system allows fast decoding. This applies in particular with memories that are sensitive to latencies read or access. A novel building approach is developed that allows the suggested rules to be extracted from current codes to fix a single explosion fault.

1.INTRODUCTION

From over years, technology growth has led to less and less geometry of devices. This is what has led to several challenges, both with known memory technologies and with new types of coming memory technologies. One sort of failure is indeed a burst error that is becoming common in many kinds of memory because of the declining functionality. Take a look at static random memory (SRAM). Soft radiation defects constitute a major challenge for SRAM reliability[1]. The technological scale also considerably enhanced the sensitivity of SRAMs to soft-errors[2]. Device geometries were modest at today's nanometric nodes and devices keep shrinking with technological scaling. A particle attack might thus impact many cells that cause multiple bit upset (MBU)[3]. This same smaller the geometries of something like the device, the increasing the number of cells impacted by a single blow. A partial b-bit burst triggered by this b-bit hit may cause this same b-bit burst window to flip several bits.

A similar issue is also present in the dynamic random access memory (DRAM)[4]. The challenge occurs because of technology scaling's narrow physical dimensions. While it may boost a chip's memory capacity, this also facilitates the interaction between near-by or neighbouring DRAM cells. Access to a memory cell therefore causes a disruption in the surrounding memory cells to lead to the cargo leaking into or out of the cell. With sufficient access, you may reverse the presently held value of both the adjoining cell.

Through a memory access anywhere at given moment, a single b-bit burst error may occur near the cell to which the explosion is located.

The essential premise of rectifying error codes which solve these problems is that a single burst of mistake should be corrected in the codes. Not all bits or symbols may change throughout the burst window b. Codes targeted at solving these problems should thus be there in the location of a burst error throughout order to fix all potential combinations of errors inside a b-bit burst window.

Another parallel decoding approach is proposed for with this project in such a novel class for single burst correction errors. The suggested parallel decoding system allows fast decoding. This applies in particular with memories that are sensitive the latencies read or access. A novel building approach is developed that allows the suggested rules to be extracted from current codes to fix a single explosion fault. Draft findings were submitted in [5] and [6] for both the proposed system. One essential characteristic of both the proposed family for codes is that even the area of both the decoding circuit was significantly

ISBN: 978-93-91303-04-04

reduced especially unless the burst size was adjusted *b*.

2.LITERATURE SURVEY

Soft errors in advanced computer systems by R. Baumann,

1. As computer devices' size and operational voltages decrease to meet the insatiable desire of customers for increased density, more functionality and less power usage, radiation susceptibility grows drastically. The main radiation concern in terrestrial applications seems to be the soft error, which allows a single radiation incident to destroy a data bit contained in either a device, so long as fresh data is put into it. This paper studies and is applicable completely the sensitivity towards soft-error in current systems. The talk includes ground radiation methods that have the biggest influence on circuit functioning as well as the influence of scaling technologies mostly on memory and logic soft error rates.

2. Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors by Yoongu Kim; Ross Daly; Jeremie Kim; Chris Fallin; Ji Hye Lee; Donghyuk Lee Memory isolation seems to be a vital feature of a dependable safe computer system. Unplanned side effects upon data that are saved at other locations should not be allowed to control a single memory location. However, when the technique of DRAM processes falls back to smaller measurements, it becomes harder to keep DRAM cells without interacting electrically. Throughout this article, we highlight DRAM chips' sensitivity to disturbance. Through reading out of the same DRAM address, they demonstrate that data inside the neighbouring addresses may be corrupted. In particular, activating the very same DRAM row corrupts information in neighbouring rows. Intel and AMD systems use malicious programmes to exhibit this phenomena, which causes multiple DRAM accesses. Researchers induce mistakes in 3 main DRAM manufacturers in many other DRAM modules (110 out of 129). We infer from all this that there is a danger of numerous deployed systems. The fundamental source of disturbances is identified as the repetitive toggling of even a DRAM line, particularly underlines intercell coupling factors that speed charging out of surrounding rows. We give a comprehensive characterization study with FPGA-based tests for trouble faults and behaviour. Our major results indicate that I it requires 139K visits to make a mistake, and (ii) it is sensitive to mistaken access at up to the one in each 1.7K cell. We suggest a low-overhead strategy to avoid mistakes after studying many possible strategies to approach the issue.

Systematic b-adjacent symbol error correcting reed-solomon codes with parallel decoding by Abhishek Das; Nur A. Touba. With technology rising, the likelihood of writing disruptions in non-volatile memory influencing surrounding memory cells keeps growing. Specifically, multilevel cell (MLC) phase change memories (PCM) is affected by these faults affecting many nearby memory cells. Reed Solomon (RS) codes provide strong protection for errors when multi-bit symbols may be corrected at once. However the decoding complexity and decoding delay are quite high further than a single symbol error correction. These study presents a systematic b-adjacent coding error, built on Reed-Solomon codes, including one step decoding technique, with low latency and low complexity. There is an universal code building process which can repair most b-adjacent symbol mistakes. In comparison with the current adjacent symbol error that corrects Reed-Solomon codes, these suggested codes are proven to obtain a greater latency throughout the decoder. Furthermore displayed is a substantially improved redundancy compared towards the orthogonal Latin Square (OLS) code correction error.

Siva Sreeramdas, S.Asif Hussain and "Dr.M.N.Giri Prasad proposed on Secure Transmission for Nano-Memories using EG-LDPC"

For even more about a decade memory cells were protected against soft errors, which made the encoder and decoder circuitry surrounding the memory blocks vulnerable to soft errors as just a result of the increased soft error rate on logic circuits and then also needed protection. This introduces a novel

way to designing fault-proof memory encoders and decoders. The primary original aspect of this research is to discover and define a new class of error-fixing codes that simplify the design of FSDs and quantify the relevance of the shielding the circuitry comprising encoders and decoders

ISBN: 978-93-91303-04-04

from passing mistakes in a certain way. With the use of the Euclidean GEM (EG-LDPC) algorithm, the error-secure sensor function is provided. Can use some of the smaller LDPC EG codes, you may accept 10% or 10% bit or nanowire defect rate as well as 10-18 device/cycle failure rate throughout the whole memory system well below a FIT rate and 1011 bit/cm2 memory level with 10 nm nano-wire pitch besides 10 mb or more memory blocks. Larger EG-LDPC codes may increase reliability and save overhead.

3.EXISTING METHOD

Latin squares are indeed the basis for OLS codes. A latent square m is also an m x m matrix which includes permutations from its rows and columns of numbers 0, 1,..., m − 1. Whenever overlaid, each ordered pair with components appears once and only, two Latin squares become orthogonal. OLS codes come from OLS. Such codes contain the number of k = m2 and the number of features which the code corrects. Their number of bits is 2 tm. The code t = 2, and hence, 4 m check bit, is utilised for the double error correction. One benefit of OLS codes was their modular architecture, as indicated throughout the introduction. To get a code that would rectify t +1 faults, just add 2m check bits to both the code which can rectify t faults. This may be beneficial for implementing adaptive bug fixing strategies. The modular feature also allows you to choose the ability to repair errors for a specified text size. As already established, OLS codes could be decoded utilizing OS-MLD, since each data bit is precisely 2t check bits, with one another bit at most another of the check bits. That allows for easy rectification if the incorrect number is t or less. The 2t bits have been replenished as well as a majority voting has been taken. That bit is wrong and has to be fixed when one value was received. If not, the piece is okay. Under the worst scenario, the rest of
both the t -1 mistakes may impact t −1 checkbits so long as they have t or less.

$$H=\begin{bmatrix}
1&0&0&0&0&0&0&1&0&0&1&0&1&0&1&1&1&0&0&0&1&0&0\\
0&1&0&0&0&0&0&0&1&0&1&1&0&1&1&0&0&1&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&1&1&0&1&0&0&1\\
0&0&0&1&0&0&0&1&0&0&1&0&0&0&1&0&1&0&1&1&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&1&1&1&1&0&0&0&0&1&1&0&0\\
0&0&0&0&0&1&0&0&1&0&0&0&1&1&0&0&0&1&0&1&0&0&1\\
0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&1&0&1&1&1&0&1&1
\end{bmatrix}$$

Fig.1. Parity check matrix for OLS code with k = 16 and t = 1.

(1) Thus, a majority of t + 1 still triggers an erroneous bit correction. In either event, the decoding commences with the recalculation of the parity control bits and control of both the stored parity control bits. OLS codes are created from of the Parity check matrix H. Such as instance, the matrix of a code with k = *16* and 8 bits which may fix individual faults appears in Fig 1. For codes which would correct more mistakes, the modular design of both the OLS codes in this matrix is part of the H matrix. For instance, eight more rows will be added to the H matrix to get a code that really can rectify two mistakes. Another H-matrix for just an SEC OLS was created as follows for just an upper bound of $k = m2$:

$$H = \begin{bmatrix} M_1 & \\ & I_{2m} \\ M_2 & \end{bmatrix}$$

Whereas I2m were 2m and M1 identify matrix, M2 were m size matrices — alternatively m2. M2 seems to be the identity matrix. Across each row there are m matrix M1. These ones upon on r th row are just in places
$(r-1)\times m+1,(r-1)\times m+2,\ldots(r-1)\times m+m-1,(r-1)\times m+m$. The matrix $M2$ is constructed as follows:

$M2 = [Im\ Im\ \ldots\ Im]$. *(2)*

When m = 4, M1 and M2 matrices may be seen plainly in Fig. 1. This G encoding matrix is only the H matrix for removing the control bit

$$G = \begin{bmatrix} M_1 \\ M_2 \end{bmatrix}.$$

(3)

In summary, this encoder uses a G matrix deriving from of the Latin squares and also has the following characteristics. It accepts k = m2 data bits (di) and makes 2tm check bits (ci) for parity.

1) Every data bit is involved in 2t parity controls precisely.

2) Participating throughout the parity tests is the pair of data bits (both bits).

In the following section these features are being used to describe the methodology presented.

ISBN: 978-93-91303-04-04

4.IMPLEMENTATION OF PROPOSED ARCHITECTURE

Burst error-correction codes from coding theory utilise ways to rectify burst faults that occur over numerous consecutive bits rather than in bits separate.

Many codes were created to fix random faults. However, sometimes channels may produce brief interval faults. These mistakes occur in either a burst, since they occur in several consecutive bits. There are various examples of burst mistakes in storage media. These problems might be caused by physical damage throughout the case of network channels including such disc scratch or lightning stroke. Things are not autonomous; they tend to just be spatial. When one bit contains a mistake, the surrounding bits may be damaged also. Random error correction is ineffective at fixing burst mistakes.

The following cyclic codes were defined: These symbols q are considered in fq to be elements. We may now see words into fq as polynomials, in which each symbol in such a word corresponds to various polynomial coefficients. They choose a fixed polynomial called an polynomial generator to create a cyclic code. Any polynomials which may be divided by such a polynomial generator are indeed the words of such a cyclic code.

In the top section of both the parity control matrix, the main concept of the suggested class and codes would be to employ identity submatrices to directly calculate magnitudes of both the burst error or perhaps the error pattern from either the bits or symbols themselves. The bottom part of both the matrix would then be built using a basic code in order to fulfil the following constraints.

1. All adjacent XORing b-adjacent syndromes should really be single. 1. 1. 1.
2. All symptoms in b-adjacent columns must be unique for certain conceivable column combinations.
3. In the previous two circumstances, multiples of both the column should be employed for XOR instead of just the original column.

Status 1 assures that there really is no miscorrected b-contiguous mistake. Condition 2 assures that no miscorrection is made of any number of errors between b-adjacent columns. These distinct symptoms specify precisely what columns next to b comprise the mistakes. Each column may additionally include multiples with non-binary codes such as Reed Solomon codes that are corrected on even a symbol basis. This same higher b-rows of both the matrix for parity control may detect these multiples. However, condition 3 has to be fulfilled also to prevent miscorrection for varying magnitudes of errors. Thus, the bottom portion of both the matrix of parity control is designed to fulfil all criteria. In the parity check matrix, an identity sub-matrix of size atleast to is attached. When a sub matrix rx-r identity being employed in place of a bx-b, the code is designed systematically. Figure 1 shows the overall structure of both the scheme's systemic parity check matrix, often known as the H-matrix.

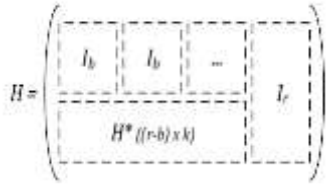


Fig. 1. General Structure of a systematic parity check matrix of the proposed scheme.

A parity check matrix of both the suggested arrangement is comparable with both the identity matrix codes of [23] and Fire code [24]. The main distinction in the designing of the suggested code is in the employment of GF(2b) symbols inside the previously described codes. So, like their corresponding lower submatrix every identical submatrix contains an element of GF(2b). The system proposes to generate the final parity check matrix that use other existing codes, BCH codes, mostly on basis of specified criteria.

ENCODING PROCEDURE

For just a systematic code, this encoding technique consists of many XOR functions with the message bits or signs which are then attached for the code word throughout the original message. Whenever a code is not systematic, a few XOR processes are further necessary to calculate parity check bits or symbols connected with the top half of both the parity check matrix throughout relation to the existing code encoding process used to produce that code. These bits and symbols may be announced at the end of both the codeword or saved independently in a specified word. These are thus termed distinct parity if kept

ISBN: 978-93-91303-04-04

separately. In Figure 2 two distinct storage types of parity are shown.

Fig. 2. (a) ECC bits stored alongside data bits. (b) ECC bits stored sepa-rately in memory (Separate Parity).

DECODING PROCEDURE

The overall process of decoding comprises the two error pattern & error locations processes. For both the proposed approach, the first step would be to use the parity matrix to calculate the syndromes. This syndrome was calculated by multiplying any coded parity matrix. This same XOR operation is indeed a basic one among all data bits or symbols that seem to have a 1 in the parity check matrix per row. This construction of both the matrix of the proposed method for parity controls seems to be that the pattern for error is expressed by the bits or symbols with higher b syndrome, in which the b of the error was fixed. In order to determine the position of both the burst mistake the remainder including its Syndrome bits or symbols are utilised.

Consider any length codeword n, c= (c0, c1, ...cn-1), with the data length k and the no.of control bits or symbols r. Therefore, n= k+ r gives the length of the codeword. This H-matrix is indeed an r- and n column matrix. r also indicates the overall amount of syndrome bits or symbols. These syndrome bits are therefore calculated by using the received codeword to multiply this same h-matrix, as indicated by equations (1). In case of binary bits, the multiplication is really just an AND operation. Multiplication was done using GF for non-binary m-bit symbols (2m). This add operation is indeed a binary and non-binary XOR operation.

$$\begin{pmatrix} S_0 \\ S_1 \\ \vdots \\ S_{r-1} \end{pmatrix} = \begin{pmatrix} h_{0,0} & \cdots & h_{0,n-1} \\ \vdots & \ddots & \vdots \\ h_{r-1,0} & \cdots & h_{r-1,n-1} \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ \vdots \\ C_{n-1} \end{pmatrix} \quad (1)$$

Next, we analyse a size b explosive mistake beginning with the codeword position. This error vector shows every one of the bits or symbols inside the modified codeword. This allows e= (0, 0,... ei, ei+1, ... ei+b-1, 0,... 0) to yield the error vector. If we add to both the codeword the error vector, then original codeword is returned. This error vector equals 0 when the received codeword is error-free. Both syndrome bits or symbols were equally zero for non-erroneous codewords. Calculating an erroneous codeword syndrome is therefore similar to computing all bits or symbol of the syndrome from it's own vector of error. Let x= imod b, thus. Bits or symbols of the calculated syndrome whenever a coding word multiplied either by suggested H-matrix with an error vector e (2).

We assume to be a multiple of b for simplicity. (S0, S1, ..., sb-1) then = (ei, ei+1,..., ei+b-1). We also look only at binary situation with k data bits and r verification bits for clarity. The mistake pattern was direct effect, as may be shown from the calculated bits of syndrome. That both individual mistake magnitude and the specified H-row are determined by the lower (r-b) syndrome bits. Therefore we know the amount of the mistake is equal to both the upper b syndrome bits when a burst error starts at position i. Hence, equation (3) is fulfilled in incorrect places, i.e. ito i+b-1. Equation (3) is indeed not valid for all of the other places. Therefore, the calculation of the error location in such a group of bits is completed, and equation (3) is met for the group of bits in error. This suggested decoding process is based on this.

This decoding works by taking each set of b-adjacent columns as just a single huge symbol and decoding and per symbol basis. Every data bit di is therefore part of b-bit symbols. An instance of 4-bit explode-correction code in Fig. 3 has indeed been presented, the information but divided into 4-bit Bi-3, Bi-2, Bi-1and Bi symbols. This b-bit burst error is just a mistake from one of the b-bit symbols and so can be calculated via equation (3). If indeed the data bit is really a component of equation (3) for any one of the b-bit symbols, this implies that the database is inaccurate. The data bit's error pattern is just the Sα syndrome value, wherein α is just the upper b-row row wherein the column is 1. Therefore, for each data bit, this same error location And then all b-bit symbols it's indeed

ISBN: 978-93-91303-04-04

one part of. The data bit would not only be incorrect if equation (3) for certain b-bit symbols that are part of this is not met.

$$\begin{pmatrix} S_0 \\ S_1 \\ \vdots \\ S_x \\ S_{x+1} \\ \vdots \\ S_{b-1} \\ S_b \\ \vdots \\ S_{r-1} \end{pmatrix} = \begin{pmatrix} e_{t+((b-x)mod\ b)} \\ e_{t+((b-x+1)mod\ b)} \\ \vdots \\ e_t \\ e_{t+1} \\ \vdots \\ e_{t+((b-x-1)mod\ b)} \\ h_{b,0}e_t + \cdots + h_{b,b-1}e_{t+b-1} \\ \vdots \\ h_{r-1,0}e_t + \cdots + h_{r-1,b-1}e_{t+b-1} \end{pmatrix}$$

$$S_\beta + h_{\beta,0}S_0 + h_{\beta,1}S_1 + \cdots + h_{\beta,b-1}S_{b-1} = 0$$
$$\forall\ b \le \beta \le (r-1)$$

5.Simulation Result:

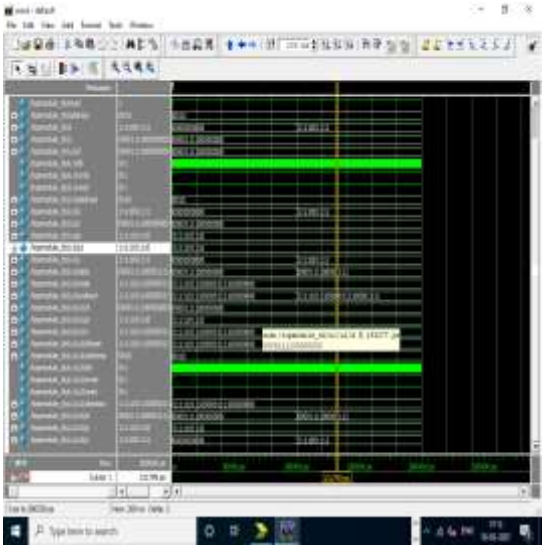


Fig 8.1 Simulation Result

Fig 8.1show the simulation result of proposed system. Where we can detect the error and correct the error.

6.CONCLUSION AND FUTURE SCOPE

This document offers a novel family of single explosion error correcting parallel decoding codes. That parity control matrix of current codes is enhanced by this coding class. Also there is a novel decoding approach that provides a one-step decoding logic that allows quick parallel decoding. Those codes are especially important for memory with latency performance. Comparisons using current systems demonstrate that in particular the decoder area with large burst sizes with such a minimum increase to redundancy was significantly reduced by the suggested class of codes. These findings reveal that, in comparison with current systems for bigger burst dimensions, the proposal system is also achieving greater decoder delay. Current plans are far more efficient than the approach intended to deal with lower burst sizes. The suggested system, however, offers an effective solution with both the decoder area as well as the delay to correct a bigger mistake of burst size whilst providing greater throughput using scaling technology even as number of bits may roll over owing to bursting failure grows. Thus since the primary sorts of soft mistakes are shifted toward localised cluster error for various forms of memory, the suggested coding class offers an efficient technique with little complexity that allows such failures to be tolerated without major increase in data redundancy.

References

[1] R. Baumann, “Soft errors in advanced computer systems,” in IEEE Design & Test of Computers, vol. 22, no. 3, pp. 258-266, May-Jun 2005.

[2] E. Ibe, H. Taniguchi, Y. Yahagi, K. Shimbo and T. Toba, “Impact of scaling on neutron-induced soft error in SRAMs from a 250 mm to a 22 nm design rule,” in IEEE Transactions on Electron Devices, vol. 57, no. 7, pp. 1527-1538, Jul. 2010.

[3] D. Radaelli, H. Puchner, S. Wong and S. Daniel, “Investigation of multi-bit upsets in a 150 nm technology SRAM device,” in IEEE Transactions on Nuclear Science, vol. 52, no. 6, pp. 2433-2437, Dec. 2005.

[4] Y. Kim, R. Daly, J. Kim, C. Fallin, J. H. Lee, D. Lee, C. Wilkerson, K. LaiandO. Mutlu, "Flipping bits in memory without access-ing them: An experimental study of dram disturbance errors", in Proc. of ACM/IEEE International Symposium on Computer Archi-tecture (ISCA), pp. 361-372, 2014.

[5] A. Das and N.A. Touba, “Systematic b-Adjacent Symbol Error Correcting Reed-Solomon Codes with Parallel Decoding” in Proc. of IEEE VLSI Test Symposium, pp. 1-6, 2018.

[6] A. Das and N.A. Touba, “Low Complexity Burst Error Correct-ing Codes to Correct MBUs in SRAMs” in Proc. ofACMGreat Lakes Symposium on VLSI(GLSVLSI), pp. 219-224, 2018.

ISBN: 978-93-91303-04-04

[7] H. O. Burton, “Some asymptotically optimal burst-correction codes and their relation to single-error-correcting reed-solom codes,” in IEEE Transactions on Information Theory, vol. 17, no. 1, pp. 92–95, Jan. 1971.

[8] S. Baeg, S. Wen and R. Wong, “SRAM Interleaving Distance Selection with a Soft Error Failure Model,” in IEEE Transactions on Nuclear Science, vol. 56, no. 4, pp. 2111-2118, Aug. 2009.

[9] R. Datta and N.A. Touba, “Generating Burst-Error Correcting Codes from Orthogonal Latin Square Codes - A Graph Theoret-
ic Approach,” in Proc. of IEEE Symposium on Defect and Fault Tol-erance, pp. 367-373, 2011.

[10] P. Reviriego, S. Liu, J.A. Maestro, S. Lee, N.A. Touba and R. Datta, “Implementing Triple Adjacent Error Correction in Dou-ble Error Correction Orthogonal Latin Square Codes,” in Proc. of IEEE Symposium on Defect and Fault Tolerance, pp. 167-171, 2013.

[11] P. Reviriego, M. Flanagan, S.-F. Liu and J. Maestro, “Multiple cell upset correction in memories using difference set codes,” in IEEE Transactions on Circuits and Systems-I: Regular Papers, vol. 59, no. 11, pp. 2592–2599, Nov. 2012.

[12] P. Reviriego, S. Pontarelli, A. Evans and J. A. Maestro, “A Class of SEC-DED-DAEC Codes Derived from Orthogonal Latin Square Codes", in IEEE Transactions on Very Large Scale Integration (VLSI) Sys-tems, vol. 23, no. 5, pp. 968-972, May 2015.

[13] J. Kim, N. Hardavellas, K. Mai, B. Falsafi and J. Hoe, “Multi-bit error tolerant caches using two-dimensional error coding,” in Proc. of IEEE/ACM International Symposium on Microarchitecture (MICRO), pp. 197–209, 2007.

[14] C. Argyrides, D. Pradhan and T. Kocak, “Matrix codes for reliable and cost efficient memory chips,” in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 19, no. 3, pp. 420-428, Mar. 2011.

[15] A. Dutta and N.A. Touba “Multiple Bit Upset Tolerant Memory Using a Selective Cycle Avoidance Based SEC-DED-DAEC Code,” in Proc. of IEEE VLSI Test Symposium, pp. 349-354, 2007.

[16] S. Shamshiri and K. T. Cheng, “Error-locality-aware linear coding to correct multi-bit upsets in SRAMs,” in Proc. of IEEE International Test Conference (ITC), Paper 7.1, 2010.

[17] A. Neale and M. Sachdev, “A new SEC-DED error correction code subclass for adjacent MBU tolerance in embedded memory,” in IEEE Transactions on Device and Materials Reliability, vol. 13, no. 1, pp. 223–230, Mar. 2013.

[18] L. S. Adalid, P. Reviriego, P. Gil, S. Pontarelli and J. A. Maestro, “MCU Tolerance in SRAMs Through Low-Redundancy Triple Adja-cent Error Correction,” in IEEE Transactions on Very Large Scale Integra-tion (VLSI) Systems, vol. 23, no. 10, pp. 2332-2336, Oct. 2015.

[19] J. Li, P. Reviriego, L. Xiao and R. Zhang, "Efficient Implementations of 4-Bit Burst Error Correction for Memories", in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 65, no. 12, pp. 2037-2041, Dec. 2018.

[20] C. Wilkerson, A. R. Alameldeen, Z. Chishti, W. Wu, D. Somasekhar and S. Lu, “Reducing cache power with low-cost, multi-bit error-correcting codes,” in Proc. of ACM/IEEE International Symposium on Computer Architecture (ISCA), pp. 83–93, 2010.

[21] K. Namba, S. Pontarelli, M. Ottavi and F. Lombardi, “A Single-Bit and Double-Adjacent Error Correcting Parallel Decoder for Multiple-Bit Error Correcting BCH Codes,” in IEEE Transactions On Device And Materials Reliability, vol. 14, no. 2, pp. 664-671, Jun. 2014.

ISBN: 978-93-91303-04-04

Design Analysis of Wallace Tree Multiplier Using Approximate Full Adder And Kogge Stone Adder

T. Keerthi Priya[1]Lakshmi Sankeerthana.P[2]Mounika.Y[3]Mythri..M[4]Charitha.G[5]
Assistantprofessor[1],UGScholars[2,3,4,5] ,[1,2,3,4,5]DepartmentofECE,Srinivasa Ramanujan Institute of Technology,Ananthapuram,AndhraPradesh

ABSTRACT - It is quite challenging for the VLSI Designers, to design and manufacture digital devices which operate at high speed and also consume less power. A Multiplier circuit is the one that performs major computations and it consumes more power among remaining in the entire electronic circuit. Usually, the operation of multiplication is proceeded by adding and shifting methods. However, the advancements made in the adders, opened the door to increase the rate of execution for the multiplier. The Circuit is designed using Verilog HDL and simulations are done using Xilinx software. In the proposed project, the advancement in Wallace Tree Multiplier is done using Kogge Stone adder and modified Approximate Full Adder. The area of the multiplier is 27% in the available area of the entire circuit. The Power consumption of the system is 0.037w.

Keywords –KSA - Kogge Stone Adder, 15-4 compressor, WTM (Wallace Tree Multiplier), Modified Approximate Full Adder, PPR - Partial Product Reduction, PPG - Partial Product Generation, Power, area.

I. INTRODUCTION

Generally, any Multiplier performs multiplication operations with binary data. So, we need to choose a multiplier that is very effective and good in performance because, if the multiplier is not effective, it works at less speed, with more time delay and it may give wrong outputs. So we are using the Wallace tree multiplier which is effective at Speed, Accuracy, Time, Low power consumption. In this design,

we are using the combination of Wallace tree Multiplier, Compressors, Approximate full adders, and a Kogge stone adder.

II. EXISTING SYSTEM

The working principle of the Wallace tree multiplier consists of 3 steps. The First step is partial product generation. In this step, by implementing the multiplication on binary data, partial products will be generated. After generating partial products the next step is the reduction of the partial product. The process of reducing the partial products is done by using full adders, half adders, and also compressors. Compressors are known as carry-save adders. In this system, a 4:2 compressor is used. By using a 4:2 compressor, if we give 4 inputs to it we will get 2 outputs. Full adders are used when there are 3 bits and half adders are used when there are 2 bits. If any single bit is found, it is passed to the further next stage/phase without any processing. This reduction process is continued until only two rows remain. The third step is the final addition, where the remaining two rows are added.

The Final stage addition is done by using a multi-bit adder. In this system Ripple carry adder is used. Ripple carry adder is one type of logic circuit in which the carry output of each present full adder is given as the carry input to the next full adder. The ripple carry adder will not allow using all the full adders simultaneously, each full adder has to wait for some time until the carry bit becomes available from its adjacent or previous full adder. So it causes an increase of the propagation time so delay is more and power consumption is also more. The disadvantages of the existing system are, the delay is more, power consumption is more and it requires more area.

III. PROPOSING SYSTEM

We are using parallel adders and approximate full adders, to overcome the disadvantages in the existing system.

Working Principle

The working principle ofWallace Tree

Multiplier involves 3 stages.

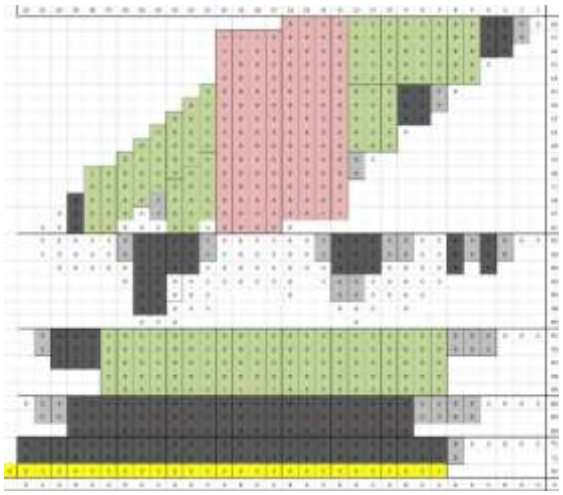
1.The first stage/phase is the Partial Products generation stage (PPG).

2.The second stage is the Partial Products Reduction (PPR) stage.

3. The third stage/phase is the Final Addition step.

In WTM, we are using a 15:4 compressor that uses 5 Modified Approximate Full Adders and two compressors of size 5:3, and also a Kogge Stone Adder (KSA) at the final stage.

The Below figure is the representation of this model.



In this figure, every partial product is represented by a dot "." A 5:3 compressor is placed between column number 13 to 20. There are 13 partial products, so to have 15 inputs for the 15:4 compressor, two numerical zero's i.e (0's) are added in the 13th column.

Finally, at the last stage, a Kogge Stone Adder (KSA) is placed to perform the final addition.

Description

We use various kinds of compressors like 5:3compressors to compress the generated partial products in the second stage. The proposed system is efficient in reducing the number of rows of partial products.

At the first stage, the full adders and half adders are employed to compress partial products.

The second stage involves the further compression of the partial products using a 5:3 compressor.

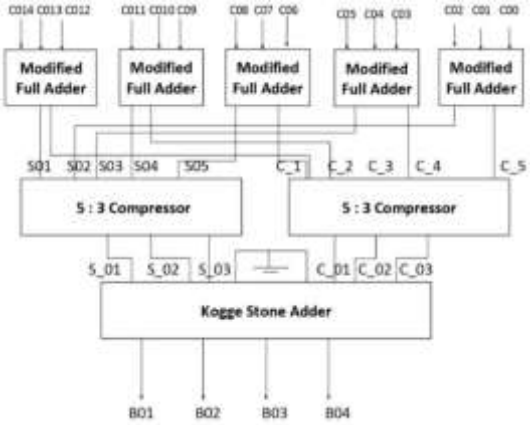
The compressed partial products in the 1st stage are given as inputs to the 5:3 compressor in the 2nd stage.

15:4 Compressor

Generally, compressors are used for Addition purposes. The 15:4 compressor takes 15 inputs i.e. (C00 – C014) and produces B01, B02, B03, B04 as four outputs. This Compressor consists of, at the first stage, there are five modified approximate full adders, and at the second stage there aretwo 5:3 compressors and at the last stage, one Kogge Stone Adder is placed so that final addition takes place.

At the first stage, each full adder produces a sum and a carry. In total, the 1st stage produces five sum bits and also five carry bits.

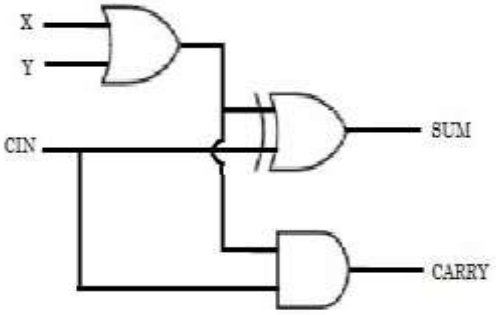
One of the 5:3 compressors in the 2nd stage gets all the sum outputs of modified approximate full adders as inputs and the other gets all carry outputs of full adders as inputs.



Modified Approximate Full Adder

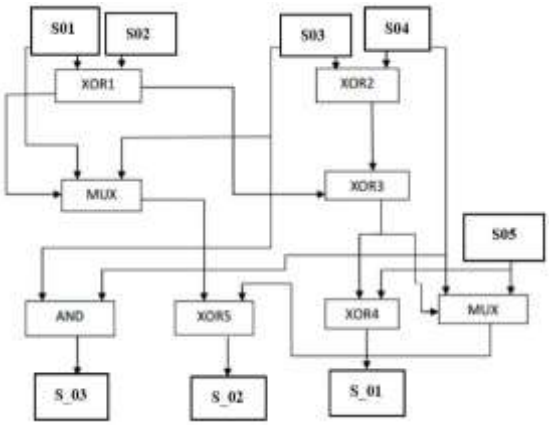
The standard or general full adder is modified by performing some process into an approximate full adder.This approximate full adder consists of only one Ex-OR Gate, one OR Gate, and one And Gate.This performs all the operations of the normal full adder and thus reducing the number of gates. Thereby, the parameters like power and area get reduced.

ISBN: 978-93-91303-04-04



5:3 Compressor

A 5:3 Compressor takes 5 inputs asS01, S02, S03, S04, S05 and produces three outputs asS_01, S_02, S_03.



Kogge Stone Adder

Kogge Stone Adder is one type of parallel prefix adder which is used for fast addition.

It involves three stages.

- Pre-processing stage
- Carry Generation Stage or phase
- Final Processing Stage

i. **Pre-processing stage**

This stage mainly involves two signals. They are

- Propagate signal
- Generate signal

$$Pi=Xi \oplus Yi \quad \text{-----> (1)}$$

$$Gi=Xi \cdot Yi \quad \text{------> (2)}$$

Eq(1) represents Propagate signal and eq(2) represents Generate signal.

We get Generate signal by EX-OR operation between Ai and Bi. Similarly, Propagate signal is obtained by And operation between Ai and Bi.

ii. **Carry Generation stage**

This phase involves the carry generation operation by using the below equations.

$$Gi=(Pi \cdot Giprev) + Gi \quad \text{-------->(3)}$$

$$Pi=(Pi \cdot Piprev) \quad \text{-------->(4)}$$

Where,

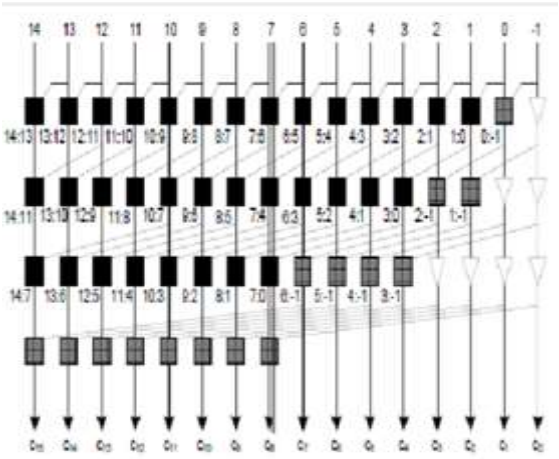
Giprev = previous Gi value

Piprev = previous Pi value

iii. **Final Processing Stage**

The final sum operation and carry outputs are determined with the help of the below equation.

$$Si = Pi \oplus Ci\text{-}1 \quad \text{-----> (5)}$$



In Kogge Stone Adder, it involves an important concept called Black cell and Grey Cell concept. In the above fig, we can observe black cells and grey cells.

ISBN: 978-93-91303-04-04

Advantages

- It is regular in shape.
- Theconsumption of Power by the circuit is less.
- The circuit complex is minimum.
- The delay is less as it operates with more speed.
- It is easy for pipelining.

Applications

The proposed Wallace Tree Multiplier are preferred and applied,

- In high-speed Digital Signal Processing Structures.
- In ALU's
- In Robotics, where speed of the circuit is high.
- In Machine learning

Tools and Programming language used:

The tools used are:

1.Xilinx ISE

2.ModelSim

Xilinx ISE (Integrated Synthesis Environment) is one of the Xilinx versions which is mainly used for Synthesis and analysis of HDL design, which is primarily used in embedded systems for FPGA and CPLD integrated circuit boards. It is also used in writing algorithm, whereas ModelSim is a logic simulator which is used in the next step for system-level testing. Modelsim is used for System-level testing and Simulation. The ModelSim is used in Behavioral simulation where the logic and timing issues are verified. The produced output and results are also verified.

The programming language used is,

Verilog HDL. It is described as a Hardware Descriptive Language which describes the behavior of electronic and digital circuits. It is commonly used for designing and verification of digital circuits at the register transfer level.

There are many Hardware Descriptive languages. In the proposed project, we are using Verilog language as it is more flexible. For our requirements, we prefer Verilog HDL compared to other languages.

It is an IEEE standard Hardware Descriptive Language.

3. IV. Simulation Output

The 16x 16 bit Wallace Tree Multiplier is designed using the 15:4 compressor. It is developed in Verilog HDL using the software Xilinx 14.7.

The Simulation results are as follows.

Power	**Delay**
0.170 W	17.709 ns

Table: The Utilization Summary of the device

Slice logic utilization	***Available***	***Used***	***Utilization***
Number of slices	8672	104	1%
Number of 4 input LUTs	17344	182	1%
No. of inputs	32	32	100%
No. of bonded IOBs	250	32	12%

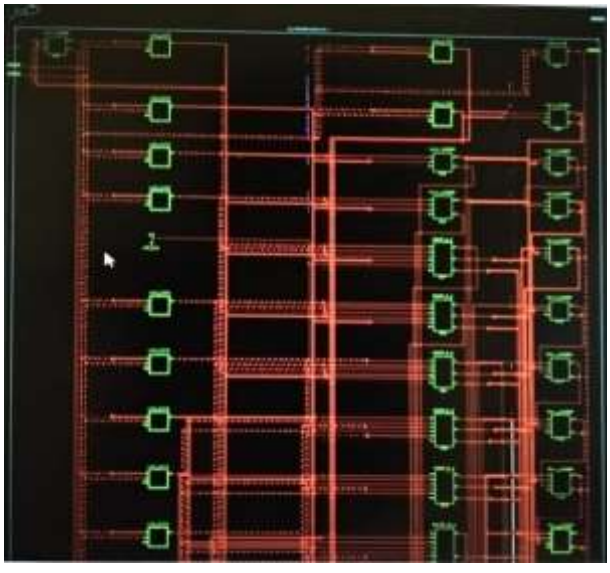


Fig: 16×16 Bit WTM Structura

ISBN: 978-93-91303-04-04

4. V. Conclusion

The Design of 16 x 16 Wallace Tree Multiplier is designed using the compressor of 15:4 , Modified Approximate Full Adders,5:3 compressors and Kogge Stone Adder. The Synthesis is done by using Xilinx 14.7 software. The simulation results are observed and verified. The Performance of the proposed system is observed. In future, with the advancements in new technologies paves way for the proposed system to be developed further and could be applied in various fields like Digital signal processing, Robotics, Machine Learning where the multiplier operates with high speed , less delay, less power consumption and works with high efficiency.

5. VI. References

[1] Sundhar ; Tharshini.S ; Priyanka ; ;"Performance and Analysis of Wallace Tree based Multiplier using Kogge Stone Adder and 15:4 Compressor", in 2019 at ICCSP, International Conference on Communication and Signal Processing .

[2] "Improvement of Wallace based Multipliers using Parallel Prefix Adders", at ICSPCCNT, International Conference on Signal Processing, Communication, Computing and Networking Technologies in 2011 by Rajaram; Vanithamani.

[3] "A high speed and Area efficient Booth recoded Wallace tree based multiplier for fast arithmetical circuits", at Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics by Jagadeshwar Rao; Sanjay Dubey in 2012.

[4] "Performance Analysis of reduced complexity Wallace Tree Multiplier using Energy CMOS Full Adder", at ICRESE, i.e, International Conference on Renewable Energy and Sustainable Energy by Shahabaz ; Sandeep; Suryawanshi Yogesh in 2013.

[5] "An Efficient High Speed Wallace Tree Multiplier", at International Conference on Information Communication and Embedded Systems (ICICES) by N. Sureka ; R. Porselvi ; K.Kumuthapriya.

ISBN: 978-93-91303-04-04

Rounding Technique Analysis for Power-Area & Energy Efficient Approximate Multiplier Design

K. Saifuddin[1], S. Archana[2], S. Rohini[3], M. Pavan Kumar[4], D. Pallavi[5]
Assistant Professor[1],UG Scholars[2,3,4,5]
[1,2,3,4,5]Department of ECE, Srinivasa Ramanujan Institute of Technology,
Anantapuramu, Andhra Pradesh, India.

Abstract: Approximate computing is perhaps the most effective data processing system for error-resistant applications including signal and image processing. Approximatively computing loses precision which depends upon that application and is accepted as that of the cost of enhancing the circuit features. The threshold for checking the interaction between precision and circuit features within the control of both the circuit designer called desired precision. This paper introduces the rounding strategy as an effective way of managing the transaction. In this respect, the assessment of rounding method efficiency by multiplier circuits as both a significant computer block in almost all of the processor systems. By comparing circuit characteristics across multipliers, and influence of both the rounding technique is explored.

1.INTRODUCTION

ENERGY Minimization is one of the most important design criteria in almost any electronic system and particularly mobile devices like smartphones, tablets and gadgets. This reduction with a low performance cost (speed) is widely sought. Their Digital Signal Processing Blocks (DSP) were crucial components for many multimedia applications of certain portable devices. That computational heart of such blocks is indeed the arithmetical logical unit in which the majority of arithmetic operations within those DSP systems involve multiplication. The improvement of both the speed and power/energy efficiency properties of multipliers thus plays a crucial role in enhancing processor efficiency.

Most DSP cores incorporate algorithms enabling video and image processing, in which the end outputs are either human-made pictures or movies. This allows us to employ approximations towards speed/energy efficiency improvement. That is because human people are restricted in their perceptive ability to see a picture or video. Besides the use of image and video processing, additional areas really aren't crucial to system's functioning in relation to the accuracy the arithmetic operations. That designer has the capacity to make trade-offs between accuracy, speed and energy usage by using approximation computation.

Apart from circuit, logic and architecture levels of algorithmes and sound layers, the approach of both the arithmetic may be accomplished at numerous design abstraction levels. Estimation may be carried out using many strategies, such as permitting timing breaches (e.g. voltage over scale or over clocking) and methods involving function approximation (e.g. changing the circuit boolean function) or a combination of those ways. A variety of approximating arithmetic blocks like supplements and multipliers have indeed been proposed at various design levels inside this field of function approximation techniques. We are focusing on offering a low-energy high-speed but approximation multiplier for error-resistant DSP applications. The suggested, area-efficient approximation multiplier is designed by changing the usual algorithm-level multiplication technique using round input values.

2.LITERATURE SURVEY

M. Alioto, “Ultra-low power VLSI circuit design demystified and explained: A tutorial,” IEEE Trans. Circuit:

Wireless networks (WSNs) are currently extensively used in applications in different fields. However, the lifespan of such a technology is still problematic and important to the success. In reality, nodes inside the wireless sensors are very often powered by restricted storage systems (e.g. tiny batteries or supercaps), which form the backbone of both the network, therefore their short lifespan is a key problem. Wake-up radio receptors are highly effective to reduce idle

ISBN: 978-93-91303-04-04

listening. These have led to a substantial number of designs suggested by the wake up radio receiver throughout the past 10 years. We describe an improved formulation and construction of sophisticated wake-up radiology, which can analyse data received (e.g. for addressing) as well as retransmit data or, as required, wake up messages towards our neighbours. With these capabilities, the energy efficiency for communication may be further improved and very low power multi-shop communication may be allowed. The test results show the functioning of the suggested architecture and also the power and range suited for future, purely asynchronous energy saving protocols MAC.

V. Gupta, D. Mohapatra, A. Raghunathan, and K. Roy, "Low-powerdigital signal processing using approximate adders," IEEE Trans. Comput.-Aided Design Integr. Circuits:*IEEE Trans.*
Considering portable multimedia devices with varied signal processing methods and architectures, low power is indeed a crucial need. Man could extract helpful information from somewhat erroneous outputs in certain multimedia programmes. We don't have precisely right numerical outputs to create, thus. Throughout this context, earlier studies uses the resilience of mistakes largely by calling voltage over, using Algorithmic and Architectural Methods to alleviate any faults. In this study, we suggest a decrease of logical complexity upon on level of transistors as an alternate approach towards the relaxation of numerical precision. With the suggested approximation arithmetic units we construct and test designs for video and picture compression algorithms to illustrate the efficiency of our method. We also develop from these approximation adders basic mathematical models regarding inaccuracy and power consumption. We also illustrate the usefulness of these approximation adders with certain quality restrictions in two digital signal processing architectures (discrete cosine transforming and finite impulse reaction filter). When compared to current implementations employing precise adders, the results of the simulation show up to 69 percent power savings utilising the suggested approximation adders.

H. R. Mahdiani, A. Ahmadi, S. M. Fakhraie, and C. Lucas, "Bio-inspiredimprecise computational blocks for efficient VLSI implementation of soft-computing applications," IEEE Trans. **Circuit*:***
The typical digital computing blocks with various designs have been devised to calculate the accurate outcomes of the computations assigned. The primary contribution for our suggested BIC is that it should deliver an appropriate estimate of the outcome at a reduced cost rather than an exact number. In terms of size, speed, and power consumption, the new structures are much more efficient compared to their exact counterparts. In this study, complete descriptions and results are presented again for Sample BIC adder and multiplier structures. Such BIC structures may then be used to create a three-layer neural network recognition with hardware defusing block of such a faded processor efficiently.

R.Venkatesan, A.Agarwal, K. Roy, and A.Raghunathan, "MACACO: Modeling and analysis of circuits for approximate computing," in Proc. Int. Config. Comput. Aided Design**:**
During recent years, term approximate computing, essentially refers to a set of approaches which reduce the need for perfect equivalency between the computing system definition and its implementation, has garnered considerable attention. For the modelling and analysis complex circuits for approximated computing, we present a systemic technique, named MACACO. The approach offered by computer metrics including the worst-case error, average case error, likelihood of mistake and error distribution may be used to examine how the approximation circuit complies with traditional proper implementation. This initial stage in MACACO is building an equivalent circuit that reflects a certain voltage and clock time behaviour of the approximation circuit. Then we build a virtual error circuit that would be the error of any input or input sequence upon on estimated output of the circuit. Furthermore, in order to determine different metrics of interest, you use traditional boolean analytical methods (SAT solvers, BDDs) and statistical approaches (Monte-Carlo Simulation). They have used the methods suggested in order to examine a variety of approximation designs regarding blocks during

ISBN: 978-93-91303-04-04

data travel. Our findings demonstrate that MACACO may assist the designer analyse the effects of approximation circuits methodically and pick among several approximation applications to facilitate the adoption of these kind of circuits in computer environments.

F. Farshchi, M. S. Abrishami, and S. M. Fakhraie, "New approximate multiplier for low power digital signal processing,"

The low power multiplier was suggested in this research. The suggested multiplier uses the approximation approach of the Broken Array Multiplier to the standard modified Booth multiplier. That process decreases the multiplier's overall power usage to 58% at the expense of a little reduction in output precision. In terms of energy usage and precision, the suggested multiplier was compared with existing approximation multipliers. Moreover, in the context of the construction of a 30-tap low-pass FIR filter, improved assessments of the suggested multiplier effect were made and the energy and accuracy of even a filter with standard booth multipliers were comparable to those of a filter. Our simulation findings reveal that the output SNR decreases by 17.1 percent at such a cost of just 0.4 dB.

P. Kulkarni, P. Gupta, and M. Ercegovac, "Trading accuracy for power with an under designed multiplier architecture,":

We present a new multiplier design that uses a modified, inexact 2-to-2 construction block with customizable error characteristics. These faulty multipliers save 31.78% - 45.4% on average on their equivalent exact designs, for just an average mistake of 1.38% - 3.32%. We demonstrate that our architecture could provide a superior 2X-8X signal-noise (SNR) ratio for similar power savings as prior power-error compensation-based over-scaling approaches through image filtering and JPEG compression as both a sampling application. We plan to save multiple power for larger concepts, showing that the advantages are very design-dependent. They compare our circuit-centered method with such a pure software adaption approach to power-quality tradeoffs for just a JPEG example. They also improve the architecture such that the multiplier may be correctly operated using such a residual adder with non-error resistant applications.

3.EXISTING SYSTEM

During 1965, Luigi Wallace, an informatician, devised the multiplier of Wallace's hardware. The WALLACE multiplier is indeed a parallel multiplier form extracted[5]. It's a little quicker and needs less doors. Parallel multipliers are used for several sorts of schemes. This WALLACE system is among the parallel multiplier techniques, which fundamentally reduces the number of additional steps necessary for partial products to also be combined.

This is done through the application of full and half adders, to minimise the number of rows across each summation phase of the matrix. Although the structure of the WALLACE multiplication more regular and less complicated, it is slower owing towards the serial multiplication process. Furthermore, compared to both the Wallace tree multiplier, this Wallace becomes less costly. Hence this work is constructed and analyses, utilizing several approaches employing complete adders with distinct logical types WALLACE multiplier.

Wallace Tree Multiplier Using Ripple Carry Adder

Ripple Carry Adder seems to be the approach was using to add extra adds to the sand executable chain to ever be carried out. Therefore many adders are employed in the adder. You may use numerous complete adders for the addition of multiple-bit integers to form a logical circuit. Every complete adder enters a Cin that is the preceding adder's Cout. This type of adder is an adder in the ribs, as each piece is fed to the next complete adder. Figs 9 to 11 depict the proposed WALLACE algorithm multiplier design employing RCA. Take three values of the same weight and provide them in a complete adder as the input. The outcome is an equal weight output wire. At the very first step, a partial product was acquired following propagation. With 3 wires, each data were received and added by adders, although with two next data in the very same phase, each phase is carried. Partial products using the same technique reduced in two layers of complete adders. During last phase, the same rib

ISBN: 978-93-91303-04-04

carry technique is used, thereby achieving product conditions p1 to p8.

4. PROPOSED SYSTEM

A rounded input that multiply is the basic notion the behind suggested approximating multiplier. Before delivering the input to both the partial product creation, a proposed method utilises rounding techniques. Fig. 1 depicts an estimated multiplier design drawing for the implementation of the suggested approach. Its multiplier was rounded via a rounding block amongst these two inputs (Multiplicand and Multiplier). Every signpost of each input will be saved, as well as the output sign including its multiplication result associated with the input signs will be calculated even before multiplication process commences. The right sign is given to both the result in the last step. The corresponding input blocks were changed to their 2's complement in case of a multiplication of negative values.

N x N partial products (partial products) were formed in traditional multipliers having N-bit input. However, the partial products formed in the rounding procedure are the mixture of active and inactive partial products. These active parts are, which have "1" as that of the Multiplier coefficient. This leads to a full multiplicand row following the rounding. Thus the lines with entire 0's were inactive partial products. There's really hence no need to cover them inside the reduction procedure.

Rounding of data entered demands a great deal of attention to ensure correctness. In general, a rounding of lower bits may be shown to produce less errors as opposed to rounding higher bits. With relation to both the bit position value, the proposing method has thus allocated rounding weights. There is a little error gap between both the exact location of the bit and a round position. A matching rounded bit score is applied for each correct bit. Error gap decreases with the rise in bit position value. The example shown in Fig.2 includes 'A' and 'B' and input 'B' is rounded to 'Br.' Fig.2 is also an example. Basically, this 'Rounding Technique' checks whether '1' and assigns '1,' with or without a slight mistake to corresponding 'Y' bit positions.

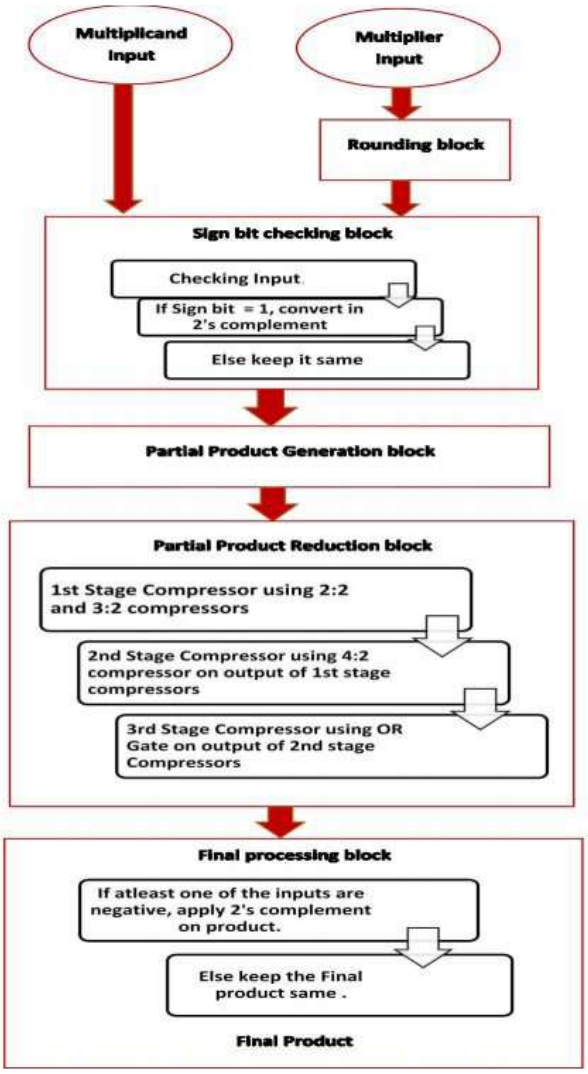


Fig. 1: 16-bit Block diagram of the algorithm

Accurate Bit Position	Approximate Bit Position
bit0	bit1
bit1	bit1
bit2	bit1
bit3	bit4
bit4	bit4
bit5	bit4
bit6	bit7
bit7	bit7
bit8	bit7
bit9	bit10
bit10	bit10
bit11	bit10
bit12	bit13
bit13	bit13
bit14	bit15
bit15	bit15

A = 0001 0011 1000 1000
B = 0000 0011 1111 1111
Br = 0000 0100 1001 0010

15 13 10 7 4 1
Leads to active partial product rows

Fig. 2: An example after rounding 'B' (16-bit)

ISBN: 978-93-91303-04-04

The reduction for partial products is really a step in which partial products were squeezed by various compressors. The methodology proposed offers flexibility to decrease the number of incomplete product lines. For example, in Figure 3, the 16-bit architecture lowers partial products into 6 rows that are designated as active partial products. As is usual, N-bit inputs were multiplied to yield N x N partial products. This length of partial products rises with O(N2) in respect of both the difficulty of computing. The proposed approach gives a $\leq O(N\times6)$ computational complexity, and a 32-bit $\leq O(N\times13)$ compute complexity. Another example using input values A, B and Br is presented to improve comprehension along with the design (Fig. 6(right)). 'B' is initially rounded to 'Br' input multiplier. N x N x N partial products will then be multiplied by the inputs. N anteN partial products are a mixture of active and inactive partial products as the result of the rounding on multiplier input. Following rounding, multiplier with '1' as coefficient affects the whole Multiplicand line as seen in fig. 3. The entire zero value line, with the coefficient "0" on the multiplier, is therefore inactive partial products. So in the reducing process, no need to cover it. Actually, only hardware can improve inactive partial items. This has led to the removal, before packaging, of any and all inactive component goods. This method plays a key role in decreasing power, time, area and efficiency. Three phases of compression are used to compress and pack its active component products. Partial items are compressed by full suppliers and half suppliers in the first step. A compressor of 4:2 is further compressed whenever the input is 16bit, while the output of 32bit is 9:2. The appropriate operations on the example are shown in Fig. 3 (right). Finally, a 2nd stage compressor output was packed with OR gate to achieve a finished product. Instead of OR, conventionally complete adders are employed. The fundamental purpose of employing OR gate rather than complete adder would be to significantly minimise the area and energy consumption.

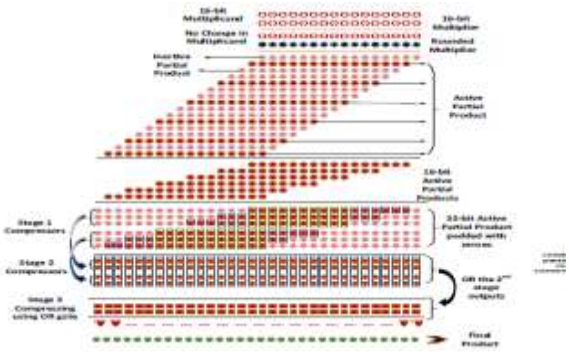


Fig. 3: Multiplier Design (left) with an example (right) (16-bit).

5.SIMULATION RESULT OF MULTIPLIER:

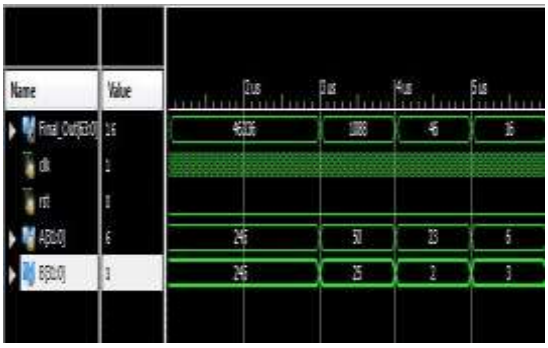


Fig 4 Simulation Result of Multiplier

Here we can give the inputs as A=6, B=3, clk as 1 and rst as 0, then the final output is 16.

Table 6.1 Comparison between power and delay

6. CONCLUSION

Compared to existing methods, the proposed approach is the best possible for both signed and unsigned information in form of power area latency and PDP effectiveness (16-bit and 32-bit). This is really the major research of the rounding methodology with a rounding pattern on such an approximation multiplier, which would be fixed in active part product ranges. The whole rounding pattern shows probable regions with less precision and regions with more accuracy in line with the likelihood of rounding. Based on the desired precision, rounding patterns be adjusted with a few additional hardware costs. The rounding pattern might well be changed to have fixed or dynamic partial product lines, but less active partial compression product line lines. In a broad variety of applications including image

ISBN: 978-93-91303-04-04

processing, machine learning and signal processing, this suggested approach may be applied. Different sizes are thus essential for maintaining precision somewhat close to the standard technique, depending upon on '1' bit position. The suggested approach creates large hardware features in comparison with DRUM, by reducing partial products flexibly.

7. FUTURE SCOPE

In our everyday lives, this multiplier plays a important function. The multipliers will play an important role in the future. By employing carry save adders, the speed of both the multipliers is improved, look ahead and so forth. Rounding patterns are designed depending on the necessary precision and various strategies for compression. With future, better technologies may minimize the area & delay.

BIBLIOGRAPHY

[1] M. Alioto, "Ultra-low power VLSI circuit design demystified and explained: A tutorial," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 59, no. 1, pp. 3–29, Jan. 2012.

[2] V. Gupta, D. Mohapatra, A. Raghunathan, and K. Roy, "Low-power digital signal processing using approximate adders," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 32, no. 1, pp. 124–137, Jan. 2013.

[3] H. R. Mahdiani, A. Ahmadi, S. M. Fakhraie, and C. Lucas, "Bio-inspired imprecise computational blocks for efficient VLSI implementation of soft-computing applications," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 57, no. 4, pp. 850–862, Apr. 2010.

[4] R. Venkatesan, A. Agarwal, K. Roy, and A. Raghunathan, "MACACO: Modeling and analysis of circuits for approximate computing," in Proc. Int. Conf. Comput.-Aided Design, Nov. 2011, pp. 667–673.

[5] F. Farshchi, M. S. Abrishami, and S. M. Fakhraie, "New approximate multiplier for low power digital signal processing," in Proc. 17th Int. Symp. Comput. Archit. Digit. Syst. (CADS), Oct. 2013, pp. 25–30.

[6] P. Kulkarni, P. Gupta, and M. Ercegovac, "Trading accuracy for power with an underdesigned multiplier architecture," in Proc. 24th Int. Conf. VLSI Design, Jan. 2011, pp. 346–351.

[7] D. R. Kelly, B. J. Phillips, and S. Al-Sarawi, "Approximate signed binary integer multipliers for arithmetic data value speculation," in Proc. Conf. Design Archit. Signal Image Process., 2009, pp. 97–104.

[8] K. Y. Kyaw, W. L. Goh, and K. S. Yeo, "Low-power high-speed multiplier for error-tolerant application," in Proc. IEEE Int. Conf. Electron Devices Solid-State Circuits (EDSSC), Dec. 2010, pp. 1–4.

[9] A. Momeni, J. Han, P. Montuschi, and F. Lombardi, "Design and analysis of approximate compressors for multiplication," IEEE Trans. Comput., vol. 64, no. 4, pp. 984–994, Apr. 2015.

[10] K. Bhardwaj and P. S. Mane, "ACMA: Accuracy-configurable multiplier architecture for error-resilient system-on-chip," in Proc. 8th Int. Workshop Reconfigurable Commun.-Centric Syst.-Chip, 2013, pp. 1–6.

[11] K. Bhardwaj, P. S. Mane, and J. Henkel, "Power- and area-efficient approximate wallace tree multiplier for error-resilient systems," in Proc. 15th Int. Symp. Quality Electron. Design (ISQED), 2014, pp. 263–269.

ISBN: 978-93-91303-04-04

Implementation of Optimized Digital Filter using Sklansky Adder

RekhaS,The Dande, NoorMohammad, T. Keerthi Priya , Sai Charan Kumar Reddy Department of ECE, Srinivasa Ramanujan Institute of Technology, Anantapuramu, Andhra Pradesh, India

***Abstract*—**In Digital age, The filters are utilized as a memory components to store the information. To plan the Digital Filters, adders utilized. Ordinarily the Adders are planned by the full Adder. Here in this paper the FIR filter is finished by PPA(parallel prefix snake). Among the few equal prefix adders, we are utilizing the Sklansky Adder and Kogge-Stone Adder. The equipment intricacy of Sklansky adder is less contrasted with different adders. Where as the Kogge Stone adder having the superior than other adder and the intricacy is more. Here, the Xilinx ISE

14.7 is utilized to carry out the filter. The comparison was happend between different particulars like lookup tables and Delay of the circuit. By this proposed framework we decrease the design intricacy and delay utilizing different boundaries.

Keywords :- KSA(Kogge-Stone Adder) SKA (Skalansky Adder) PPA(parallel prefix adder)

I. INTRODUCTION

Digital filters square measure plays a crucial role within the Digital Signal processing. The Phenomenal performance is the main reasons that DSP are more fashionable. Filters having two uses the primary use is Signal separation and it is required once the signal has been contaminated with interference, noise or alternative signals and the second use is Signal restoration and it is employed once the signal has beendistorted in some way.

A muddled Digital Signal Processing system contains of assortment of Multipliers and Adder. The viable style of Digital Signal Processing machine upgrade the capability of the framework. An Adder, which is a rudimentary part is frequently utilized in the few organizations that square measure utilized in the frameworks like Controllers and Processing chips. In this framework capability is speed up adder and multiplier factor.Two sort of filters are available in the Digital area. They are FIR and IIR. They are altogether different basically. The Structured FIR digital filter can smoothly done with high performance. So that the FIR filter are widely used. These FIR digital filter are used in our studies also.

A Finite Impulse Response filter is generally executed by utilizing a progression of delays, multipliers, and adders to make filter's output.

In this paper we are using the PPA(Parallel Prefix Adder) instead of using the serial adder. Different type of PPA are there in that we are using the Sklansky and Kogge Stone adder.

EXISTING WORK

A. Kogge-Stone Adder

The KSA or KS is a parallel prefix adder. Normally, the speed of parallel operations are very high. The performance is very high. The Kogge Stone adder required huge region to implement this is the main limitation of KS. It contain lower FanOut at every single phase, builds execution or potential for common CMOS process nodes.

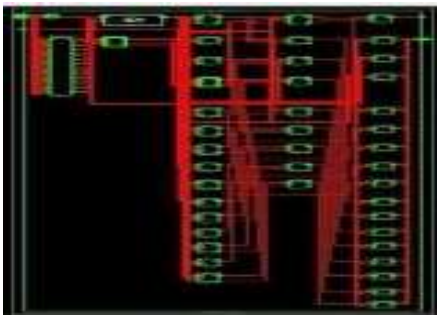


Fig 3. Kogge Stone Adder

Fig 4. Output of KSA

Carries are to be generated the prefix adder can be

implemented in different ways based on the different different requirements. Here we using the "Tree Structure form" to enhance the speed of Athematic operation. The PPA produce less delay during operation. So that PPA are high speed adders and these adders used in the industries for the high capability arithmetic structures.

The parallel prefix addition is carry out in 3 steps.

1. Pre-processing stage
2. Carry generation network
3. 3. Post processing stage

B. Sklansky Adder

The **Sklansky adder** construct recursively 2- bit **adder** then 4-bit , 8-bit, 16**, 32 bit adder** and etc,. by bordering every time 2 small **adders**. The architecture is very easy and systematic, but effect from the Fan-Out problems. Besides in some conditions, it is possible to use less "BK" cells with the same addition delay.

Fig 5. Sklansky Adder

II. DIGITAL FILTER IMPLEMENTION

A Finite Impulse Response Filters are frequently just authorized essentially 3 Digital Hardware components, a Unit Delay , Multiplier, and an Adder. The unit delay simply refreshes its yield once per trail period, utilizing the worth of contribution as its new output value inside the convolution sum.

The above figue the common FIR Filter structure , for the given circit we are giving the input of Xn. Firstly the coefficients are multiplied by the H0 multiplier later it gives input to adder similarly the delayed signal is applied to H2 multiplier. The output of both H1 and H2 multiplier are added by adder. In the same the FIR operation is to be done.

KSA in FIR filter

The Finite Impulse Response was carried out by the KSA. Here we are look at the attributes of FIR filter by differing the adders in FIR filter. The Digital filter was carried out by the D-Flip Flop are in the arrangement structure, which are associated with multiplier to multiply the given sources of info. All the multiplier yields are associated with the adders. In this adder position we are utilizing the diverse sort of adders and noticed the yields. Here we are looking at between the Kogge Stone and Sklansky adder. By the reenactments results, we saw that lookup table and power consumption of Finite Impulse Response filter planned by KSA is more contrasted than Sklansky adder. The equipment intricacy of Finite Impulse Response Filter with the KSA is more. This is decreased by utilizing Sklansky adder instead of Kogge stone Adder.

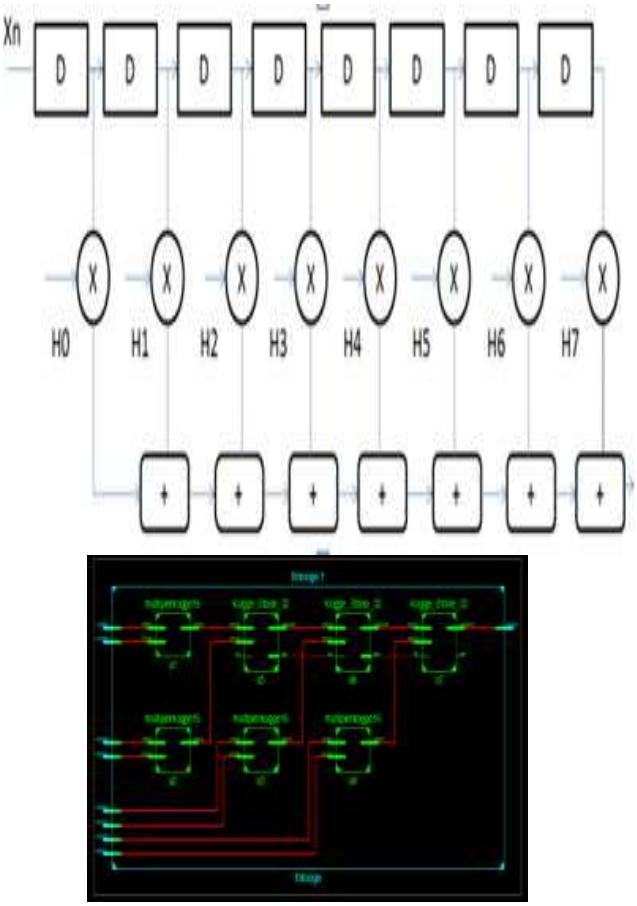


Fig 10. Block Diagram of Finite Impulse Response filter desined by KSA

A. SKA in Finite Impulse Response filter

In existing framework, The equipment intricacy of Finite Impulse Response filter is more with kogge stone. So that in the proposing framework we are utilizing the Sklansky adder for planning of FIR filter.

ISBN: 978-93-91303-04-04

Ordinarily the Skalansky adder is adjusted adaptation of the Kogge stone adder, in view of that reason the equipment intricacy is less contrasted than the FIR filter plan with the Kogge stone adder. The Digital filter was executed by the D Flip Flop are in the arrangement structure, which are associated with multiplier to multiply the given data sources. All the multiplier yields are associated with the adders. In this adder position we are utilizing the distinctive kind of adders and noticed the yields. By the reenactments results, we saw that lookup tables and power consumption of FIR filter planned by Sklansky adder is less contrasted and Kogge Stone adder. At long last, by this paper we reduce the architecture intricacy of the FIR .

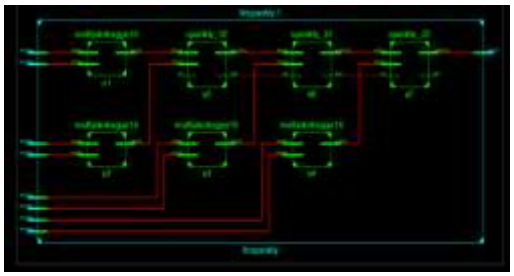


Fig 12. Block Diagram of Finite Impulse Response filter designed by SKA.

Fig 13. Output of Finite Impulse Response filter designed by SKA.

Conclusion:

The results of Finite Impulse Response filter are displayed in the Xilinx ISE 14.7. The consequence of the FIR filter carried out by the Kogge Stone Adder is contrasted with Finite Impulse Response filter executed by SKA. After comparing the results we saw that the Finite Impulse Response filter planned by Sklansky adder having less Lookup Tables than the Finite Impulse Response filter utilizing Kogge stone adder. In the event that the LUT's of the filter are less the architectural intricacy of the filter is additionally less

Refrences:

[1] Haichen Zhao, Shaolu Hu, Linhua Li, Xiaobo Wan. “NLMS Adaptive FIR Filter Design Method”.

[2] Aashu Ghalyan, Virender Kadyan,Performance Analysis and verification of Multipliers.

[3]K. Rawwat, T. Darwish, and M. Bayoumi, “.A low power carry select adder with reduces area”, Proc. Of Midwest Symposium on Circuits and Systems, pp. 218- 221, 2001.

[4] Megha Talsania and Eugene John “A Comparative Analysis of Parallel Prefix Adders”.

[5]M.Santhanaraj, SImmanuel Alex Pandian. ”Compre- hensive Optimal Fir Filter Design Procedures With Various Impacts”.

SOLAR BASED BIOMETRIC IGNITION SYSTEM USING ARDUINO

Siddhartha Valmiki[1], Lokesh Saana[2], Naveen Kumar Janapati[3], Divya Lingutla[4]

Assistantprofessor[1],UGScholars[2,3,4]
[1, 2, 3, 4]Department of Electronics and Communication Engineering,
Srinivasa RamanujanInstitute of Technology(SRIT),
Anantapur, Andhra Pradesh

ABSTRACT - Security is the major concerning issue looked by everyone when we are away from our vehicles. In the current circumstance satisfactory response for the above issue isn't yet found. Now-a-days environment conditions are radically affecting by contamination brought about via air toxins from gas and diesel-controlled vehicles. These causes long haul medical problems for individuals and fuel rates are additionally expanding step by step. we need to go for different choices like electrical vehicles. Electric vehicles are fall into various classes they are Battery controlled vehicles, sun powered based vehicles, battery and fuel-based vehicles. The main thought of this project is to improve security, executing sun-oriented framework for recharging batteries using Arduino. Arduino is an built with microcontroller, stage dependent and easy to use the device for programming purpose. Sun oriented board is adjusted at the highest point of the vehicle for getting most extreme sun-oriented radiation. This framework captures the maximum intensity of sunlight as far as extreme force point is concerned. At that point when the light power diminishes, its arrangement changes automatically for getting maximum intensity of light. Fingerprint sensor goes about as a keyless structure for starting purpose of a vehicle. This undertaking shows execution of solar powered vehicle by which maximum power point can be caught by adjusting the sun-oriented alignment. Then, this vehicle is likewise theft free while we are utilizing fingerprint sensor to start the vehicle.

Keywords—Arduino, Solar panel, Fingerprint sensor, LDR, LCD Display.

Introduction

Now-a-days climate conditions are drastically impacting by pollution caused by air pollutants from gasoline and diesel-powered vehicles. Security is the major issue facing by everyone once we left from our vehicles surroundings. The key idea of this project is to enhance security and implementing solar powered system using Arduino. Biometrics word is came from 'Bio' and 'Metrics' in that 'Bio' means 'life' and 'Metrics' means 'to measure'. The main method utilized in Biometrics are Fingerprint, Voice, Face, Palm, Iris etc., the only purpose of this project is to supply biometric safety system to civilian. Fingerprint sensor is employed to make fingerprint-based security on vehicle to start or stop the vehicle engine. During this project we are using two concepts one is solar tracking system and another is finger print sensor. Solar tracking system works 40% more efficient than the traditional tracking system and fingerprint sensor provides security by authenticating a person. We are using fingerprint sensor keyless framework for starting purpose of the vehicle. It shows the solar powered vehicle with biometric ignition. This project shows implementation of solar powered vehicle by which maximum point are often captured by aligning the solar axis tracker quickly. Meanwhile, this vehicle is additionally theft free while we are using fingerprint sensor to start out the vehicle. It provides more security compared to manual password or face recognition system. We are interfacing solar tracker and fingerprint sensor to the Arduino uno. It will take less time to start out the vehicle compare to other starting techniques. Solar tracker is aligned at the top of the vehicle for capturing maximum solar energy. The solar panels are dependent on weather conditions, sometimes it produces less electricity. In such cases we can manually charge the batteries. In this way, we are going to implement the solar tracker for capturing maximum intensity of light to recharge the batteries and the security for the vehicle will be provided by means of fingerprint sensor.

ISBN: 978-93-91303-04-04

Literature survey

A fingerprint locking system uses the user's fingerprint to unlock a system it works with the help of a fingerprint sensor module. The fingerprint sensor can also be interface with the Arduino. The Fingerprint module notifies the given fingerprint is authorized or not. Unauthorized person warning is conformed by sending Picture and OTP to the owner. When the authorized user accesses the system it conforms by sending the pictures or the OTP through the SIM for an authorized user. Then it confirms the authentication after given the correct OTP to the module. After the GSM module sends the data to the database if it matches the user can access the systemIt is a slow process to unlock because we need to enter OTP. It takes time to get the OTP depending on mobile network connection. Admin has to be alert on the notification from the system. A user always needs to be alert to check the messages from the module. the owner should not lose their mobiles in that particular case. Because anyone who knows technology can block our mobile from any notifications [1].

We can start the vehicle engine based on the voice recognition technique. The owner enrols their voice by speaking into the microphone interfaced with the module. After any person tries to unlock the system, first the module checks the user is authorized or not, if not the engine won't be run. For authorized users, it will automatically run. It works purely depends on the human voices. If the persons voice doesn't then the engine cannot start. This project's main theme is to implement a voice recognition system through authorized words. For noise disturbances it works with less efficient manner. voice recognition taking more time when compare to finger print and If a person has cold, their voice will automatically change then identification of the person will be difficult to recognize [2].

A solar photovoltaic cells depends single pivot global positioning framework on Arduino Uno stage is carried out in this project for accomplishing most extreme force during a day. The main thought of this project is executing a programmed main hub sun oriented global positioning framework. Arrangement of sun oriented board with the Sunlight for getting most extreme sunlight based radiation is tested. This framework tracks the most extreme force of light as far as greatest force point (MPP). At the point when the light force diminishes, its arrangement changed naturally for getting most extreme light force. It purely works depending on weather. In rainy sessions, night times they produce less solar energy than our proposed system [3].

This is the digital locking system can be used to make it more secure for access compare to conventional key locking. In this project, the traditional key is replaced by digitalized password to unlock the system. The author's main theme is to implement a security-based system with the key features of an email notifier to the owner and also sending person images who tries to unlock the system. This project is run by Bluetooth paired with the smartphone. This module can notify us when unauthorized person try to unlock the password. It Takes more time to access password and authentication also it has Low security compare to fingerprint. This project requires an internet to work. Sometimes Its possible to forget password that cases we cannot unlock [4].

In this paper its prototype is works based on the biometric fingerprint sensor to unlock the door. The fingerprint is more secure than the other biometrics and the digital password and other conventional techniques. This project can easily overcome the RFID and other digital password techniques. It provides access to authorized persons only. it won't allow unauthorized persons to access the system. We can also add or remove the users from the system. This facility is for only authorized users only, others cannot modify the system. It is less secure because the car glasses may break and we can open car doors [5].

This technology supports renewable source of power, This paper's main theme is by using renewable solar energy we can run electric automobiles by inbuilt solar panels on the automobiles. The solar power electric vehicle is supported through charging or discharging by the batteries.. Hence the Solar powered electric vehicle results in pollution less transportation. This Solar powered electric vehicle has using solar plate there is no tracking of sunlight in this project. It is using a constant solar plate so it absorbs less power when the sun is in opposite direction. It is less compatible compare to solar tracker [6].

Proposed technique

Methodology:

This project is to improve security and implement solar powered system using Arduino. Arduino is a microcontroller device, it can be interfaced to any electronic module. Solar panel is aligned at the top of the vehicle for capturing maximum solar light radiation. This system captures the maximum intensity of sunlight in terms of MPP (maximum power point). When the sunlight intensity decreases, its alignment changes linearly for getting the maximum sunlight intensity. Fingerprint sensor acts as a keyless

ISBN: 978-93-91303-04-04

framework for starting purpose of a vehicle. This project shows implementation of solar powered vehicle by which maximum power point can be captured by aligning the solar axis tracker quickly. Authorized persons only can start the vehicle. We can register the persons finger prints in the flash memory of the Arduino. When a person's fingerprint matches with the registered fingerprints then only the engine will get started, otherwise the engine won't get start for unauthorized access.

Block diagram:

The block diagram (Fig.1) shows the arrangement of this proposed system. Arduino ATmega328P act as the microcontroller which plays a major role in this system. Fingerprint module and LDR are the inputs to the Arduino. LCD display, DC motor, stepper motor acts as output devices in this project. We are giving the supply by the rechargeable batteries. These batteries will store the power given by the solar panel. We can also give the power supply through the external power source. Arduino contains 12 Digital pins and 6 Analog pins. LDR is connected to the analog pins of the Arduino. DC motor and stepper motor are connected to the Arduino through driver circuit. It protects the Arduino for any back EMF of motors. DC motor, Stepper motor and LCD display connected to the digital pins of the Arduino. Based on the finger print given by the user, Arduino will decide to turn on or off the dc motor. LCD display will displays the information regarding the person is authorised or not.

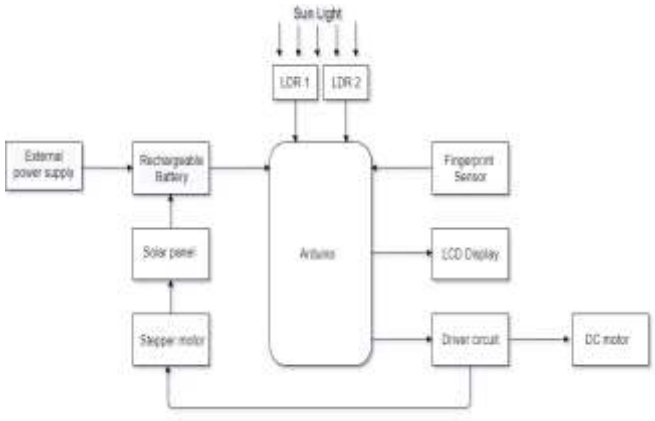
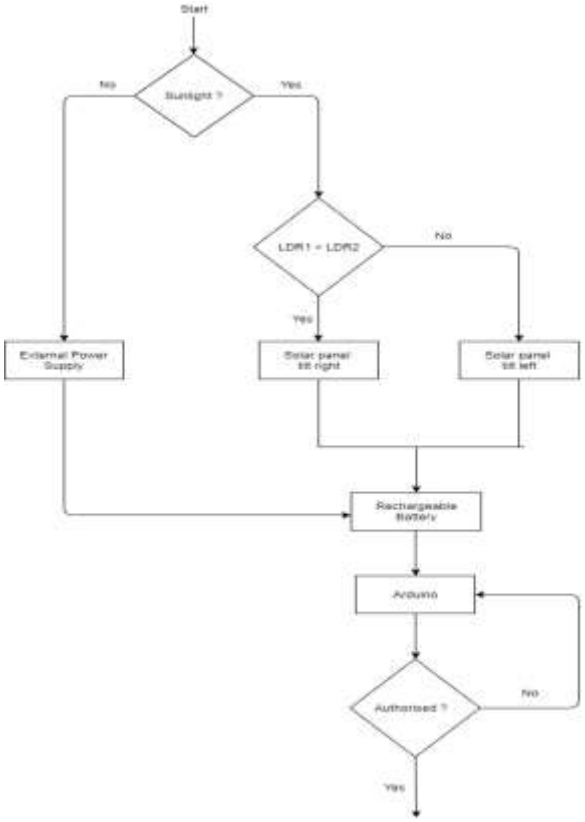


Fig 1. Block Diagram

Flow chart:



Run

Working:

In this model we are integrating both solar tracking system and fingerprint system to start the vehicle by user authentication. The solar tracker moves to and fro based on sunlight to produce the maximum electricity. This electric power is stored in a battery which is used to drive vehicle and also to access the fingerprint system. In this system the main controller is Arduino, this is programmed in the manner that the LDR sensor and also in accordance with the detection of the sunlight that will provide information to which direction the solar panel has to turn with the help of stepper motor. In this project 2 LDR's are used, one for right rotation and another for left rotation purpose. Based on the light intensity fall on the both LDR. Depending on the light falling on the LDR the solar panel will align itself to that particular direction with the help of stepper motors. We are using single axis solar tracker for capturing maximum intensity of the sunlight as shown in fig 2.

ISBN: 978-93-91303-04-04

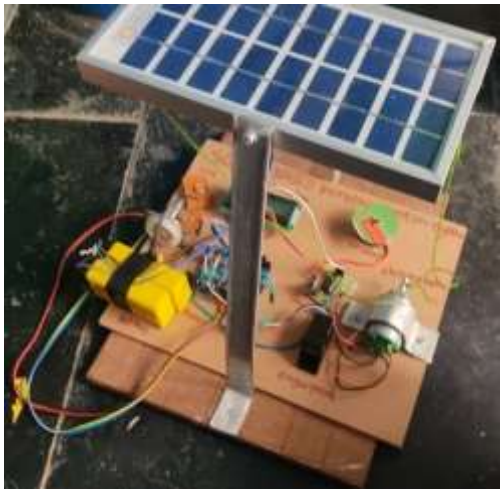


Fig 2. Picture of solar based biometric ignition system

Security for the vehicle will be provided by using a fingerprint sensor. This fingerprint sensor acts as a tool to match the fingerprints of a person and has a 95% success rate in providing authentication. So that only authorised users can be given access to start the vehicle. The rechargeable batteries were used for storing the solar energy and also batteries can be recharge with the help of external power supply. This battery can work for electronic devices like fingerprint module, Arduino, DC motors etc., It has the capacity to store 3000mAH DC 5v/9v/12v.

We can notice the results of LCD for authorized and unauthorised persons.

A. Authorized person

- When a person place the finger in the fingerprint sensor. It checks that finger in the registered fingerprints when it matches it sends the data to LCD display. It displays the person is authorised. Then the DC motor will be run as shown in fig 3.

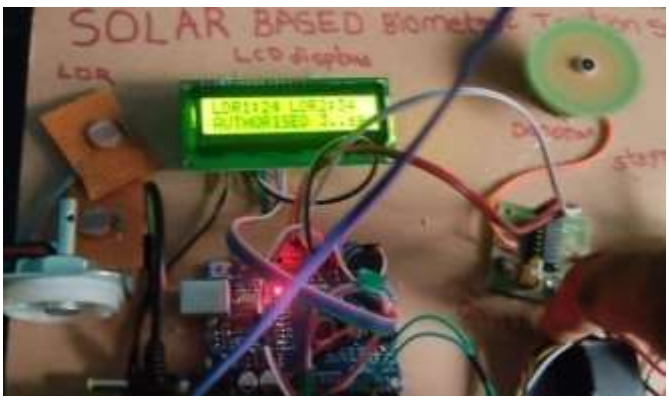


Fig 3. LCD display for Authorised person

B. Unauthorised person

- When a person places the finger in the fingerprint sensor. It checks that finger in the registered fingerprints when it doesn't match with the stored fingerprints, it will displays the data on LCD display. It won't displays the person is authorised. Then the DC motor will be in off condition as shown in fig 4.

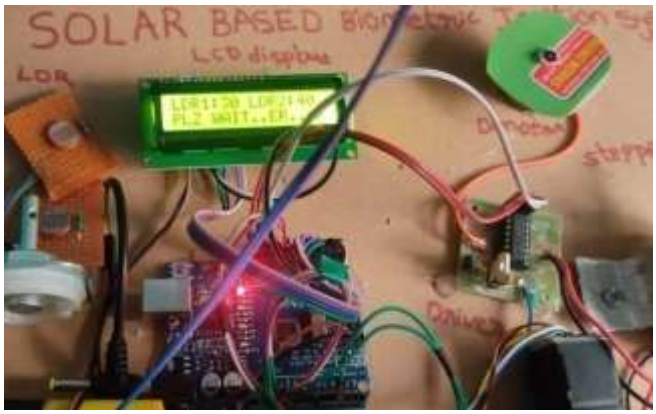


Fig 4. LCD display for Unauthorised personArduino is an open source microcontroller we can bu ild code by using Arduino IDE. 2 LDR's are connected to the analog pins, it captures sun light, based on the intensity captured by the each LDR, the solar panel rotates accordingly. The solar panel is connected to the stepper motor. Between stepper motor and the Arduino, L2923D driver circuit is arranged, it is used to drive the stepper motor for the protection of Arduino. One LDR is represents left side rotation and another is for right side rotation. The solar power is stored in the rechargeable batteries, that stored power is using for the working of entire project. We are using fingerprint sensor to the taking of persons fingerprint who are need to access the vehicle. The Authorized persons fingerprints are already stored in the Arduino so that Arduino checks the given fingerprint is matched or not. When it matches Arduino sends the signal to L2923D driver circuit, it is used to drive the motors and protect the Arduino from back EMF generated by the motors. The driver circuit is connected to the DC motor, when the persons fingerprint is authorised then the DC motor will be run and the LCD will displays the person is authorized. When the fingerprint doesn't matches then the LCD won't display the person is authorised and the DC motor won't run.

ISBN: 978-93-91303-04-04

Result

In order to know the output of the Solar based Biometric Ignition system. We placed the solar panels in the sunlight to store the power in the rechargeable batteries for 2 hours. We used 2 rechargeable batteries with the capable of 1500mAH. It works for 8 hours without recharging. We registered our fingerprints in the Arduino, then checked our fingerprints to start the DC motor it works and the LCD is also displays as Authorised. Then we checked with unauthorised user as a result the DC motor would not run and LCD won't display as authorised. We can also run the entire module with the using of External DC 5v power supply also in case of rainy conditions when the batteries are not charged.

Conclusion

This works as a well operating prototype of a fingerprint based vehicle staring system. It given the appropriate output for respective input. The fingerprint sensor requests for user fingerprint, process it and give appropriate output depends on fingerprint stored in the Arduino. The system can also able to enroll new user's fingerprint at request but we should store the fingerprint before dumping the code into arduino. Arduino program editing can be done in the Arduino IDE we can edit the code any number of times. Hence, fingerprint technology improves the safety, its possible for the vehicle to be employed by only authorized users. Implementing this technique on vehicles makes the achievement of our vehicle security system comes during a cheap and simply available form. The output is viewed with the utilization of DC motor. This Biometric recognition system is safer and also convenience than the traditional methods of person recognition.

References

[1] N Meenakshi, M Monish, K J Dikshit, S Bharath, "Arduino Based Smart Fingerprint Authentication System," 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai, India, 25-26 April 2019.

[2] Winda Astuti, E. Byan Wahyu Riyandwita, IEEE Student Conference on Research and Development (SCOReD), "Intelligent automatic starting engine based on voice recognition system", 13-14 Dec. 2016.

[3] Prachi Rani, Omveer Singh, Shivam Pandey, "An Analysis on Arduino based Single Axis Solar Tracker", 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2-4 Nov. 2018.

[4] Advait Churi, Anirudh Bhat, Ruchir Mohite, Prof. Prathamesh P.Churi ," IEEE International Conference on Advances in Electronics, Communication and Computer Technology", "E – zip: An electronic lock for secured system" Rajarshi Shahu College of Engineering, Pune India. Dec 2-3, 2016.

[5] Jayasree Baidya, Trina Saha, Ryad Moyashir, Rajesh Palit, IEEE 7th Annual Computing and Communication Workshop and Conference , Design and implementation of a fingerprint based lock system for shared access, January 2017.

[6] Manivannan S, Kaleeswaran E,, "Solar Powered Electric Vehicle", 2016 First International Conference on Sustainable Green Buildings and Communities (SGBC), 18-20 Dec. 2016

ISBN: 978-93-91303-04-04

BIOMETRIC VOTING MACHINE BASED ON FINGERPRINTSCANNER AND ARDUINO

N. KHADHAR BASHA, VIMALA P, SALIMA D, RAGHAVA S,VARA LAKSHMI P Electronics and Communication Engineering, Srinivasa Ramanujan Institute OfTechnology, Rotarypuram , Anantapuramu, 515701, Andhra Pradesh, India

ABSTRACT

The design of a biometric votingsystem employing a fingerprint scannerand an Arduino is described in this paper. A person must register their fingerprint with the system, which will be saved centrally in the Arduino. The voter must place his or her finger over the fingerprintmodule, and if the fingerprint matches thepre-stored data, he or she can cast a vote..It is easy to use and has a simple hardwaredesign. It decreases polling time, makes it easier to transport polling boxes to polling centres, reduces voting centre staff, and ensures easy and accurate counting.

Keywords: Biometric, LCD, EVM, fingerprint, keys.

INTRODUCTION

Biometrics is the technology of measuring and studying biological information. Biometrics refers to technology that measure and examine human body characteristics. The area of biometrics became and has in view thatelevated directly to many sorts of physical identity. Among the numerous human fingerprints continue to be a completely not unusual place identifier and the biometric technique of preference amongst regulation enforcement. These principles of humanidentity have result in the improvement of fingerprint scanners that serve to fast pick out people and

assign get right of entry to privileges. The simple factor of those devices is likewise to

have a look at the fingerprint information of an person and evaluate it to a database of different fingerprints.

In our project we have used fingerprint scanner and Arduino to avoid the unauthorized voters to cast their votes. Only enrolled voters can cast their votes using this biometric voting machine. It saves the polling time and staff at voting centre.

LITERATURE SURVEY

Prof. Sunita Patil, Amish Bansal, Utkarsha Raina, Vaibhavi Pujari, Raushan Kumar, "E-Smart Voting Machine with Secure Data Identification Using Cryptography" This describes the E-smart voting system (ESVS) that is biometric authentication voting machine along with OTP based verification machine. At first, person have to punch in its Aadhar number in the ESVS. The ESVS makes use of the Aadhar number toauthenticate the person via OTP on the wayto be obtained on their registered Aadhar related cell number. Issue in receiving OTP because of network issues.

Fig (1): Block Diagram

1. OBJECTIVE OF RESEARCH

The biometric balloting machine needs the person

to enrol fingerprint beforevote casting. The project makes use of arduino device and fingerprint generation to layout a machine that ask to person to scan fingerprint as an identification, themachine reads the information from fingerprint and confirms the informationthat is saved in database. If the input suits with database saved in arduino the device lets in the person to cast vote, else voter

ISBN: 978-93-91303-04-04

is unauthorized.

2. EXISTING SYSTEM

A ballot paper is a form in which citizens fill out inorder to exercise their proper to vote. Ballot papers listing the applicants running for an election and the voter can mark their choices accordingly, that could taken into consideration as reputable documents.

An EVM is designed with devices specifically manage unit and voting unit that are joined collectively with the aid of using a cable. Voters can cast their vote by

party names that is listed and respective keycan be pressed to cast their vote.

The disadvantages in these systems are Post-election it takes greater quantity oftime to count number and claim results via poll paper machine. Individuals need to be recognized who've already voted.

PROPOSED SYSTEM

We have designed an advanced system by using fingerprint module and Arduino. In this biometric based voting machine, a person has to enroll a fingerprintID with the system stored in Arduino. During the election process person should place a finger over fingerprint module, if the fingerprint matches with prestored information then the person is allowed to cast a vote. If fingerprint is unmatched thenperson is unauthorized voter. It has simple hardware design and easily accessible.

3. UIREMENTS

A. Hardware Requirements:

This device is based on fingerprint identification of voters, the requirements are as follows

- Fingerprint moduleR305 - For fingerprint identification
- Arduino Uno - To save information
- LCD - For showing results
- Connector wires - For connecting the components
- Resistors - For reducing current flow

HARDWAREDESCRIPTION Fingerprint Scanner R305

Keypad

A keypad is **a** hard and fast of Fingerprint processing particular consists of factors namely enrolment and matching. The fingerprint reader can carry out lesser increase and may be constant into various end products. Fingerprint sensor is an optical kind. Capacity of Storage is 1000,Speed of scanning is 0.5 sec, Speed of verification is 0.3 sec and safety level is 5.

4. Arduino UNO

Arduino Uno board is a microcontoller based on the ATmega328P. It is programmable with the Arduino IDE through a type B USB cable. Arduino Software (IDE) consists of a serial screen which permits easy textual information to be despatched to and from the board.

LCDs allow displays a lot thinner thancathode ray tube (CRT) technology.

5. Power Supply

Power supply is a connection with a supply of electrical energy. A device that supplies electricity or different forms of strength to an output load is known as a power supply unit (PSU). This electricity deliver is needed to transform AC signal toDC signal. Reduces the amplitude of the signal16*2 LCD (Liquid Crystal Display)

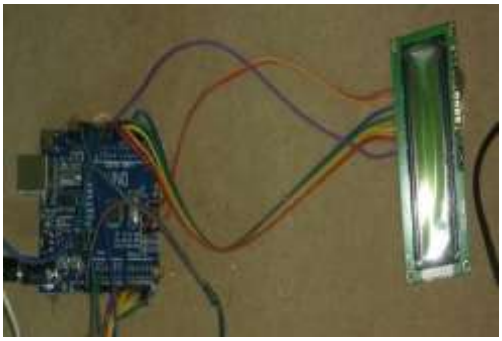
It is a form of flat panel which makes use of liquid crystals. LCDs have a big and ranging as they can be seen in electronic devices. LCDs have been a hugedemand in electronic purposes, whichconsist of light-emitting diode (LED).buttons organized in a block which commonly undergo digits and different symbols however now no longer a whole set of alphabetical letters. Keypads are discovered on many alphanumeric keyboards and on different gadgets which includes calculators, mixture locks

ISBN: 978-93-91303-04-04

and phones which require in large part numeric input. An enter tool, now and again a part of a general laptop keyboard, along with a separate grid of numerical andcharacteristic keys organized for efficient information entry.

B. Software Requirements

- Embedded C



- Arduino compiler

6. FINGERPRINT ENROLLMENT

The first voter saves their fingerprint during the registration process. When the enrol command is given, the userhas place finger to register by a placing a finger. Next, user has to place the same

finger to conform the finger registration andverifies that it matches the first scan, then two fingerprints will be stored. in the givenid. This unique ID is saved in the controller's fingerprint module memory for future reference. After all registrations, the system is ready for polling process.

After Power supply is given, LCD displays Welcome to voting booth. Then presiding officer start voting process. Nowvoting process can be started. First, voter should place finger over fingerprint module, then the module reads the finger data and checks with prestored information stored in the Arduino. If voter 1 isauthorized voter can proceed to vote to the displayed party names by using the keypad.Like wise after all the voters casted their vote, finally presiding officer ends the voting process.

ALGORITHM OF PROPOSED SYSTEM VOTING PROCESS

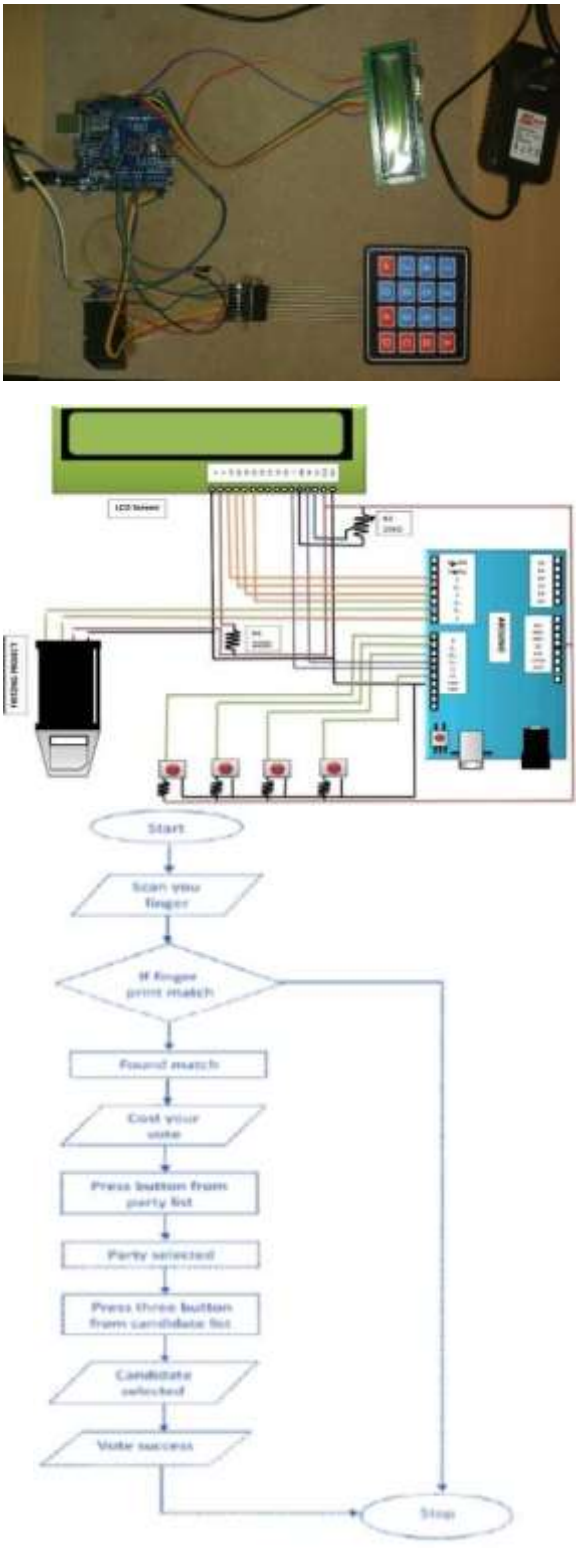


Fig (2): Flowchart of proposed system

Step 1: Start
Step 2: Scan your finger
Step 3: Fingerprint matched
Step 4: Cast your vote
Step 5: Press a key from the keypad
Step 6: Party selected
Step 7: Voted
Step 8: Stop

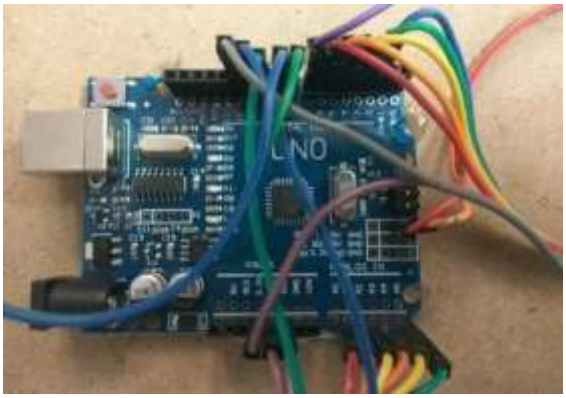


Fig (3): System Design Schematicdiagram

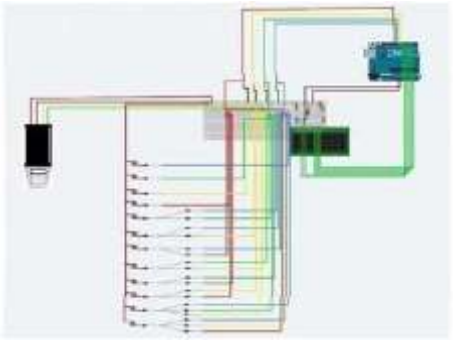


Fig (4): Circuit diagram

Fig (5): Complete system-beginning stage

7. CONNECTIONS

We have shown the connections of the LCD screen and the Arduino board**,** the **VSS** and Cathode pins of the LCD are connected to the GND pin of Arduino and the VDD and Anode pins are connected to the 5V pin of Arduino seem to turn on the LCD screen to the digital pin of the Arduino.

We showed the connectionsfrom the fingerprint module to the Arduinoboard. To transfer data between the fingerprint module and the Arduino board, the TX transmitter pin of the fingerprint module is connected to the RXD receiver pin of the Arduino board and the RX receiver pin of the fingerprint module is connected to the TXD transmission pin of the Arduino board connected. To power thefingerprint module via Arduino**,** the GND pin of the module is connected to the GNDpin of Arduino and the VCC pin of the module is connected to the 5V pin of Arduino.

8. ADVANTAGES IN THE PROPOSED SYSTEM

- The system is easy to use.
- Arduino is a simple control system, powered by a +5 VDC power supply, soit requires less power.
- Economically feasible.
- Requirement of election staff is less.
- Due to its size, it is easy to transport.
- Only authorized users can vote.

9. CONCLUSIONS

This machine overcomes many of the issues faced during vote casting period through paper ballot machine. The performance of this machine relies upon the interface, its usability. This will truly makecertain a more secure voting technique which could be very a lot what's required for a wholesome increase of a developing nation.

In this paper, the proposed Fingerprint based voting machine that's faster and secure. The new machine prevents get entry to unauthorized voters, ease of use. The machine additionally prevents more than one votes through the identical character and tests eligibility of the

ISBN: 978-93-91303-04-04

voter. This system Reduces the staff at polling center, It offers smooth and fast counting without any troubles, Provisioning of vote casting preventive measures.

10. REFERENCES

- Vishal Vilas Natu, 2014. Smart-Voting using Biometric "International Journal of Emerging Technology and Advanced Engineering, 4(6).

- Khasawneh, M., M. Malkawi and O. Al-Jarrah, 2008. A Biometric-Secure e- Voting System for Election Process, Proceeding of the 5th International Symposium on Mechatronics and its Applications(ISMA08),Amman, Jordan.

- VirendraKumarYadav, SaumyaBatham, Mradul Jain, Shivani Sharma, 2014. An Approach to Electronic Voting System using UIDAI, International Conference on Electronics and Communication Systems.

- Chaum,D.L.,1981.Untraceable Electronic Mail, Return Addresses andDigital Pseudonyms, Communicationsof the ACM, 24(2): 84-88.

- VirendraKumarYadav, SaumyaBatham, Mradul Jain, Shivani Sharma, 2014. An Approach to Electronic Voting System using UIDAI, 2014 International Conference on Electronics andCommunication Systems.

ISBN: 978-93-91303-04-04

WIRELESS NOTICE BOARD USING INTERNET OF THINGS

[1]M.Dharani, [2]M.Geethika Brahmini, [3]B.Kalyan, [4]K.Alekya, [5]N.Gowthman
[1,2,3,4] B.Tech Student, Department of ECE, Annamacharya Institute of Technology and Sciences,
[3]Associate Professor, Annamacharya Institute of Technology and Sciences, Tirupathi, Andhrapradesh

ABSTRCT

This paper present a technology based digital notice board using Internet of Things (IoT). Down the years display boards constituted one of the major roles in mass communication medium. In order to reduce paper work, time and man power, the proposed model introduces an online digital notice board using IoT, which connects things to the internet. It can access the Notice board from anywhere across the world through internet. In proposed model is the authorized admin enables to post the message from any corner and this message can be portrayed on the LED display. The proposed model funds with multiple applications like help desks in transporting stations like railway, airways and bus stations which offers travelers to have up to date/updated information. It has a better impact in jammed regions as in supermarket to provide a hike and detrimental cost prices. Lesser to the infinity each remote areas of the world can be portrayed on the screen with the updated news and it can be possible only by the IoT.

Keywords: IoT, Digital Notice Board, Led Display, WI-FI Module, Power Supply

Introduction To Embedded Systems:

Now a day's the notice board is used widely in extreme way. These notice boards can be used in many places like educational institutions, stations etc to display notices or some information to the people who need it. As the technology was increasing day by day, the use of it was also increasing. So, traditional notice board can be replaced with digital notice board that means the conversion of analogue to digital systems including Wi-Fi systems. Since the whole world is running out through internet, our project is mainly based on Wi-Fi module. By using a website we can pass a message to a digital notice board in a wireless communication. To avoid the use of manual work done by a separate person, attempting to digitalize the information. The main objective of our project is by sitting anywhere we can add or remove the message that is to be displayed on the LED screen.

An Embedded system is a computer system designed for specific control functions within a larger system and often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts. By contrast a general-purpose computer, such as a personal computer (PC) is designed to be flexible and to meet a wide range of end-user needs. Embedded systems control many devices in common use today. Embedded systems contain processing cores that are typically either microcontrollers or digital signal processors (DSP) [1]. The key characteristic however is being dedicated to handle a particular task. They may require very powerful processors and extensive communication, for example air traffic control systems may usefully be viewed as embedded, even though they involve mainframe computers and dedicated regional and national networks between airports and radar sites each radar probably includes one or more embedded systems of its own.

Fig 1.1: Embedded system design calls

ISBN: 978-93-91303-04-04

An embedded system is not a computer system that is used primarily for processing, not a software system on PC or UNIX not a traditional business or scientific application. High-end embedded & lower end embedded systems. High-end embedded system - Generally 32, 64 Bit Controllers used with OS. Examples Personal Digital Assistant and Mobile phones etc. Low0er end embedded systems - Generally 8, 16 Bit Controllers used with a minimal operating systems and hardware layout designed for the specific purpose.

II. LITERATURE REVIEW:

In the early 1800's, the path to IoT began with basic forms of long distance communication. In 1832, Baron Shillings [8] in Russia invented the first electromagnetic telegraph. Although the patent for telephone was received in 1876, the 1900's has seen the rise of connectivity. First commercial modem was created by AT&T in 1962 [2]. The present day technology leader, the mobile phone was first invented in 1973 by Martin Cooper while working for Motorola [3]. This invention also introduced cellular data, which is now a big part of IoT [1].The first IoT device was invented by John Romkey, a smart toaster that works with the help of internet. The term IoT is being used more widely since the starting of 21st century. This project will provide a simple design and implementation of a Wireless Notice Board using IoT [9].

In today's information-saturated world, there is a vast range of tools communication that offices, colleges & schools can make use of for keeping Employees, students, parents and staff informed. Notice boards and outdoor poster displays are a useful addition for any office/ college campus in facilitating the distribution of information to campus users and visitors.

They are a convenient communication tool for displaying important information including events, announcements, timetables and schedules to employees, parents, students and teachers. Unlike digital tools, these allow for the sharing of information within the campus premises, which gives the information added geographical relevance.

III PROPOSED METHOD:

The Smart Notice Boards are very useful in our daily life. These are used in different sectors like schools, colleges, shopping complex, highways, offices etc. This project is used for displaying the required information on the LED screen by using IoT technology. This project is designed by using Arduino technology. The block diagram representing the proposed model is shown below in Figure

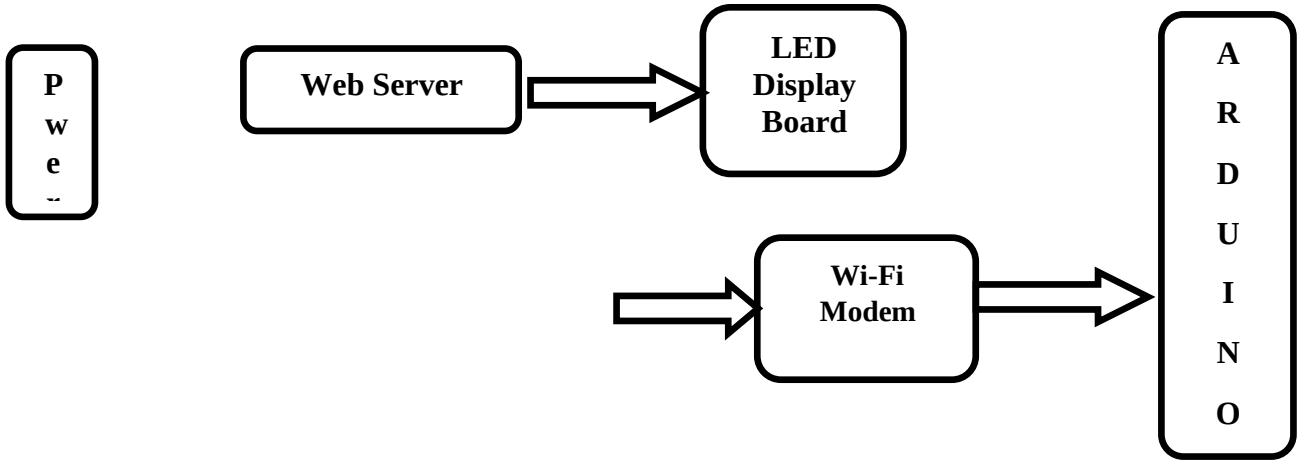


Fig: 1.2 Block Diagram of wireless Electronic Notice Board using IoT

ISBN: 978-93-91303-04-04

This project uses regulated 5V, 500mA power supply. 7805 three terminal voltage regulator is used for voltage regulation. Full wave bridge rectifier is used to rectify the ac output of secondary of230/12V step down transformer. It requires a 2.5A power supply to run the Arduino. Mainly power supply is given to the pin at Wi-Fi module. In this wireless electronic notice board the transformer, which consists of two windings primary and secondary is used for converting the 220V to 24V ac because this system is directly connected to the power supply.The voltage regulator is used for providing the fix 12 volts, DC to the microcontroller. In the absence of voltage regulator, the higher voltage may be damage the LED matrix display or microcontroller and in this system these two components are too much important.

This system uses led matrix of 16×16 resolution. 16×16 matrix consists of 256 dots or pixels. There is a LED for each pixel and these LEDs are connected to total of 16 pins. The whole LED matrix operates on 12 volts DC. Every LED is connected through a resistor to limit the current through LEDs, also a current driver circuit can be used to ensure a uniform brightness of LEDs.NodeMCU is an IoT module based on ESP8266 Wi-Fi module [7]. It uses Lua scripting language and is an open source Internet of Things (IoT) platform. This module has CH340g USB to TTL IC [4]. The features are open source IoT platform, easily programmable, low cost &easy to implement, Wi-Fi enabled. The message to be displayed on LED matrix will be received from ESP8266 Wi-Fi module. Wi-Fi is a technology for wireless local area networking with devices based on the IEEE 802.11 standards [6].

The output of the basic web server implementation will be a static web page displaying text. The IP address assigned is printed in the console. Whenever a user enters this IP address in the browser, the browser sends a connection request to the server. Once the connection is established, the file to be displayed is requested. On receiving this request, the server will send the data to be displayed. The digital notice board allows the user to display the notices wirelessly. The system uses the Wi-Fi module for communication purpose, connected to Arduino board and a LED screen display. For displaying the notice a webpage has been created with the IP address that is generated only when the credentials like network name and password are similar and the user can access the webpage before sending the notice. All the programming related to the system had been done using embedded language. Initially, the programs are executed. After successful execution of the programs an IP address is generated. With the help of IP address we can access the webpage. The webpage includes the text area in which we can enter the message and can be updated. The sent message is received at Wi-Fi module, which then transmits it serially to the LED matrix. Finally the message is displayed on the LED display [5].

IV CONCLUSIONS:

The implementation of Wireless Noticeboard using IoT is done successfully. The communication is properly done without any interference between different modules in the design. Design is done to meet all the specifications and requirements. Software tools are used to dump the source code into the microcontroller, Orcad Lite for the schematic diagram have been used to develop the software code before realizing the hardware.

Circuit is implemented in Orcad and implemented on the microcontroller board. The performance has been verified both in software simulator and hardware design. The total circuit is completely verified functionally and is following the application software.

It can be concluded that the design implemented in the present work provide portability, flexibility and the data transmission is also done with low power consumption.

REFERENCES:

[1] Divyashree M, and Harinag Prasad S " IoT based web controlled notice board"
Interational Research Joural of Engineering and Technology (IJRIER) Volume 5, Issue 4, 2018.

[2] S. Rubin Bose and J. Jasper Prem "Design and Implementation of Digital Notice

Board Using IoT", International journal of recent innovation in engineering and research (IJRIER) 2017.

[3] Sharma, D. K., Tiwari, V., Kumar, K., Botre, B. A., & Akbar, S. A. (2015). "Small and medium range wireless electronic notice board using Bluetooth and ZigBee". 2015, Annual IEEE India Conference (INDICON).

[4] Simha, K., Shreya, Kumar, C., Parinitha, C., &Tantry, S. (2016). "Electronic notice board with multiple output display". 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES).

[5] M. Arun, P. Monika and G. Lavanya, "Raspberry Pi Controlled Smart e-Notice Board using Arduino", International Journal of Computing and Technology (IJCAT), Volume 3, Issue 5, May 2016.

[6] Khera, N., Shukla, D., & Awasthi, S. (2016). "Development of simple and low cost Android based wireless notice board". 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).

[7] S.Arulmurugan, S.Anitha, A.PriyangaP, S.Sangeethapriya, "Smart Electronic Notice Board Using WI-FI", IJISET - International Journal of Innovative Science, Engineering & Technology, Volume 3, Issue 3, ISSN No. 2348 7968, March 2016.

[8] Ajinkya Gaikwad, Tej Kapadia, Manan Lakhani, Wireless Electronic Notice Board, International Journal on Advanced Computer Theory and Engineering (IJACTE)Volume-2, Issue-3, ISSN No. 2319 2526, 2013.

[9] SaloniSahare, Rajat Kadwe and Sheetal Garg, "A Survey Paper on Android Controlled Notice Board", International Journal of Trend in Research and Development, Volume 4(1), ISSN No. 2394-9333, jan-2016.

PARALLEL DECODING FOR BURST ERROR DETECTION AND CORRECTING

K.Shashi Kumar, Thilak.D[1] Sushma.K[2] , Dhamini.C[3] ,Venkata Sai Ramya.V[4] Electronics and Communication Engineering, Srinivasa Ramanujan Institute OfTechnology, Rotarypuram , Anantapuramu, 515701, Andhra Pradesh, India

ABSTRACT: From over years, technology growth has led to less and less geometry of device. It mistakes or cluster mistakes in various memory types are getting more and more prevalent. Some of the processes that create clustered mistakes include multiple bit upset caused by particle hits, write trouble errors and magnetic field coupling. A novel class of single burst error codes was introduced throughout this project that corrects an explosion of any magnitude in such a codeword. A code-building process is described that allows us to create an existing scheme, e.g. Hamming codes. The novel approach for decoding that suggested class of codes, particularly allows quicker decoding, also was described. Different Hamming code constructs and BCH codes have indeed been proposed for this project as well as the decoding difficulty and duplication are compared with current techniques. The approach described reduces the decoder complexity throughout all circumstances, especially for larger burst error sizes, to little or no increased data redundancy. Throughout this research, a parallel decoding system is demonstrated using a novel family of single explosive error correction codes. The suggested parallel decoding system allows fast decoding. This applies in particular with memories that are sensitive to latencies read or access. A novel building approach is developed that allows the suggested rules to be extracted from current codes to fix a single explosion fault.

1.INTRODUCTION

s. This is what has led to several challenges, both with known memory technologies and with new types of coming memory technologies. One sort of failure is indeed a burst error that is becoming common in many kinds of memory because of the declining functionality. Take a look at static random memory (SRAM). Soft radiation defects constitute a major challenge for SRAM reliability[1]. The technological scale also considerably enhanced the sensitivity of SRAMs to soft-errors[2]. Device geometries were modest at today's nanometric nodes and devices keep shrinking with technological scaling. A particle attack might thus impact many cells that cause multiple bit upset (MBU)[3]. This same smaller the geometries of something like the device, the increasing the number of cells impacted by a single blow. A partial b-bit burst triggered by this b-bit hit may cause this same b-bit burst window to flip several bits.

A similar issue is also present in the dynamic random access memory (DRAM)[4]. The challenge occurs because of technology scaling's narrow physical dimensions. While it may boost a chip's memory capacity, this also facilitates the interaction between near-by or neighbouring DRAM cells. Access to a memory cell therefore causes a disruption in the surrounding memory cells to lead to the cargo leaking into or out of the cell. With sufficient access, you may reverse the presently held value of both the adjoining cell.

Through a memory access anywhere at given moment, a single b-bit burst error may occur near the cell to which the explosion is located.

The essential premise of rectifying error codes which solve these problems is that a single burst of mistake should be corrected in the codes. Not all bits or symbols may change throughout the burst window b. Codes targeted at solving these problems should thus be there in the location of a burst error throughout order to fix all potential combinations of errors inside a b-bit burst window. Another parallel decoding approach is proposed for with this project in such a novel class for single burst correction errors. The suggested parallel decoding system allows fast decoding. This applies in particular with memories that are sensitive the latencies read or access. A novel building approach is developed that allows the

ISBN: 978-93-91303-04-04

suggested rules to be extracted from current codes to fix a single explosion fault. Draft findings were submitted in [5] and [6] for both the proposed system. One essential characteristic of both the proposed family for codes is that even the area of both the decoding circuit was significantly reduced especially unless the burst size was adjusted *b*.

2.Literature Survey

Soft errors in advanced computer systems by R. Baumann, s computer devices' size and operational voltages decrease to meet the insatiable desire of customers for increased density, more functionality and less power usage, radiation susceptibility grows drastically. The main radiation concern in terrestrial applications seems to be the soft error, which allows a single radiation incident to destroy a data bit contained in either a device, so long as fresh data is put into it. This paper studies and is applicable completely the sensitivity towards soft-error in current systems. The talk includes ground radiation methods that have the biggest influence on circuit functioning as well as the influence of scaling technologies mostly on memory and logic soft error rates.

11. Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors by Yoongu Kim; Ross Daly; Jeremie Kim; Chris Fallin; Ji Hye Lee; Donghyuk Lee Memory isolation seems to be a vital feature of a dependable safe computer system. Unplanned side effects upon data that are saved at other locations should not be allowed to control a single memory location. However, when the technique of DRAM processes falls back to smaller measurements, it becomes harder to keep DRAM cells without interacting electrically. Throughout this article, we highlight DRAM chips' sensitivity to disturbance. Through reading out of the same DRAM address, they demonstrate that data inside the neighbouring addresses may be corrupted. In particular, activating the very same DRAM row corrupts information in neighbouring rows. Intel and AMD systems use malicious programmes to exhibit this phenomena, which causes multiple DRAM accesses. Researchers induce mistakes in 3 main DRAM manufacturers in many other DRAM modules (110 out of 129). We infer from all this that there is a danger of numerous deployed systems. The fundamental source of disturbances is identified as the repetitive toggling of even a DRAM line, particularly underlines intercell coupling factors that speed charging out of surrounding rows. We give a comprehensive characterization study with FPGA-based tests for trouble faults and behaviour. Our major results indicate that I it requires 139K visits to make a mistake, and (ii) it is sensitive to mistaken access at up to the one in each 1.7K cell. We suggest a low-overhead strategy to avoid mistakes after studying many possible strategies to approach the issue.

Systematic b-adjacent symbol error correcting reed-solomon codes with parallel decoding by Abhishek Das; Nur A. Touba With technology rising, the likelihood of writing disruptions in non-volatile memory influencing surrounding memory cells keeps growing. Specifically, multilevel cell (MLC) phase change memories (PCM) is affected by these faults affecting many nearby memory cells. Reed Solomon (RS) codes provide strong protection for errors when multi-bit symbols may be corrected at once. However the decoding complexity and decoding delay are quite high further than a single symbol error correction. These study presents a systematic b-adjacent coding error, built on Reed-Solomon codes, including one step decoding technique, with low latency and low complexity. There is an universal code building process which can repair most b-adjacent symbol mistakes. In comparison with the current adjacent symbol error that corrects Reed-Solomon codes, these suggested codes are proven to obtain a greater latency throughout the decoder. Furthermore displayed is a substantially improved redundancy compared towards the orthogonal Latin Square (OLS) code correction error.

Siva Sreeramdas, S.Asif Hussain and “Dr.M.N.Giri Prasad proposed on Secure Transmission for Nano-Memories using EG-LDPC”

For even more about a decade memory cells were protected against soft errors, which made the encoder and decoder circuitry surrounding the memory blocks vulnerable to soft errors as just a result of the increased soft error rate on logic circuits and then also needed protection. This introduces a novel way to designing fault-proof memory encoders and decoders. The primary

ISBN: 978-93-91303-04-04

original aspect of this research is to discover and define a new class of error-fixing codes that simplify the design of FSDs and quantify the relevance of the shielding the circuitry comprising encoders and decoders from passing mistakes in a certain way. With the use of the Euclidean GEM (EG-LDPC) algorithm, the error-secure sensor function is provided. Can use some of the smaller LDPC EG codes, you may accept 10% or 10% bit or nanowire defect rate as well as 10-18 device/cycle failure rate throughout the whole memory system well below a FIT rate and 1011 bit/cm2 memory level with 10 nm nano-wire pitch besides 10 mb or more memory blocks. Larger EG-LDPC codes may increase reliability and save overhead.

3.EXISTING METHOD

Latin squares are indeed the basis for OLS codes. A latent square m is also an m x m matrix which includes permutations from its rows and columns of numbers 0, 1,..., m − 1. Whenever overlaid, each ordered pair with components appears once and only, two Latin squares become orthogonal. OLS codes come from OLS. Such codes contain the number of k = m2 and the number of features which the code corrects. Their number of bits is 2 tm. The code t = 2, and hence, 4 m check bit, is utilised for the double error correction. One benefit of OLS codes was their modular architecture, as indicated throughout the introduction. To get a code that would rectify t +1 faults, just add 2m check bits to both the code which can rectify t faults. This may be beneficial for implementing adaptive bug fixing strategies. The modular feature also allows you to choose the ability to repair errors for a specified text size. As already established, OLS codes could be decoded utilizing OS-MLD, since each data bit is precisely 2t check bits, with one another bit at most another of the check bits. That allows for easy rectification if the incorrect number is t or less. The 2t bits have been replenished as well as a majority voting has been taken. That bit is wrong and has to be fixed when one value was received. If not, the piece is okay. Under the worst scenario, the rest of both the t *-1* mistakes may impact t *−1* checkbits so long as they have t or less.

$$H=\begin{bmatrix}
1&0&0&0&0&0&0&1&0&0&1&0&1&0&1&1&1&0&0&0&1&0&0\\
0&1&0&0&0&0&0&0&1&0&1&1&0&1&1&0&0&1&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&1&1&0&1&0&0&1\\
0&0&0&1&0&0&0&1&0&0&1&0&0&0&1&0&1&0&1&1&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&1&1&1&1&0&0&0&0&1&1&0&0\\
0&0&0&0&0&1&0&0&1&0&0&0&1&1&0&0&0&1&0&1&0&0&1\\
0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&1&0&1&1&1&0&1&1
\end{bmatrix}$$

Fig.1. Parity check matrix for OLS code with k = 16 and t = 1.

(1) Thus, a majority of t + 1 still triggers an erroneous bit correction. In either event, the decoding commences with the recalculation of the parity control bits and control of both the stored parity control bits. OLS codes are created from of the Parity check matrix H. Such as instance, the matrix of a code with $k = 16$ and 8 bits which may fix individual faults appears in Fig 1. For codes which would correct more mistakes, the modular design of both the OLS codes in this matrix is part of the H matrix. For instance, eight more rows will be added to the H matrix to get a code that really can rectify two mistakes. Another H-matrix for just an SEC OLS was created as follows for just an upper bound of $k = m2$:

$$H = \begin{bmatrix} M_1 & \\ & I_{2m} \\ M_2 & \end{bmatrix}$$

Whereas I2m were 2m and M1 identify matrix, M2 were m size matrices — alternatively m2. M2 seems to be the identity matrix. Across each row there are m matrix M1. These ones upon on r th row are just in places
$(r-1)\times m+1,(r-1)\times m+2,\ldots(r-1)\times m+m-1,(r-1)\times m+m$. The matrix $M2$ is constructed as follows:

$M2 = [Im\ Im\ \ldots\ Im]$. *(2)*

When m = 4, M1 and M2 matrices may be seen plainly in Fig. 1. This G encoding matrix is only the H matrix for removing the control bit

$$G = \begin{bmatrix} M_1 \\ M_2 \end{bmatrix}.$$

(3)

In summary, this encoder uses a G matrix deriving from of the Latin squares and also has the following characteristics. It accepts k = m2 data bits (di) and makes 2tm check bits (ci) for parity.

1) Every data bit is involved in 2t parity controls precisely.

ISBN: 978-93-91303-04-04

2) Participating throughout the parity tests is the pair of data bits (both bits).
In the following section these features are being used to describe the methodology presented.

4.IMPLEMENTATION OF PROPOSED ARCHITECTURE

Burst error-correction codes from coding theory utilise ways to rectify burst faults that occur over numerous consecutive bits rather than in bits separate.
Many codes were created to fix random faults. However, sometimes channels may produce brief interval faults. These mistakes occur in either a burst, since they occur in several consecutive bits. There are various examples of burst mistakes in storage media. These problems might be caused by physical damage throughout the case of network channels including such disc scratch or lightning stroke. Things are not autonomous; they tend to just be spatial. When one bit contains a mistake, the surrounding bits may be damaged also. Random error correction is ineffective at fixing burst mistakes.
The following cyclic codes were defined: These symbols q are considered in fq to be elements. We may now see words into fq as polynomials, in which each symbol in such a word corresponds to various polynomial coefficients. They choose a fixed polynomial called an polynomial generator to create a cyclic code. Any polynomials which may be divided by such a polynomial generator are indeed the words of such a cyclic code.
In the top section of both the parity control matrix, the main concept of the suggested class and codes would be to employ identity submatrices to directly calculate magnitudes of both the burst error or perhaps the error pattern from either the bits or symbols themselves. The bottom part of both the matrix would then be built using a basic code in order to fulfil the following constraints.
1. All adjacent XORing b-adjacent syndromes should really be single. 1. 1. 1.
2. All symptoms in b-adjacent columns must be unique for certain conceivable column combinations.
3. In the previous two circumstances, multiples of both the column should be employed for XOR instead of just the original column.

Status 1 assures that there really is no miscorrected b-contiguous mistake. Condition 2 assures that no miscorrection is made of any number of errors between b-adjacent columns. These distinct symptoms specify precisely what columns next to b comprise the mistakes. Each column may additionally include multiples with non-binary codes such as Reed Solomon codes that are corrected on even a symbol basis. This same higher b-rows of both the matrix for parity control may detect these multiples. However, condition 3 has to be fulfilled also to prevent miscorrection for varying magnitudes of errors. Thus, the bottom portion of both the matrix of parity control is designed to fulfil all criteria. In the parity check matrix, an identity sub-matrix of size atleast to is attached. When a sub matrix rx-r identity being employed in place of a bx-b, the code is designed systematically. Figure 1 shows the overall structure of both the scheme's systemic parity check matrix, often known as the H-matrix.

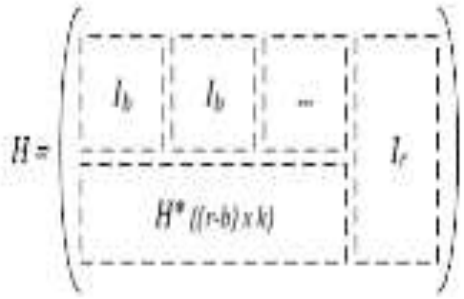


Fig. 1. General Structure of a systematic parity check matrix of the proposed scheme.

A parity check matrix of both the suggested arrangement is comparable with both the identity matrix codes of [23] and Fire code [24]. The main distinction in the designing of the suggested code is in the employment of GF(2b) symbols inside the previously described codes. So, like their corresponding lower submatrix every identical submatrix contains an element of GF(2b). The system proposes to generate the final parity check matrix that use other existing codes, BCH codes, mostly on basis of specified criteria.

ENCODING PROCEDURE

For just a systematic code, this encoding technique consists of many XOR functions with the message bits or signs which are then attached for the code word throughout the original

ISBN: 978-93-91303-04-04

message. Whenever a code is not systematic, a few XOR processes are further necessary to calculate parity check bits or symbols connected with the top half of both the parity check matrix throughout relation to the existing code encoding process used to produce that code. These bits and symbols may be announced at the end of both the codeword or saved independently in a specified word. These are thus termed distinct parity if kept separately. In Figure 2 two distinct storage types of parity are shown.

Fig. 2. (a) ECC bits stored alongside data bits. (b) ECC bits stored sepa-rately in memory (Separate Parity).

DECODING PROCEDURE

The overall process of decoding comprises the two error pattern & error locations processes. For both the proposed approach, the first step would be to use the parity matrix to calculate the syndromes. This syndrome was calculated by multiplying any coded parity matrix. This same XOR operation is indeed a basic one among all data bits or symbols that seem to have a 1 in the parity check matrix per row. This construction of both the matrix of the proposed method for parity controls seems to be that the pattern for error is expressed by the bits or symbols with higher b syndrome, in which the b of the error was fixed. In order to determine the position of both the burst mistake the remainder including its Syndrome bits or symbols are utilised.

Consider any length codeword n, c= (c0, c1, ...cn-1), with the data length k and the no.of control bits or symbols r. Therefore, n= k+ r gives the length of the codeword. This H-matrix is indeed an r- and n column matrix. r also indicates the overall amount of syndrome bits or symbols. These syndrome bits are therefore calculated by using the received codeword to multiply this same h-matrix, as indicated by equations (1). In case of binary bits, the multiplication is really just an AND operation. Multiplication was done using GF for non-binary m-bit symbols (2m). This add operation is indeed a binary and non-binary XOR operation.

$$\begin{pmatrix} S_0 \\ S_1 \\ \vdots \\ S_{r-1} \end{pmatrix} = \begin{pmatrix} h_{0,0} & \cdots & h_{0,n-1} \\ \vdots & \ddots & \vdots \\ h_{r-1,0} & \cdots & h_{r-1,n-1} \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ \vdots \\ C_{n-1} \end{pmatrix}$$

(1)

Next, we analyse a size b explosive mistake beginning with the codeword position. This error vector shows every one of the bits or symbols inside the modified codeword. This allows e= (0, 0,... ei, ei+1, ... ei+b-1, 0,... 0) to yield the error vector. If we add to both the codeword the error vector, then original codeword is returned. This error vector equals 0 when the received codeword is error-free. Both syndrome bits or symbols were equally zero for non-erroneous codewords. Calculating an erroneous codeword syndrome is therefore similar to computing all bits or symbol of the syndrome from it's own vector of error. Let x= imod b, thus. Bits or symbols of the calculated syndrome whenever a coding word multiplied either by suggested H-matrix with an error vector e (2).

We assume to be a multiple of b for simplicity. (S0, S1, ..., sb-1) then = (ei, ei+1,..., ei+b-1). We also look only at binary situation with k data bits and r verification bits for clarity. The mistake pattern was direct effect, as may be shown from the calculated bits of syndrome. That both individual mistake magnitude and the specified H-row are determined by the lower (r-b) syndrome bits. Therefore, we know the amount of the mistake is equal to both the upper b syndrome bits when a burst error starts at position i. Hence, equation (3) is fulfilled in incorrect places, i.e. ito i+b-1. Equation (3) is indeed not valid for all of the other places. Therefore, the calculation of the error location in such a group of bits is completed, and equation (3) is met for the group of bits in error. This suggested decoding process is based on this.

This decoding works by taking each set of b-adjacent columns as just a single huge symbol and decoding and per symbol basis. Every data bit di is therefore part of b-bit symbols. An instance of 4-bit explode-correction code in Fig. 3 has indeed

ISBN: 978-93-91303-04-04

been presented, the information but divided into 4-bit Bi-3, Bi-2, Bi-1and Bi symbols. This b-bit burst error is just a mistake from one of the b-bit symbols and so can be calculated via equation (3). If indeed the data bit is really a component of equation (3) for any one of the b-bit symbols, this implies that the database is inaccurate. The data bit's error pattern is just the Sα syndrome value, wherein α is just the upper b-row row wherein the column is 1. Therefore, for each data bit, this same error location And then all b-bit symbols it's indeed one part of. The data bit would not only be incorrect if equation (3) for certain b-bit symbols that are part of this is not met.

$$\begin{pmatrix} S_0 \\ S_1 \\ \vdots \\ S_x \\ S_{x+1} \\ \vdots \\ S_{b-1} \\ S_b \\ \vdots \\ S_{r-1} \end{pmatrix} = \begin{pmatrix} e_{l+((b-x) mod\ b)} \\ e_{l+((b-x+1) mod\ b)} \\ \vdots \\ e_i \\ e_{i+1} \\ \vdots \\ e_{l+((b-x-1) mod\ b)} \\ h_{b,0}e_l + \cdots + h_{b,b-1}e_{l+b-1} \\ \vdots \\ h_{r-1,0}e_l + \cdots + h_{r-1,b-1}e_{l+b-1} \end{pmatrix}$$

$$S_\beta + h_{\beta,0}S_0 + h_{\beta,1}S_1 + \cdots + h_{\beta,b-1}S_{b-1} = 0$$
$$\forall\, b \le \beta \le (r-1)$$

5.SIMULATION RESULT:

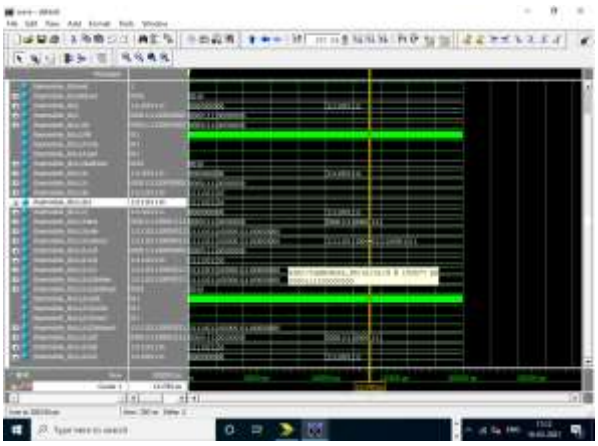


Fig 8.1 Simulation Result

Fig 8.1show the simulation result of proposed system. Where we can detect the error and correct the error

6.Conclusion And Future Scope:

This document offers a novel family of single explosion error correcting parallel decoding codes. That parity control matrix of current codes is enhanced by this coding class. Also there is a novel decoding approach that provides a one-step decoding logic that allows quick parallel decoding. Those codes are especially important for memory with latency performance. Comparisons using current systems demonstrate that in particular the decoder area with large burst sizes with such a minimum increase to redundancy was significantly reduced by the suggested class of codes. These findings reveal that, in comparison with current systems for bigger burst dimensions, the proposal system is also achieving greater decoder delay.
Current plans are far more efficient than the approach intended to deal with lower burst sizes. The suggested system, however, offers an effective solution with both the decoder area as well as the delay to correct a bigger mistake of burst size whilst providing greater throughput using scaling technology even as number of bits may roll over owing to bursting failure grows. Thus since the primary sorts of soft mistakes are shifted toward localised cluster error for various forms of memory, the suggested coding class offers an efficient technique with little complexity that allows such failures to be tolerated without major increase in data redundancy.

References

[1] R. Baumann, “Soft errors in advanced computer systems,” in IEEE Design & Test of Computers, vol. 22, no. 3, pp. 258-266, May-Jun 2005.

[2] E. Ibe, H. Taniguchi, Y. Yahagi, K. Shimbo and T. Toba, “Impact of scaling on neutron-induced soft error in SRAMs from a 250 mm to a 22 nm design rule,” in IEEE Transactions on Electron Devices, vol. 57, no. 7, pp. 1527-1538, Jul. 2010.

[3] D. Radaelli, H. Puchner, S. Wong and S. Daniel, “Investigation of multi-bit upsets in a 150 nm technology SRAM device,” in IEEE Transactions on Nuclear Science, vol. 52, no. 6, pp. 2433-2437, Dec. 2005.

[4] Y. Kim, R. Daly, J. Kim, C. Fallin, J. H. Lee, D. Lee, C. Wilkerson, K. LaiandO. Mutlu, "Flipping bits in memory without access-ing them: An experimental study of dram disturbance errors", in Proc. of ACM/IEEE International Symposium on Computer Archi-tecture (ISCA), pp. 361-372, 2014.

[5] A. Das and N.A. Touba, "Systematic b-Adjacent Symbol Error Correcting Reed-Solomon Codes with Parallel Decoding" in Proc. of IEEE VLSI Test Symposium, pp. 1-6, 2018.

[6] A. Das and N.A. Touba, "Low Complexity Burst Error Correct-ing Codes to Correct MBUs in SRAMs" in Proc. ofACMGreat Lakes Symposium on VLSI(GLSVLSI), pp. 219-224, 2018.

[7] H. O. Burton, "Some asymptotically optimal burst-correction codes and their relation to single-error-correcting reed-solom codes," in IEEE Transactions on Information Theory, vol. 17, no. 1, pp. 92–95, Jan. 1971.

[8] S. Baeg, S. Wen and R. Wong, "SRAM Interleaving Distance Selection with a Soft Error Failure Model," in IEEE Transactions on Nuclear Science, vol. 56, no. 4, pp. 2111-2118, Aug. 2009.

[9] R. Datta and N.A. Touba, "Generating Burst-Error Correcting Codes from Orthogonal Latin Square Codes - A Graph Theoret-

ic Approach," in Proc. of IEEE Symposium on Defect and Fault Tol-erance, pp. 367-373, 2011.

[10] P. Reviriego, S. Liu, J.A. Maestro, S. Lee, N.A. Touba and R. Datta, "Implementing Triple Adjacent Error Correction in Dou-ble Error Correction Orthogonal Latin Square Codes," in Proc. of IEEE Symposium on Defect and Fault Tolerance, pp. 167-171, 2013.

ISBN: 978-93-91303-04-04

Secure Medical Data Transmission Model for Healthcare Systems

Maruthi Kumar D, Sai Akhila N, Sarala P, Pavan Kumar A, Vijay Kumar B
DepartmentofECE,Srinivasa Ramanujan InstituteofTechnology,Anantapur,

AndhraPradesh

ABSTRACT

An associated healthcare system will be simple for patients to access and track their wellbeing data and consider consistent correspondence with physicians. Because of utilization of the IoT in the medical services area, these days the security of the clinical information turned into a major issue for medical services administrations. An efficient security model that enables to hide the information (indicative content information) in clinical images is necessary. The proposed model is created by the utilizing 1 level or by 2 level discrete wavelet transform steganography methods combined with encryption. AES and RSA crypto schemes are used for encryption. The new technique begins with the encryption of medical information and afterward disguising it a cover picture utilizing 2-D discrete wavelet transform in 1 level or 2 level or 3 level. To hide diverse content sizes, we can utilize both grayand dim scale pictures as cover pictures. The proposed model can conceal the patient's clinical info into communicated cover picturewith imperceptible &insignificant decay in the got new-stego picture.

Keywords - *Hybrid Encryption, Cryptography, Steganography, 2D-DWT-1 level, 2D-DWT-2 level*

INTRODUCTION

IOT enables exchange of data with other devices and systems over the internet. Data privacy plays a vital role during its transmission. Due to the advancement of IOT in the healthcare sector, transferring of medical data became a daily routine. There is a need of a secure model to provide sufficient security and to restrict third party from accessing the data. A secure medical data transmission model can be achieved by using hybrid encryption and steganography techniques.

Cryptography is the process of encoding the data into cipher text so that only intended persons can read and access the data. The proposed hybrid encryption scheme involves two algorithms namely AES and RSA calculations. AES uses secret key encryption that takes plain content as 128 bit blocks and converts them to encode text utilizing keys of 128, 192, and 256 bits. RSA is a public key encryption technique that is generally utilized in encryption for secure information transmission. It utilizes variable measured key going from (2-2048) bits. Steganography is the art of concealing the data in an ordinary file or image. This is combined with the hybrid encryption scheme so as to obscure the fact that there is sensitive data hidden in the file.

LITERATURE SURVEY

Abdulaziz Shehab, Mohamed Elhoseny, Khan Muhammad, Arun Kumar Sangaiah, Po Yang, Haojun Huang, Guolin Hou; Secure and Robust Fragile Watermarking Scheme 2018, Volume: 6 , Issue: 99
This paper proposes another delicate watermarking-based strategy for picture verification and self retrieval for clinical applications. The proposed strategy can find the picture altering and recuperate the first picture. This proposed scheme significantly improves both finding data altercation accuracy and PSNR of recovered images.

Jain, M., Choudhary, R. C., & Kumar, A. (2016). Secure medical image steganography with RSA cryptography using decision tree. 2016 2nd International Conference on (pp. 291-295), IEEE
This paper proposes another method for placing the patient's clinical data into the clinical cover image by concealing the information utilizing choice tree idea. This strategy is based on RSA computation for encoding data and steganography for hiding the data.

Abdel-Nabi, H., & Al-Haj, A. (2017). Efficient joint encryption and data hiding algorithm for medical picture security. 2017 8th International Conference on (pp. 147-152). IEEE

ISBN: 978-93-91303-04-04

This paper proposes a proficient crypto-watermarking calculation to get clinical images sent in tele-medication applications. The proposed method utilizes standard encryption strategies and reversible watermarking procedures to give security to the sent clinical pictures just as to control access advantages at the recipient side. This methodology accomplishes both the realness and trustworthiness of the images.

EXISTING SYSTEM

Cryptography is the process of encoding the plain text into an unreadable format known as cipher text so as to restrict the unauthorized access. Encryption process is done at the sender side using a secret key and thus a cipher text is produced. At the recipient side, the encoded text is deciphered to from the plain text using the key. The encoded text can be easily accessed by anyone who possesses the secret key. The secret keys have to be exchanged before starting the communication. During the key exchange, if any unauthorized person is listening to the channel (eavesdropping), then that person

can easily attain the key and decrypt the cipher text. Both sender and receiver may not be noticing this eavesdropping. Thus the confidentiality of the data that is being transmitted is lost. So usage of cryptographic techniques only, for data security may not be reliable as it may lead to unauthorized access of data being transmitted. Hence conventional encryption methods fail to give the desired result of protection.

PROPOSED SYSTEM:

Objective

The principle aim of this model is to improve the security and to maintain the confidentiality of patient's medical data to get an efficient and secure healthcare system.

Methodology

This paper proposes a safe model for clinical information transmission utilizing steganography and hybrid encryption strategies. The proposed model contains four stages:

1. The patient's clinical information is enciphered using two encryption techniques.
2. The encoded information is hidden in a cover picture utilizing 2D discrete wavelet change of 3-level produce a stego picture.
3. The hidden data is recovered from stego picture by using the 2D discrete wavelet transform of 3- Level.
4. The retrieved information is deciphered to recover its actual form.

The proposed system for secure transmission of clinical information is as illustrated

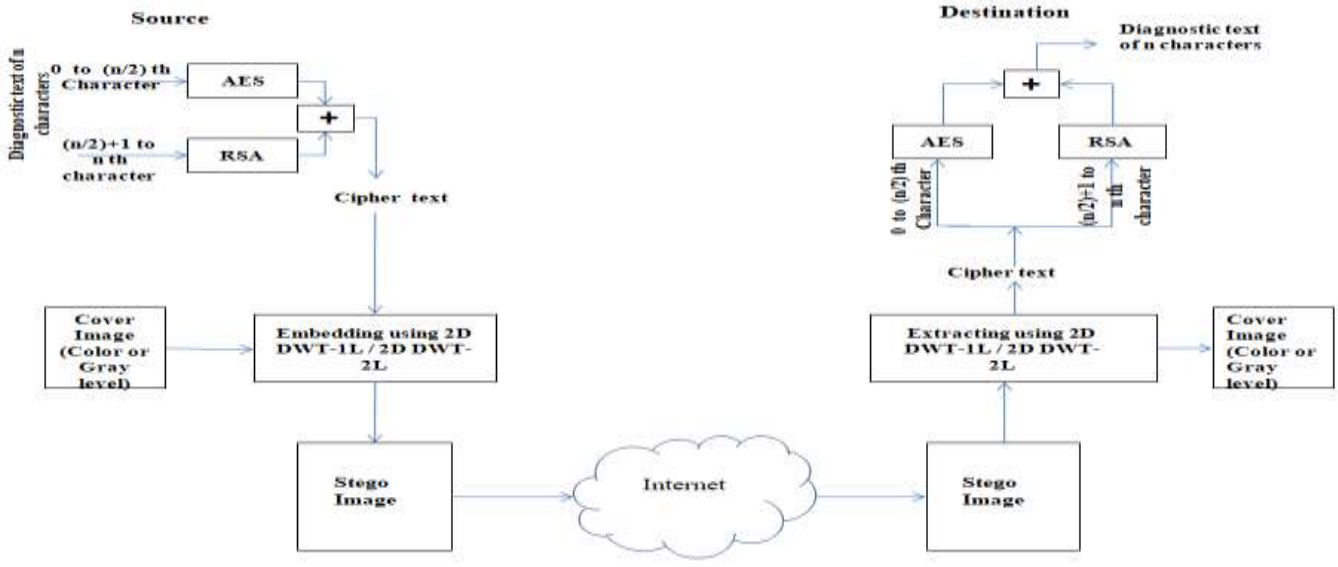


Fig. 1: Block diagram of Proposed

ISBN: 978-93-91303-04-04

1. Data Encryption :

The proposed model uses a hybrid encryption which is accomplished utilizing AES and RSA schemes. The diagnostic medical data that has to be transmitted is known as plain text. The plain text T of length 'n' characters is divided into two blocks T_1 and T_2 such that T_1 contains 0 to (n/2) th character of T and T_2 contains (n/2)+1 to nth character of T. The text thus divided is subjected to encryption. The AES scheme is utilized to encipher text T1 utilizing a public key 's'. The RSA cryptographic scheme is utilized to encipher text T2 utilizing a public key 'm'. To improve the level of security, the private key has to be used to decrypt the RSA encrypted text at the recipient side, is encoded using AES before transmitting. After encryption, plain text T_1 and T_2 are converted into encrypted text C_1 and C_2 respectively. The hybrid cipher C is formed by combining cipher texts C_1 and C_2.

2. **Embedding Procedure:**

This step involves steganography technique implemented by using a Haar - DWT. A cover image (either color or gray level) is selected and is decomposed into sub-band images using 2D DWT of 1-level or 2-level. The 2D-DWT can be implemented by continuous change utilizing LPF and HPF as shown in Fig.2

The cover image is divided into four sub-band frequencies a HH, a HL, a LH, and a LL bands.

The Encrypted text is then placed into the disintegrated picture.

.

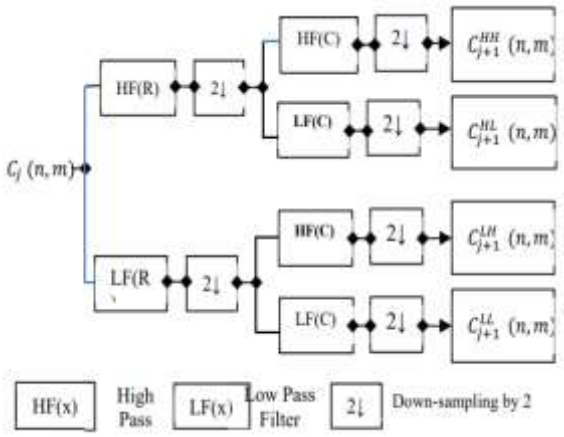


Fig. 2. Decomposition Procedure of DWT-2L

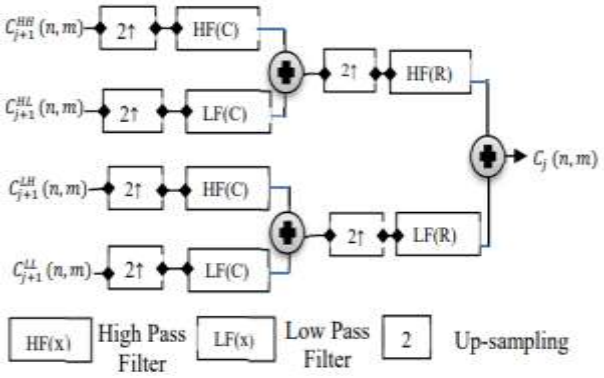


Fig. 3. Synthesis Procedure of DWT-2L

After inserting the text into image inverse 2D DWT is used to generate stego image as represented in Fig 3. The embedding procedure is illustrated in Fig.4

ISBN: 978-93-91303-04-04

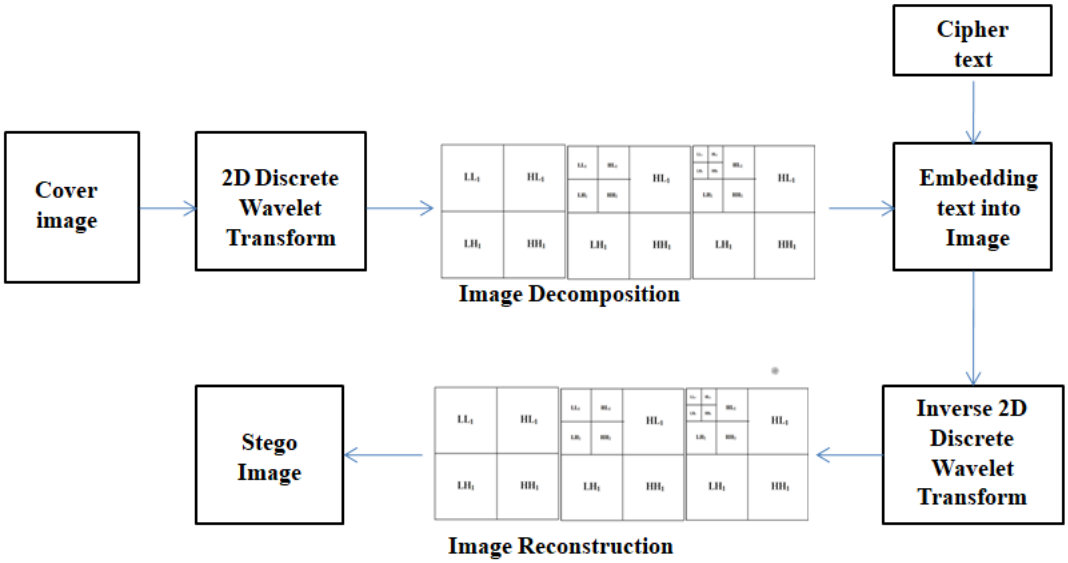


Fig. 4: Embedding text into image using 2D DWT- 3 Level

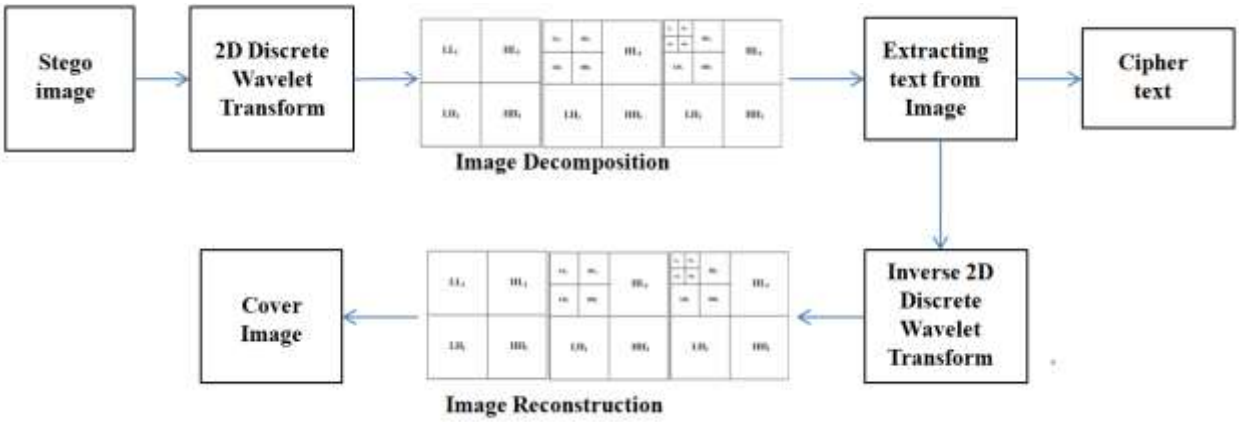


Fig. 5: Extracting text from image using 2D DWT- 3 Level

ISBN: 978-93-91303-04-04

5. Extraction Procedure:

At the receiver end, the received stego image is again subjected to 2D DWT to form four decomposed sub-band images of different frequency bands. The embedded text is then retrieved from the decomposed image. The entire embedding procedure is illustrated in Fig. 5.

6. Data Decryption Scheme:

Decryption is the converse of the encryption. The hybrid cipher text that is retrieved from the stego image which is of length 'n' characters is then divided into two blocks C_1 and C_2 such that C_1 contains 0 to (n/2) th character of C and C_2 contains (n/2)+1 to nth character of C. The text thus divided is subjected to decryption. The AES algorithm is used to decrypt text C_1 and RSA algorithm is used to decrypt text C_2 using respective decryption keys.

After decoding, encoded text C1 and C2 are changed over into decoded text T1 and T2 respectively. The deciphered text T1 and T2 is then merged to obtain original data T, which is the clinical data that is conveyed by the sender.

Advantages in Proposed system

- By using hybrid encryption technique in data transmission confidentiality, authentication, data integrity, non - repudiation of data can be improved.
- Steganography improves data imperceptibility which helps in reducing data manipulation attacks.

Conclusion

The proposed secure clinical information transmission model improves the security of information that is sent over web by making the information unperceivable and difficult to decipher accordingly, improving protection principles of communicated clinical information of patients.

References

[1] Abdel-Nabi, H., & Al-Haj, A. (2017). Efficient joint encryption and data hiding algorithm for medical images security. 2017 8th International Conference on (pp. 147-152). IEEE.

[2] Yin, J. H. J., Fen, G. M., Mughal, F., & Iranmanesh, V. (2015). Internet of Things: Securing Data using Image Steganography. 2015 3rd International Conference on (pp. 310-314). IEEE.

[3] Sreekutty, M. S., &Baiju, P. S. (2017). Security enhancement in image steganography for medical integrity verification system. 2017 International Conference on (pp. 1-5). IEEE

Third Eye For Blind Using Ultrasonic Sensor And Health Monitoring

D. Maruthi Kumar[1], Brunda.J[2], Kalpana .M[3], Sandhya. L[4], Eswar Sai Rahul Reddy. K[5]

[1, 2, 3, 4,5] Department of ECE, Srinivasa Ramanujan Institute of Technology, Anantapur, Andhra Pradesh.

Abstract: The "Third Eye for blind using ultrasonic glove and health monitoring" is intended to assist blind people in overcoming their visual impairment. When conducting daily duties, the visually handicapped experience a number of difficulties. The development of practical solutions to assist the visually impaired is gaining popularity. The proposed solution is developing an ultrasonic glove which detects the obstacle and alerts the user to change his direction of movement through a voice module. This glove is also designed for health monitoring. It continuously monitor their pulse rate and body temperature using heart rate sensor and LM35. When a user falls, a MEMS sensor detects it, and a message is delivered to the concerned person via the GSM module.

Keywords: Ultrasonic Glove, voice module, LM35, Heart Rate Sensor, MEMS Sensor, GSM Module.

I.INTRODUCTION

The ability to see is one of the most important aspects of human physiology. Our senses of sight is crucial to our understanding of our surroundings. From the research provided by the WHO, there are around 285 million individuals who are visually impaired, with 39 million of them blind (WHO). Furthermore, 90% of visually handicapped people live in developing countries. The first tool for blind people was a walking stick, but the main disadvantage is that it requires training before use. With technological advancements, it is now possible to discover a solution that allows visually impaired people to travel freely both indoor and outdoor environment.

The key qualities of this project are that it is beneficial to both visually impaired and elderly people. Obstacles such as vehicles and stones in outdoors and stairs, walls, and furniture in the indoors are identified and alerted to the user via the speech module. Sensors like the LM35 and the pulse sensor are used to continuously monitor body temperature and heart rate. The MEMS sensor detects a person's fall, and a message is delivered to the individual concerned via the GSM module.

II.EXISTING SYSTEM

The smart stick was created with obstacle detection and navigation. Infrared, ultrasonic, and water sensors were used. This project also makes use of a GSM module and GPS. The stick's position and navigation are detected via GPS. If the blind person is in danger, the GSM module can send a notification to the concerned person. The power source for the system is a 9V battery. The Arduino Uno microcontroller ATmega328P is used in this system. This system has a GSM module that allows it to call in an emergency. When the distance between the visually impaired person and the obstacle is reduced, the intensity of beep sound rises. When an obstruction is recognised, a spoken warning message is delivered through earphone. Obstructions such as downhill stairs, holes, and other obstacles can also be detected by this technology. The fundamental disadvantage of this method is that it cannot be folded.

III.PROPOSED SYSTEM

Blind Glove is an innovative glove designed for blind people for navigation in indoor and outdoor environment.

Our proposed system first uses ultrasonic sensors to detect obstacles using ultrasonic waves. When the obstacle is detected then sensor passes data to

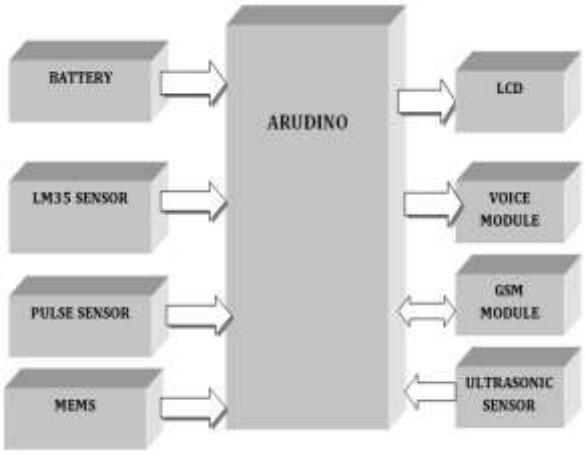
the microcontroller, the microcontroller calculates distance between the blind person and obstacle.

Pulse sensor will detect the heart beat of blind person, If pulse is abnormal then it will be send message to microcontroller. If the pulse detected in the sensor is higher than normal level then

microcontroller executes the code the microcontroller sends a signal to voice module and send sms through gsm.

Temperature sensor will detect the temperature of blind person, If temperature is abnormal then it will be send message to microcontroller. If the temperature detected in the sensor is higher than normal level then microcontroller executes the code the microcontroller sends a signal to voice module and send sms through gsm.

Mems sensor will detect the falling of blind person, If mems is abnormal then it will be send message to microcontroller. If the value detected in the sensor is higher than normal level then microcontroller executes the code the microcontroller sends a signal to voice module and send sms through gsm.



BLOCK DIAGRAM DESCRIPTION

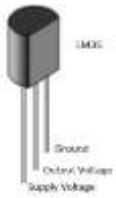
Fig3: MEMS

1. LM35:

The LM35 series of precision integrated-circuit temperature sensors have an output voltage that is proportional to the temperature in Celsius (Centigrade). It measures the temperature of range -55 to 150°C. Figure of LM35 is shown below(fig1)

2. Pulse sensor:

Knowing your heartbeat rate is extremely important when exercising, researching, and so forth. However, calculating the heartbeat rate might be difficult. The pulse sensor, sometimes known as a heartbeat sensor, is utilised to solve this problem. This is a plug-and-play sensor that is primarily developed for Arduino boards. We can get quick and accurate heartbeat readings by utilising this circuit. This circuit can be used in mobile applications with a current of 4mA and a voltage of 5V.



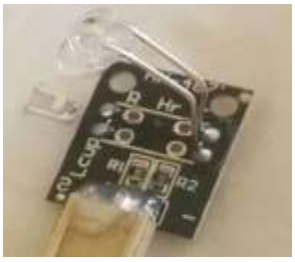


Fig1. LM35 *Fig2: Pulse sensor*

3. MEMS Sensor: The Acronym of MEMS is Micro Electro-Mechanical System. MEMS inertial sensors are low-cost, high-accuracy inertial sensors that are employed in a wide range of industrial applications. This sensor is based on the micro-electro-mechanical-system, which is a

chip-based technology. These sensors are used to detect and measure external stimuli such as pressure, after which it responds to the pressure that is sensed using some mechanical mechanism.

Ultrasonic Sensor: Ultrasonic sensor is used to measure the distance by sending ultrasonic waves and receives the reflected wave when this waves hits the obstacle. This sensor has 4 pins they are, VCC, Trigger, Echo and Ground. It's theoretical measuring distance is 2 to 450 cm and practical measuring distance is 2 to 80cm.

ISBN: 978-93-91303-04-04

Fig4: Ultrasonic Sensor

5.GSM Module: GSM stands for global system for mobile communication. Following commands are used

- ❖ AT : For serial interfacing.
- ❖ ATD : used to Dail.
- ❖ ATA : Used to Answer.
- ❖ ATO : Used to return to the online data set.
- ❖ AT+CMGS : Used to send SMS.
- ❖ AT+CMGL : To view list of SMS messages.
- ❖ AT+CMGR : To read SMS messages.

Fig5: GSM

6. Voice Module: APR33A3 voice module is used in this project. It provides high quality recording and playback audio at 8KH sampling rate with 16 bit resolution. It has 8 channels to record 8 voices. It has built in audio recording microphone amplifier.

Fig6: APR33A3 voice module

7. LCD : LCD(Liquid crystal display) is a flat panel display that operates primarily with liquid crystal. LCDs have wide range of applications and it is the most commonly connected device to any microcontroller.

Fig7: LCD module

8. Arduino UNO: It is a widely used open source microcontroller board based on microchip ATmega328P which is developed by Arduino.cc. It has 14 digital pins and 6 analog pins. It is programmed by using Arduino IDE. It is powered by using 9V battery or external USB cable. Among 14 digital pins 6 pins are used for PWM output. It has 32KB flash memory, clock speed is 16MHz.

Fig8: Arduino UNO

ISBN: 978-93-91303-04-04

IV.EXPERIMENTAL RESULTS

Fig9: Message is sent during Abnormal Condition

Fig10: Temperature, pulse rate, distance displayed in lcd

T: Temperature in ˚C

P: Pulse rate

X, Y: Axis in mems sensor

26 is distance measured by Ultrasonic sensor in centimeters(cm)

When the obstacle is closer system alerts the user to change his direction through voice module.

V.CONCLUSION

The project's goal of designing and implementing a Smart Glove for the blind has been entirely realised. This glove serves as a foundation for future generations of assistive gadgets that will enable the vision impaired travel securely both indoors and outdoors. It is both efficient and cost-effective. It performs well when identifying obstructions within 3 metres. This system provides a low-cost, dependable, portable, low-power, and robust navigation solution with a quick response time. It is lightweight and simple to operate. When the individual's health is in danger, the lm35 and pulse rate sensor are used to send a GSM message to the concerned person.

Continuous health monitoring is done by using lm35 and heartrate sensor by GSM message is sent to concerned person when the person is in risk. Finally this device is not only useful for visually impaired but also for elder persons.

.

VI.REFERENCES

[1]. Ultrasonic Distance Meter by Md Arefi and Mollick published in International Journal of Scientific and Engineering Research in March 2013.

[2]. Ultrasonic stick for blind by Agarwal, Kumar and Bhardwaj, published in International Journal of engineering and computers in April 2015.

[3]. Voice operated outdoor navigation system for blind people by Koleey and Misra, published in International journal of emerging trends and technology in 2012.

[4]. Smart stick for visually impaired: Obstacle detection, artificial vision, and real-time help via GPS by S. Dhambare and Sakare published in National Conference of Information and Communication Technology in 2011.

[5]. A smart walking stick is an electronic aid for visually impaired people by Hazzaz, Ranasaha, Sayemul Islam.

[6]. Assistive infrared sensor based smart stick for blind people by Ayat Nada, A. Fakhar and Ahamed FSaddiq

ISBN: 978-93-91303-04-04

CLASSIFICATION AND DETECTION OF SKIN CANCER

[1]M.Dharani, [2]B.Vishnu, [3]S.Venkata Pradeep, [4]K.Naga Bhushan, [5]V.Parasuram
[1,2,3,4] B.Tech Student, Department of ECE, Annamacharya Institute of Technology and Sciences
[3]Associate Professor, Annamacharya Institute of Technology and Sciences, Tirupathi, Andhrapradesh

ABSTRCT:

The non-invasive medical computer vision or medical image processing plays increasingly significant role in clinical diagnosis of different diseases. Such techniques provide an automatic image analysis tool for an accurate and fast evaluation of the lesion. The steps involved in this study are collecting Dermoscopy image database, pre-processing, segmentation using thresholding, statistical feature extraction using Gray Level Co-occurrence Matrix (GLCM), Asymmetry, Border, Color, Diameter, (ABCD) etc., feature selection using Principal Component analysis (PCA), calculating total Dermoscopy Score and then classification using Support Vector Machine (SVM). Then features are calculated based on the GLCM, which gives low accuracy comparative to the SVM method. The results show that the achieved classification accuracy is 92.1%.

Keywords: Support Vector Machine (SVM), Principal Component Analysis (PCA), Skin cancer, Gray Scale Co-occurrence Matrix (GLCM).

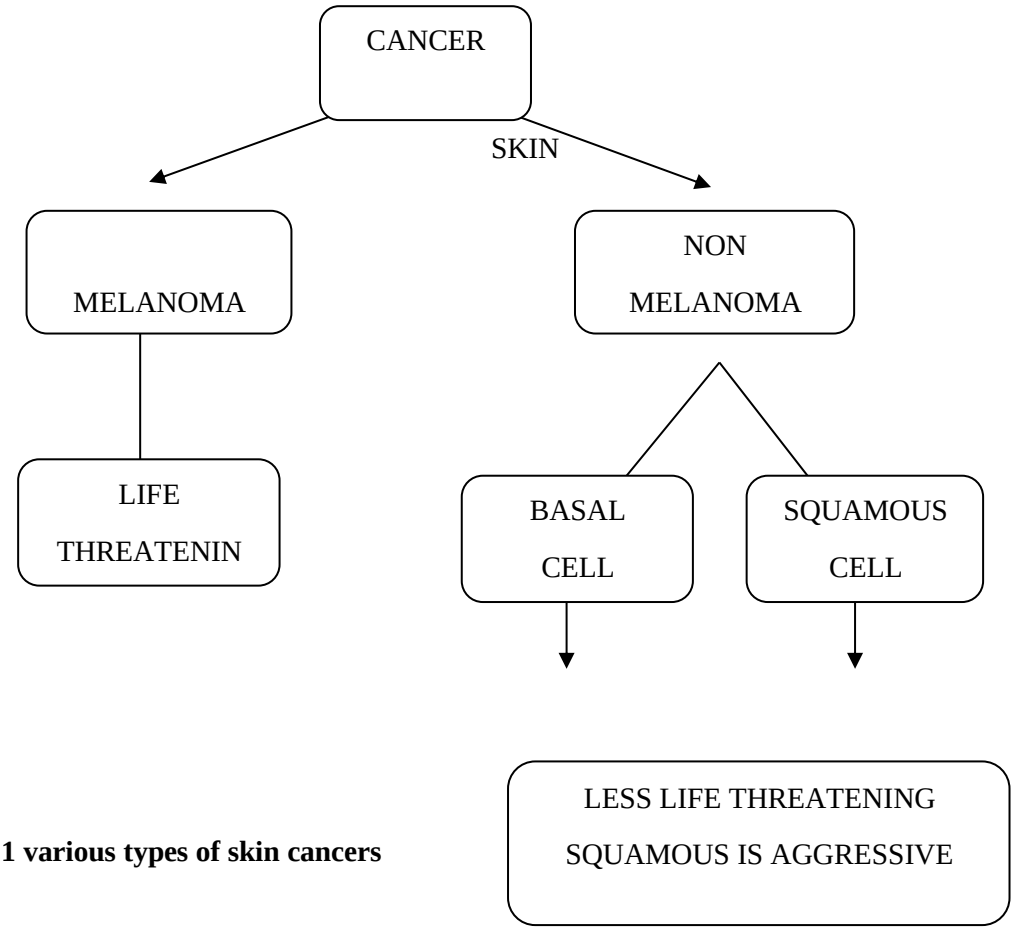


Fig 1.1 various types of skin cancers

Introduction:According to WHO and Lee et al, Caucasian populations generally have a much

ISBN: 978-93-91303-04-04

higher risk of getting skin cancer disease than dark-skinned populations. Naturally, brown and black people can usually safely tolerate relatively high levels of sun exposure without getting sunburns or greatly increasing their skin cancer risk. In contrast, people with pale or freckled skin, fair or red hair and blue eyes belong to the highest risk group. Followed by people with dark hair and eyes who do not normally get sunburns are at medium risk of skin cancer developing. Skin is the outer most region of our body and it is likely to be exposed to the environment which may get in contact with dust, Pollution, micro-organisms and also to UV radiations. These may be the reasons for any kind of Skin diseases and also Skin related diseases are caused by instability in the genes this makes the skin diseases more complex [2].

The human skin is composed of two major layers called epidermis and dermis. The top or the outer layer of the skin which is called the epidermis composed of three types of cells flat and scaly cells on the surface called SQUAMOUS cells, round cells called BASAL cells and MELANOCYTES, cells that provide skin its colour and protect against skin damage. As the diagnostic classification currently do not represent the diversity of the disease, these are not sufficient enough to make a correct prediction and also treatment to be provided for that disease. Adding to this cancer cellsare often diagnosed late and treated late, it is diagnosed when the cancer cells have mutated and spreads to the other internal parts of the body. At this stage therapiesor treatments are not very effective. Due to these kinds of issues skin cancer percentage is taken over by the heart related diseases as the most affected and it is the cause of death among all ages in the world. The other reasons for which the disease might have taken over to a very serious state can be because of people's ignorance. Among all the types of skin disease skin cancer is found to be the deadliest kind of disease found in humans. This is found most commonly among the fair skin. Skin cancer is found to be 2types Malignant Melanoma and Non-melanoma as shown in Fig1.1. Malignant Melanoma is one of the deadly.

and dangerous type cancers, even though it's found that only 4%of the population is affected with this, it holds for 75% of the death caused due to skin cancer. Melanoma can be cured if it identified or diagnosed in early stages and the treatment can be provided early, but if melanoma is identified in the last stages, it is possible that Melanoma can spread across deeper in to skin and also can affect to the parts of the body, then it becomes very difficult to treat. Melanoma is caused due to presence of Melanocytes which are present within the body.

Exposure of skin to UV radiation is also one of the major reasons for the cause of Melanoma. Dermoscopy is a technique, that is used to exam the structure of skin. An observation-based detection technique can be used to detect Melanoma using Dermoscopy images. The accuracy of the dermoscopy depends on the training of the dermatologist. The accuracy of Melanoma Detection can be 75%-85% even though the experts in skin use dermoscopy as a method for diagnosis. The diagnosis that is performed by the system will help to increase the speed and accuracy of the diagnosis. Computer will be able to extract some information, like asymmetry, color variation, texture features, these minute parameters may not be recognized by the human naked eyes. There are 3 stages in an automated dermoscopy image analysis system ,(a) pre-processing (b) Proper Segmentation, (c) feature extraction and selection. These gmentation is the most important and also plays a key role as it affects the process of fore coming steps. Supervised segmentation seems to be easy to implement by considering the parameters like shapes, sizes, and colors along with skin types and textures. This system-based analysis will reduce the diagnosing time and increases the accuracy. Dermatological Diseases, due to their high complexity, variety and scarce expertise is one of the most difficult terrains for quick, easy and accurate diagnosis especially in developing and under-developed countries with low healthcare budget. Also, it's a common knowledge that the early detection in cases on many diseases reduces the chances of serious outcomes. The recent environmental factors have just act edascatalyst for theses kin diseases [3].

II. LITERATURE REVIEW:

Fatima, et al. introduced a Multi-Parameter

Extraction and Classification System (MPECS) to aid an early detection skin cancer melanoma. The system is based on the extraction of 21 feature from the detected image using six phase transformation based tree structure model for evaluation and the classification of skin lesion images into melanoma and dysplastic nevus. The proposed tree structure model will utilize the semantic representation of the extracted spatial frequency information contained in the skin lesion images including textural information.

Doukas, et al. developed a smart phone based system to perform a self-assessment of theimages.Thesystemusesamobileapplicationtoac quireandidentifythemolesinskin images and approaches. After the extraction of these features, a statistical analysis is performed.

Patwardhan,etal. Provided a method which is based on the use of wavelet

classify them as melanoma, nevus and benign lesions based on their brutality. The system implemented using 11 classifiers and the experimental result shows that the Support Vector Machine (SVM) has the highest accuracy of 77.06%, then the Multilayer Perceptron of 75.15%. Semi-automatic or fully automatic border detection methods. The features to perform skin lesion segmentation used in various papers are shape, color, texture, and luminance. Many border detection methods are reported in the literature.

III PROPOSED METHOD:

Proposed an image processing-based system to detect, extract and classify the lesion from the dermoscopy images, the system will help significantly in the diagnosis of melanoma skin cancer. More specifically, we proposed a new method to extract the lesion regions from digital dermoscopy images which will be discussed in the next section, where block diagram is shown in

Fig 1.2

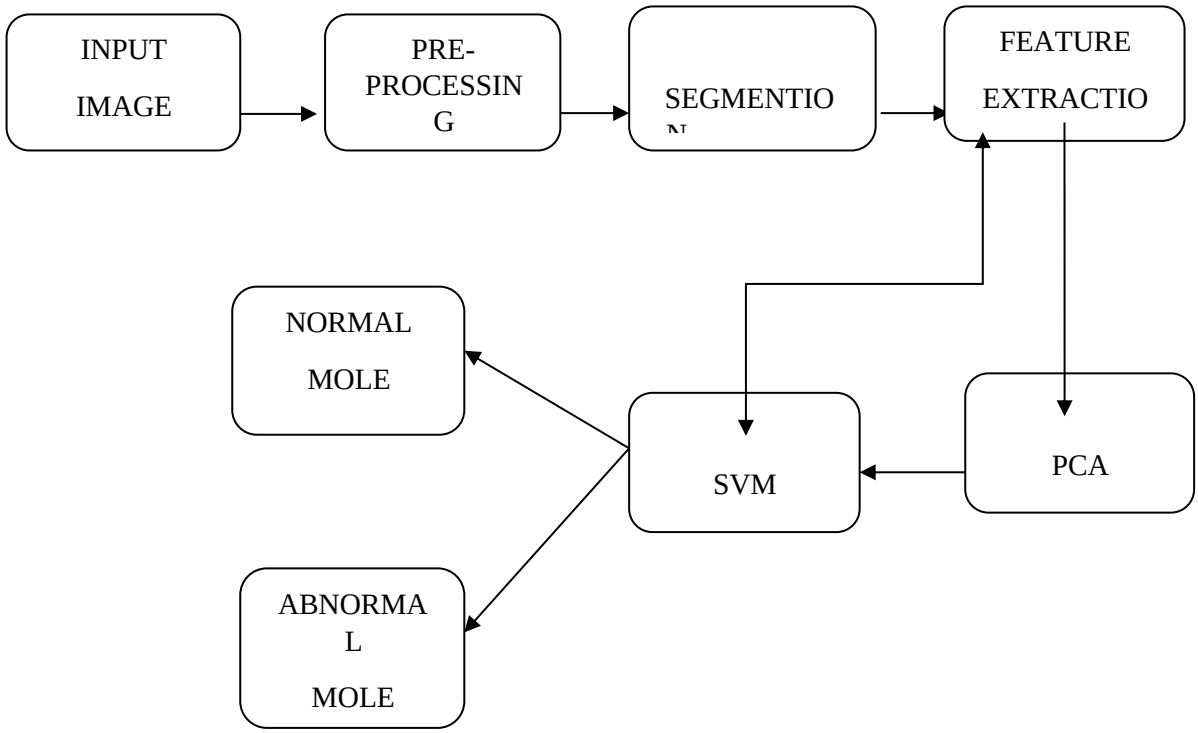


Fig: 1.2 Block Diagram of proposed skin cancer detection

ISBN: 978-93-91303-04-04

The images were collected from the ISIC dataset; the ISIC dataset provide the collection of images for melanoma skin cancer. ISIC melanoma project was undertaken to reduce the increasing deaths related to melanoma and efficiency of melanoma early detection. This ISIC dataset contains approximately 23,000 images of which we have collected 30-40 images and trained and tested over these images [7].

This step includes Converting the RGB acquired skin image to gray image, Contrast enhancement, Histogram modification and
, Noise Filtering. Contrast enhancement and histogram modification are proposed since some of the acquired images are not homogenous due to incorrect illumination during the image acquisition. While the histogram modification techniques such histogram equalization isused to enhance the contrast of the image and, therefore, making the segmentation more accurate. Noise filtering using median filter is implemented to reduce the impact of hair cover on the skin.
Contrast enhancement is a process that makes the image features stand out more clearly by making optimal use of the colors available on the display or output device. Contrast manipulations involve changing the range of values in an image in order to increase contrast. Contrast enhancement of color images is typically done by converting the image to a color space that has image luminosity as one of its components, such as the L*a*b* color space.
The histogram of an image normally refers to a histogram of the pixel intensity values as shown in Fig4.3. This histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. Image processing technique that adjusts the contrast of an image by using its histogram. To enhance the image's contrast, it spreads out the most frequent pixel intensity values or stretches out the intensity range of the image.

Thesecondstageafterpreprocessingisdetectingand segmentingtheregionofinterest (ROI) which represents the lesion region. The segmentation stage includes steps: Image thresholding, image filling, image opening, converting extracted region to gray level, and then performing histogram equalization to the extracted gray level image.
We use the Otsu thresholding method since the ROI is homogenous and, therefore, the thresholding becomes dynamic depending on the histogram of the enhanced image. After that, image filling is applied to remove background pixels from inside the detected object and, therefore, make the ROI clear. Image opening is used to remove the extra background pixels which represent a part of non-ROI and, also, to smooth the contour of the object’s boundary and breaks narrow isthmuses and eliminates thin protrusions. Finally, the extracted region is cropped then converted to a gray level image and the histogram image is calculated

IV CONCLUSIONS:

In this paper an effective detection of skin cancer cells is proposed. Skin cancer is the most common type of cancer, which affects the life of millions of people every year. About three million people are diagnosed with the disease every year. Cancer detection from skin images is an important task for disease diagnosis and cancer treatment planning. Existing tissue counter analysis method have 11 feature and less accuracy 77.06%.To avoid these limitations, GLCM algorithm with the SVM classification method is proposed for detecting skin cancer class labels in skin cancer dermatoscopic images. To identify the type of skin cancer the steps involved in this study are collecting dermoscopy image database, preprocessing, segmentation using thresholding, statistical feature extraction using Gray Level Co-occurrence Matrix (GLCM), Asymmetry, Border, Color, Diameter, (ABCD) etc., feature selection using Principal component analysis (PCA), calculating total Dermoscopy Score and then classification using Support Vector Machine (SVM).Four features are chosen that are trained tested by using various classification techniques like Support vector machine (SVM) have been done. These detected class labels are compared with original labels for performing the evaluation. The methodology actually has a good result with accuracy of 92.1%.

ISBN: 978-93-91303-04-04

REFERENCES:

[1] SkinCancerFundation.Skincancerinformation ,2016.[Online; accessedon2016/08/20,availableat*http://www.skincancer.org/skin-cancer-information*].

[2] American Skin Cancer Association (2010). Skin Cancer Primer" a comprehensive introduction to Skin cancers (9th edition Ed.) Available:

[3] J.A. Jaleel, S. Salim, and R.B. Ashwin, "Computer aided detection of skin cancer", In: Proc. of the 2013 International Conference on Circuits, Power and Computing Technologies, pp.1137-1142, 2013.

[4] P.B.Nikam and V.D.Shinde, "Skin Image Classification and Detection Using Distance Classifier Method in Image Processing," International Journal of Engineering Research & Technology (IJERT) vol. 2, 2013.

[5] AndrzejMaterka and Michal Strzelecki, ""Texture Analysis Methods – A Review",

[6] Technical University of Lodz, InstiB11 report, Brussels 1998.

[7] A. Breslow, Thickness, cross-sectional area and depth of invasion in the prognosis of cutaneous melanoma, Ann. Surg. 172 (1970), 902–908.

[8] M. Guillaud, A. Doudkine, D. Garner, C. MacAulay and B. Palcic, Malignancy associated changes in cervical smears: systematic changes in cytometric features with the grade of dysplasia, Analyt. Cell. Pathol. 9 (1995), 191–204.

[9] J. Smolle, A. Okcu, W.R. Hofmann, E. Pfaffenthaler, P.R. Fink, E. Richtig and H. Kerl, Automated measurement of melanoma cross-sectional area, Am. J. Dermatopathol. 20 (1998), 155– 159.

[10] S. a. E. N. Sharma, "Skin Cancer Detection and Segmentation Using Artificial Neural Network Techniques," International Journal of Engineering Sciences & Research Technology, August 2014.

[11] KwaitIncp, "Intranational Skin Cancer Collaboration: Melonoma Project"; https://isic-archive.com/#images 2016.

[12] SkinVisionBV,"Skin Cancer Picture", https://skinvision.com/moleimages/normal, 2016.

ISBN: 978-93-91303-04-04

COLLEGE CAMPUS GRIEVANCE MANAGEMENT SYSTEM

Y. Venkata Ramesh[1]B. Yasaswini Sai Akhila[2]K. Sushma[3]G. Sai Kumari[4]SK. Chandini[5]
Asistant Professor[1], UG Scholars[2,3,4,]
[1,2,3,4,5]Department of Computer Science and Engineering
Geethanjali Institute of Science and Technology, Gangavaram(V),kovur(M), SPSR Nellore (Dt), Andra Pradesh.

ABSTRACT-College Campus Grievance Management System is used to deal with all types of grievances from students and faculty. This app provides helping hand to student & staff by acknowledging & solving their problems such that they can share their inconvenience with the institute. It maintains the healthy environment between the Stakeholders of the institute and ensure a student friendly & democratic environment in Campus. Existing Solutions for this Problem is handwritten documents and Web application. The disadvantages of this handwritten documents are being misplaced, access time, lack of Security and in web application efficiency depends on performance, availability, Browser support. Our app will overcome all this disadvantages. The system protects the complainant's identity and at the same time allows the authority to verify the authenticity of the complaint. Students registered to our app can raise a complaint and the people who are responsible will solve it and student can track the status of the complaint which makes a better relation between student and institution.

Keywords: Grievance, Complainant

I. INTRODUCTION

Grievance is any discomfort or feeling of injustice in connection with one's situation that is brought to the notice of the management. Here grievance is related to the discomfort of the students and faculty in an educational institution. The problems of the students and faculty are solved by raising their complaint after registering successfully in the application.

II. LITERATURE SURVEY

S.Chander, A.Kush[1] in assessing grievance redressing mechanism in India measured the performance of four Indian states in grievance redressal process by providing online services through various portals, In the study the importance of complaints and their handling mechanism is highlighted to combat corruption in the bureaucracy.

Dipankar Maitra, A.Pandey[2] Solution towards Effective Complaint Registration System in Indian Scenario The fear from disclosure of identity of people when they want to complaint and difficulty of authorities in establishing authenticity of the complaint registered .The solution is, complaint registration should be such that it protects complainant's identity and at the same time allows the authority to verify the authenticity of the complaint.

Varun Gauri[3] in his study analyzed that the redress procedures help address accountability problems in the implementation of social policies and provide information to policy makers regarding policy design. Procedures for redressing grievances and complaints regarding basic service delivery are under-developed in many countries, and deserved further analysis, piloting and support.

Rajesh Yadav, SarveshMohania [4] their study focuses on the grievance management in life insurance services by the ombudsman in India. By collecting the secondary data from IRDA and research papers from various journals the study concluded that in grievance management role of insurance ombudsman is important and constant increase in number of complaints received by various Ombudsman across the India shows that the policy holders are gaining their confidence and trust in the institution of Insurance Ombudsman.

Nripendra P. Rana,Yogesh Kumar Dwivedi [5] in their study validated the integrated IS success model is used to examine the success of the online public grievance redressal system (OPGRS)by measuring intention to use and user satisfaction from the perspective of the citizens in India.

ISBN: 978-93-91303-04-04

III. EXITING SYSTEM

College campus grievance is managed through web application where the students can post their complaints under different categories. The complaints posted are accessed by the redressal committee. The student registers with this website by mentioning the essential details and login with registered number and password to access the facilitiesshould login to post complaints and it will be secured in the database and complaints will be viewed by the redressal Committee and will beforwarded to the institute or department based on the problems. Another existing system is handwritten documents in which the user post complaints in the form of hard copies. The main disadvantages of these handwritten documents are less security, loss of data, sending complaints to the respective grievance heads is difficult.

V. PROPOSED SYSTEM

The proposed system is "College Campus Grievance Management System" which is an android application. This application is customized to deal with all types of grievances regarding college management, hostel, canteen, departmental issues from students and faculty. The user registered to this app can raise a complaint at all times from anywhere through a mobile. The respective heads will solve it and the user can track the status of the complaint. The system protects the complainant's identity and at the same time allows the authority to verify the authenticity of the complainant.

The student or faculty who wants to raise a complaint should register with the app first. After successful registration, the admin will approve the user to login by validating the user. After user logging in can give complaints, based on the category, the complaint will be sent to respective grievance heads. Grievance heads will try to solve the complaints and update status and comments, which can be seen by the user.

ARCHITECTURE

There are three types of modules in this system:

1. Admin Module:

Admin has privileges to Authenticate and approve users. He can access the complete database.He can view all grievances and track their status.

2. Complainant Module

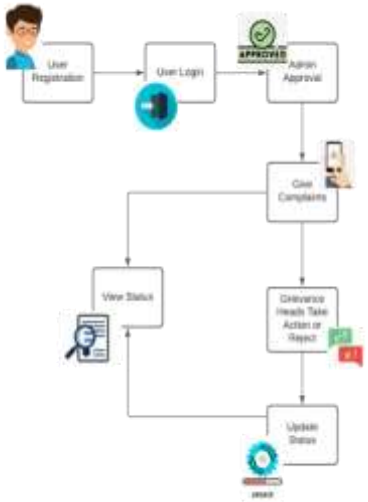
Complainants are of 2 types:

- Students
- Faculty

In this module, students and faculty can upload their grievances without revealing their identity. A complainer can also track their status of the grievance.

3. Grievance Module

Grievance heads will act regarding the complaints and try to solve the problems. They will also update the status of the complaints whether it can be solved or not.



VI. USER INTERFACE

Fig 1: Login Screen

Fig 2: Register Screen

3: Admin Screen

Fig 4: Dashboard

VII. CONCLUSION

By Using this app user can successfully post a complaint to respective heads at all time and from anywhere. User can easily track the status regarding the complaint whether solved or not and the reasons behind that. User can fearlessly post a complaint without having a doubt of revealing the identity to the grievance heads. Ultimately, we conclude that our app is user friendly and it is the solution for the drawbacks of existing systems.

VIII.REFERENCES

[1]Subhash, C., Ashwani K.: Assessing grievances redressing mechanism in India. Int. J. Comput. Appl. 52(5), 12–19 (2012). [2]Dipankar, M.: Solution towards effective complaint registration system in Indian scenario. In: IJCA Proceedings on National Conference on Advancement of Technologies—Information Systems & Computer Networks (ISCON—2012), vol. 1, pp. 1–2 (2012).

[3]Varun, G.: Redressing grievances and complaints regarding basic service delivery. World Dev. 41, 109–119 (2013).

[4] Nripendra, P.R., Yogesh, K.D., Michael, D.W., Vishanth, W.: Investigating success of an e-government initiative: validation of an integrated IS success model. Inf. Syst. Front. 17(1), 127–142 (2015).

[5] Rajesh, K.Y., Sarvesh, M.: Role of insurance ombudsman and grievance management in life insurance services in Indian perspective. Int. Lett. Soc. Humanist. Sci. 31,9–13 (2014).

ISBN: 978-93-91303-04-04

SECURE ACCESS MECHANISM FOR CLOUD SERVICES USING BIOMETRIC BASED AUTHENTICATION

Y.V.Ramesh[1] D. Sreeja[2]G. Ruchitha[3]G. Lasya sree[4]K . Sri Vaishnavi[5]
Assistant Professor[1], UG Scholar[2, 3, 4, 5]
[1, 2, 3, 4] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

ABSTRACT

The demand for remote data storage and computation service is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services. In this project, we design a new biometric-based authentication protocol to provide secure access to a remote (cloud) server. In the proposed approach, we consider biometric data of a user as a secret credential. We then derive a unique identity from the user's biometric data, which is further used to generate the user's private key. In addition, we propose an efficient approach to generate a session key between two communicating parties using two biometric templates for a secure message transmission.

KEYWORDS

Biometric templates , Wireless sensor networks, Authentication scheme, Node anonymity, Falsification, Token-based security system, Kerberos network authentication service.

I. Introduction

Cloud services are a norm in our society. However, providing secure access to cloud services is not a trivial task, and designing robust authentication, authorization and accounting for access is an ongoing challenge, both operationally and research-wise. A number of authentication mechanisms have been proposed. based on the underlying assumption that the remote server responsible for authentication is a trusted entity in the network. Specifically, a user first registers

with a remote server. This is needed to ensure the authorization of the owner.

II. Literature survey

To In this section, we mainly discuss existing the biometric-based user authentication schemes that have been presented in the literature. Based on the authentication types and factors being used, the user authentication protocols can be classified into three categories:

1) single-factor

2) two-factor

3)three-factor.

In a single-factor authentication protocol, only one factor can be used (for example, user's smart card/mobile device or password or personal biometrics). In a two-factor authentication scheme, the user's smart card or mobile device and password can be used. On the other hand, in a three-factor authentication scheme, the user's smart card/mobile device, password and biometrics can be used.Jiang et al. designed a password based user authentication scheme for wireless sensor networks (WSNs). This is atwo-factor authentication scheme as it relies on both a smartcard and some password. During the user registration process,an authorized user registers or re-registers with the trusted gateway node . The GWN then issues a smart cardhaving the relevant credentials that are stored on the smart card. In addition, all the deployed sensor nodes are registered through a secure channel with the GWN and obtain their respective secret credentials. Using the pre-loaded credentials, a legitimate user authenticates with a designated sensor node with the help of the GW N during the login and authentication phases. However, Das later showed that this particular scheme is vulnerable to privileged insider attacks, where an internal user of the trusted authority (i.e., an insider attacker) having the registration information of a registered user can mount other attacks in the system, such as user impersonation attacks. Moreover, it was also shown that this

scheme does not provide proper authentication, and fails to support new sensor node deployment in a target field. As a countermeasure, Das presented an improved and efficient three factor authentication scheme, where the three factors are a smart card, the user's password and the user's personal biometrics. However, the scheme proposed by Das does not preserve sensor node anonymity

III. Proposed system

In this section, we first discuss about the system model and threat model used in the system proposed is biometric-based authentication protocol (BioCAP), prior to presenting the various phases in BioCAP.

A. System Model

An overview of BioCAP which comprises three entities. These entities are client(s) (C), authentication server(s) (AS) and some resource server (RS). AS contains a database of users' registered data, while AS generates RS's private key during the deployment phase and it is shared between AS and RS. In addition, both AS and RS include a large repository of a similar set of synthetic fingerprint images. Some synthetic fingerprint databases, such as some publicly available databases, are used in the proposed approach.

B.Thread Model

We follow the broadly-accepted "Dolev-Yao (DY) threat model" in this paper. The DY model permits an adversary, say A not only to intercept the messages during communication, but also allows to modify, delete or even inject false messages during communication among the network entities. Thus, under the DY model, the communication among the network entities happens over a public channel. We further assume that the clients are not trusted in the network, whereas the authentication servers (AS) and resource server (RS) are semi-trusted entities in the network. In the password-based authentication mechanism, password guessing attack is feasible if low-entropy passwords are used. On the other hand, in the biometric-based authentication mechanism biometric data guessing attack using brute-force attacks is computationally infeasible. However, A can perform other potential attacks, such as replay, man-in-the-middle, privileged-insider, denialof-service and biometric data guessing attacks, and also stolen smart card and password guessing attacks (for password based authentication schemes).

C. User's Private Key Generation

From a captured user's fingerprint image, we extract all minutiae points. In order to increase the accuracy in feature extraction, we first align the fingerprint image. From this aligned fingerprint image, we select the consistent region. The consistent region can be defined as the fingerprint region, which has a high chance of appearance in any captured fingerprint image. We select this consistent region to extract the minutiae points. To select a set of minutiae points from the consistent region, we propose to use a horizontal segment. Horizontal segment is a small area of the consistent region, which has the highest number of minutiae points. We select these minutiae points to generate a Trellis diagram of the convolution coding and finally, a codeword from it. The details process of codeword generation is discussed.

D. Session Key Generation

To generate a session key between two principles P1 (say, client C) and P2 (say, authentication server AS), we take two different biometric fingerprint data. P1 takes C's fingerprint image and P2 takes a synthetic fingerprint image. The session key generation process is denoted as process. This process starts execution as soon as P1 loads its application to begin a session

E. Message Authenticator Generation

In BioCAP, AS initiates an authenticator after the completion. To generate an authenticator, AS randomly selects one minutiae point from the fingerprint I2. Let the randomly selected minutiae point be Pr(x, y), r is a random number, $1 \leq r \leq n$, n is the number of minutiae points of the fingerprint I2. Let Bv be the authenticator, that is, $Bv = (x * r1)(y*r2)$. AS then encrypts Bv using the session key K. Let the encrypted form of the

ISBN: 978-93-91303-04-04

authenticator. AS sends Bv as the biometric-based authenticator. The recipient encrypts Bv using the session key K. Let the encrypted form of Bv .Recipient then compares B. If there is a match, then the recipient believes that the message is from the genuine sender.

F. User Registration

Prior to the registration process, BioCAP executes process and both C and AS possess their current session key say K. C does the following. Block-based feature extraction: C's application captures a new fingerprint image (say Ireg) of C. We extract minutiae points from Ireg and make minutiae pairs. In order to generate a pair of minutiae points, we first divide into a number of small square blocks. We traverse each block in make the pairs of minutiae points by considering each minutiae point belongs to each block to all the minutiae points belong to its surrounding eight connected blocks. This way, we traverse all the blocks and make pairs of minutiae points. We calculate the Euclidean distances and angles of all the straight lines so obtained .

G. User Authentication

A user's authentication process begins with the session key generation with PreCalcu process. Let, the session key between C and AS at this time be K. The user authentication process is carried out in two phases. In the first phase, C fetches the secret from the database of AS. In the second phase, C uses the fetched secret to send his biometric feature to AS for verification purpose.

The GWN then issues a smart card having the relevant credentials that are stored on the smart card. In addition, all the deployed sensor nodes are registered through a secure channel. A legitimate user authenticates with adesignated sensor node with the help of the GW N during login and authentication phases. The internal authority having the registration information of a registered user can mount other attacks in the system, such as user impersonation attacks.

IV. Results

No	Test case	Input	Expected output	Observed output	Result
1	Log in	Enter Wrong User Name and Password	Invalid login details	User name and Password are invalid	Pass
2	Log in	Enter User Name and Password	Login successful	Login successful	Pass
3	Mobile number	Enter alphanumeric characters	Mobile number must be digits only	Mobile number in 10 digits only	Fail
4	Upload file	Browse file	File uploaded successfully	File upload successful	Pass

V. Conclusion

Biometric has its unique advantages over conventional password and token-based security system, as evidenced by its increased adoption (e.g., on Android and iOS devices). In this paper, we introduced a biometric-based mechanism to authenticate a user seeking to access services and computational resources from a remote location. Our proposed approach allows one to generate a private key from a fingerprint biometric reveals, as it is possible to generate the same key from a fingerprint of a user with 95.12% accuracy.

VI. References

[1] C. Neumann, S. Hartman, K. Raeburn, "The kerberos network authentication service (v5)," RFC 4120, 2005.
[2] "OAuth Protocol." [Online]. Available: http://www.oauth.net/
[3] "OpenID Protocol." [Online]. Available: http://openid.net/

ISBN: 978-93-91303-04-04

[4] G.Wettstein, J.Grosen, and E.Rodriguez, "IDFusion: An open architecture for Kerberos based authorization," Proc. AFS and Kerberos Best Practices Workshop, June 2006.
[5] Kehne, J. Schonwalder, and H. Langendorfer,
[6] "A nonce-based protocol for multiple authentications," ACM SIGOPS Operating System Review, vol. 26, no. 4, pp. 84–89,

A Comparative Study of Supervised Machine LearningAlgorithms for Credit Card Fraud Detection

Dr. V. Sireesha[1] A. Sri Bhargavi [2] K. Manasalakshmi [3] N. Usha Rani [4] G. Nirupa [5]

Professor and Head of the Department (HOD)[1], UG Scholar[2, 3, 4,5]

[1, 2, 3, 4,5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore,Andhra Pradesh.

ABSTRACT:

Credit card use has become extremely common or offline mode. But with the remarkable increase in number of users, credit card frauds in our day-to-day life. They have revolutionized the wayf creating cashless payments and made making any kind of payments convenient for the customer. Along with the remarkable increase in number of users, credit card frauds have also been crept into the phenomenon. The credit card information of a particular individual can be stolen illegally and can be used for fraudulent transactions. In this paper, a specimen of the publicly available dataset has been collected from a website called Kaggle. As the dataset is found highly Imbalanced, SMOTE (Synthetic Minority Oversampling Technique) is used to make it balanced. About 2,84,807 records of transactions made by the credit card holders are considered and run through Logistic Regression, K- Nearest Neighbour, Naive Bayes, Decision Tree, Random Forest and a comparison is done among them to find the best approach to detect these fraudulent transactions. Random forest is found to be the best approach to detect the credit card frauds as it got the highest AUC value i.e., about 97.11% on thorough examination.

Keywords:

Credit card, credit card Fraud, Machine Learning, supervised machine learning, imbalanced dataset, SMOTE. Introduction

Credit card is a small piece of plastic cardissued by financial institutions. It gives customers a pre-set credit limit with which he/she can make cashless payments [1]. Nowadays, the usage of these cards has becomecommon. With the help of these card transactions can be done either in online modehave also been crept into the phenomenon. The credit card information of a particularindividual can be stolen illegally and can be used for fraudulent transactions. A fraudulent transaction is an unauthorised transaction carried out with one's credit card. This is a very relevant problem that demands the attention of communities such as machine learning and data science where the solution can be automated. Millions of transactions takeplace in milli or micro seconds.so it is very difficult to differentiate between legitimate and fraudulent transactions with poor models, hencean efficient model should be used. the existing approaches supervised and unsupervised and combination of both supervised and unsupervised as a hybrid model can be used fordetecting these fraudulent transactions [4].

In this paper, a specimen of the publicly available dataset has been collected from a website called Kaggle. As the dataset is found highly Imbalanced, SMOTE (Synthetic Minority Oversampling Technique) is used to make it balanced. About 2,84,807 records of transactions made by the credit card holders are

onsidered from Kaggle and run throughLogistic Regression, K-Nearest

Neighbour,Naive Bayes, Decision Tree, Random Forest and a comparison is done among them to find the best approach to detect these fraudulent transactions.[3]

1.Literature survey

Credit card frauds can be detected by using various machine learning algorithms like supervised or unsupervised. Sometimes we can also use the hybrid models for detecting these credit card frauds. Hybrid models provides you accurate more accurate result as they encapturethe capabilities of both supervised and unsupervised [9].

ISBN: 978-93-91303-04-04

It is observed that the dataset, used for analysing these frauds are highly imbalanced. Ifwe apply the algorithms on this imbalanced data then it won't produce the accurate results. Hence, we are converting this imbalanced dataset into balanced dataset by using SMOTEoversampling technique [7]. This technique may significantly improve the functioning of certain models as they work on a more Balanced dataset.[9]

2.Machine Learning

Machine learning has proved itself its potentialby providing various solutions to our problems in day-to-day life. It basically provides the system with the "ability to learn". It is able to use previously procured data and analyze it

frauds.

Step-1: Collect the imbalanced dataset:

The dataset required for this paper is collected from a website called Kaggle. The dataset contains about 2,84,807 records of transactions made by the European credit card holders. Among them 492 records of transactions are fraudulent and remaining are legitimate transactions. The dataset is imbalanced dataset [10].

Step-2: Pre-processing of data and feature selection.

In this we will check whether there are any outliers (or) missing values in the dataset are not. Once pre-processing is done, then extract the features from the dataset. About 30 featuresare available from our dataset. Step-3: convert imbalanced dataset to balanced dataset.

As we discussed earlier that the dataset is imbalanced so when we use this dataset, we cannot predict the frauds easily hence we are converting the imbalanced dataset into balanced dataset. This conversion can be done either by using oversampling or under samplingtechnique. Here we are using SMOTE (Synthetic Minority Oversampling Technique) as the fraudulent transactions are very less.

Step-4: Generating the training data from the dataset.

In this phase we are generating the training data from the dataset just by splitting the dataset into training dataset and testing dataset as per the user interest split ratio. Here we have splitedthe dataset in the ratio 90:10 (90% -training dataset, 10% -testing dataset). Step-5: Train the algorithm using the training data

In this phase we actually use the training datasetfor training the algorithm which are using. In this paper we are using 5 supervised machine learning algorithms.

1. **Logistic regression**:

Logistic regression is a statistical model that itin its basic form uses logistic function to model a binary dependent variable. [12]

The logit function is the algorithm of the odds ratio. It takes the input in the range of [0,1]and transform them to values over real number range.

The logit function can be defined as

$$\text{Logit}(p)=\log\left(\frac{p}{1-p}\right)$$

But to define this logit function we need odds ratio.

Odds ratio= p /1-p where p =probability of positiveevent.

Sigmoid function gives you the effective results.

$$\emptyset(z) = \frac{1}{1-e^{-z}}$$

2. **K-Nearest Neighbor (KNN)**

KNN is the simplest algorithm which is also known as "Lazy learning Model".it defines the similarities between the actual data and thenewly available data.

The pseudocode for the KNN is:
1.select the number k neighbor.
2. calculate the Euclidean distance of k-neighbor and we will consider the smallest distance as k.

ISBN: 978-93-91303-04-04

3. take the k-nearest neighbor, as per calculated

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

Euclidean distance.

4. Among these k-neighbor, count the number of data points in each category.

5. Assign the new datapoint to that category for which the neighbor is maximum.[11]

3. Naïve Bayes Classifier.

Naïve bayes classifier is a supervised machine learning model where the decision depends on Bayes theorem. It is also called as probabilistic algorithm. For example: if we consider an object then depending upon its probability classification is done. Here we are using gaussian the classifier which is a normal distribution. Here predictors take the valuescontinuously but actually it has to take discretevalue.[7]

4. Decision Tree

Decision tree may be a tree like structure during which each internal node represents a "test" onan attribute. Where each branch represents the outcome of the test and each leaf node represents a class label. The path from roots to leaf represents classification rules [6].

5. Random Forest

It is basically an ensemble classifier that uses multiple decision trees so that dependence of each of them is on a particular dataset similar distribution throughout the tree. After

generating the multiple decision tree, the outputis derived by majority [5].

12. 5. Evaluation metrics

The performance of above-mentionedalgorithms is done with the help of recall, precision and AUC.

1. Recall/(sensitivity)

It is the amount of correct positive results divided by amount of all relevant samples (all samples should have been identified as positive).

$$\text{Recall} = \frac{True\ Positive}{True\ Positive + False\ Negative}$$

2. Precision

It is the amount of correct positive results divided by the amount of positive results predicted by the classifier**.**

3. Area under the roc curve(AUC)

The Area Under the Curve (AUC) is the measure of the ability of a classifier to distinguish between classes and is used as a summary of the ROC (Receiver Operating Characteristic curve).The higher theAUC,the better the performance of the model at distinguishing between the positive and negative classes.

Performance Evaluation

The performance evaluation for the algorithms used, is done based on recall(sensitivity), precision and AUC.

Let us discuss the performance evaluation of each algorithm used in this paper using the above metrics. Here Accuracy is the parameterwhich is not considered for finding the best approach.

For Logistic Regression

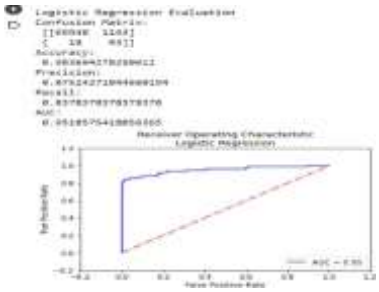


Figure-2 Performance evaluation for logistic regression

- **For K-Nearest Neighbor**

Figure-3 Performance evaluation for KNN

- **For Naïve Bayes**

Figure-4 Performance evaluation for Naïve Bayes

- **For Decision Tree**

ISBN: 978-93-91303-04-04

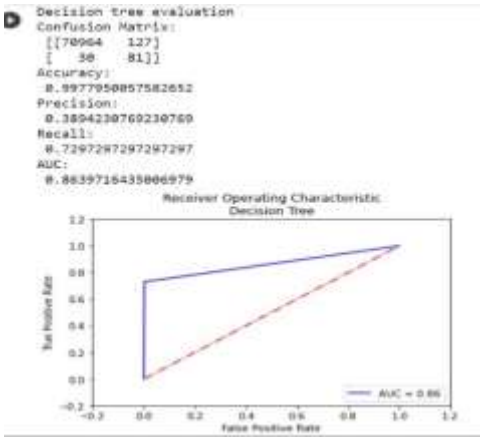


Figure-5 Performance evaluation for Decision tree

- **For Random Forest**

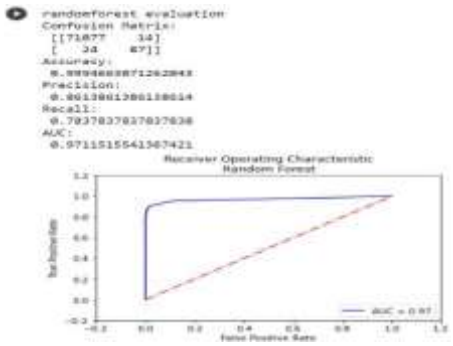


Figure-6 Performance evaluation for Random Forest

The below table-1 discusses the performance of algorithms used in this study for detecting the frauds using the above-mentioned evaluation metrics.

	Logistic regression	KNN	Naive bayes	Decision tree	Random forest
Accuracy	98.36	94.62	99.24	99.77	99.94
Precision	75.24	12.32	13.33	38.94	86.13
Recall	83.78	42.34	70.27	72.97	78.37
AUC	95.18	70.13	95.58	86.39	97.11

Table - 1: Comparison of various evaluation metrics for the algorithms used

7. Conclusion

After the comparative analysis of the supervised Machine Learning Models, we can infer that the Random Forest Model is the best approach to be used for detecting credit card

frauds. Among all the supervised machine learning algorithms used, Random Forest has highest AUC value i.e., about 97.11%. Hence, we conclude that the random forest is an efficient model among all the algorithms used. But we have not achieved 100%efficiency hence to improve the performance of the modelwe can use unsupervised machine learning algorithms along with this model.

8. REFERENCES

[1] International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016 Copyright to IJARCCE DOI 10.17148/IJARCCE.2016.510939 Credit Card Fraud Detection Ishu Trivedi1 , Monika2 , Mrigya Mridushi3 Student, Dept. of Computer Science and Engineering, Sikkim Manipal Institute of Technology, Rangpo, India1, 2, 3

[2] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, “Data mining for credit card fraud: A comparative study,” Decis. Support Syst., vol. 50, no. 3, pp. 602-613, 2011.

[3] S P Maniraj ,Aditya Saini, Swarna Deep Sarkar ,Shadab Ahmed, “Credit Card Fraud Detection using Machine Learning and Data Science”,International Journal Of Engineering Research &Technology(IJERT),ISSN-2278-0181,VOL-8,Issue 09,September 2019.

[4] K. Chaudhary, J. Yadav, and B. Mallick, “A review of Fraud Detection Techniques: Credit Card,” Int. J. Comput. Appl., vol. 45, no. 1, pp. 975-8887, 2012.

[5] Vaishnave Jonnalagadda, Priya Gupta, Eesita Sen, “Credit card fraud detection using Random Forest Algorithm”,2019 International Journal Of Advance Research, Ideas and Innovations in Technology.

[6] Han, J.,& Camber, M. (2000). Data Mining Concepts and Techniques. San Diego, USA: Morgan Kaufman.

[7] J. O. Awoyemi, A. O. Adetunmbi and S. A. Oluwadare, ’’Credit card fraud detection using machine learning techniques: A comparative analysis,” 2017 International Conference on

Compu
[8] ting Networking and Informatics (ICCNI), Lagos, 2017, pp. 1-9
[9] Abdallah, Aisha, Moht Aizaini Maaros, and Anazida Zainan. “Fraud Detection System: A Survey.” Journal Of Network and Computer Applications 68(2016): 90-113.
[10] S. Mittal and S. Tyagi, "Performance Evaluation of Machine Learning Algorithms for Credit Card Fraud Detection", 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2019.
[11] Thadtah, Fadi, et al. “Data imbalanced in classification: Experimental evaluation.” Information Sciences 513(2020): 429-441.
[12] RahulPowar, Rohan Dawakhar, Pratichi,” Credit Card fraud Detection Using Machine learning”, International Journal Of Advanced Scientific Research And Engineering Trends., vol5,issue9,September 2020.
[13] Hala Z Alenzi, Nojood O Aljehane,”Fraud detection in Credit Cards using Logistic Regression”,International Journal of Advanced Computer science and applications(IJACSA),vol 11,No.12,2020.

Searching By Syntactic Schemes on Protected Data Using Effective Matching Technique

Dr.V. Sireesha[1] Md. Shahabaz[2] Sk. Juneed[3] P. Sai Krishna[4] Head Of Department, M.E, Ph.D.
Department of CSE, Geethanjali Institute of Science and Technology, Nellore, A.P

Abstract:

The demand for data security is crucial. One such a path of storing data in a virtualized manner is Cloud Computing. Cloud computing is defined as the way of storing data over virtualization concept. Cloud computing offers the Data owners to store, retrieve and update their data whenever necessary. To be more accurate, the data owner could go for private cloud. But, due to the possibility of restricting the accessing and locking up of data, it is slightly problematic to store in private cloud. This paper, provides an effective method of providing security to data owner, on a public cloud, by using syntactic schemes of Effective Matching Technique.

Keywords- Information security, Cloud, Cloud Computing, Effective Matching, Syntactic Schemes.

INTRODUCTION

Information Security is a crucial task in today's fastening world. Information or data that is being accessed by, is being prone to cyber-attacks. Hence, there is an utmost need of providing security to data. By storing information on to the cloud, one can expect data security, but due to the fact that, storing data on a private cloud could limit the possibilities of Data accessing, updating and retrieving. Recent cases of Apple Fappening and Uber security breaches has made the highlights of security of data. Majority of the owners of

Organizations, now are in an alternative method of choosing a secure way of data transactions [1].

Abstract – Information security is defined as the process of securing data from unauthorized users. Due to the increasing number of internet users, the demand for data security is crucial. One such a path of storing data in a virtualized manner is Cloud Computing. Cloud computing is defined as the way of storing data over virtualization concept. Cloud computing offers the Data owners to store, retrieve and update their data whenever necessary. To be more accurate, the data owner could go for Cloud Computing is a method of providing resources and tools to manage whenever needed. The ideology of cloud computing refers to storage of information in a virtualized format. Due to increase in storing of data exponentially, cloud computing offers a greater aspect of elasticity, scalability and feasibility [3]. There are various cloud providers, who provide cloud services in the methods of IaaS (Infrastructure as Service), PaaS (Platform as Service) and SaaS (Software as Service), such as Amazon, Google, Alibaba, IBM etc., Majority of the cloud providers offers a mix of services, such as Amazon offers IaaS, PaaS, SaaS, whereas IBM offers a combination of Infrastructure and platform. Platform as a service provides a physical infrastructure to the Data Owner, where he is in charge of managing the remaining pool of resources. Software as a service provides the host software on the premises, whereas Infrastructure provides the on-demand services for the infrastructure.

InformationSecurity provides Confidentiality, Integrity, Privacy, Availability and Quality. These principles of Information Security give an in detail of what one can expect. According to Security magazine regarded 2020 as the worst year for security breachers, totaling 8.3billion records of data has been breached, including the data from Microsoft, Keepnet labs, BlueKai and Whisper to name some. These Data breaches has raised a concern of providing security and confidentiality

private cloud. But, due to the possibility of restricting the accessing and locking up of data, it is slightly problematic to store in private cloud. This paper, provides an effective method of providing security to data owner, on a public cloud, by using syntactic schemes of Effective Matching Technique.

Keywords- Information security, Cloud, Cloud Computing, Effective Matching, Syntactic Schemes.

INTRODUCTION

Information Security is a crucial task in today's fastening world. Information or data that is being accessed by, is being prone to cyber-attacks. Hence, there is an utmost need of providing security to data. By storing information on to the cloud, one can expect data security, but due to the fact that, storing data on a private cloud could limit the possibilities of Data accessing, updating and retrieving. Recent cases of Apple Fappening and Uber security breaches has made the highlights of security of data. Majority of the owners of

Organizations, now are in an alternative method of choosing a secure way of data transactions [1].

Cloud Computing is a method of providing resources and tools to manage whenever needed. The ideology of cloud computing refers to storage of information in a virtualized format. Due to increase in storing of data exponentially, cloud computing offers a greater aspect of elasticity, scalability and feasibility [3]. There are various cloud providers, who provide cloud services in the methods of IaaS (Infrastructure as Service), PaaS (Platform as Service) and SaaS (Software as Service), such as Amazon, Google, Alibaba, IBM etc., Majority of the cloud providers offers a mix of services, such as Amazon offers IaaS, PaaS, SaaS, whereas IBM offers a combination of Infrastructure and platform. Platform as a service provides a physical infrastructure to the Data Owner, where he is in charge of managing the remaining pool of resources. Software as a service provides the host software on the premises, whereas Infrastructure provides the on-demand services for the infrastructure.

InformationSecurity provides Confidentiality, Integrity, Privacy, Availability and Quality. These principles of Information Security give an in detail of what one can expect. According to Security magazine regarded 2020 as the worst year for security breachers, totaling 8.3billion records of data has been breached, including the data from Microsoft, Keepnet labs, BlueKai and Whisper to name some. These Data breaches has raised a concern of providing security and confidentiality of data in a cloud. To provide an authentic and

secure way of storing a data and accessing it, using Effective Matching Technique, colloquially noted as Effective Matching on the protected Data [4].

Effective Matching is a technique used in Information Security, which provides the task of outsourcing the requested documents in an Optimal preference task. Before leveraging the documents on to the cloud, the data owner, encrypts the document and outsources it onto the cloud. Data owner then forwards the indices relating to the encrypted documents to the user. End- user when in need of requesting the documents to download, sends the decryption key request and if the request is granted, then the end-user will be able to download the required document. The Cloud server has an optimizer which is used to calculate any RLP problem. By treating queries as consumers, documents as products and optimal information as product, we deliver a similar approach as of minimum word transportation cost totality (MWTCT) to calculate the distance between two words and to further leverage it for an optimal or effective matching, we propagate the the transportation of word(TW) into linear programming (LP). Ready-made optimizers are made available whenever a linear program function is being used for the purpose of optimal match. This proposed work prepares for the best of optimal matching, security and verifiability of the documents. Our new ideas are summarized as follows:

1. Behaving the matching between queries and documents as an effective matching task, we initiate the theorems of linear programming (LP) to propose a secure demonstrable syntactic searching scheme that performs semantic effective matching on the encrypted text.
2. For secure semantic effective matching on the encrypted text, we formulate the transportation of word(TW) problem and propose a secure transformation technique to transform TW problems into random linear programming (LP) problems for obtaining

the encrypted minimum word transportation cost in totality(MWTCT) as measurements between queries and documents.

3. For supporting demonstrable searching, we explore the duality theorem of LP and present a novel insight that using the intermediate data produced in the matching process as proof to verify the correctness of search results [11].

2. RELATED WORK

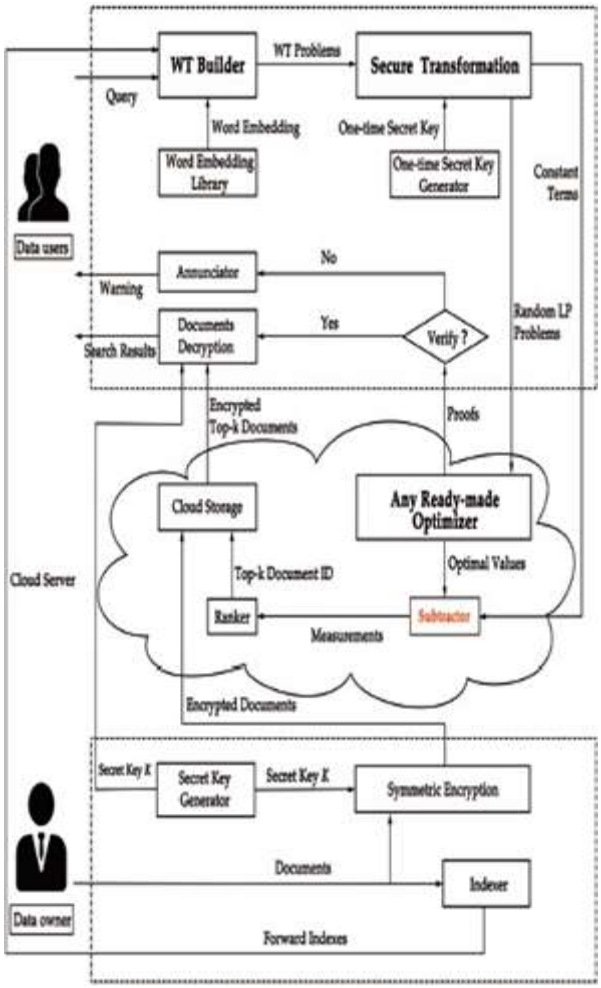
2.1 Verifiable keyword-based semantic

ISBN: 978-93-91303-04-04

search over encrypted cloud data:
With the increased demand for tier services in cloud, there has been a threat for propounding the information that is processed over the cloud. In such a case, the pragmatic way of developing a semantic searching scheme over protected data is developed, followed by initializing the preliminaries with the identifiable keywords based encryption or protection on the cloud. The great way of analyzing the usage of keyword based encryption is that great flexibility and scalability of services provided by the cloud users[4]. Although the existing schemes in the cloud computing does provide the affordability of using it at convenience, but the way of predefining the keywords accordingly with the hypothetical results are not up to the mark for correspondence. The proposed scheme does not also support correctness of the results nor it provides the verifiability of the information requested. To give the flexibility and requested agility, the proposed project does claim the enhancability of providing the verifiability and security or protection of the information. However, this paradigm of cloud computing does not provide the verifiability and protecting of data before it is leveraged on to the cloud. Hence, to tackle this, a demonstrable scheme has been proposed.

2.2Achieving effective cloud search In recent years, customer-oriented cloud computing platform has involved as the development of smart devices combined with the emerging cloud computing technologies. A diversity of cloud services are delivered to the customers with the propose that an effective and reliable cloud search service is achieved [3]. For customers, they want to find the most preferred products or information, which is highly beneficial in the "pay as you go" cloud computing platform. As sensitive information (such as photo albums, emails, personal health records, financial records, etc.) are protected before leveraging to cloud, normal keyword search techniques are useless. Meanwhile, existing search approaches over protected cloud data support only exact or fuzzy keyword search, but not syntactic-based multi- keyword ranked search [9].

2.3 Secure semantic expansion-based search over encrypted cloud data supporting similarity ranking:
With the appearance of cloud computing, an increasing number of facts statistics are outsourced to the general public cloud for financial financial savings and simplicity of access [6]. However, the privatives facts needs to be encrypted to assure the security. To put in force green statistics utilization, seek over encrypted cloud statistics has been a outstanding challenge. The present answers depended absolutely at the submitted question key-word and didn't don't forget the semantics of key-word. Thus, the quest schemes aren't smart and additionally miss a few semantically associated documents. In view of the deficiency, as an attempt, we endorse a semantic enlargement primarily based totally comparable seek answer over encrypted cloud data. Our answer should go back now no longer handiest the precisely matched documents, however additionally the documents inclusive of the phrases semantically associated with the question keyword. Then each the encrypted metadata set and record series are uploaded to the cloud server.



Again so as in step with the entire relevance score. Eventually, distinct protection evaluation suggests that our answer is privacy-maintaining and stable beneathneath the preceding searchable symmetric encryption (SSE) protection definition [7].

3.PROPOSED WORK

The proposed work is implemented in the following format:

Fig:1 implementation of proposed work

As illustrated in Fig. 1, there are three entities involved in our system: the data owner, end users, and the cloud server.

3.1 Data Owner:

To Understand the function of data owner, two algorithms are best fit:

1. Initialize ()- Probabilistic algorithm designs the initialize function initially. To initialize we use initialize ().
2. EncDoc () – is a deterministic encryption algorithm used to protect the documents before leveraging it on to the cloud.

3.2 Cloud server:

The cloud server is an intermediate service provider that stores the encrypted cloud server performs SeaPro () for leveraging any ready-made optimizer to solve the Ω, then obtains the encrypted minimal phrase transportation cost values with Δ. The cloud ranks the values in ascending order and returns the top k protected documents to users. In the process, the cloud server also provides proofs Λ for proving the truth of the search results.

3.3 End-User:

Data users are the searching requesters that send the trapdoor of a query to the cloud server for acquiring top-k related documents. Specifically, users input arbitrary query words q, then perform BuildRLP () to generate word transportation problems Ψ, after transform Ψ to random linear programming problems Ω and the corresponding constant terms Δ as a trapdoor. Afterward, users receive top k protected documents and proofs Λ returned from the cloud. Users perform VerDec () to decrypt documents when Λ passes our verification mechanism.

4. METHODOLOGY

In this section, we present the detailed design of our scheme that consists of three phases, namely, Initialization, Search & Prove, Verification &Decryption.

4.1 Initialization:

In this phase, the data owner performs Initialize () to initialize our scheme. To describe this algorithm in detail, we split it into three algorithms, as follows:

K ← KeyGen () is a probabilistic secret key generation algorithm, corresponding to the "Secret Key Generator". The data owner takes the security parameter ε as input, then generates secret key K for encrypting documents.

C ← EncDoc (K, F) is a deterministic algorithm, corresponding to the "Symmetric Encryption". The data owner takes the documents dataset F and the secret key K as input, then generates the protected dataset.

I ← Build Index(F) is a deterministic building index algorithm, corresponding to the "Indexer". The data owner takes F as input, then generates forward indexes I as semantic information of documents. The data owner first calls KeyGen () and EncDoc () to generate a secret key K for encrypting documents dataset F and get the ciphertext dataset C, then outsources C to the cloud server. Afterward, the owner calls Build Index () to build forward indexes I. In this algorithm, the data owner extracts keywords and calculates weights for building forward indexes as semantic information of documents. Finally, the owner sends the secret key K and indexes I to data users.

4.2 Search and Prove:

In this phase, the cloud server performs SeaPro () to search documents and generate proofs. To describe this algorithm in detail, we split SeaPro () into two algorithms, namely, SolveRLP () and Rank (), as follows:

(Π, Λ) ← SolveRLP(Ω) is a deterministic algorithm, corresponding to the "Any Ready-made Optimizer". The cloud server takes RLP problems Ω as input, then generates the optimal values Π and proofs Λ for RLP problems.

(Γ, E) ← Rank (Π, Δ, C, k) is a deterministic ranking algorithm, corresponding to the "Subtractor" and "Ranker". The cloud server takes

ISBN: 978-93-91303-04-04

optimal values Π, the constant terms Δ, the ciphertext dataset C and the number k as input, first calculates all the measurements E, then generates the top-k related encrypted documents Γ.
the cloud ranks measurements E in ascending order and obtains the top-k related encrypted documents Γ. Finally, the cloud returns the top-k related encrypted documents Γ and proofs Λ to the users.

4.3 Verification and Decryption:

In this phase, data users perform VerDec () to verify the correctness of the search results and decrypt the top-k encrypted documents. To describe this algorithm in detail, we split it into Verify () and DecDoc (), as follows:

then generate the result of verification 0 or α, where α ∈ N *, N* denotes the positive integer set. Y ← DecDoc (K, Γ) is a deterministic decryption algorithm, corresponding to the "Documents Decryption". The users take the top-k related encrypted documents Γ and secret key K as input, then generate the top-k related plaintext documents Y for the query q. The users first call Verify () to verify the correctness of the search results. The Verify () will output 0 when the verification pass; otherwise, this algorithm calls "Annunciator" to output α as the warning which denotes the number of failing proofs. The users call DecDoc () to decrypt the top-k encrypted documents Γ with the secret key K and obtains the top-k related documents Y if the proofs Λ pass our result verification mechanism.

5. RESULTS

This project specifies the necessity of authentication, verifiability and security of the information that is stored over the public cloud. Here, the results related with the project are observed.

Data Owner Page:

Description: This is the Data Owner login page. The Data owner could login using his credentials or if he is a new user, he could register as a new owner.

Encryption Key Request:

Fig: 5.2 Encryption key request

Description: Data Owner uses Encryption key request to upload the information over the cloud.

File Updating:

Fig: 5.3 File Updating Description: After the data owner has encryption key, the data owner can upload the information.

Fig: 5.4 Grant Key Permission Description: In this, the data owner could see who is requesting for authorization and the data owner can accept or deny his request.

The process of encrypting the documents before outsourcing it onto cloud is a great way of ensuring the security and confidentiality of information. Using Syntactic searching scheme overprotected data, enhances the capabilities of retrieving the requested query documents without leveraging any sensitive information. Effective Matching Technique, also referred as verifiable

ISBN: 978-93-91303-04-04

semantic search, outsources the documents requested by the end user with decryption request as a bridge between the Data owner and the cloud user. This work ensures the correctness of matching user query words effectively.

REFERENCES

[1] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy, 2000, pp. 44– 55.

[2] Z. Fu, J. Shu, X. Sun, and N. Linge, "Smart cloud search services: verifiable keyword-based semantic search over encrypted cloud data," IEEE Trans. Consum. Electron., vol. 60, no. 4, pp. 762–770, 2014.

[3] Z. J. Fu, X. M. Sun, N. Linge, and L. Zhou, "Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query," IEEE Trans. Consum. Electron., vol. 60, no. 1, pp. 164–172, 2014.

[4] T. S. Moh and K. H. Ho, "Efficient semantic search over encrypted data in cloud computing," in Proc. IEEE. Int. Conf. High Perform. Comput. Simul., 2014, pp. 382–390.

[5] N. Jadhav, J. Nikam, and S. Bahekar, "Semantic search supporting similarity ranking over encrypted private cloud data," Int. J. Emerging Eng. Res. Technol., vol. 2, no. 7, pp. 215–219, . H. Xia, Y. L. Zhu, X. M. Sun, and L. H. Chen, "Secure semantic expansion- based search over encrypted cloud data supporting similarity ranking," J. Cloud Comput., vol. 3, no. 1, pp. 1–11, 2014.

[6] Z. Fu, L. Xia, X. Sun, A. X. Liu, and G. Xie, "Semantic-aware searching over encrypted data for cloud computing," IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2359–2371, Sep. 2018.

[7] Z. J. Fu, X. L. Wu, Q. Wang, and K. Ren, "Enabling central keyword based semantic extension search over encrypted outsourced data," IEEE Trans. Inf. Forensics Security., vol. 12, no. 12, pp. 2986–2997, 2017.

[8] Y. G. Liu and Z. J. Fu, "Secure search service based on word2vec in the public cloud," Int. J. Compute. Sci. Eng., vol. 18, no. 3, pp. 305–313, 2019.

[9] E. J. Goh, "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, pp. 216–

[10] 234, 2003.

[11] R. Curtmola, J. Garay, S. Kamara, and

ISBN: 978-93-91303-04-04

FINDING BIPOLAR DISORDERS USING MACHINE LEARNING ALGORITHMS

Vudduru Bharathi[1] K. Geethanjali[2] M. Bhavitha[3] M. Priyanka[4] T. Vandana[5]
Associate Professor[1], UG Scholar[2, 3, 4, 5]
[1, 2, 3, 4, 5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

Abstract:

As we know that people around the world work hard to keep up with this racing world. However, due to this each individual is dealing with many distinct health issues, one of the most known issue is depression or stress which may eventually lead to death or other brutal activities. These abnormalities can be called as the Bipolar disorder which can be treated by undergoing some treatment suggested by psychologists. For this research, data has been taken from working people which comprises of all kinds of questions for despondent detection and the dataset has been run through some machine learning algorithms named Random Forest, Support Vector Machine, Decision Tree and Logistic Regression.

Keywords:

Bipolar disorder, Random Forest, Support Vector Machine, Decision Tree, Logistic Regression.

1. INTRODUCTION

Mental health can effect everyday living, relations, and physical health. In any case, this connection additionally works the other different way. Factors in individuals' lives, relational associations, and physical variables would all be able to add to mental health issues. Caring for mental disorder can improve a person's perspective over life in a positive way. Doing this can help in achieving peace in life. Conditions, for example, stress, depression, despondency, and nervousness would all be able to influence mental health and disturb an individual's everyday practice.

Mental disorders impact around 25 percent of elders; just about 6 percent are truly disabled and named having real mental sickness .These disorders are habitually associated with endless physical infirmities, for instance, coronary disease and diabetes. They in like manner increase the risk of physical injury and going through disasters, severity, and suicides. Suicide alone was at danger for 35,345 deaths in the U.S in 2019 (the latest year for which last data are available), making it the tenth driving explanation behind death. Among adolescents and young adults, suicide is responsible for extra deaths than the blend of harmful development, heart ailment, innate irregularities, respiratory disorder, influenza, iron efficiency, and kidney and liver disease.

The treatment of mental disorder has been held somewhere around the inclination that disorders of feeling, thinking, and direct somehow need realness and rather reflect particular weakness or poor life choices. Most crisis offices are unwell prepared to address the issues of patients amidst mental health emergencies. Most protection plans see mental disorder and dependence as special cases to standard thought, not part of it. Regardless of a general social move towards sympathy, our overall people in spite of everything will when all is said in done view the mentally wiped out and those with tendency as morally broken instead of as wiped out.

2. LITERATURE SURVEY

Many approaches have been done and studied by the scientists on the prediction and some of them are mentioned below.

Incorrect way of treating mental disorder may lead to irredeemable degradation in patient's mental health and it may also lead to death. Around millions of patients around the globe are not treated properly. In this research work, a novel report build a semi-robotized framework that guides in starter determination of the mental issue tolerant. The test constructs the semi-computerized structure dependent on a coordination of the technology of hereditary calculation, arrangement information mining and AI. The classifier/mental examiner will have the option to make an educated, shrewd and fitting evaluation that will prompt a precise forecast. The investigator will be a definitive selector of the discovery and treatment plan.

Mental illness deeply impact on each member of the family and also the person and also the society. Interpersonal organizations permit people with mental disorders speak with the people who are also diagnosed with mental disorder with the help of online communication, giving indications about mental illness issues. Mental illness often happens in mixes, e.g., a person with a nervousness disorder may likewise create sadness. The merging of the mental

conditions gives the spotlight to our work of arranging the web networks with an enthusiasm for misery.

To this, we have slithered a vast collection of 730,100 comments sent by 98,500 clients in 324 online networks. In this process, they have taken highlighted comments and utilized these to donate to the system. An AI technique is used to define a combined framework to display mental health co-happening on the web networks from these highlights. At the end, they executed exact approved model over the slithered dataset.

ML and text examination have displayed progressively valuable in various health based applications, especially in the medium of investigating on the web information for ailment plague and cautioning indications of an assortment of mental illness outgrowth. However, focus on cognitive bending, an antecedent and side effects of cerebral disorder, for example, nervousness and discouragement. Distinct journals have been gathered and marked them depending on the misshaped designs. At that point made use of LIWC to get the highlighted text and applied Machine Learning techniques to the subsequent vectors.

In this paper, mental health issues have become a huge issue in society and it also affects the daily routine work of an individual. There are many health issues which occur due to stress and depression. In this individual situation, a target measure for distinguishing the degrees of stress while taking in consideration of mind could extensively increase the related destructive impacts. So that, in this work, an AI formation included with EEG signal is designed. The end results explain that the developed system gives accuracy of 95%. The designed EEG form gives a multilevel quantified stress objective. It can also be used to construct computerized tool for detecting stress.

Pre-detection of cerebral diseases may help in getting better treatment and also increases the living quality of the person. It is very much mandatory to treat such problem at the early stage to prevent loss of lives. AI and ML methods are mostly helpful for diagnosing and treating of any health issues. In this research, they have taken and utilized seven ML algorithms to find accuracy for 5 health related issues. A set of data consisting of 59 cases is taken for the process. All the algorithms are applied on the dataset and they have given a good accuracy with only a small difference.

3. PRESENT WORK

A comparative study of machine learning algorithms such as Random Forest, Decision Tree, Support Vector Machine (SVM) and Logistic Regression has been carried out in the context of Health Care.

The present work considers the stress detection among the tech people. The dataset considered is a survey among the working people, which considered all possible question for stress detection.

The designed approach utilizes the ML algorithm for stress identification; Support Vector Machine, Decision Tree, Logistic Regression and Random forest are used on the dataset for learning and detection. The present work finds the suitable algorithm for mental disorder prediction.

The code was developed in Python and libraries which are necessary are used. The dataset is downloaded from kaggle. The data is then divided into training dataset and testing dataset.

4. RESULTS AND ANALYSIS

The system is developed using Python language with necessary libraries. Implemented using four machine learning algorithms on the dataset for bipolar disorders detection shows that Random forest model gives highest accuracy compared to other models. Support Vector Machine and Logistic Regression algorithms have same accuracy and Decision Tree algorithm got least accuracy compared to other algorithms.

Algorithm	Accuracy
Random Forest	0.734127
Support Vector Machine	0.722222
Logistic Regression	0.722222
Decision Tree	0.650794

TABLE I: Comparison of Model Accuracies

The above table represents the accuracy of machine learning algorithms for mental disorder detection. The below figures show the accuracies of all algorithms.

ISBN: 978-93-91303-04-04

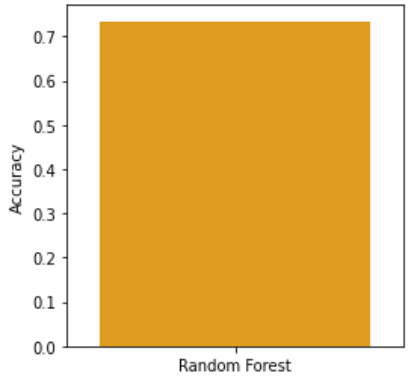


Figure-1: Accuracy of Random Forest

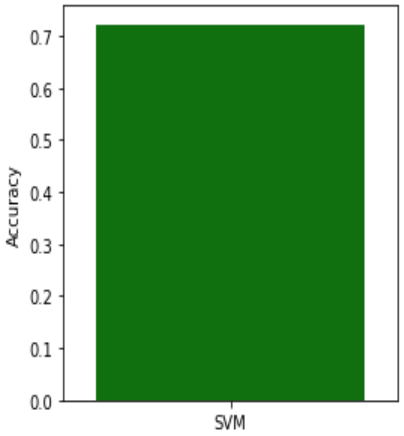


Figure-2: Accuracy of Support Vector Machine

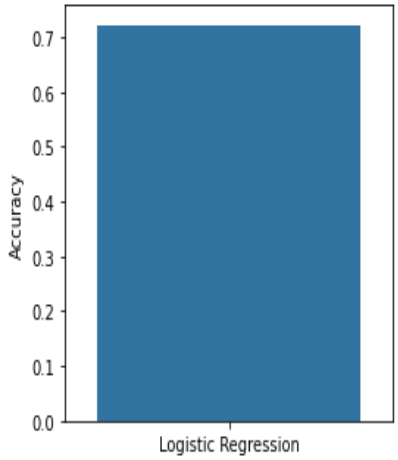


Figure-3: Accuracy of Logistic Regression

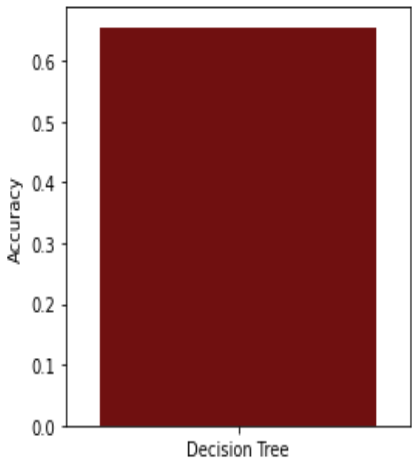


Figure-4: Accuracy of Decision Tree

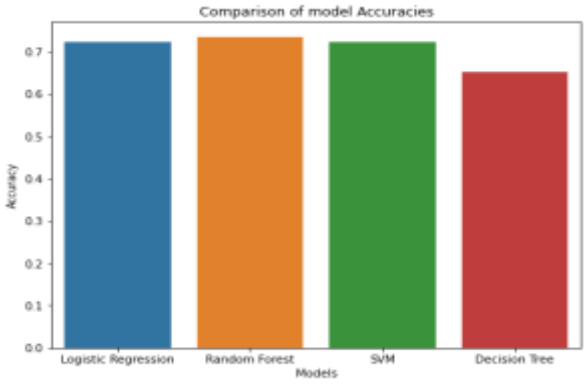


Figure 5: Bar Graph for comparison of Model Accuracies

5. CONCLUSION

There are various methods which are utilized for detection of mental illness among individuals of various ages. The method utilized by these systems utilizes the method of detection via analyzing the mental disorder detection through the set of questionnaires, in order to predict the downturn levels among various age groups. The machine learning algorithms are utilized for bipolar disorders detection. The dataset with 1259 samples are considered for study. We utilized SVM, Decision Tree and Random Forest and Logistic Regression for learning and detection. The experimental outcomes demonstrated that the Random Forest achieves the most elevated accuracy around 73.41% compared to all algorithms.

6. REFERENCES

[1] Mental Disorder Detection: Bipolar Disorder Scrutinization using Machine Learning, published in 2019.

ISBN: 978-93-91303-04-04

[2] Intelligent data mining and machine learning for mental health diagnosis using genetic algorithm Azar, Ghassan & Gloster, Clay & El- Bathy, Naser & Yu, Su&Neela, Rajasree&Alothman, Israa. (2015). Intelligent data mining and machine learning for mental health diagnosis using genetic algorithm. 201-206. 10.1109/EIT.2015.7293425

[3] A Framework for Classifying Online Mental Health-Related Communities With an Interest in Depression B. Saha, T. Nguyen, D. Phung and S. Venkatesh, "A Framework for Classifying Online Mental Health-Related Communities With an Interest in Depression," in IEEE Journal of Biomedical and Health Informatics, vol. 20, no. 4, pp. 1008- 1015, July 2016.

[4] Detecting Cognitive Distortions Through Machine Learning Text Analytic T. Simms, C. Ramstedt, M. Rich, M. Richards, T. Martinez and C. Giraud-Carrier, "Detecting Cognitive Distortions Through Machine Learning Text Analytics," 2017 IEEE International Conference on Healthcare Informatics (ICHI), Park City, UT, 2017, pp. 508-512.

[5] Machine Learning Framework for the Detection of Mental Stress at Multiple Levels Subhani, Ahmad & Mumtaz, Wajid & Mohamad Saad, Mohamad Naufal & Kamel, Nidal & Malik, Aamir. (2017). Machine Learning Framework for the Detection of Mental Stress at Multiple Levels. IEEE Access. PP. 1-1. 10.1109/ACCESS.2017.2723622.

[6] Prediction of Mental Health Problems Among Children Using Machine Learning Techniques Sumathi, Ms & B., Dr. (2016). Prediction of Mental Health Problems Among Children Using Machine Learning Techniques. International Journal of Advanced Computer Science and Applications. 10.14569/IJACSA.2016.070176.

[7] Benefiting from Online Mental Status Examination System and Mental Health Diagnostic System Hajar Mat Jani, Ph.D College of Information Technology University Nasional Km. Malaysia (2010).

[8] Development of Classification Features of Mental Disorder Characteristics Using The Fuzzy Logic Mamdani Method Meza Silvana, Ricky Akbar, Derisma, Mia Audina, Firdaus (2019).

[9] A Preliminary Attempt to Rules Generation for Mental Disorders Jerzy Gomula, Wieslaw paja, Krzysztof Paneerz and Jaroslaw Szkola (2010).

[10] Study on Mental Disorder Detection via Social Media Mining Iwan Syarif, Nadia Ningtias, Tessy Badriyah (2019).

ISBN: 978-93-91303-04-04

Secure and Efficient Search Scheme for Encrypted Images using KNN Search in Cloud Environment

K.Sree Lakshmi[1] K.Jyothsna[2] K.Sai Lekhana[3] V.Sai Nithisha[4]K.Sandhya RanI
Assistant Professor[1], UG Scholar[2, 3, 4, 5]
[1,2,3,4,5]Department of CSE, Geethanjali Institute of Science and Technology, Nellore

ABSTRACT

The Content-Based Image Retrieval(CBIR) technique Has attracted much attention from many areas (i.e., cloud computing). Although existing privacy-preserving CBIR schemes can guarantee image privacy while supporting image retrieval.To address these challenging issues , in this project we present a similarity search for Encrypted Images in secure with a tree-based data structure and Assymetric scalar product preserving encryption (ASPE) , which Implemented faster search than linear search.First the feature descriptors extracted by the Convolutional Neural Network (CNN) models are used to improve search accuracy . Next, an encrypted hierarchical index tree by using K-means clustering based on Affinity Propagation(AP) clustering is devised , which can improve search efficiency.Then a limited key-leakage k-Nearest Neighbour(KNN) algorithm is proposed to protect key from being completely leaked to untrusted image users.

Keywords: Content-Based Image Retrieval,K-Nearest Neighbour, Search accuracy, Search Efficiency

1.INTRODUCTION

By the rapid development and popularization of cloud computing, many people enjoyvariousconveniences brought by cloud services, such as storing images on the cloud. However,directly outsourcing images to the public cloud inevitably raises privacy concerns. Once themassive images (e.g., patients medical images) containing highly sensitive information havebeen leaked to unauthorized entities, it will incur serious consequences or unnecessary trouble. Encryption mechanism can alleviate image data security and privacy concerns to someextent, but it invalidates the Content-Based Image Retrieval (CBIR) technique over ciphertext,and even causes other concerns. Fortunately, various schemes related to privacypreserving CBIR have been studiedlike[1]–[8]. in practice,However these schemesStillface many challenges (i.e., low search accuracy, low search efficiency, key leakage, etc.). Specifically, schemes [1], [2], [3], [5] directly distributed keys to users,leading to the risk of image users leaking keys, schemes [3], [5] sacrificed accuracy to improve efficiency, and schemes [1], [4], [6], [7], [8] brought a lot of overhead to achieve high security.

There are also works [9], [10] that combine global features and local features with certainweights in order to form new features or apply Convolutional Neural Network (CNN) modelmimicking human visual cognition to extract feature vectors,which achieve acceptable accuracy. For the later, the similarity between images is measured by Euclidean distance,Cosine distance, Hamming distance, and Jaccard similarity coefficient. Especially, AsymmetricScalar-productPreserving Encryption (ASPE) algorithm [11] while using random numbers and matrices to encrypt feature vectors can calculate the Euclidean distance of highdimension space more accurately. At the same time, other works [4], [12] using Secure Multiparty Computation (SMC), Homomorphic Encryption (HE) to calculate Euclidean distance can also improve search accuracy.

2.RELATEDWORKS

A.Content-based multi-source encrypted image retrieval in clouds with privacy preservation.

In this paper, we propose a secure CBIR scheme that supports Multiple Image owners with Privacy Protection (MIPP). We encrypt image features with a secure multi-partycomputation technique, which allows image owners to encrypt image

features with their own keys. This enables efficient image retrieval over images gathered from multiple sources, while guaranteeing that image privacy of an individualimage owner will not be leaked to other image owners. We also propose a new method for similarity measurement of images that can avoid revealing image similarity information to the cloud. Theoretical analysis and experimental results demonstrate that MIPP achieves retrieval accuracy and efficiency simultaneously, while preserving image privacy.framework is efficient and feasible for practical applications shows that the proposed image retrievalvectors.

B.fast nearest neighbor search scheme overoutsourced encrypted medical image.

Medical imaging is crucial for medical diagnosis, and the sensitive nature of medicalimages necessitates rigorous security andprivacy solutions to be in place. In a cloud-based medical system for Healthcare Industry 4.0, medical images should be encrypted prior to being outsourced. However, processing queries over encrypted data without first executing the decryption operation is challenging and impractical at present. In this paper, we propose a secure and efficient scheme to find the exact nearest neighbor over encrypted medical images. Instead of calculating the Euclidean distance, we reject candidates by computing the lower bound of the Euclidean distance that is related to the mean and standard deviation of data. Unlike most existing schemes, our scheme can obtain the exact nearest neighbor rather than an approximate result. We, then, evaluate our proposed approach to demonstrate its unity.

C .Search in my way: Practical outsourced image retrieval framework supporting unshared key

The traditional privacy-preserving image retrieval schemes not only bring large computational and communication overhead butalso cannot well protect the image and query privacy in multi-user scenarios. To solve the above problems, we first propose a basic privacypreserving content-based image retrieval (CBIR) framework which significantly reduces storage and communication overhead compared with the previous works.Furthermore, we design a new

efficient key conversion protocol to support unshared key multi-owner multi-user image retrieval without losing search precision..Moreover, our framework supports unbounded attributes and can trace malicious users according to leaked secret keys, which significantly improve the usability of multi-source data sharing.Strict security analysis shows that the user privacy and outsourced data security can be guaranteed during the image retrieval process, and the performance analysis using real-world dataset.

D. Towards privacy preserving content -based image retrieval in cloud computing.

Content-based image retrieval (CBIR)applications have been rapidly developed along with the increase in the quantity, availability and importance of images in our daily life. However, the wide deployment of CBIR scheme has been limited by its the severe computation and storagerequirement. In this paper, we propose a privacy-preserving content-based image retrieval scheme, which allows the data owner to outsource the image database and CBIR service to the cloud, without revealing the actual content of the database to the cloud server. Local features are utilized to represent the images, and earth mover's distance (EMD) is employed to evaluate the similarity of images. The EMD computation is essentially a linear programming (LP) problem. The proposed scheme transforms the EMD problem in such a way that the cloud server can solve it without learning the sensitiveinformation. In addition, local sensitive hash (LSH) is utilized to improve the search efficiency. The security analysis and experiments show the security and efficiency of the proposed scheme.

3.PROPOSED METHODOLOGY

In this project we propose a similarity Search for Encrypted Images in secure cloud computing (SEI) to solve the above challenges. Specifically, we employ the CNN model to extract feature vectors to improve search accuracy, and then build a hierarchical index tree in a bottom-up

ISBN: 978-93-91303-04-04

manner based on the clustering algorithm to improve search efficiency. Besides, we design an optimized ASPE algorithm, which does not require the image owner to share sdkwith image users, to achieve limited key-leakage for untrusted image users. To summarize, our contributions are set out as follows.

• **High search accuracy.** SEI achieves a high search accuracy by using the pre-trained CNN model to extract feature vectors. The CNN model simulating the human visual perception process can more accurately represent the image content, which makesthe similarity measurement between images more accurate and search results more accurate.

• **High search efficiency.** SEI uses the optimized Kmeans clustering algorithm to classify images and constructs a hierarchical index tree in a bottom-up manner based on the clustering results. SEI avoids traversing the entire image database when performing search operation and reduces the search time to sublinear time

• **Limited key leakage.** TheSEI provides a secure trapdoor generation process with limited key-leakage , which not only prevents untrusted image users from completely leaking keys privacy but also avoids the online help of the image owner when the image user generates trapdoors locally.

4.RESULTS

The implementation involves various steps.

They are:

- Image Owner
- Image User
- Cloud Server

Image Owner:

Fig: Image Owner login Page

Description: This is image owner login page the image owner can login and add the images.

Fig: Image Owner Home Page

Description: This is image owner home page .In this the page admin can add images, check the user search requests, can view all the images and Encrypts the images and stores in cloud server.

Fig: All images

Description: This are the images that we have added .

Image User:

Fig: User Registration Form

Description: This is User Registration form, In this the image user can register .

ISBN: 978-93-91303-04-04

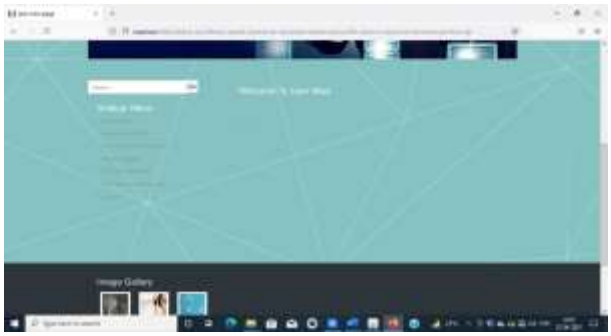


Fig: Image User Home Page

Description: This is Image user home page, In this the user can login and then request key from image owner by entering the key the image user can search similar images.

Fig: User Profile

Description: These is the user profile consists of user name, phone no, mail id, date of birth and address of the user

Cloud Server:

Fig: Cloud server login page

Description: This is cloud server login page, In this the page admin can login and view the users search history and the images that are encrypted and stored in cloud server.

Fig: Cloud server Home page

Description: This is cloud server home page, In this the page admin can authorize the image user after registering ,can view all the images ,can search all users history list, can search all images ranking chart.

Fig: Users search history list

Description: This search history list of all the users. This data shows what the user searched

5.CONCLUSION

In this project, we investigate similarity search for encrypted images in secure cloud computing. Concretely, we will introduce a clustering improvement method andgive the design method of the hierarchical index tree. With these two techniques, SEI can efficiently perform the retrieval process and achieve high accuracy based on features extracted bythe CNN model. Further, we consider untrusted image users in SEI and hence propose a similarity calculation method with limited key-leakage.We also give strict security analysis and conduct experiments on a real-world

ISBN: 978-93-91303-04-04

dataset, which indicate that SEI is secure and feasible in practice.

6.REFERENCES

[1] X. Wang, J. Ma, X. Liu, and Y. Miao, "Search in my way: Practical outsourced image retrieval framework supporting unshared key," in Proc. IEEE Conference on Computer Communications (INFOCOM' 19). IEEE, 2019, pp. 2485–2493.

[2]Y. Miao, X. Liu, K.-K. R. Choo, R. H. Deng, J. Li, H. Li, and J. Ma, "Privacy-preserving attribute-based keyword search in shared multi-owner setting," IEEE Transactions on Dependable and Secure Computing, 2019

[3] Z. Xia, L. Jiang, D. Liu, L. Lu, and B. Jeon, "Boew: A contentbased image retrieval scheme using bag-of-encrypted-words in cloud computing," IEEE Transactions on Services Computing, 2019.

[4] M. Li, M. Zhang, Q. Wang, S. S. Chow, M. Du, Y. Chen, and C.Lit, "Instantcryptogram: Secure image retrieval service," in IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, 2018, pp. 2222–2230.

ISBN: 978-93-91303-04-04

Realtime Face mask Detection And Alert Sytem Using Artificial Intelligence

Dr. V. Sireesha[1] S. Sivasankar [2] B. Deepak Surya [3] M. Abhilash Chowdary [4] SD. Hasim Hussain[5]

Professorand Head oftheDepartment(HOD)[1], UGScholar[2,3,4,5]
[1,2,3,4,5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

Abstract

Due to the global COVID-19 pandemic, computer vision education has received increasing attention to improve public health services. At the time of death, because a pair of classification and detection are usedunder the video image, detecting small objects in image processing is a more difficult task. Deep neural network detection has shown useful object detection with excellent performance, namely mask detection. For inevitable natural diseases, it is auniquetopic because of the benefits it brings to people. Added mask detection that works with Caffe and can measure real-time performance through a powerful GPU.Then, we have some people who use or do not use masks to train people with mask images but no mask images. The results of detection, location and detection experiments showthat the average loss after training for 4000 epochsis0.0730. Aftertraining4000epochs, the MAP value is0.96.

Key Words:
Facemask, Machine Learning, Convolutional Neural Networks, Caffe.

I.Introduction

The global COVID-19 pandemic has caused epidemics of dangerous diseases all over the world. At the same time, this situation has been criticized and is increasing in all countries announced by the World Health Organization [1-3]. According to this epidemic, the bodies of more than 114 countries developed flu symptoms within6.4 days (2 to 14 days). Millions of people get sick in one day. In the disaster phase, everyone should raise awareness and of course take some actions on their own. On this issue, the nationalgovernmentauthorities and workplaces must strictly abide by the necessary rules,
and constantly measure and protest the healthofthepeople. As a result, the semicroorganismsmovefrom one area to another and spread the virus. Shake hands, microorganisms in the mouth, and share accessories with others. Today, people who wear masks for their own safety are worried about reducing sprouting and sprouting. Reduce the number of people. Because of this radical theme, we illustrate our work by locating the masks of people who wear masks and people who are not in crowded outdoor areas. Computer vision training is the actual field of image recognition, descriptive image conversion, analysis and results.

II. Literaturesurvey

Outbreak of pneumonia of unknown etiology in Wuhan, China: The thriller and the miracle. As of December 2019, a complete of forty one instances of pneumonia of unknown etiology were showed in Wuhan, Hubei Province, China. Wuhan is a primary transportation hub with more than eleven million residents. Most of the sufferers went to the neighborhood community. Fish and wild animals. The marketplaceclosing month. At the countrywide press conference held today, Dr. Dr. XuJianguo, academician of the Chinese Academy of Engineering, and a group of scientists introduced this new typeoutbreak was caused by the new coronavirus 2019 (2019-nCoV) provisionally named by the World Health Organization.

1 The coronavirus-specific nucleic acid sequence of 2019-nCoV is different from the known nucleic acid sequence of the human coronavirus species. These are similar to certain corona beta viruses identified in bats. 2,3 Virus-specific nucleic acidsequencewerefoundinthelungfluid,
bloodandthroat swabs of 15 patients, and the isolated viruses showed typical corona discharges. virus. The appearanceundertheelectronmicroscope. In order to better understand the new coronavirus used in the development of antiviraldrugsandvaccines, moreresearchis being conducted. We welcome the

excellent work done so far. Scientists and epidemiologists ruled out several highly infectiouspathogens, includingSARS, which caused hundreds of deaths. More than ten years ago and MERS. Due to the outbreak, the Hong Kong authorities quickly stepped upthedisinfectionoftrainsandairplanesand thecontrolofpassengers, whichundoubtedly alleviated environmental problems. Last month, most patients went to the Wuhan fish and wildlife market. This fish and wildlife marketalsosellsliveanimalssuchaspoultry, bats, marmots and snakes. All patients immediatelyreceivedsupportivetreatmentin isolation and quarantine. Among them, 7 caseswereseverelyilland1casedied.Sofar, 42 confirmed patients are from China, except for one Thai patient from Wuhan. Eight patientshavebeencuredanddischargedfrom hospital. Came out of the hospital last week. 2019-nCoVnow has been isolated from multiple patients and seems to be theculprit.

Severe acute respiratory disorder Covid 2 (SARS-CoV-2) and Covid infection 2019 (COVID-19): The pestilence and the difficulties.

Toward the finish of 2019, the development of Chinese Coronavirus 2 (SARS-CoV-2; previously known as New Coronavirus 2019 or 2019-nCoV) illness (COVID-19) caused serious intense respiratory condition, which is a significant worldwide The episode is a significant flare-up. ...A general medical problem. As of February 11, 2020, World Health Organization (WHO) information showsthatinexcessof43,000affirmedcases have been found in 28 nations/locales, of which >99% are in China. In January 2020, the World Health Organization proclaimed COVID-19 as the 6th worldwide general wellbeing crisis. SARS-CoV-2 is closely related to two bat-derived coronaviruses suffering from acute respiratory syndrome- Bat-SL-CoVZC45 andBat-SL-CoVZXC21:it is through droplets in the air or direct contact between people Spread between and from the transferor. Individuals through beads or direct contact. The normalbrooding season of contamination is assessed to be 6.4 days, and the gauge multiplication rate is somewhere in the range of 2.24 and 3.58. -2 (new coronavirus pneumonia or Wuh pneumonia), the most common symptom is fever and then cough. On the chestcomputed tomography image, the most common findingistheopacityofthegroundglasswith bilateral lung involvement. Shows that inexcess of 43,000affirmedcases have been found in 28 nations/locales, of which >99% are in China. In January 2020, the World Health Organization proclaimed COVID-19 as the 6th worldwide general wellbeing crisis. SARS-CoV-2 is closely related to two bat-derived coronaviruses suffering from acute respiratory syndrome-

Bat-SL-CoVZC45 andBat-SL-CoVZXC21:it is through droplets in the air or direct contact between people Spread between and from the transferor. Individuals through beads or direct contact. The normalbrooding season of contamination is assessed to be 6.4 days, and the gauge multiplication rate is somewhere in the range of 2.24 and 3.58. -2 (new coronavirus pneumonia or Wuh pneumonia), the most common symptom is fever and then cough. On the chestcomputed tomography image, the most common findingistheopacityofthegroundglasswith bilateral lung involvement.The only SARS- CoV-2 pneumonia case in the United States has responded well to the treatment and is currently undergoing clinical testing in China. Currently, infection control is mainly used to prevent the spread of SARS-CoV-2. However, the health authorities need to continuetomonitorthesituationclosely. The more we understand this new virus and the outbreaks associated with it, the betterwecan respond.

The study of disease transmission and pathogenesis of Covid illness (COVID-19) episode

Covid infection (COVID-19) is brought about by SARS-COV2 and is a conceivably lethal illness that has caused extraordinary public concern. In view of the huge numberof tainted individuals entering the wet creature market in Wuhan. It is conjectured that this might be the source of the zoonotic illness of COVID-19. The spread of COVID-19 from person to person resulted in the

ISBN: 978-93-91303-04-04

isolation of patients who later received various treatments.

In order to fight the current epidemic, human-to-human COVID- 19 transmission has been introduced. Unique consideration and endeavors ought to be made to secure or lessen transmissionamong weak gatherings including youngsters, clinical staff and the older. Side effects, the study of disease transmission, transmission, pathogenesis, phylogenetic examination and the future heading of controlling the spread of this lethalinfection.

Existing system

In the existing method, we only use images to create a model, and only use user input to predict theresult.

There is no recognition, compare it with the image, and then ge ttheresult through imageprocessing.

Drawbacks

Accuracy rate isslow

Thereisnoreal-timedetectionfroma videostream

Proposed system

The proposed method includes the use of CNN with a deep learning framework for video surveillance. Use instead of using amask.

Facts have proved that artificial neuralnetworkisapowerfulfeatureextraction method. From the original data.

This study proposes to use a convolutional neural network to design a mask classifier, andconsider the influence of the number of convolutional neural layers on the predictionaccuracy.

Advantages

The CNN process includes the recognition and classification of images based on the learned features.Inthemulti-layerstructure,it is very effective for obtaining and evaluatingtherequiredgraphicimage characteristics.

The forecast is very fast and accurate and can be used in real-time applications.

Conclusion

This article contains research on the use of convolutional neural network deep learning technology to detect real-time masksthrough alarm systems. This process can provide fast and accurate results for mask recognition. ThetrainedmodelcanusetheCNNVGG-16 model to complete the work and obtain results with 99% accuracy. In addition, the study is a useful tool to combat the spread of the COVID-19 virus by detecting whether a person is wearing a mask and issuing an alarm when not wearing a mask. Other tasks include physical distance integration. In this case, the camera can detect people with or without masks, and it can also measure the distance between each person. If thephysical distance is not properly maintained, analarm will be triggered .From CNNa ndcomparethe maximum accuracy of each model to improve athletic performance. Inside It is recommended to identify and identifypeople wearing masks. In addition, the researchers recommend the use of other optimizers, better parameters ettings, fine-tuning,andthe use of adapt ive learning with data transmissionmodels.

References

[1] Yu, P., Zhu, J., Zhang, Z., & Han, Y. (2020). A Familial Cluster of Infection AssociatedWiththe2019NovelCoronavirus Indicating Possible Person-to-Person Transmission During the Incubation Period. The Journal of irresistible infections, 221(11), 1757–1761. https://doi.org/10.1093/infdis/jiaa077

[2] Chavez, S., Long, B., Koyfman, A. and Liang, S. Y. Covid Disease (COVID-19):An introduction for crisis doctors. Am J Emerg Med, https://doi:10.1016/j.ajem.2020.03.036 (2020).

[3] World Health Organization. Coronavirus disease 2019 (COVID-19) Situation

Report– 142, 2020, [cited 10 June 2020], https://www.who.int/docs/default-source/coronaviruse/situationreports202006 10-covid-19-sitrep- 142.pdf?sfvrsn=180898cd_6

[4] Bai, Y., Yao, L., Wei, T., Tian, F., Jin,D. Y., Chen, L., & Wang, M. (2020). Presumed Asymptomatic Carrier Transmission of COVID-19. JAMA, 323(14), 1406–1407. Advance online publication. https://doi.org/10.1001/jama.2020.2565

Centers for Disease Control and Prevention. Break Infection Prevention and Control Recommendations for PatientswithSuspected or Confirmed Coronavirus Disease 2019 (COVID-19) in Healthcare Settings. 2020 [cited 5 June 2020]. https://www.cdc.gov/Covid/2019-ncov/hcp/contamination controlrecommendations.html

ISBN: 978-93-91303-04-04

Predicting Crop Yield in Indian Agriculture Using Ensemble Learning Model

P. Chandrakala[1]G.Sowkya[2] V. Poojitha[3] V. Niharika[4] SK.Ameena[5]V.Sai Tejaswi [6]
Assistant Professor[1], UG Scholar[2, 3, 4, 5,6]
[1, 2, 3, 4, 5 ,6]Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

ABSTRACT:

Crops are one of the major resources in India. Predicting the yield of a crop is a major task of research. Machine learning is one of the areas used for prediction. In this project, we use advanced regression methods such as Random Forest, Gradient Boost and Decision tree algorithms to predict the yield of crops in India. The prediction of crop yield is done based on parameters such as state, district, season, area, rainfall etc. Accuracy has been considered as a parameter for evaluation. This project predicts the yield of almost all kinds of crops that are planted in India.

KEYWORDS:

Crop yield prediction, Random Forest, Decision tree, Gradient Boost

---

13. I.INTRODUCTION

In our investigation, which we found in the past research papers is that everyone uses climatic components like precipitation, light and rustic parts like soil type, supplements moved by the earth (Nitrogen, Potassium, etc) notwithstanding the issue is we need to amass the data and a short time later an outcast does this assumption and a short time later it is unveiled to the farmer and this requires a huge load of effort for the farmer and he doesn't understand the science behind these factors. To improve on it and which can be clearly used by the farmer this paper uses essential factors like which state and locale is the farmer from, which crop and in what season (as in Kharif, Rabi, etc) In India, there are more than 100 harvests planted around the whole country. These yields are requested for better plan and discernment.

The data for this investigation has been acquired from the Indian Government Repository [1]. The data involves qualities – State, District, Crop, Season, Year, Area and Production with around 2.5 Lakh discernments. The fig. 1. depicts the states and areas of India which envision what order of harvests are notable in which season. We used advanced backslide techniques – Lasso, ENet and Kernel Ridge and further we used stacking of these models to restrict the bungle and to gain better gauges.

II.LITERATURE SURVEY

An improved crop yield prediction model using bee hive clustering approach for agricultural data sets

Agrarian researchers over the world interest the prerequisite for a capable instrument to anticipate and additionally foster the yield improvement. The prerequisite for a fused collect advancement control with exact farsighted yield the board theory is incredibly felt among developing neighborhood. The multifaceted design of anticipating the reap yield is significantly due to multi-dimensional variable estimations and detachment of farsighted showing approach, which prompts mishap in crop yield. This assessment paper suggests a reap yield assumption model (CRY) which works on a flexible pack approach over dynamically revived genuine gather educational file to predict the collect yield and further foster the dynamic in precision cultivation. CRY uses apiary exhibiting approach to manage separate and request the collect subject to trim advancement configuration, yield. CRY described dataset had been had a go at using Clementine over existing harvest space data.

An intelligent system based on kernel methods for crop yield prediction

This paper presents work on fostering a product framework for foreseeing crop yield from environment and ranch information. At the center of this framework is a strategy for unaided parceling of information for finding spatio-transient examples in environment information utilizing piece strategies which offer solidarity to manage complex information. For this reason, a vigorous weighted part k-implies calculation consolidating spatial imperatives is introduced. The calculation can viably deal with commotion, exceptions and autocorrelation in the spatial information, for successful and proficient information examination, and accordingly can be utilized for anticipating oilpalm yield by investigating different components influencing the yield.

Fuzzy Logic based Crop Yield Prediction using Temperature and Rainfall parameters predicted through ARMA, SARIMA, and ARMAX models.

Farming assumes a critical part in the economy of India. This makes crop yield expectation a significant undertaking to assist with boosting India's development. Yields are delicate to different climate wonders like temperature and precipitation. Consequently, it gets urgent to incorporate these highlights while anticipating the yield of a harvest. Climate anticipating is a confounded cycle. In this work, three techniques are utilized to conjecture ARMA (Auto Regressive Moving Average), SARIMA (Seasonal Auto Regressive Integrated Moving Average) and ARMAX (ARMA with exogenous factors). The presentation of the three is looked at and the best model is utilized to anticipate precipitation and temperature which are thus used to foresee the harvest yield dependent on a fluffy rationale model.

Crop Yield Prediction Using Data Analytics and Hybrid Approach

Farming information is being delivered continually and enourmosly. Thus, farming information has come in the time of huge information. Brilliant advances contribute in information assortment utilizing electronic gadgets. In our venture we are going to examinations and mine this horticultural information to get valuable outcomes utilizing advancements like information investigation and AI and this outcome will be given to ranchers for better harvest yield as far as effectiveness and usefulness.

A study on various data mining techniques for crop yield prediction.

India is a nation where farming and agribusiness related enterprises are the significant wellspring of living for individuals. Horticulture is a significant wellspring of economy of the country. It is likewise one of the country which experience the ill effects of significant normal cataclysms like dry spell or flood which harms the harvest. This prompts gigantic monetary misfortune for the ranchers consequently prompting the self destruction.

Anticipating the yield well ahead of time preceding its reap can help the ranchers and Government associations to make proper arranging like putting away, selling, fixing least help value, bringing in/sending out and so forth Foreseeing a harvest well ahead of time requires a methodical investigation of gigantic information coming from different factors like soil quality, pH, EC, N, P, K and so on As Prediction of yield manages enormous arrangement of data set subsequently making this expectation framework an ideal contender for use of information mining.

14. III.PROPOSED SYSTEM

In this section we the system model of the project in figure 1.

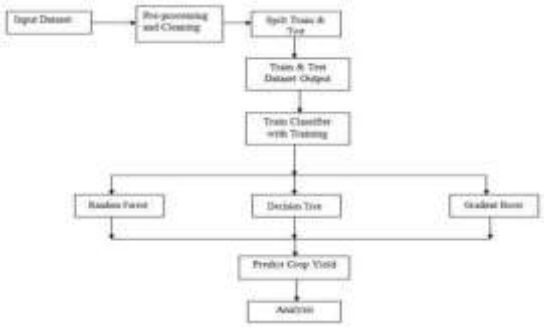


Fig. 1: System Overview

Implementation Modules

Preprocessing

For the given data set, there are quite a few ‘NA’ values which are filtered in python. Furthermore, as the data set consists of numeric data, we used robust scaling, which is quite similar to normalization, but it instead uses the interquartile range whereas normalization is something which normalization shrinks the data in terms of 0 to 1.

Stacked Regression

- This is a kind of ensembling but a little of enhancement of averaging. In this, we add a meta model and use the out of fold predictions of the other models used to train the main meta model.
- Step-1: the total training set is again divided into two different sets. (train and holdout)
- Step-2: train the selected base models with first part (train).
- Step-3: Test them with the second part.

(holdout)

- Step-4: Now, the predictions obtained from test part are inputs to the train higher level learner called meta-model.

Graphical Analysis

In this phase of the Implementation user can get the clear picture analysis of the cause of death analysis. Various factors take into consideration for the graph

ISBN: 978-93-91303-04-04

analysis. In this phase plot the charts like pie graph, bar.

Implementation Algorithms

This venture utilized arrangement strategy for forecast. Calculation has been chosen by assessing each regulated AI method. The objective of order is to anticipate future occasion by every classifier. In this work four classifiers are utilized in particular Random Forest, Decision Tree Regression and Gradient Boosting Regression. The expectation aftereffect of all classifiers are broke down and analyzed.

RANDOM FORESTREGRESSOR

- It creates multi choice trees from which every choice tree utilizes a piece of information test and predicts the outcome.
- Then the outcome which was accomplished by greatest number of trees is considered as the last forecast.
- Random woods is a Supervised Learning calculation which utilizes gathering learning strategy for arrangement and relapse. Arbitrary woodland is a stowing strategy and the trees in irregular backwoods run in equal with no communications.
- A Random Forest works by building a few choice trees during preparing time and yielding the mean of the classes as the expectation of the relative multitude of trees.

DECISION TREE REGRESSION

- Trees are constructed through an algorithmic approach that identifies ways to split the data set based on different conditions.
- It is one of the most widely used practical methods for supervised learning.
- These are non-parametric method used for both classification and regression.

GRADIENT BOOST REGRESSION

- Gradient boosting method converts the weak learners into strong learners by boosting their capability.
- A sequential process of learning from the previous trees and increasing the model accuracy.
- One of the most used and efficient method.

IV.RESULTS AND ANALYSIS

The system is developed using Python language with necessary libraries. We have implemented this by using three machine learning basic and ensemble algorithms on the dataset for predicting crop yield.

The below figure shows the comparison of accuracy of all the three algorithms and It clearly states that Random Forest Regression algorithm gives highest accuracy which best suits to reach the motive of our project.

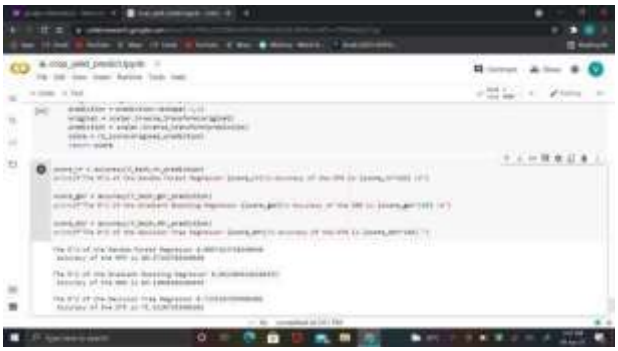


Fig:accuracy of all three algorithms

Algorithms	Accuracy
Random Forest Regressor	88.5726
Gradient Boost Regression	84.1204
Decision Tree Regression	71.3110

Table 1: Comparison of accuracy of all three algorithms

Comparison between Random Forest Regression, Decision Tree, and Gradient Boost Regression algorithms have been shown in Table1 based on Accuracies of each algorithm.

15. V.CONCLUSION

When we apply stacked regression, the result has been so improvised than when those models were applied individually. The output which has been shown in figure is currently a web application, but our future work would be building an application where the farmers can use it as app and converting the whole system in their regional language.

16. VI.REFERENCES

[1]“data.gov.in.”[Online].Available: https://data.gov.in/

ISBN: 978-93-91303-04-04

[2] Ananthara,M.G.,Arunkumar, T., & Hemavathy, R. (2013, February). CRY—an improved crop yield prediction model using bee hive clustering approach for agricultural data sets. In 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (pp. 473-478). IEEE.

[3] Awan, A. M., & Sap, M. N. M. (2006, April). An intelligent system based on kernel methods for crop yield prediction. In Pacific-Asia Conference on Knowledge Discovery and Data Mining (pp. 841846). Springer, Berlin, Heidelberg.

[4] Bang, S., Bishnoi, R., Chauhan, A. S., Dixit, A. K., & Chawla, I. (2019, August). Fuzzy Logic based Crop Yield Prediction using Temperature and Rainfall parameters predicted through ARMA, SARIMA, and ARMAX models. In 2019 Twelfth International Conference on Contemporary Computing (IC3) (pp. 1-6). IEEE.

[5] Bhosale, S. V., Thombare, R. A., Dhemey, P. G., & Chaudhari, A. N. (2018, August). Crop Yield Prediction Using Data Analytics and Hybrid Approach. In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA) (pp. 1-5). IEEE.

[6] Gandge, Y. (2017, December). A study on various data mining techniques for crop yield prediction. In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 420-423). IEEE.

[7] Gandhi, N., Petkar, O., & Armstrong, L. J. (2016, July). Rice crop yield prediction using artificial neural networks. In 2016 IEEE Technological Innovations in ICT for Agriculture and Rural Development (TIAR) (pp. 105-110). IEEE.

[8] Gandhi, N., Armstrong, L. J., Petkar, O., & Tripathy, A. K. (2016, July). Rice crop yield prediction in India using support vector machines. In 2016 13th International Joint Conference on Computer Science and Software Engineering (JCSSE) (pp. 1-5). IEEE.

[9] Gandhi, N., Armstrong, L. J., & Petkar, O. (2016, July). Proposed decision support system (DSS) for Indian rice crop yield prediction. In 2016 IEEE Technological Innovations in ICT for Agriculture and Rural Development (TIAR) (pp. 13-18). IEEE.

[10] Islam, T., Chisty, T. A., & Chakrabarty, A. (2018, December). A Deep Neural Network
Approach for Crop Selection and Yield Prediction in Bangladesh. In 2018 IEEE Region 10 Humanitarian Technology Conference (R10 -HTC) (pp. 1 - 6).
IEEE.

[11] Jaikla, R., Auephanwiriyakul, S., & Jintrawet, A. (2008, May). Rice yield prediction using a support vectorregression method. In 2008 5th International Conference on Electrical Engineering/Electronics,Computer,Telecommu
nications and Information Technology (Vol. 1, pp. 29-32). IEEE.

[12] Kadir, M. K. A., Ayob, M. Z., & Miniappan, N. (2014, August). Wheat yield prediction: Artificial neural network based approach. In 2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T) (pp. 161- 165). IEEE.

[13] Manjula, A., & Narsimha, G. (2015, January). XCYPF: A flexible and extensible framework for agricultural Crop Yield Prediction. In 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO) (pp. 15). IEEE.

[14] Mariappan, A. K., & Das, J. A. B. (2017, April). A paradigm for rice yield prediction in Tamilnadu. In 2017 IEEE Technological Innovations in ICT for Agriculture and Rural Development (TIAR) (pp. 18-21). IEEE.

ISBN: 978-93-91303-04-04

An Efficient Certificateless 0-Rtt Anonymous Aka Protocol Against Bad Randommness

N. Shivanagamani[1]B. Sushma[2]R. Kala sravani[3]K. Seema singh[4]
Associate Professor[1], UG Scholar[2, 3, 4]
[1, 2,3,4]Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

ABSTRACT

In cloud computing, resources are cloud users via the public channels. Keyagreementprovidessecure channel establishment over a public channel for the secure communications between a cloud user and a cloud service provider. The Existing key agreement protocols for cloud computing have some disadvantages, e.g., realizing low connection delay, eliminating certificate management problem, enhancing user privacy and avoiding bad randomness. To overcome these problems, our team proposed a certificateless 0-RTT anonymous AKA protocol against bad randomness for secure channel establishment between cloud provider and cloud user in cloud computing. A0-RTT protocol, is used to speed up the efficiency of the secure channel establishment process. Further our protocol not only satisfies the traditional security attributes (e.g., known-key security, unknown key-share), but also strong security guarantees, i.e., user privacy and bad randomness resistance.

KEYWORDS

Cloud computing, secure channel, Anonymous authentication, Bad randomness resistance, Zero round trip time.

I.Introduction

In cloud computing, resources are cloud users via public channels. Due to the characteristics of cloud computing and the openness of the public channels, an attacker can perform various attacks, such as impersonation, eavesdropping, forging, and tampering.

Besides, user privacy is also of great concern in cloud computing [1], which prevents an attacker from identifying whether two messages are from the same cloud user. The cloud contains sensitive information which cannot be accessed by unauthorised users e.g., medical records, financial data. If user privacy is not good, an attacker may eavesdrop the communications to a cloud. Based on which, the attacker may deduce sensitive information, including who are using the cloud, how often, and what amount of data is being exchanged, even the communications are encrypted.

Zero round trip time (0-RTT) [20], [13] is a negotiation mode that enables one entity (e.g., cloud user) to send data encrypted using a session key along with the session key negotiation message to a previously visited entity?To speed up the connections to the servers that users frequently used an AKA protocol supports 0-RTT.[4] Most of the existing AKA protocols (including those support 0-RTT) are designed in traditional PKI-based cryptosystem which suffers from the burdensome certificate management problem and the issues. [5] Certificateless public key cryptography is introduced to eliminate the certificate management problem in PKI-based cryptosystem. However, few certificateless AKA supports 0-RTT is proposed [16] with formal security analysis.

II.Literature Survey

Two lightweight privacy-preserving and public auditing protocols. Our protocols are ensures ononline/offline signatures, by which an end device needs to perform lightweight computations when a file to be outsourced is available. Simple security models [7], which catch the intuition behind known 0-RTT KE protocols; namely that the first key should remain indistinguishable from a random value, even if the second (resp. first) key is revealed. [19] We call this property strong key independence.

A secure and privacy-preserving communication scheme for the VC establishment and the data dissemination [9]. The proposed scheme allows a group of vehicles that are geographically close to each other to form a VC securely, anonymously and dynamically. [10], [12] The authors will deal with security problems in cloud computing systems and show how to solve these problems using a quantitative security risk assessment model named Multi-dimensional Mean Failure Cost.

III.Proposed system

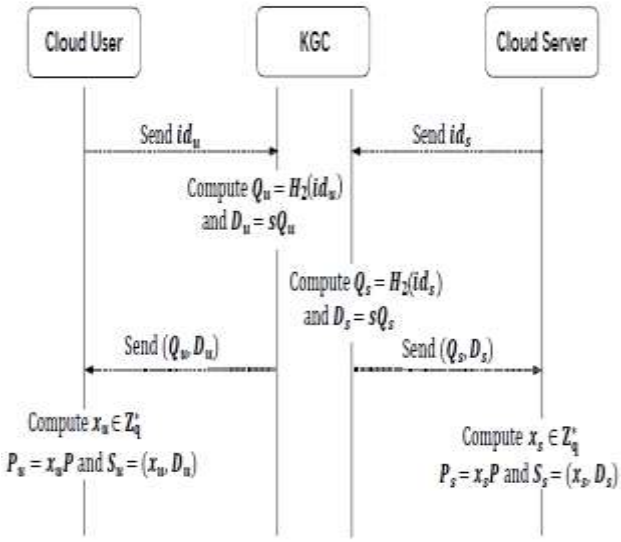


Fig: work flow of the system for finding the best approach

The work flow of this paper is described as follows:

1.Data owner uploads the data in cloud server.

Here, the data owner uploads their data in the cloud server.The data owner encrypts the data file and place in the cloud to provide security.TheData owner can manipulate the encrypted data file and set access privilege to that data file.

2.Cloud server manages the data storage.

The cloud server manages a cloud for data storage. The encrypted data files are storedin the cloud for sharing with data consumers. Consumers need to download the encrypted data files and decrypt them.

3. KDC to generate secrete key for the end users.

Key Distribution center who is trusted to store verification parameters and offer public query services for these parameters such as generating secret key based on the file and send to the corresponding end users. It is responsible for capturing the attacker.

4.End user access the encrypted data.

Here, the user can only access the data file with the encrypted key if the user has the privilege to access the file. Access privileges are set and controlled by data owner. Users may try to access data files either within their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. He is sending request to KDC to generate secret key and KDC will generate the secrete key and send to corresponding end user.

5.Unauthorized users

Unauthorized users tries to access the cloud. Those unauthorized users are called Attackers.

The performance of abovementioned algorithm is done with some of the stages as follows:

Case 1: Server(s) generates its private-public key pair as follows:

S-PartialPrivate-Extract: On input params, the master key s and a cloud server's identity ids submitted by S through a secure channel [14], the KGC computes S's partial private key $D_s = SQ_s$ and returns D_s to S, nwhere $Q_s = H2(id_s)$.

S-PrivatePublic-Extract: After that receiving the partial privatekey D_s of S from the KGC [18], S takes as inputparams, D_s, chooses a secret value $x_s 2 Z_q^*$, computesa public value $P_s = x_s P$ and S's private key$S_s = (x_s; D_s)$ and outputs public key $(id_s; P_s)$..

Case 2: User (u) generates his private-public key pair and seed asfollows:

U-PartialPrivate-Extract: On input params, s and acloud user's identity id_usubmitted by U via a securechannel, the KGC computes U's partial privatekey Du = SQ_uandmoves Du to U, where with$Q_u = H2(id_u)$.

U-PrivatePublic-Extract: After receiving the partial privatekey D_u of U from the KGC, U takes as inputparams, Du, chooses a secret value $x_u z_q$ and aseed $x_k \in \{0,1\}^*$, computes a public value $P_u = x_u P2$ f0; 1gand output private Key $S_u = (x_u; D_u)$, seed $x_k$and public key$(id_u; P_u)$.

The process of this algorithm as follows:

1. Registration and Establishment:

The main agenda is to provide a certificateless 0-RTT anonymous AKA protocol against bad randomness for cloud computing. As a 0-RTT protocol [8], we require that a cloud user has already visited a CSP, and stored the identity and public key of the CSP locally (which are about 512 bits). [3] , [21] For the first communication between a cloud user and a CSP, other heavier mutual

ISBN: 978-93-91303-04-04

authentication protocols should be used, which is beyond the discussion of this paper. However, this protocol only needs to be run once. This implies the cloud user has already authenticated the CSP [15]. Let U's private public key pair be (S_u= (x_u; Du); (id_u; P_u)), U's seed be x_k and S's private-public key pair be (S_s = (x_s; Ds); (id_s; P_s)).

2. Key Update:

To update the seed of U, U just needs to run the seed generation algorithm in U-PrivatePublic-Extract.[22] In order to update the private key U, U has to run both U-PartialPrivate- Extract and U-PrivatePublic-Extract.

3. Form Symmetric Bilinear Map toAsymmetric One:

The above certificateless 0-RTT anonymous AKA protocol is realized by using symmetric bilinear map [17], i.e., the bilinear map is defined to be ê:$G_1 \times G_1 \rightarrow G_2$. We note that a protocol implemented using asymmetric bilinear map [6], i.e., the bilinear map is defined to be ê: $G1 \times G'_1 \rightarrow G2$ with$G1 \neq G'1$, we show our protocol can be realized by using asymmetric bilinear map with minor modifications [11].

We need to change our System Setup phase andthe calculation method of the hash value Q_s. In the System Setup phase, the bilinear map is defined to be ê: $G_1 \times G'1 \rightarrow G2$, where the generator of G'_1 is $P' \in G'$. In addition, a new hash function H'_2:{0, 1}*$\rightarrow G'_1$ is chosen. The new system parameters is params: {q, G_1, G'_1, G_2, ê, P, P′, P_0, H, H_1, H_2, H'_2,H_3, H_4}. For Q_s, it is calculated by computing $Q_s = H'_2$ (id_s).

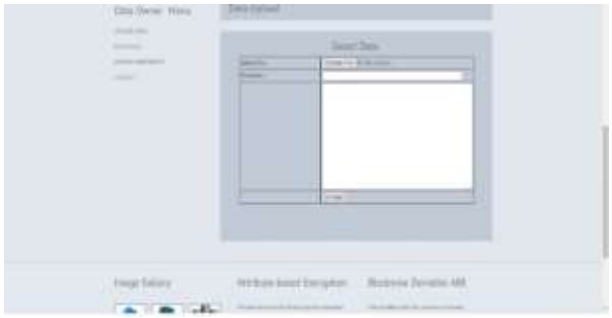
Comparison of the computational overheads as shown below:

T_E - Time to compute exponential operation
T_H - Time to compute Hash operation
T_M - Time to compute multiplication operation
T_P -Time to compute bilinear map operation

IV. Results

Fig 1: Home Page

Home page consists of Data owner, Cloud server, KDC, End user.

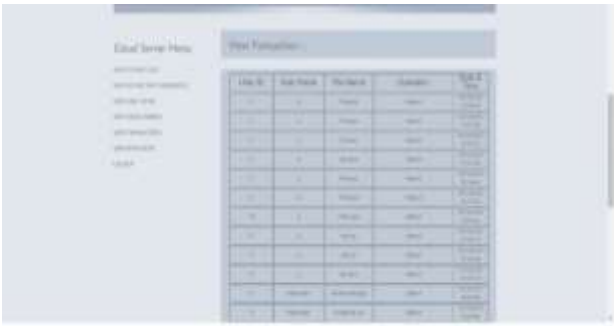


In this page, Data owner upload their encrypted data file.

	Cloud user	**Cloud server**	**Total**
AKA	T_M+3T_P+ 2T_E	2T_H+T_M+3 T_P+2T_E	2T_H+2T_M+6T $_P$+4T_E
User authentication key agreement	5T_M+2T_P +T_E	2T_H+5T_M+ 2T_P+T_E	2T_H+10T_M+4 T_P+2TE
Certificateless key agreement protocol	4T_M+2T_P	2T_M+2T_P	6T_M+4T_P
Cryptography	2T_E	2T_E	4T_E
0-RTT protocol	T_H+5T_M+T $_P$	T_H+3T_M+T $_P$	2T_H+8T_M+T_P

ISBN: 978-93-91303-04-04

The data is successfully encrypted in cloud server, now user can access the encrypted data file with the help of KDC.



In this page, the data owner can view the file transactions of their uploaded files and also can view the end userstransaction when they access their files.

V.Conclusion

Our team has proposed an efficient certificateless 0-RTT anonymous AKAprotocol against bad randomness for cloud computing. Itsolved the challenges like reducing connection delay, eliminatingcertificate management problem, enhancing userprivacy and avoiding bad randomness facing in cloud computing.Simulation the results show that our protocol has verylow latency and enables fast secure and anonymous channelestablishment for cloud computing.

References

[1] M. Jouini and L. Rabai, "A security framework for secure cloud computing environments," in Cloud Security: Concepts, Methodologies,Tools, and Applications, 2019, pp. 249–263.

[2] J. Li, L. Zhang, J. Liu, H. Qian, and Z. Dong, "Privacy-preservingpublic and auditing protocol for low-performance end devices incloud," IEEE Transactions on Information Forensics and Security,vol. 11, no. 11, pp. 2572–2583, 2016.

[3] H. Krawczyk and H. Wee, "The OPTLS protocol and TLS 1.3," in2016 IEEE European Symposium on Security and Privacy, 2016, pp.81–96.

[4] B. Hale, T. Jager, S. Lauer, and J. Schwenk, "Simple securitydefinitions for and constructions of 0-rtt key exchange," in 15thInternational Conference on Applied Cryptography and Network Security,2017, pp. 20–38.

[5] L. Zhang, "Key management scheme for secure channel establishmentin fog computing," IEEE Transactions on Cloud Computing,doi: 10.1109/TCC.2019.2903254

[6] G. Han, X. Miao, H. Wang, M. Guizani, and W. Zhang, "CPSLP:a cloud-based scheme for protecting source location privacy inwireless sensor networks using multi-sinks," IEEE Transactions onVehicular Technology, vol. 68, no. 3, pp. 2739–2750, 2019.

[7] C. A. Ardagna, M. Conti, M. Leone, and J. Stefa, "An anonymousend-to-end communication protocol for mobile cloud environments,"IEEE Transactions on Services Computing, vol. 7, no. 3, pp.373–386, 2014.

[8] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Socialphishing," Communications of the ACM, vol. 50, no. 10, pp. 94–100,2007.

[9] "Icloud Data Breach: Hackingand celebrity photos." [Online].Available: s/2014/09/02/iCloud-data-breach-hacking-and-nude-celebrity-photos/#4194819e2de7

[10] L. Garber, "Denial-of-service attacks rip the internet," Computer,vol. 33, no. 4, pp. 12–17, 2000.

[11] Q. Pei, B. Kang, L. Zhang, K. Choo, Y. Zhang, and Y. Sun, "Secureand privacy-preserving 3D vehicle position schemes for vehicularad hoc network," EURASIP Journal onWireless Communicationsand Networking, vol. 2018, no. 1, p. 271, 2018.

[12] E. Rescorla, "The transport layer security (TLS) protocolversion 1.3," no. RFC 8446, 2018. [Online]. Available:https://www.rfc-editor.org/rfc/pdfrfc/rfc8446.txt.pdf

[13] "Introducing zero round trip time resumption (0-RTT)."Available:https://blog.cloudflare.com/introducing-0-rtt/

[14] S. S. Al-Riyami and K. G. Paterson, and the protocol is "Certificateless public keycryptography," in 9th International Conference on the Theory andApplication of Cryptology and Information Security, 2003, pp. 452–473.

[15] M. Alt, W. Barto, A. Fasano, and A. King,"Entropy poisoning from the hypervisor,". Available:https://pdfs.semanticscholarorg /06cd/9aacf17a9c13fbb7e524a4e48e8edc5 6457.pdf

[16] D. Bernstein, T. Lange, and R. Niederhagen, "Dual EC: A standardizedback door," in The New Codebreakers: Essays Dedicated toDavid Kahn on the Occasion of His 85th Birthday, 2016, pp. 256–281.

[17] "DRBG validation lists." and Available: http://www.fbcoverup.com/docs/library/2015-10-30-NIST-DRBG-Validation-List-updated-Oct-23-2015.

[18] W. Diffie and M. Hellman, "New directions in cryptography,"IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654,1976.
[19] V. Padmanabhan and the other J. Mogul, introduce the "Improving http latency," ComputerNetworks and ISDN Systems, vol. 28, no. 1&2, pp. 25–35, 1995.
[20] "Making the internet safer and faster with TLS1.3.". Available: https:// un used-css.com/blog/making-the-internet-safer-and-faster-with-tls-13
[21] J. Roskind, QUIC: Multiplexed stream transport over UDP, Google,2013.
[22] L. Zhang, "Provably secure certificateless one-way and two-partyauthenticated key agreement protocol," in 15th International Conferenceon Information Security and Cryptology, 2012, pp. 217–230.

ISBN: 978-93-91303-04-04

IOT BASED WEATHER MONITORING SYSTEM

Dr. Y.Pavan Kumar [1] Saiteja Akula [2] Bharath Kumar M [3] Bhargav Rao S [4]
Associate Professor[1], UG Scholar[2, 3, 4]
[1, 2, 3, 4] Department of CSE, Geethanjali Institute of Science and Technology, Nellore,A.P

Abstract: The technology used here is Internet of Things (IoT), which is an advanced and efficient solution forconnecting the things to the internet and toconnect the entire world of things in anetwork. Here things might be whatever like electronic gadgets, sensors and automotive electronic equipment. The system proposed here is solution formonitoring the weather conditions at aparticular place and make the informationvisible anywhere in the world. The systemdeals with monitoring and keeps track of temperature, humidity. The system displays these readings in real time on a display. It also keeps track of historical information on time basis. This data will be displayed on LCD and sends theinformation to the web page and then plot the sensor data as graphical statistics. The data updated from the implemented system can be accessible in the internet from anywhere in the world.

Keywords: Iot; Lcd; Temperature; Humidity; Sensor;

1. INTRODUCTION

The Internet of Physical Things is a network where all physical objects connect to the Internet via network equipment and exchange data. The Internet of Things can be managedremotely via an existing network infrastructure. IoT is a good, highlyintelligent technology that reduces human effort and allows easy access to physical devices. This method also has a special control function, which allows you to controldevices without any interaction with people. Simply put, this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones,

coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. Internet

of Things represents a general concept for the ability of network devices to sense and collect data from the world aroundus, and then share that data across the Internetwhere it can be processed and utilized for

arious interesting purposes. All kinds of ordinary household gadgets can be modified to work in an IoT system. Wi-Fi network adapters, motion sensors, cameras, microphones and other instrumentation can be embedded in these devices to enable themfor work in the Internet of Things. Home automation systems already implement primitive versions of this concept for things like light bulbs, plus other devices like wireless scales and wireless blood pressure monitors that each represent early examples of IoT gadgets. The "Internet of Things" is awork of art that became clear in 2009. The Internet of Things is actually changing our world. It helps to renew our life and society as a whole, creating different things that make our lives run smoothly. By 2020, an estimated 50 billion devices will beconnected to the Internet and networks and the market will be $14 trillion. The Internet of Things is a growing theme of certain things, social and monetary, linked to gigantic dimensions. Customer items, different types of goods, cars and trucks,modern and modern spare parts, sensors and other conventional products are combined with the Internet and the exceptional data search capabilities that promise to change the way we work, live and play. The impact of the Internet of Things on the Internet of Things and the economy is significant: according to some estimates, the number of IoT devices will reach $100 billion by 2025 and total revenues will exceed $11 trillion.

2. LITERATURE SURVEY

This paper is done by N. Gahlot, V. Gundkal, S. Kothimbire, and A. Thite in the year 2015.Zigbee is used for high-level communication protocols used to create

personal area networks with small, low- power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection. Here for the weather monitoring the parameters used are temperature humidity and rain level sensor. The data is being sensed in real time and displayed in the real time in the lcd screen and in the website without any previous datapresent.

3. PROPOSED SYSTEM

The main objective of this project is to originate electronic device or network that can capture and restore temperature and humidity and after that send data to the cloudor website for its analysis. Here we can use the Arduino Uno as a microcontroller for thesimple brain of the system. When we use theArduino as a microcontroller, we need a Wi-Fi module to establish your Internet connection. Temperature humidity sensors are used at a certain location, must be integrated into the system. The sensor continuously monitors temperature changes and sends data to the microcontroller. The microcontroller transfers the data for its storage and visualization to cloud. We can also use IOT platforms such as ThingSpeak IoT to collect data into the cloud for analysis.

Figure1: Welcome Screen of Project

The power requirements for oursystem (sensors and boards) are much less compared to the existing instruments in the market hence enabling us to use solar cells aspower supply. This not only cuts down on cost but allows us to leave the monitoring system in remote, areas where power is not easily available, for long periods of time. Addition of solar panels also helps our designbe eco-friendly. The data uploaded to the webpage can easily be accessible from anywhere in the world. The data gathered in these web pages can also be used for future references. Unlike the existing system where data has tobe physically transferred. Due to the presenceof fewer moving parts less amount ofmaintenance will be needed cutting down onmaintenance charges.

5. RESULTS

Step1: When the code is dumped and all the components are connected, when switched on the power you will see a message “WELCOME” on the LCD screen.

Step2: Then automatically all the components such as the sensors (Temperature and Humidity), modules such as Wi-Fi module and other operationalamplifiers such as LM358 are will be initialized.

Step3: Especially when the Wi-Fi module is connected to the internet, it shows a message “CONNECTED”.

ISBN: 978-93-91303-04-04

Figure2: System Connected to Internet

Step4: Then the process starts, the sensors start to sense the change in the environment where the project is placed.

Step5: Then the data that is sensed is converted from the analog data to digital data and will be displayed real-time on the LCD screen that is placed on the project.

Figure3: Realtime Display of Temperature and Humidity

In the above figure you can see the real time temperature and the humidity that is been sensed by the sensors in the environment which is displayed on the LCD screen attached on the project. “H” represents the humidity that is present in the weather that the project is placed. Humidity shows “ON” when it senses the humidity >0 (greater than zero as I written in the code), Then the number “2” is displayed in the second line of the LCD screen. Which states that humidity is sensed and its ready to be uploaded into the ThingSpeak platform.

Figure 4: Uploading of Humidity Data

In the above image you can see the counter as “11” where it’s the timer which is being uploaded to the cloud, After the timer ends, ifHumidity is sensed then automatically number”2” is displayed and timer starts and this process continues until the power is on. We put a timer of 25 seconds in this period the data is transmitted via serial communication between the Wi-Fi module and the cloud.

Step6: Now after uploading the humidity value to the cloud again the sensors start sensing the change in the environment and ready to be displayed, since in India average temperature is 30 degrees Celsius, we put a condition that if temperature is above the 35degree Celsius its uploaded to server.

Figure 5: Sensing the Temperature

In the above figure you can see the real time temperature is been sensed. “T” represents the temperature. Current temperaturerecorded is 43 degrees Celsius. Humidity shows “ON” when it senses the temperature
>35 (greater than 35 as I written in the code),Then the number “1” is displayed in the second line of the LCD screen. Which states that change in temperature is sensed which satisfies the condition so that its ready to be uploaded into the ThingSpeak platform.

In the above image you can see the counter as“13” where it’s the timer which is beinguploaded to the cloud, in this period the data is transmitted via serial communicationbetween the Wi-Fi module and the cloud.

6. CONCLUSION

Here we learnt that how present system is better and also more efficient than the other systems. It is exceptionally compatible. It reduces human efforts. This terminate that present project work is a huge success and will provide a considerable way for saving weather

ISBN: 978-93-91303-04-04

parameters of real time and will help farmers, industries, normal people as well asothers whose daily life is related with weatherand its parameters. It can be used to getrequired information about for each or particular area for many years. The collectedinformation will used to determine the best conditions required for plants to grow if we talk about agriculture and the farmer canmodify the environment conditions which is more suitable for the plan growth.

7. REFERENCES

[1] N. Gahlot, V. Gundkal, S. Kothimbire, and A. Thite, "Zigbee based weather monitoring system," Int. J. Eng. Sci. IJES, vol. 4, pp. 61-66, 2015.

[2] S. Pooja, D. Uday, U. Nagesh, and S. G. Talekar, "Application of MQTT protocol forreal time weather monitoring and precision farming," in 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques(ICEECCOT), 2017, pp. 1-6

[3] K. Krishnamurthy, S. Thapa, L. Kothari, and A. Prakash, "Arduino based weather monitoring system," International Journal of Engineering Research and General Science, vol. 3, pp. 452-458, 2015.

[4] Y. Wang and Z. Chi, "System of wireless temperature and humidity monitoring based

on Arduino Uno Platform," in 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), 2016, pp. 770-773.

[5] Nashwa El-Bendary, Mohamed Mostafa M. Fouad, Rabie A. Ramadan, Soumya Banerjee and Aboul Ella Hassanien, “Smart Environmental Monitoring Using Wireless Sensor Networks”, K15146_C025.indd, 2013.

[6] S. Devi Mahalakshmi, Rajalakshmi.P, “IOT Based Crop-Field Monitoring and Irrigation automation system using the Arduino micro controller”. Mepco Schlenk Engineering College (Autonomous).

[7] R. K. Kodali and A. Sahu, "An IoT based weather information prototype using WeMos," in 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), 2016, pp. 612-616.

[8] Kamilaris, A., Gao, F., Prenafeta-Boldú, F.X. and Ali, M.I., 2016, December. Agri- IoT: A semantic framework for Internet of Things-enabled smart monitoringapplications. In Internet of Things (WF-IoT),2016 IEEE 3rd World Forum on (pp. 442- 447). IEEE

[9] C. Xiaojun, L. Xianpeng, and X. Peng, "IOT-based air pollution monitoring and forecasting system," in 2015 International Conference on Computer and Computational Sciences (ICCCS), 2015, pp. 257-260.

[10] D. Amaxilatis, O. Akrivopoulos, G. Mylonas, and I. Chatzigiannakis, "An IoT- based solution for monitoring a fleet of educational buildings focusing on energy efficiency," Sensors, vol. 17, p. 2296, 201

ADVANCED ROBOT FOR DEFENCE APPLICATION USING IOT

Ms. Sree Lakshmi P [1] Bhavitha NC [2] Ramya C [3] Navya Sree K [4] Malini P [5] Dhahaseem SK Md [6]
Associate Professor [1] , UG Scholar [2,3,4,5,6]
[1,2,3,4,5,6] Department of ECE, Audisankara College of Engineering For Women, Gudur, Andhra Pradesh.

Abstract:

A Robot is a mechanical or virtual artificial machine. In practice, it is usually an combo ofelectrrical &mechanical system which, by its appearance or movements, tells that a sense that it has its own capable of doing work own. The word robot can refer to both physical &virtual software agents, but the later are usually referred to as Robots. There is no consensus on which machines qualify as robots, but there is general agreement among experts and the public, that robots tend to do some or all of the following: move around, operate a mechanical arm, sense and manipulate their and environment, and exhibit intelligent behavior, especially behavior which mimics humans or animals.

In today's advanced technology, robotics is fastest growing and very interesting field. ROBOT has various input and output to sense the environment and take appropriate action in order to efficiently complete that task . It has an infrared sensor which is used to sense the obstacles coming in between the path of ROBOT, Camera to capture the pictures of the environment and actuator like motors, grippers and arms to perform actions of movements which are necessary in the operation. With the development and research of technology, scientist has come up with invention of military robots. This makes soldier's life more secure on war field by having a protection to their life.. Military robots are used to perform various risky task like monitor war field, diffuse live unexploded bombs, detect landmines and shoot enemies and many more such hazardous things. Nowadays, many countries take the helps of these robots to take dangerous jobs. These military robots appointed with the integrated systems like sensors, gripper, weapons, cameras and actuators. Depending on our need we are having the purpose of robot whch it comes in different shapes and features.

This project is built with Arduino uno micro controller, this project is placed on a robot base, which moves forward, backward, left and right, this robot base is mounted with an inductive metal detector. When any metal is detected on its way, then a high signal is sent to the micro controller which switches ON the buzzer. The entire robot controlling is done through the wifi module and the monitoring of robot movements is done through the website using IOT.

Index Terms –Robot, Arduino UNO, wifi Module, IOT

INTRODUCTION :

The robot is basically electro-mechanical machine or device that is controlled either by computer program or with electronic circuit to perform variety of physical tasks. With the gradual development in technology, scientists come up with new ideas and inventions of different versatile robots. In the today's life robots are becoming indispensible part of human life [1]. The robotic technology also provides automation in hospital, office and factory and many other applicaions. Besides automation, this technology also implemented in Defense forces,

17. BACK GROUND WORK

Entertainment, Space exploration, Security systems and many dangerous mission execution systems [3]. As the terror always remains the India's first enemy so, the robots are going to save human life. Countries like India are still facing and confronting with regular threats from terrors and losing many of the lives of the soldiers. Both Kashmir and Mumbai terror attacks have consummated that as far as possible, the future of warfare will be handled by robots and unmanned machines to protect human life [3]. Currently, the Indian Army has Daksh Military robot to combat

in battle field. As the technology proliferate rapidly in automation field by incorporating Military Robots as Soldiers in war field to reduce grievance and demise in war fields and used in versatile fields [2]. DTMF is known as Dual Tone Multi Frequency which is generated by cell phone when any key is pressed. When any key is pressed then it make connection between the tones of Rows and Columns which will generate dual tone frequency. This dual tone
is used to determine which key is pressed in that particular row or column [4]. In defense areas, Robot are usually miniature in size, so they are enough capable to enter in tunnels, mines and small holes in building and also have capability to survive in harsh and difficult climatic conditions for long time without causing any harm to the mankind[2]. Military robots were designed from last few decades for the mankind of the soldiersand for their welfare. But still there are some problems in earlier developed military robots in various aspects.

18. PROPOSED SYSTEM

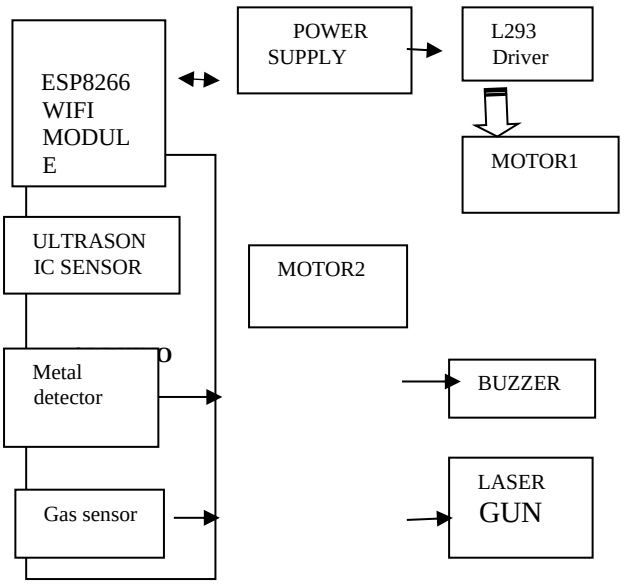


FIG. 1.BLOCK DIAGRAM

HARDWARE REQUIREMENTS

- Arduino Uno
- Ultrasonic Sensor
- Esp8266 Wifi Module
- Laser Gun
- L293d Driver Circuit
- Power Supply
- Dc Motor
- Lcd
- Proximity Sensor (Metal Detector)
- Buzzer.

ARDUINO

The Arduino Uno is a microcontroller board based on the ATmega328. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button,which can be used as the heart of the project

It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started and dump your code into this very easily.

The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter and continues the process

SOFTWARE REQUIREMENTS

- ARDUINO IDE
- C-LANGUAGE

SOFTWARE DESCRIPTION

Arduino Software (IDE)

The Arduino Integrated Development Environment - or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino and Genuine hardware to upload programs and communicate with them and do the interfacing between them and helps in the final output.

ISBN: 978-93-91303-04-04

PERFORMANCE&RESULTS

Fig 2. Hardware kit

Fig. 3. Controlling It Through The IOT With Displaying Of The Parameters.

CONCLUSION

When we consider military robots today, there has been a huge development as compare to those robots which are used in earlier times. Today, military ground robots & unmanned vehicles are used worldwide for different purposes. However, the significant growth of the current military robots comes as the nature of combat changes in every region while the globally integrated enterprise replaces nationalistic dominance. It can be said that military robot automation of the defense process is the next wave of military evolution. This proposed system gives an exposure to design a simple robot that can be used to do multifunction in defense and can save soldier lives. Manual control is also employed to control the robot from the control room which is located far away from the border area as the machine always don't know the decision making in every critical situation. The system uses non-commercial WIFI module for wireless communication, since this provides access to the yet unpublished specifications and permission to create products for market using the specifications. Our system is aimed towards the wifi module up to 300 meters distance. In future we can increase the distance depending on our necessities. The proposed system is focusing on the welfare infantry to minimize the causalities to a great extent and mainly to have a security for the soldiers during their war field. This also helps in remote bomb detection and also we can monitor the surroundings through the camera in web page and so that we can move according to it.

6. REFERENCES

[1] Robotic Systems Joint Project. (February 2012). OfficeUnmanned ground systems road map by Materiel Decision Authority (MDA): Macro USA, McClellan, CA.

[2] Shanker, N. M., & Yadav, A. P., International Journal of Computer Science & Communication,. RF controlled terrorist fighting robot by. Abhinav Kumar Singh, 1(1, January–June), 109–112.

[3] Chandramouli, G. (2009, April 22–24). 7th Sense: A Multipurpose Robot for Military by L.Srinivasavaradhan. MR. a G.Maniprashanna MEMSTECH, 2009, Polyana - Svalyava (Zakarpattya), Ukraine.

[4] Hotzj, J., & Kitzmiller, R. Continued testing of the Cannon Caliber

electromagnetic Gun System (CCEMG) By: M.D. Werstc.E. Penneyt. IEEE Transactions on Magnetics, 9th EML Symposium, Edinburgh, Scotland, May 1998. 5, 35(1, January), and Pp (pp. 388–393).

[5] Desidoc. (2007). Landmine detection technologies to trace explosive vapour detection technique, C.Kapoor1 and G. K. Kannan. Defense Science Journal, 57(6, November), 797–810

[6] Naghsh, M., Gancet, J., & Tanoto, A. (August 1–3, 2008). Analysis and design of human–robot swarm interaction in firefighting by amir. Chris roast. Proceedings of the 17th IEEE International Symposium on Robot and Human Interactive Communication. Technische Universität München.

[7] Ocari: Optimization of Communication for Ad Hoc Reliable Industrial Network stuan Dang* PhD Member IEEE. 9. Catherine Devic* Et Al***EDF (Electricité De France) R&D – Step. 10. Department of control Systems & Information Technologies Group France 1-4244-9701-0/06/$20.00 © 2008 IEEE.

[8] http://www.Robotnik.Es/Automation/Productos/Agvs/Robotnikp01-E.Html

[9] http://www.armyofrobots.com

[10] .http://www.microcontroller.com. www.microchip.com/pic

Performance Comparison of Different Classification Algorithms for Crime Prediction

Sk. Asiff [1]K.Sarvani[2] Ch. Vyshnavi[3] Ch. Bhavana[4] K.Sowmya[5] Associate Professor[1], UG Scholar[2,3,4,5]

[1,2,3,4,5]DepartmentofCSE,GeethanjaliInstituteofScienceandTechnology,Nellore, AndhraPradesh.

ABSTRACT

Crime prediction is of great significance to the formulation of policing strategies and implementation of crime prevention and control. Machine learning is the current mainstream prediction method. The main objective of this project to make a comparative study of different machine learningclassificationalgorithm.Suchas Linear Regression, K-Nearest Neighbor, Support Vector Machine, Naive Bayes, Decision Tree, Random Forest forCrime Prediction. Results obtained show that Random Forest performs better than remainingalgorithms.

KEYWORDS

Machine Learning, Crime Hotspots, Random Forest, K-Nearest Neighbor, Naive Bayes, Logistic Regression,Decision Tree, Support VectorMachine.

INTRODUCTION

The research on crime prediction currently focuses on two major aspects: crimeriskareapredictionandcrimehotspot prediction.

Thecrimeriskareaprediction,basedonthe relevant influencing factors of criminal activities, refers to the correlation between criminal activities and physical environment, which both derived from the “routine activitytheory”.

Many studies have carried out empirical research on crime prediction indifferenttime periods, combining

demographic and economic statistics data, land e data, mobile phone data and crime history data.
The research on crime prediction currently focuses on two major aspects: crime risk area prediction [2], [3] and crime hotspot prediction [4], [5]. The crime risk area prediction, based on the relevant influencing factors of criminal

Machine learning algorithms have gained popularity. The most popular Neighbor(KNN), random forest algorithm, support vector machine Some compared the linear methods of crimetrendprediction[14],somecompared
Bayesian model and BP neural network [15], [16], and others compared the spatiotemporal kernel density method with the random forest method in different periods of crime prediction [12]. Among these algorithms, KNN is an efficient supervised learning method algorithm [17], [18]. SVM is a popular machine learning model because it can not only implement classification and regressiontasks.

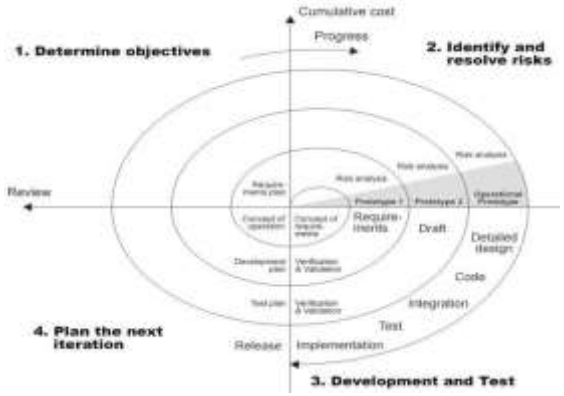
LITERATURE SURVEY

The focus of crime hotspot predictionistoforecastfutureconcentration of criminal events in a geographical space. Theoretical criminology provides the necessary theoretical basis. Specically, several related criminological theories not only provide guidance for us to understand the important inuence of location factors in the formation and aggregation of criminal events, but also provide a basic mechanism forthepolicetouseinformationofcrimehot spots for crime prevention or control. It mainly includes routine activity theory, rational choice theory, and crime patterns theory. These three theories are generally considered as the theoretical basis of situational crime prevention.

Routine activity theory [30]was jointly proposed by Cohen and Felson in 1979, and has now been further developed through integration with other theories. This theory believes that the occurrence of most crimes, especially predatory crimes, needs the convergence of the three elements including motivated offenders, suitable targets, and lack of ability to defend in time and space. Rational choice theory [31] was proposed by

space" through daily activities.

SYSTEM ANALYSIS



To provide flexibility to the users, the interfaces have been developed that are accessiblethroughabrowser.TheGUI'Sat the top level have been categorizedas

1. Administrative userinterface.
2. The operational or generic user interface.

The 'Administrative user interface' concentrates on the consistent informationthat is practically, part of theorganizational activities and which needs proper authenticationforthedatacollection.These interfaces help the administrators with all the transational states like Data insertion, Data deletion and Date updating along with the extensive data searchcapabilities.

The 'operational or generic user interface' helps the end users of the system in transactions through the existing data and SYSTEM DESIGN

The most creative and challenging phaseof thelifecycleissystemanddesign.Theterm design describes a final system and the process by which it is developed. It refer to the technical specifications that will be applied in implementation the candidate system. The design may be defined as "the process of applying various techniques and principles for the purpose of defining a device, a process or a system in sufficient details to permit its physicalrealization".

The design's goal is how the output is to be producedandinwhatformatsamplesofthe output and input are also presented.Second input data and database files have tobe designed to meet the requirements of the proposed output. The processing phase is handled through the program construction and testing. Finally details related to justification of the system and an estimate oftheimpactofthecandidatesystemonthe users and the organization are documented and evaluated by management as a step towardimplementation.

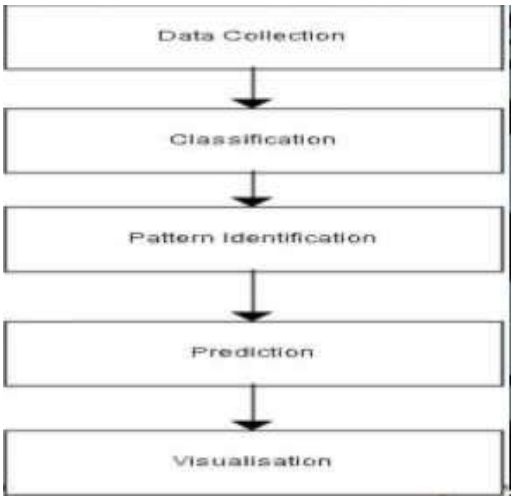
The importance of software design can be stated in a single word **"Quality".** Design provides us with representation of software that can be assessed for quality. Design is the only way that we can accurately

PRESENT WORK

In this project, random forest algorithm, KNN algorithm, Support Vector Machine algorithm**,**DecisionTree algorithm, Logistic Regression algorithm ,Naïve Bayes algorithm used for Crime Prediction

First, historical crime data alone are used as input to calibrate the models. comparison would identify the most effective model.

Second,builtenvironmentdatasuchasroad network density and poi are added to the predictive models as covariates, to see if prediction accuracy can be further improved.



ISBN: 978-93-91303-04-04

19. ALGORITHMS

LogisticRegression

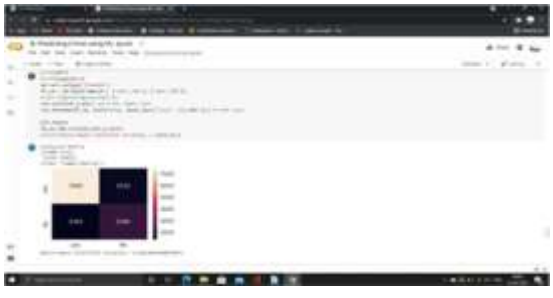
In statistics, the logistic model (or logit model) is used to model the probability ofa certain class or event existing such as pass/fail,win/lose,alive/dead,healthy/sick.

This can be extended to model several classes of events such as determining whether an image contains a cat, dog, lion, etc.

NAÏVE BAYE'S

Naïve Bayes is a simple technique for constructing classifiers:models that assign class labels to problem instances,represented as vectors of feature values,where the class labels are drawn from some finite set.

There is not a single algorithm for training such classifiers,but a family of algoriyhms based on a common principle:all naïve bayes classifiers assume that the value of a particular feature is independent of the value of any other feature



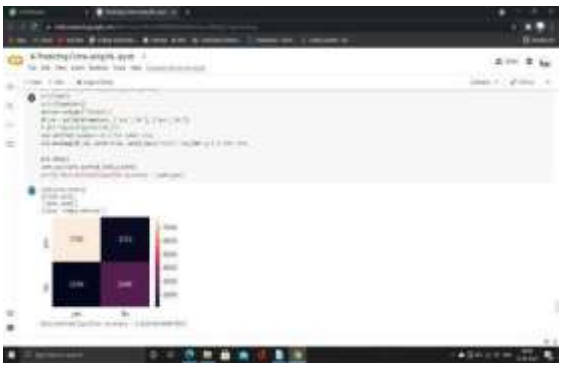
K- Nearest Neighbor

K-NN is a type of classification where the

function is only approximated locally and all computation is deferred until function evaluation. Since this algorithm relies on distance for classification, if the features represent different physical units or come in vastly different scales then normalizing the training data can improve its accuracy dramatically.

Support Vector Machine

In machine learning, support-vector machines (SVM's, also support-vector networks) are supervised learning models with associated learning algorithms the analyze data for classification andregression analysis.



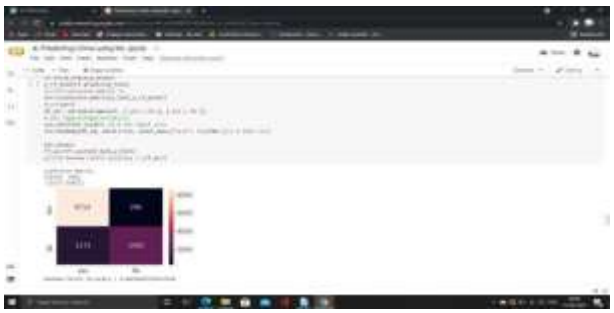
SVM maps training examples to points in space so as to maximize the width of thegap between the two categories. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall.

Random Forest

Itgeneratesmultidecisiontreesfromwhicheach decision tree uses a part of data sample and predicts the result. Then the result which was achieved by maximum number of trees is consideredasthefinalprediction.

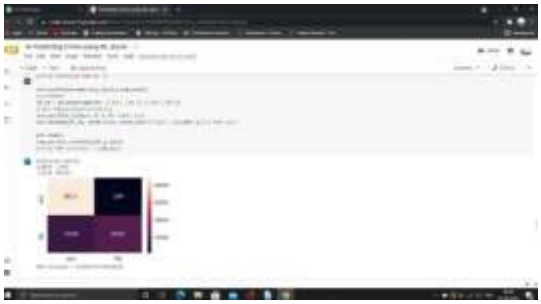
Random forest is a Supervised Learning algorithm which uses ensemble learning method for classification and regression. Random forest is a bagging technique and the trees in random forests run inparallel.

ISBN: 978-93-91303-04-04



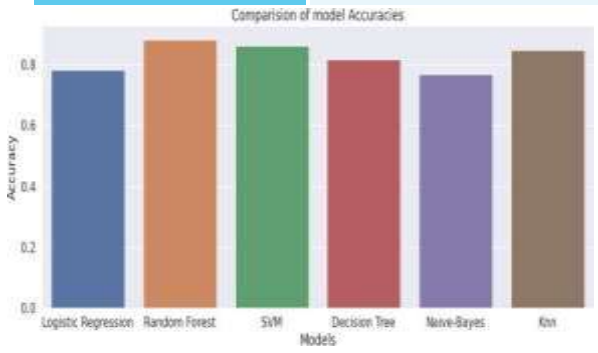
Decision Tree

Trees are constructed through analgorithmic approachthatidentifieswaystosplitthedata set based on different conditions It is one of the most widely used practical methods for supervisedle



RESULT

Algorithm	Accurate value
Logistic Regression	0.78196864804647
Random Forest	0.88302697541179
SupportVector Machine	0.86273573645261
K-Neighbors Classifier	0.81634439404790
NaiveBayes Classifier	0.81634439404790
DecisionTree Classifier	0.81634439404790



Comparision of above algorithms Random Forest gives accurate output.So Random Forest is the best algorithm for Crime Prediction.

CONCLUSION

In this project,six machine learning algorithms are applied to predict the occurance of crime hotspots in a town real dataset can be taken from Kaggle.The following conclusions are drawn:The prediction accuracies of the random forest model are better than those of the other models. It can be better extract the pattern and regularity from historical crime data, The addition of urban built environment covariates further improves the prediction accuracies of the Random Forest model. The prediction results are better than those of the original model using historical crime data alone.

ISBN: 978-93-91303-04-04

Secure and Efficient Search Scheme for Encrypted Images using KNN Search in Cloud Environment

K.Sree Lakshmi[1] K.Jyothsna[2] K.Sai Lekhana[3] V.Sai Nithisha[4]K.Sandhya Rani[5]

Assistant Professor[1], UG Scholar[2, 3, 4, 5]

[1, 2,3,4,5]Department of CSE, Geethanjali Institute of Science and Technology, Nellore,

Andhra Pradesh.

ABSTRACT

The Content-Based Image Retrieval(CBIR) technique Has attracted much attention from many areas (i.e., cloud computing). Although existing privacy-preserving CBIR schemes can guarantee image privacy while supporting image retrieval.To address these challenging issues , in this project we present a similarity search for Encrypted Images in secure with a tree-based data structure and Assymetric scalar product preserving encryption (ASPE) , which Implemented faster search than linear search.First the feature descriptors extracted by the Convolutional Neural Network (CNN) models are used to improve search accuracy . Next, an encrypted hierarchical index tree by using K-means clustering based on Affinity Propagation(AP) clustering is devised , which can improve search efficiency.Then a limited key-leakage k-Nearest Neighbour(KNN) algorithm is proposed to protect key from being completely leaked to untrusted image users.

KEYWORDS

Content-Based Image Retrieval,K-Nearest Neighbour, Search accuracy, Search Efficiency

1.INTRODUCTION

By the rapid development and popularization of cloud computing, many people enjoyvariousconveniences brought by cloud services, such as storing images on the cloud. However,directly outsourcing images to the public cloud inevitably raises privacy concerns. Once themassive images (e.g., patients medical images) containing highly sensitive information havebeen leaked to unauthorized entities, it will incur serious

consequences or unnecessary trouble. Encryption mechanism can alleviate image data security and privacy concerns to someextent, but it invalidates the Content-Based Image Retrieval (CBIR) technique over ciphertext,and even causes other concerns Fortunately, various schemes related to privacypreserving CBIR have been studiedlike[1]–[8]. in practice, However these schemesStillface many challenges (i.e., low search accuracy, low search efficiency, key leakage, etc.). Specifically, schemes [1], [2], [3], [5] directly distributed keys to users,leading to the risk of image users leaking keys, schemes [3], [5] sacrificed accuracy to improve efficiency, and schemes [1], [4], [6], [7], [8] brought a lot of overhead to achieve high security.

There are also works [9], [10] that combine global features and local features with certainweights in order to form new features or apply Convolutional Neural Network (CNN) modelmimicking human visual cognition to extract feature vectors,which achieve acceptable accuracy. For the later, the similarity between images is measured by Euclidean distance,Cosine distance, Hamming distance, and Jaccard similarity coefficient. Especially, AsymmetricScalar-productPreserving Encryption (ASPE) algorithm [11] while using random numbers and matrices to encrypt feature vectors can calculate the Euclidean distance of highdimension space more accurately. At the same time, other works [4], [12] using Secure Multiparty Computation (SMC), Homomorphic Encryption (HE) to calculate Euclidean distance can also improve search accuracy.

2.RELATEDWORKS

A.Content-based multi-source encrypted image retrieval in clouds with privacy preservation. In this paper, we propose a secure CBIR scheme that supports Multiple Image owners with Privacy Protection (MIPP). We encrypt image features with a secure multi-partycomputation technique, which allows image owners to encrypt image features with their own keys. This enables efficient image retrieval over images gathered from multiple sources, while guaranteeing that image privacy of an individualimage owner will not be leaked to other image owners. We also propose a new method for similarity measurement of images that can avoid revealing image similarity

information to the cloud. Theoretical analysis and experimental results demonstrate that MIPP achieves retrieval accuracy and efficiency simultaneously, while preserving image privacy.framework is efficient and feasible for practical applications shows that the proposed image retrievalvectors.

B.fast nearest neighbor search scheme overoutsourced encrypted medical image.

Medical imaging is crucial for medical diagnosis, and the sensitive nature of medicalimages necessitates rigorous security andprivacy solutions to be in place. In a cloud-based medical system for Healthcare Industry 4.0, medical images should be encrypted prior to being outsourced. However, processing queries over encrypted data without first executing the decryption operation is challenging and impractical at present. In this paper, we propose a secure and efficient scheme to find the exact nearest neighbor over encrypted medical images. Instead of calculating the Euclidean distance, we reject candidates by computing the lower bound of the Euclidean distance that is related to the mean and standard deviation of data. Unlike most existing schemes, our scheme can obtain the exact nearest neighbor rather than an approximate result. We, then, evaluate our proposed approach to demonstrate its unity.

C .Search in my way: Practical outsourced image retrieval framework supporting unshared key. The traditional privacy-preserving image retrieval schemes not only bring large computational and communication overhead butalso cannot well protect the image and query privacy in multi-user scenarios. To solve the above problems, we first propose a basic privacypreserving content-based image retrieval (CBIR) framework which significantly reduces storage and communication overhead compared with the previous works.Furthermore, we design a new

efficient key conversion protocol to support unshared key multi-owner multi-user image retrieval without losing search precision..Moreover, our framework supports unbounded attributes and can trace malicious users according to leaked secret keys, which significantly improve the usability of multi-source data sharing.Strict security analysis shows that the user privacy and outsourced data security can be guaranteed during the image retrieval process, and the performance analysis using real-world dataset.

D. Towards privacy preserving content -based image retrieval in cloud computing.

Content-based image retrieval (CBIR)applications have been rapidly developed along with the increase in the quantity, availability and importance of images in our daily life. However, the wide deployment of CBIR scheme has been limited by its the severe computation and storagerequirement. In this paper, we propose a privacy-preserving content-based image retrieval scheme, which allows the data owner to outsource the image database and CBIR service to the cloud, without revealing the actual content of the database to the cloud server. Local features are utilized to represent the images, and earth mover's distance (EMD) is employed to evaluate the similarity of images. The EMD computation is essentially a linear programming (LP) problem. The proposed scheme transforms the EMD problem in such a way that the cloud server can solve it without learning the sensitiveinformation. In addition, local sensitive hash (LSH) is utilized to improve the search efficiency. The security analysis and experiments show the security and efficiency of the proposed scheme.

3.PROPOSED METHODOLOGY

In this project we propose a similarity Search for Encrypted Images in secure cloud computing (SEI) to solve the above challenges. Specifically, we employ the CNN model to extract feature vectors to improve search accuracy, and then build a hierarchical index tree in a bottom-up manner based on the clustering algorithm to improve search efficiency. Besides, we design an optimized ASPE algorithm, which does not require the image owner to share sdkwith image users, to achieve limited key-leakage for untrusted image users. To summarize, our contributions are set out as follows.

• High search accuracy. SEI achieves a high search accuracy by using the pre-trained CNN model to extract feature vectors. The CNN model simulating the human visual perception process can more accurately represent the image content, which makes the similarity measurement between images more accurate and search results more accurate.

• High search efficiency. SEI uses the optimized Kmeans clustering algorithm to classify images and constructs a hierarchical index tree in a bottom-up manner based on the clustering results. SEI avoids traversing the entire image database when performing search operation and reduces the search time to sublinear time

• Limited key leakage. TheSEI provides a secure trapdoor generation process with limited key-leakage , which not only prevents untrusted image users from completely leaking keys privacy but also avoids the online help of the image owner when the image user generates trapdoors locally.

4.RESULTS

The implementation involves various steps.

They are:

- Image Owner
- Image User
- Cloud Server

Image Owner:

Fig: Image Owner login Page

Description: This is image owner login page the image owner can login and add the images.

Fig: Image Owner Home Page

Description: This is image owner home page .In this the page admin can add images, check the user search requests, can view all the images and Encrypts the images and stores in cloud server.

Fig: All images

Description: This are the images that we have added .

Image User:

Fig: User Registration Form

Description: This is User Registration form, In this the image user can register .

Fig: Image User Home Page

Description: This is Image user home page, In this the user can login and then request key from image owner by entering the key the image user can search similar images.

ISBN: 978-93-91303-04-04

Fig: User Profile

Description: These is the user profile consists of user name, phone no, mail id, date of birth and address of the user

Cloud Server:

Fig: Cloud server login page

Description: This is cloud server login page, In this the page admin can login and view the users search history and the images that are encrypted and stored in cloud server.

Fig: Cloud server Home page

Description: This is cloud server home page, In this the page admin can authorize the image user after registering ,can view all the images ,can search all users history list, can search all images ranking chart.

Fig: Users search history list

Description: This search history list of all the users. This data shows what the user searched

5.CONCLUSION

In this project, we investigate similarity search for encrypted images in secure cloud computing. Concretely, we will introduce a clustering improvement method andgive the design method of the hierarchical index tree. With these two techniques, SEI can efficiently perform the retrieval process and achieve high accuracy based on features extracted bythe CNN model. Further, we consider untrusted image users in SEI and hence propose a similarity calculation method with limited key-leakage.We also give strict security analysis and conduct experiments on a real-world dataset, which indicate that SEI is secure and feasible in practice.

6.REFERENCES

[1] X. Wang, J. Ma, X. Liu, and Y. Miao, “Search in my way: Practical outsourced image retrieval framework supporting unshared key,” in Proc. IEEE Conference on Computer Communications (INFOCOM’ 19). IEEE, 2019, pp. 2485–2493.

[2] Y. Miao, X. Liu, K.-K. R. Choo, R. H. Deng, J. Li, H. Li, and J. Ma, “Privacy-preserving attribute-based keyword search in shared multi-owner setting,” IEEE Transactions on Dependable and Secure Computing, 2019

[3] Z. Xia, L. Jiang, D. Liu, L. Lu, and B. Jeon, "Boew: A contentbased image retrieval scheme using bag-of-encrypted-words in cloud computing," IEEE Transactions on Services Computing, 2019.

[4] M. Li, M. Zhang, Q. Wang, S. S. Chow, M. Du, Y. Chen, and C.Lit, "Instantcryptogram: Secure image retrieval service," in IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, 2018, pp. 2222–2230.

ISBN: 978-93-91303-04-04

Tumor Detection and Classification of MRI Brain Image using Discrete Wavelet Transforms and Support Vector Machines

M. Sivalingamaiah P. Dhanya sree [2] A. Likhita [3] U. Gayathri [4] K. Anjana55

Associate Professor[1], UG Scholar[2,3,4,5]

[1,2,3,4,5]Department of ECE, Srinivasa Ramanujan Institute of Technology (SRIT), Anantapur, Andhra Pradesh

Abstract:

The Abnormal growth of tissue or the uncontrolled division of cells in any part of our body forms a tumor. There maybe two types of tumors in brain, (i)Primary tumor sand (ii)Secondary tumors. The tumors that forms from the tissues of the brain or the brain's immediate surroundings are called Primary tumors like benign or malignant. The tumors that are formed in another a part of the bodyand then spreads to the brain are called Secondarytumors likemetastasis. The brain tumor affects Cerebrospinal fluid and causes strokes and hence the detection of tumorwithin the brain is more important. The proposed system helps in classifiyingnormal brain and tumor brain.The tumors like benign and malignant, metastasis are often detected by taking resonance image(MRI) of brain as input andtherefore the detection and classification of MRI brain tumors are implemented using Discrete wavelet transforms and support vector machines respectively.

Keywords:

Tumor, Brain, Classification, Detection, Wavelet transforms, Support vector machines.

Introduction:

The cerebrum tumor is framed because of strange development of uncontrolled destructive cells inside the mind. A mind tumor possibly considerate and harmful. The favorabletumor has uniform designs and contains latent disease cells. The threatening tumor has non-uniform designs and contains non-uninvolved malignancy cells. To identify cerebrum tumor we can ready to utilize either MRI or CT filter, MRI checked pictures would give significant data with respect to synapses. X-ray filters give an extremely nitty gritty diagnostics of the greater part of the significant organs and tissues in our body and subsequently inside the proposed framework MRI is utilized for tumordiscovery.The mind MR picture contains two sections which are to be isolated for the extraction of cerebrum tumous. A piece of locale contains the tumor cells, though the subsequent district contains the conventional synapses.The existing system is predicted on the edge detection through which we will able to detect the tumor accurately but not classify it.within the proposed system, The investigation manages the extraction of highlights from the image by applying Discrete wavelet transforms and therefore the classification is done by using support vector machines. Our output results in making decision easy by clinical experts.

Previous work: Advanced Edge Detection Technique For Brain Tumor Detection In MR Images.

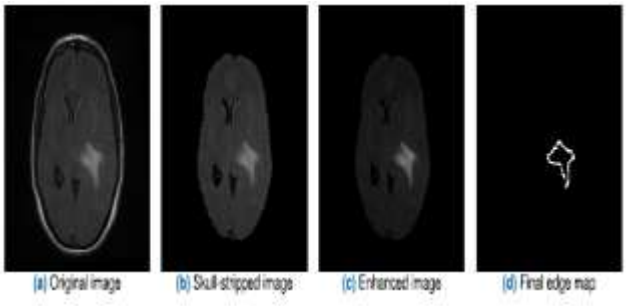
In Previous work an optomised edge detection technique has used to detect the tumor in brain. where edge is the Sudden and significant change in the intensity of an image.In existing framework two stages are performed on input dark scale MRI check picture. In initial step picture upgrade, skull stripping and difference improvement happens. To feature the space of interest Balance Contrast Enhancement Technique is utilized.

In Skullstripping step we can ready to eliminate the non mind tissues like skull, scalp and so forth from cerebrum pictures. Difference improvement should be possible by without changing the histogram example of the information picture the differentiation of the picture can be extended or compacted. The means engaged with edge recognition are Image Smoothening, Edge focuses discovery and Edge Localization.

The grey scale MR brain image is taken as input, the image smoothing can be done by Removing or suppressing the noise without affecting the quality of image. The variation of intensity can be detected and the noise gets discarded to detect the

ISBN: 978-93-91303-04-04

edges in the image. In the edge localization step The processes like thinning,linking etc are carried out to locate the edges clearly, and hence edges of the tumor are detected accurately. To obtain the optimal edges and to remove the false edge fragments the edge detection method is trained with the appropriate training MR images.



This existing method mainly works on Sobel edge detection algorithm. This also uses localization concept to detect the sharp edges of an image. Based on trained images and by using optimal edge filter and thresh-holding algorithm the output image is obtained.

Proposed system: Tumor Detection and Classification of MRI Brain Image using Discrete Wavelet Transforms and Support Vector Machines

Methodology:

To over come the drawbacks in existing system we are proposing a new system trough which we can able to detect the tumor and classify it. The proposed system involves three steps, they are:

(i) Pre-Processing
(ii) Training SVMs
(iii) Getting output from MR brain image input.

Pre-Processing:

During this step the image enhancement starts by first converting the grey scale image to black and white image, and noise gets eliminated by applying 2-Dimenctional Gaussian smoothing operator.

Training SVMs:

During this step the SVMs are trained with some standard and already classified brain MR images.

Getting output from MR brain image input:

During this step the input MR brain image gets classified based on the trained images and their properties through SVMs, finally the classified output with tumor type are going to be displayed.

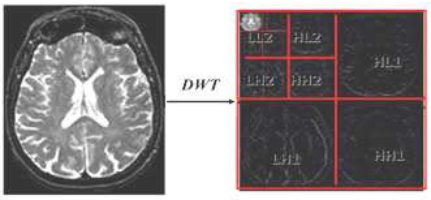
DWT:

Inside the proposed framework to dissects the picture at various recurrence groups with various goals we are utilizing Discrete Wavelet Transforms. DWT utilizes two arrangements of capacities, called scaling capacities and wavelet capacities, which are identified with low pass and high pass channels, separately. The division of the picture into various recurrence groups is simply gotten by progressive high pass and low sit back space picture. The first picture is first gone through a half band high pass channel and a low pass channel. After the sifting, half of the examples are regularly killed reliable with the Nyquist's standard, since the picture presently includes a most noteworthy recurrence of □/2 radians as opposed . The picture can consequently be sub separated by 2, just by taking out each and every other example. This comprises one degree of division and may numerically communicated as follows:

$$y_{high}[k] = \sum_{n} x[n] \cdot g[2k - n]$$

$$y_{low}[k] = \sum_{n} x[n] \cdot h[2k - n]$$

where yhigh[k] and ylow[k] are the yields of the high pass and low pass channels individually,aftersub dividing by 2.



This division parts the time goal since just a large portion of the measure of tests presently portrays the entire picture. Notwithstanding, this activity

ISBN: 978-93-91303-04-04

makes the recurrence goal twofold, since the waveband of the picture currently ranges just a large portion of the past waveband, successfully diminishing the vulnerability inside the recurrence considerably. The above technique is otherwise called the sub band coding, is regularly rehashed for additional division. At each level, the sifting and sub examining will end down the middle the measure of tests (and thus a fraction of the time goal) and a large portion of the waveband crossed (and henceforth recurrence goal duplicates).

K-Means:

To upgrade the productivity of yield the bunching procedure is also engaged with the Proposed framework, Clustering is a technique for classifing information objects into various classes, comparative information objects has a place with an identical class and divergent information objects has a place with various classes. In alternate manner, we endeavor to discover equivalent sub classes inside the information such information focuses in each bunch are just about as same as conceivable steady with a similitude measure like euclidean distance or relationship distance. The decision of which comparability measure to utilize is application explicit.

In contrast to directed getting the hang of, bunching is considered as a solo learning procedure since we don't have the ground truth to coordinate with the yield of the grouping calculation to genuine names to assess its exhibition. We just need to endeavor to explore on the construction of the information by classifiying the information focuses into unmistakable sub classes. This methodology is generally used in clinical picture division and it's applications are utilized for mind tumor identification as ordinary or unusual and to search out the tumor inside the cerebrum.

K methods calculation is an iterative calculation that attempts to segment the dataset into K pre-characterized unmistakable non-covering sub classes, where every datum has a place with only one class.

The manner in which k-implies calculation works is as per the following:

1)Determine number of groups K.

2)Introduce centroids by first rearranging the dataset then arbitrarily choosing K information focuses for the centroids without substitution.

3)Continue to emphasize until there's no change to the centroids. i.e task of information focuses to bunches isn't evolving.

4)Register the amount of the squared distance between information focuses and any remaining centroids.

5)Dole out every datum to the nearest group (centroid).

6)Register the centroids for the groups by taking the run of the mill of the all information focuses that has a place with each bunch.

Feature Extraction:

During this step the features of the given input image are extracted. These features include smoothness, entropy, variance, skewness, idm, correlation, homogeneity, mean and variance. And on the idea of those features the image is analysed and therefore the detection of the tumor region is been done.

SVMs:

SVM is absrevation of Support Vector Machine. SVMs are one among the principal forecast techniques, being upheld by measurable learning systems or VC hypothesis proposed by Vapnik and Chervonenkis. Given a gathering of preparing models, each set apart as having a place with in any event one of two classifications, SVM analyzes preparing guides to focuses in space so on boost the width of the hole between the 2 classes. New models are then planned into that exact same space and gets assessed to have a place with a classification upheld which side of the hole they fall. For the most part the bigger the edge, the lower the speculation blunder of the classifier. All the more officially, A help vector machine develops a hyperplane or gathering of hyperplanes during a high or boundless dimensional space, which might be utilized for order, relapse and so on.

Conclusion:

In this task we have computerized the conclusion technique for the cerebrum tumor recognition by the utilization of picture preparing. Aside from a

ISBN: 978-93-91303-04-04

few existing mind tumor division and identification methods are available for MRI of cerebrum picture our venture has demonstrated to give an over all exactness by upto 97%. Every one of the means for identifying mind tumor that have been talked about beginning from MR picture obtaining, pre-preparing steps to effectively arrangement of the tumor utilizing the two division procedures is been finished. Pre-preparing includes activities like wavelet based strategies has been talked about. Quality upgrade and sifting are significant in light of the fact that edge honing, upgrade, commotion expulsion and undesirable foundation evacuation are improved the picture quality just as the identification system. Among the diverse separating procedure, Gaussian channel stifled the commotion without obscuring the edges and it is better anomaly without decreasing sharpness of the pictures, diminishes the clamor, improve the picture quality VM and SOM will gives compelling and precise outcomes for cerebrum tumor discovery. These order procedures can initially identify climate there is tumor or not and in the event that it is there, they can decide the kind of the tumor, climate it is kindhearted or harmful.

References:

- A distinctive approach in brain tumor detection and classification using MRI,2017.
- Hybrid approach for brain tumor detection and classification in magnetic resonance images, 2015.
- Tumor detection and classification of MRI brain image using wavelet transform and SVM,2017.

and comparitively more effective than other sifting strategies. After the picture quality improvement and clamor decrease talked about here, division strategy for a mind tumor from MRI of cerebrum picture is been carried out. Order based division portions tumor precisely and gives reasonable outcomes for enormous data set anyway undwanted conduct can happen on the off chance that any place a class isn't addressed in preparing information.

Group based division performs is straight forward, speedy and gives reasonable outcomes for no clamor picture aside from commotion pictures it might prompts genuine error inside the division. Despite a few managing of issues, an automization of mind tumor division utilizing mix of limit based and arrangement with S.

ISBN: 978-93-91303-04-04

An IOT-based System for Auto-mated Health Monitoring and Surveillance in Post-Pandemic Life

Thippeswamy C,Sravani S,Swapna Bai N,Sai Sudeshna B,Thathi Reddy
Electronics and Communication Engineering,
Srinivasa Ramanujan Institute Of Technology,Rotarypuram , Anantapuramu, 515701,
Andhra Pradesh, India

ABSTRACT:

In this project, associate degree implementation of reasonable medical technology health watching sensing element system is developed and incontestible to live blood saturation levels (SpO2), pulse and vital sign at the same time. The embedded system is predicated on Rasberry pi platform because of responsibleness and plug and play capability. The planned pulse oximetry sensing element uses spectrophotometry to calculate the magnitude relation of ventilated haemoprotein to deoxygenated haemoprotein that then is employed to calculate the share of ventilated blood levels. The accuracy of pulse measuring instrument is increased exploitation lightweight emitting diodes driver circuits, sample and hold circuits so that a variable baseline is established for various skin tones as well as the finger breadth wherever the measurements are undertaken. The embedded sensing element system is meant to watch SpO2, pulse associate degreed vital sign and show the obtained results on an liquid crystal display. The measured vital organ also are transmitted exploitation Wi-Fi module to the net, forming net of things platform for the designed embedded system of sensors. The low value embedded sensing element system reportable during this study is accustomed monitor key health parameters of patients in hospitals or reception. The planned reasonable medical technology sensing element system is used as wearable wireless sensing element which might be used as a plug and play sensing element with Rasberry pi to watch human key health parameters.

Keywords:IoT, health monitoring, sCOs

INTRODUCTION

Internet of Things (IoT) development brings new opportunities in several applications, as well as sensible cities and smart tending. Currently, the first usage of the IoT in tending may be categorised as remote observance and real-time health systems. dominant and managing dire situations, like the one in 2020 once the coronavirus disease (COVID-19) took over the planet, may be achieved with the help of IoT systems, while not imposing severe restrictions on folks and industries. COVID-19 causes metastasis symptoms and seems to be additional contagious as compared to severe acute respiratory syndrome in 2003 . a way to regulate the unfold of viruses, till a vaccinum is on the market, is to look at physical (or social) distancing. By implementing higher systems for police work, healthcare, and transportation, contagious diseases can have less likelihood of spreading . An IoT system, combined with computing (AI), may offer the following contributions once considering a virulent disease : rising peace victimization police work and image recognition systems, utilizing drones for provide, delivery, or medical aid, contact tracing and limiting people's access to public places through apps and platforms empowered with AI associate degree IoT system for tending is usually composed of the many sensors connected to a server; it offers realtime observance of associate degree surroundings or users.

LITERATURE SURVEY:

J. A. Lewnard and N. C. Lo, ''Scientific and ethical basis for social distancing interventions against COVID-19,'' Lancet Infect. Dis. , vol. 20, no. 6, pp. 631–633, 2020, doi: 10.1016/S1473-3099(20)30190-0.

The incidence of coronavirus illness 2019 (COVID-19; caused by severe acute metabolic process syndrome coronavirus) has since up exponentially, currently poignant all United Nations agency regions. the amount of cases

according to this point is probably going to represent a sarcasm of actuality burden as a results of shortcomings in police work and diagnostic capability poignant case ascertainment in each high-resource and low-resource settings. By all scientifically meaty criteria, the globe is undergoing a COVID-19 pandemic.

P. A. Laplante and N. Laplante, ‘‘The net of Things in healthcare: Potential applications and challenges,’’ IT Prof., vol. 18, no. 3, pp. 2–4, May 2016, doi: 10.1109/MITP.2016.42.

Exciting new applications of net of Things (IoT) technology area unit arising, notably in health care, wherever the investing effects will considerably improve patients' well-being whereas assuaging the matter of

sourcee resources. however the packaging around these applications way outpaces the truth. moreover, there's a true risk that these investing technologies can split up caregivers from patients, doubtless leading to a loss of caring. during this article, the authors review a number of the foremost promising applications for IoT in health care and therefore the important challenges ahead.

EXISTING SYSTEM:

Designing of a continuous smart health monitoring system is the hot topic for researchers. A remote healthcare monitoring system has more advantages for those who are living in rural areas and not able to reach the hospital center on time and from the other aspect, the strain on hospital medical resources like doctors, patients, and wards would also have decreased. The continuous healthcare monitoring system is generally relying on wireless sensor network which

decreases the rate of energy consumption and extend the coverage area for communication. According to, smart healthcare monitoring and giving more attention to people health is the difficult tasks that people must be aware of. The development of sensors has brought huge facilities to the hospital environment. Sensor is used for the evaluation of different signs like ECG, motion, temperature, blood pressure and heart beating. Besides WSN, RFID technology is also used to localize equipment in hospitals.Wireless localization network is used to monitor the patient’s present conditions and track the inner side area of the patient. The three main standards WSN, RFID, and GSM are utilized jointly to check sick people in healthcare center, as well as supervise their psychological status. Constrained application protocol (Coap) also playsa key role in connection and monitoring of medical sensors. The adoption of CoAP inhuman services play an outstanding role, since the CoAP worked in highlights like, resource monitoring (particular advantageous for continuous checking of sick people' essential signs) and disclosure empower a dynamic condition where the accessible resources are directly found and designed.Received signal strength indicator (RSS) and particle filters on which localization and tracking system relay while bi-axial accelerometers are utilized to categorize the patient’s movement conditions. Moreover, the different technologies and technological standards used for data access and storage, visualization and healthcare analysis techniques are essential parts of a continuous healthcare structures. The development of electronic healthcare monitoring platform has changed the traditional way of healthcare method, compromise IOT into these systems which have increased adaptability, intelligence, and interoperability.

PROPOSED SYSTEM:

To implement a remote health care observation system. In these sensors to watch the medical parameters like pressure, pulse and Temperature unit designed and interfaced to the micro-controller. The patient or users will send these information to the doctor instead of visiting the doctor directly within the hospital.The details square measure transferred to the info server. This information will then be accessed from any a part of the planet.

ISBN: 978-93-91303-04-04

HARDWARE COMPONENTS:

RASPBERRYPI3: The Raspberry Pi has a Broadcom BCM2835 System on Chip module. It has a ARM1176JZF-S processor.
The Broadcom SoC used in the Raspberry Pi is equivalent to a chip used in an old smartphone (Android or iPhone). While operating at 700 MHz by default, the Raspberry Pi provides a real world performance roughly equivalent to the 0.041 GFLOPS.

POWER SUPPLY: Power supply is a reference to a source of electrical power. A device or system that supplies electrical or other types of energy to an output load or group of loads is called a power supply unit or PSU. The term is most commonly applied to electrical energy supplies, less often to mechanical ones, and rarely to others.

LCD (LIQUID CRISTAL DISPLAY):A liquid crystal display (LCD) is a thin, flat display device made up of any number of color or monochrome pixels arrayed in front of a light source or reflector. Each pixel consists of a column of liquid crystal molecules suspended between two transparent electrodes, and two polarizing filters, the axes of polarity of which are perpendicular to each other.

PULSE SENSOR: The Heartbeat rate information knowing is very useful while doing exercise, studying, etc. But, the heartbeat rate can be complicated to calculate. To overcome this problem, the pulse sensor or heartbeat sensoris used.

BP SENSOR: Blood Pressure (BP) is one of the important vital signs. It is the pressure exerted by the circulating blood on the walls of blood vessels. Blood Pressure is expressed as the ratio of the systolic pressure over diastolic pressure.

TEMPERATURE SENSOR: TheLM35seriesare precisionintegrated-circuittemperature sensors,whoseoutputvoltageislinearlyproportiona ltotheCelsius(Centigrade)temperature. The LM35 thus has an advantage overlineartemperaturesensorscalibratedin ° Kelvin, as the user is not required tosubtract a largeconstantvoltagefromitsoutputtoobtainconve nientCenti-grade scaling.

SPO2 SENSOR: Pulse oximetry is a noninvasive method for monitoring a person's oxygen saturation. Peripheral oxygen saturation (SpO_2) readings are typically within 2% accuracy (within 4% accuracy in the worst 5% of cases) of the more desirable (and invasive) reading of arterial oxygen saturation (SaO_2) from arterial blood gas analysis.

SOFTWARE REQUIREMAENTS:

- **Python**
- **Python compiler**

PROCEDURE:

The architectural design to health monitor of covid patients.This implementation model we used raspberry pi board, Sensors and as an embedded device for sensing. Nowadays treatment of most of the heart-related diseases requires continuous as well as long term monitoring. IoT is very useful in this a specters it replaces the conventional monitoring systems with a more efficient scheme.SPO2 sensor monitor the oxygen level of a person continuously, monitor oxygen levels and send message to microcontroller. After receiving message from spo2 sensor, microcontroller

ISBN: 978-93-91303-04-04

executes necessary action.. The LCD display with 16x2 configurations is used to user to know the status.

Heartbeat sensor monitor the heartbeat rate of a person continuously, monitor heartbeat rate and send message to microcontroller. After receiving message from heartbeat sensor, microcontroller executes necessary action.. The LCD display with 16x2 configurations is used to user to know the status.

BP sensor monitor the blood pressure of a person continuously monitors blood pressure and send message to microcontroller. After receiving message from heartbeat sensor, microcontroller executes necessary action.. The LCD display with 16x2 configurations is used to user to know the status.

Temperature sensor monitor temperature of a person continuously monitors temperature and send message to microcontroller. After receiving message from temperature sensor, microcontroller executes necessary action. . The LCD display with 16x2 configurations is used to user to know the status.

By using the wifi module ,data will be uploaded into the Thing speak server.

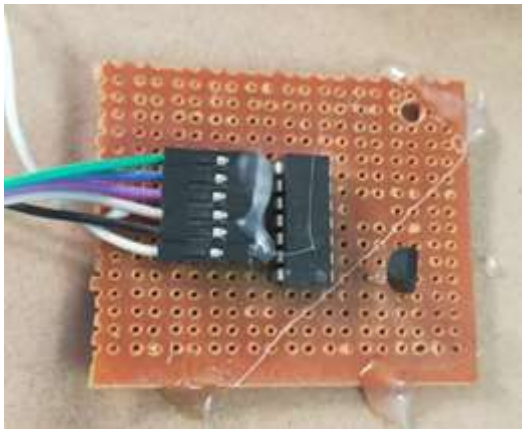


Figure:Pulse sensor

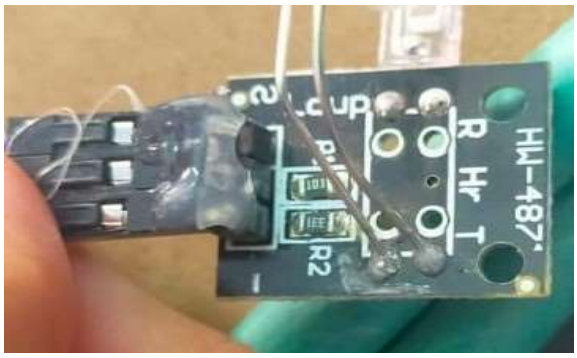


Figure:BP sensor

RESULT AND DISCUSSION:

By this procedure we get the results temperature in fahrenheit,oxygen saturation,pulse rate

and blood pressure.These factors are displayed in Liquid crystal display(LCD) and the displayed data store in cloud server. By connecting the wifi module and login by using the username and password we can access the information anywhere in IOT app.

ISBN: 978-93-91303-04-04

Figure:Displayed values in LCD

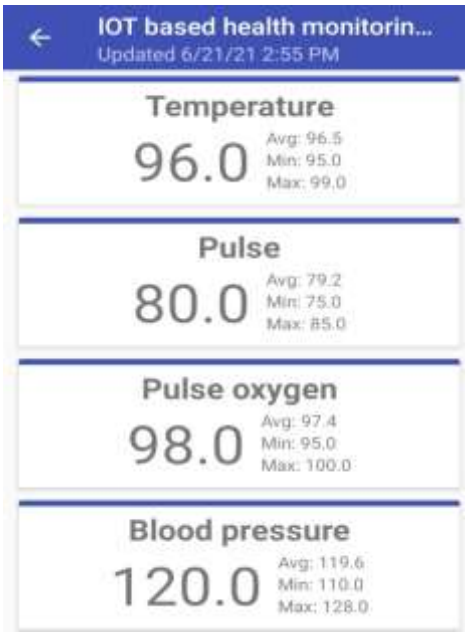


Figure: Displayed values in IOT app

CONCLUSION:

In this project, an IoT framework is presented to monitor participants' health conditions and notify them to maintain physical distancing. The proposed system integrates a wear-able IoT node with a smartphone app, by which the IoT sensor node can collect a user's health parameters, such as temperature and blood oxygen saturation, and the smartphone connects to the network to send the data to the server. The paper proposed a Radio Frequency (RF) distance-monitoring method which operates both for indoor and outdoor environments to notify users to maintain the physical distancing. Applying on body parameters makes it possible to monitor participant's' health conditions and to notify individuals in real time.. The thingspeak-based server is implemented to process received data from an IoT node using a cellular network. In addition, locally processing the data makes it possible to use the IoT node in the environments without internet connectivity or fog-based networks. The system can assist participants in monitoring their daily activities and minimize the risk of exposure to the Coronavirus.

REFERENCES:

[1] D. S. W. Ting, L. Carin, V. Dzau, and T. Y. Wong, "Digital
[2] technology and COVID-19," Nat. Med., vol. 26, no. 4, pp. 459-461, 2020, doi: 10.1038/s41591-020-0824-5.
[2] J. A. Lewnard and N. C. Lo, "Scientific and ethical basis for social-distancing interventions against COVID-19," Lancet Infect. Dis. , vol. 20, no. 6, pp. 631-633, 2020, doi: 10.1016/S1473-3099(20)30190-0.
[3] S. Woolhandler and D. U. Himmelstein, "Intersecting U.S. Epidemics: COVID-19 and Lack of Health Insurance," Ann. Intern. Med., vol. 173, no. 1, pp. 63-64, 2020, doi: 10.7326/M20-1491.
[4] E. Christaki, "New technologies in predicting, preventing and control-ling emerging infectious diseases," Virulence, vol. 6, no. 6, pp. 558–565, 2015, doi: 10.1080/21505594.2015.1040975.
[5] T. L. Inn, "Smart City Technologies Take on COVID-19," Penang in-stitude, 2020. Accessed: Aug. 2, 2020. [online]. Available: https://pe-nanginstitute.org/publications/issues/smart-city-technologies-take-on-covid-19/
[6] L. Setti, F. Passarini, G. De Gennaro, P. Barbieri, M. G. Perrone, M. Borelli, J. Palmisani, A. Di Gilio, P. Piscitelli, and A. Miani, "Airborne Transmission Route of COVID-19: Why 2 Meters/6 Feet of Inter-Per-sonal Distance Could Not Be Enough," Int. J. Environ. Res. Public Health, vol. 17, no. 8, pp. 2932-2937, 2020, doi: 10.3390/ijerph17082932.
[7] R. A. Calvo, S. Deterding, and R. M. Ryan, "Health surveillance dur-ing covid-19

UNDER WATER IMAGE ENCHANCEMENT USING DEEP CNN

Pujitha G,Srinath Shardhuli L,Sabiha Sulthana S,Pavan Kumar Naik M
Department of Electronics and communication Engineering
Srinivasa Ramanujan Institute Of Technology,Anatapuramu District

Abstract:

For consuming of Underwater resources underwater image enhancement is more important.Due to light absorption and scattering, the visibility of images appear low contrast and distorted color casts. To avoid this problem, we use a convolutional neuralnetwork based image enhancement model, i.e., Deep CNN, which is used to perform underwater detection and classification according to the characteristics of underwater vision. Unlike the existing works that require the parameters of underwater imaging model estimation or impose inflexible frameworks applicable only for specific scenes .In this model we directly reconstructs the clear underwater image by attaching on an automatic end-to-end and data-driven training mechanism. Notifying with underwater imaging models and optical properties of underwater scenes, at first synthesize ten different marine image databases. This experiment results on real-world and synthetic underwater images demonstrate that the presented method generalizes well on different underwater scenes and outperforms the existing methods both qualitatively and quantitatively. This results enhanced and accurate images of underwater scenes.

Keywords: Deep CNN, Adaptive histogram equalization, YCbCr, Max-RGB, Image preprocessing, object detection, Contour segmentation.

Introduction:

By using digital cameras, Underwater images can be captured.and to enhance the quality and reduce the noise, gray are used along with the convolution nueral network to enhance the underwater images.To remov the foggy and hazy effects present due to absorption and scattering Deep CNN is used.The output can be shown clearly and also we can detect the object clearly.we use matlab sofware to run the code

Existing system: We use various image enhancement algorithms such as AHE, BBHE, CLAHE and Gamma correction for underwater image enhancement. In this we use Adaptive Histogram Equilization Method.

Histogram equalization –In order to increase the contrast of the image, we do histogram equalization in this step. We have used MATLAB's image processing toolbox function called adapthiseq.

Adaptive Histogram Equalization (AHE) —this method used here is tocompute many histograms for the same image, each histogram correspond to a section of theimage. This improves the contrast locally. Drawback of using AHE is that it canover-amplify noise in the local region. AHE is still preferred over ordinary HE because it enhances the contract better.

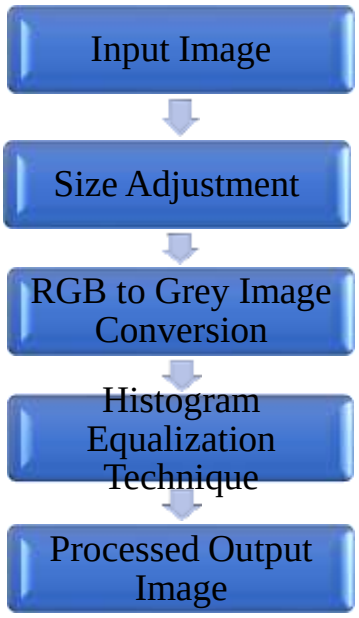


Fig1: Block Diagram of Adaptive histogram equilization

ISBN: 978-93-91303-04-04

Proposed system: To remove the problem of hazy and foggy artifacts in deep water a method of Deep CNN is proposed.Proposed system contains two steps.At first we adjust the color and remove noise, improve the quality of the image, and in the second step we use Dee Convolutional Neural Networks to improve the Image resolution.

Fig: Block diagram of proposed system

The underwater images get darker as we go deep in water. This is due to scattering phenomenon of light. *Color Correction* involves RGB and Shades of Grey method. Light containing different wavelengths of red blue and green enter the water. Going deep in water almost all the red light is reduced to 50% but the blue and green lights continues to a greater depth. So, most of the underwater images are subjected to green and blue color.

In *Image super resolution using Deep CNN*,It contains features of images and convert it into lower dimension ,but characteristics are still won'tchange.*DLCNN* consists three layers.

i) Convolutional layer: The first layer extracts basic features such as horizontal and diagonal edges.

ii) Pooling layer: The spatial volume of input image are reduced after convolution. Between 2 convolutional layers, pooling layer is used.. The third layer is expensive if we add between the layers.ll.

iii) Fully Connected Layer: FC Layer connects neurons in first layer to neurons in second layer. To classify images in different categories,FC layer is used

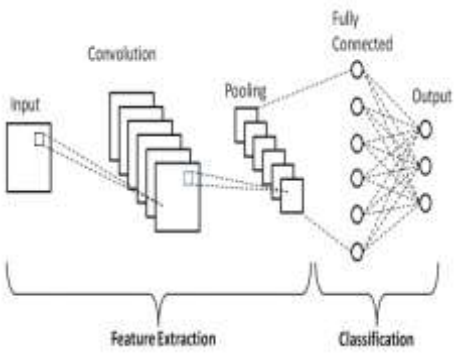


Image Restoration is the process after CNN and Conventional method of deconvolution is used for eliminating noise and to improve.the quality.

Hence, the underwater is considered and the process of color correction is used for removing foggy and hazy artifacts and then Image super Resolution is done by Convolutional Neural Networks. And as a result we can an image which is more clear, and effective than the original captured image.

Conclusion: Underwater images quality can be improved by using this project.As we underwater resources are important in development process and Also to preserve the resources present in underwater.we use adaptive histogram equilization, color correction, Gamma correction methods to Enhancevthe imges.A Deep cNN Method is Also used to detect the object and Also for improving the quality of the image.For Real world applicatios this technique is very useful.The primary colour such as Max RGB and shades of gray are used For color correction..Many different image'svpresent in the underwater can be seen clearly by using this technique.

References:

1. Tang, C., von Lukas, U.F., Vahl, M., Wang, S., Wang, Y., Tan, M.: Efficient underwater image and video enhancement based on Retinex. SIViP 13(5), 1011–1018 (2019)

2. Khosravi, M.R., Samadi, S.: Data compression in ViSAR sensor networks using non-linear adaptive weighting. EURASIP J. Wirel. Commun. Netw. 2019(1), 1–8 (2019)

3. Sethi, R., Sreedevi, I.: Adaptive enhancement of underwater images using multi-objective PSO. Multimed. Tools Appl. 78(22), 31823–31845 (2019)

4. Anwer, A., Ali, S.S., Khan, A., Mériaudeau, F.: Real-time underwater 3D scene reconstruction using commercial depth sensor. In 2016 IEEE International Conference on Underwater System Technology: Theory and Applications (USYS) 2016 Dec 13 (pp. 67–70). IEEE.

5. A Deep Learning Approach for Underwater Image Enhancement by Javier Perez(B) , Aleks

A NOVEL APPROACH TO PROVIDE PROTECTION FOR WOMEN BY USING SMART SECURITYDEVICE

1.Sadiya M 2.SaiSumanth Rao 3.Sirisha V 4.Sivakumar Reddy Madhusudhana Y

Srinivasa Ramanujan Institute Of Technology,Anatapuramu District

Abstract:In our country, eventhough it has a super Women safety is a important tissue due to rising crimes against women these days. power and an economic development but still there are many crimes against women. Women are less secure and have many issues regarding their security purpose.They have to undergo among variousbdifficult situations and have to prove themselves every time in all critical conditions. So, for their security and safety purpose the government has provided security through rules and regulation to the society. Although there are many existing systems for security purpose need of advanced smart security system is increased. In order to overcome such problems smart security system for women is implemented. This project provides the security system to Women and it describes about safe and secure system for women which comprises of an Arduinobcontroller and sensors such as temperatureLM35,flexsensor,MEMSAccelerometer, pulseratesensor, soundsensor. Abuzzer, LCD, GSM& GPS are used in this project.

When the Women is in danger or threat, the device senses the body parameters like changing temperature voice of the victim by sound sensor, heartbeat rate by pulse sensor, the movement of victim by flex sensor. This sensors crosses the threshold limit and the device gets activated. Using GPS and GSM modules, to measure & compute it's position in the earth and to provide a data link to a remote network.

INTRODUCTION :-

In today's

world,thesafetyofwomenisindanger especiallyinIndia.Therateofcrimesagainstwomen isnot decreasing but infact increasing,harassment,molestation,eveteasing,kidnapping and domestic violence. Many preventive measures have been taken by the Government to stop these misbehaving activities but still has not be affected the growing rate of these crimes and has remained unaffected.Women safety is a crucial concern in India and a lot of organisations started working on it after Nirbhaya's case. Women should adopt some selfdefense tips and tricks so that it proves helpful during the worst sceneries for them. Countless videos and information about such defensive techniques are available online for educating women's safety.

To develop this project, that's the reason it can act as a rescue device and protect at the time of danger. The main focus on this project is to serve the purpose of providing security to women so that they never feel helpless while facing such social challenges. This system is to built & can detect the location and health condition of a person by using electronic parameters like GPS, GSM, LCD, buzzer, MEMSAccelerometer, flexsensor, soundsensor, temperaturesensor, it helps to detect the real time situation of the women in bad conditions. Using HDcamera, it detects the feature which we can ensure our privacy and it also detects the abnormal condition of a women while she is victimized.

LITERATURE SURVEY :-

1.Performance & Analysis of Effective Iris Recognition System Using Independent Component Analysis by Dr.AntoBennet M, Sankara narayanan S, SankarBabuG

To remove artifacts, two postprocessing techniques that carry out optimization in the Fourier domain are developed. Decompressed iris images obtained from two public iris image data bases are evaluated by visual comparison, twoobjectiveimage quality assessment metrics, and eight iris recognition methods. To improve the efficiency, sensitivity and reduce the complexity. In existing system use the Principal component analysis will work with different parameters in the image insequence manner and independent component analysis will work with different

ISBN: 978-93-91303-04-04

parameters in the image in sametime, but the output is not reliable for a large set of images, in neural network, for each and everytime, the large set of feature for image database get loaded for training process, it will increase the time complexity of the whole system. In this proposed system we use the ICA(IndependentComponentanalysis) and Gabor filter to improve the sensitivity, specificity and reducing time complexity in the existing system. The concept of Gaborfilter will analysis the input image in several phases and pick a better one through 500 iterations. A new approach for personal identification based on iris recognition is presented in this paper. The core of this paper details the steps of iris recognition, including image processing, feature extraction and classifier design. This paper is implemented using MATLAB.

2.Women Security System using GSM & GPS by A.H. Ansari, Balsarf PratikshaP, Maghade TejalR, Yelmame Sneha.

The world is becoming unsafe for women in all aspects. The crime against women are increasing at a higher rate. The employed women are feeling unsafe due to increasing crimes. This paper proposes a quick responding mechanism that helps women during trouble. When someone is going to harass, she can just press the button and the location information is sent as an SMS alert to few predefined numbers interms of latitude and longitude. The controller used is ATMEGA328P. It is interfaced with a push button, a GPS module, a GSM modem and a LCD Display(16×2). If the switch is pressed, the controller take the current location information from the GPS module and send those data to the predefined number using a GSM modem. The program is developed in 'C' language. The purpose of this project is to feel safe for the women.

3.RFID Based Security System for Women BY Azhaguramyaa VR, Sangamithra D, Sindhja B.

In recent years, acts of assault and violence against women are rising at a menacing rate. With escalation of female employees in industries and other sectors, it is now becoming a necessity for females to travel at late hours and visit distant and isolated locations as a part of their work regime. However, the exponential increase in assault, violence and attacks against women in the past few years, is posing a threat to the growth and development of women. Defence is n't the only measure that can suffice against this increasing abuse. A security solution that creates a sense of safety among women needs to be devised. In instances of attack, it is largely reported that women are immobilized. There is thus, a need of simpler safety solution that can be activated as simply via RFID and GSM and can instantly send out alerts to the near one sand to family members of the victim . The system can be implemented in the form of a partial wear able and partial portable system ,the information is passedvto RFID reader which communicates with PIC microcontroller and through GSM the " help" message is sent to 2 predefined contacts (parents , police).

EXISTING SYSTEM :-

In both Women and children based Security System, the victim is the only person to press the Emergency button, bit this emergency button is possible in all conditions. Because there are two reasons the mobile has to grab by the children or women. This is the main disadvantage occurs if the mobile fallsdown or if it is switch off condition. It is difficult to access the victim location and another disadvantage is children doesn't know how to use smart phone and how to take care of Mobile things this will be the main advantage in Security System.

So cost of the System is very high and these are the main drawback in Security System. So we are avoiding these drawbacks by implementing new solution which works autonomously insituations. This new system provide protection for both children and women by ringing buzzer and send location to nearest police station and registered mobile numbers. So that we can easily track the victim.

PROPOSED SYSTEM :-

This Architecture consists of Arduino controller as a main source which receives input signals from sensors and receives signal from human. Some of the basic sensors are temperature, pulserate, flex,

ISBN: 978-93-91303-04-04

sound, MEMSAccelerometer, GSM and GPS, buzzer, LCD display and Mobile power supply Arduino. These are the main components present in the architecture.

>Todetecttheheartrateofthevictim.

>To detect the temperature of the person.

>To know the flexibility bending position of the person.

>To detect the sound from the surroundings.

>MEMS Accelerometer which makes the difference in electricpotential, change in the capacitance.

>GSM modem-tells the exact location of the victim by latitudes and longitudes.

>GPS module- helps to track the location of the victim.

Fig:- Block diagram of proposed system

4.WORKING PRINCIPLE:

The Working principle trailing this Smart Security Device is to detect parameter of a victim body i.e; grasping the bsignals from the relevant sensors which are in contact with the women who are in mint condition and also it captures the face of the swindler images and hence after detecting signals, the sensor transmits the output electrical signals to the controller. The Arduino receives the signal from the sensor as an analog/digital input signal and hence it generates the output parameters of each sensor and displays it on the LCD display.

The sensors which are used in the proposed system are flex sensor, temperature sensor, MEMS accelerometer, sound sensor, pulse rate sensor along with Arduino M071 0v7670 Cmos module . The respective sensor is used to detect signals of human (women or victim) who is in anomalous situations.

Whenever the values of any sensor signal crosses the above threshold limit therefore it is indicating that the women is in threat and according to victim condition, when 4 sensors out of 5 sensors crosses the threshold limit the buzzer is activated and camera captures the swindler image.

Consequently the GPS transmits the location of the victim to the Arduino and then the Arduino transmits the signals which are detected by the senors are send to the GSM. Assuredly the alert message “I am in danger” along with the latitudinal and longitudinal location is send to the registered contact numberand mail. Thus exhilarating of sensor and buzzer traces the location of victim using GPS and with the help of GSM 800L used sends the message of location to the analogous contacts with a 10secs delay.

5.HARDWARE DISCRPTION:

A.*ARDUINO CONTROLLER:*The Arduino Uno is a microcontroller board based on the ATmega328. It has 20 digital input/output pins (of which 6 can be used as PWM outputs and 6 can be used as analog inputs), a 16 MHz resonator, a USB connection of ATmegaU2 IC controller, a power jack, an in-circuit system programming (ICSP) header, and a reset button SPI and I2C modules.
It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.
The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features an ATmega16U2 programmed as a USB-to-serial converter. This auxiliary microcontroller has its own USB bootloader, which allows advanced users to reprogram it.

*Senors interfacing to Arduino:*sensors are widely used in almost ever field.sensors give another dimension to your project and can be used ininfinte applications.

ISBN: 978-93-91303-04-04

Firstly, there are different type of sensors which can record different type data. All sensors work differently e.g. Temperature sensor ,flex sensor, pulse rate sensor, mems accelerometer, sound sensor etc.

Although all sensors work differently but when it come to interfacing these sensors with Arduino microcontroller the process is pretty much the same.sensor record the physical data by changing the voltage at their output pin in response to different physical condition.

Arduino Uno has a set of Analog input pins which can are used to take analog input signals from a sensor.

Remember there are two types of signals:

1. **Digital Signals**: These signals have only two values i.e. 1 or 0 (on or off).
2. **Analog Signals**: These signals have values in a range. In the case of Arduino it scales the value in the range from 0 to 255.

So, we will connect our LDR with A0 pin of the Arduino Uno.For better understanding we will control an LED on the basis of the sensor data.

Connect the LED to D13 (digital pin 13) of Arduino UNO.

Note that here we are connecting our LED to pin 13 which has an inbuilt resistor. So we don't need to connect an external resistor but if we use any other pin then you will have to connect an external resistor to protect you LED.

So sensors simply records the data and sends it to then Arduino Uno which generates signals to control the LED.

B.*POWER SUPPLY*: The power supply of 5v is supplied to the Arduino through the USB cable.

C.PULSE *SENSOR*: The An alternate name of this sensor is heartbeat sensor or heart rate sensor.The working principle behind this sensor can be done by connecting it from the fingertip or human ear to Arduino board . So that rate can be easily calculated. The heartbeat rate information knowing is very useful while doing exercise, studying, etc. But , the heartbeat rate can be complicated to calculate. To overcome this problem, the pulse sensor or heartbeat sensor is used.

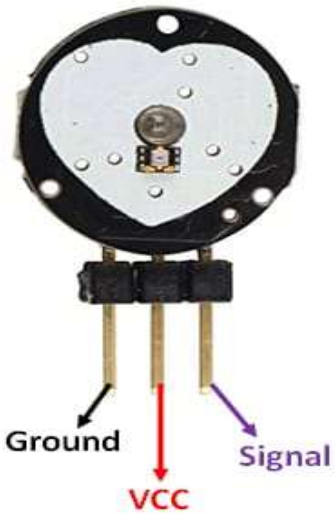


Fig no:1

*D.TEMPERATURE SENSOR:*TheLM35seriesare precisionintegrated-circuittemperature sensors,whoseoutputvoltageislinearlyproportionalt otheCelsius(Centigrade)temperature. The LM35 thus has an advantage overlinear temperaturesensorscalibrated in ˚ Kelvin, as the user is not required tosubtract a largeconstantvoltagefromitsoutputtoobtainconveni entCenti-grade scaling. The LM35 does not require anyexternal calibrationortrimmingtoprovidetypicalaccuracieso f±1⁄4˚C at roomtemperature and±3⁄4˚C overafull−55to+150˚C temperaturerange. Low cost isassured by trimming andcalibrationatthewaferlevel.TheLM35'slowoutp utimped- ance, linear output, andprecise inherent calibrationmakeinterfacingtoreadoutorcontrolcircu itryespecially easy.Itcanbeused with singlepower supplies, orwith plus andminussupplies.Asitdrawsonly60µAfromitssup ply,ithasverylowself-heating,lessthan0.1˚Cinstillair.TheLM35isratedtoo perateovera−55˚to+150˚Ctemperature range, whiletheLM35Cisratedfora−40˚to+110˚Crange(−1 0˚with improvedaccuracy).TheLM35series isavailablepack-aged in hermetic TO-46 transistor packages,while the LM35C, LM35CA, and LM35D arealso available in theplasticTO-92transistorpackage.TheLM35Disalsoavail-ableinan8-

leadsurfacemountsmalloutlinepackageandaplastic TO-220package.

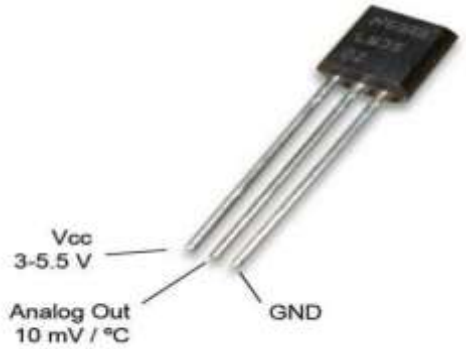


Fig no:2

E.SOUND SENSOR: A sound sensor is defined as a module that detects sound waves through its intensity and converting it to electrical signals.

Sound detection sensor works similarly to our Ears, having diaphragm which converts vibration into signals. However, what's different as that a sound sensor consists of an in-built capacitive microphone, peak detector and an amplifier (LM386, LM393, etc.) that's highly sensitive to sound.

With these components, it allows for the sensor to work:

1. Sound waves propagate through air molecules
2. Such sound waves cause the diaphragm in the microphone to vibrate, resulting in capacitance change
3. Capacitance change is then amplified and digitalized for processing of sound intensity

Apart from building various electronic projects with Arduino (covered in the later section) and more, sound sensors are used in many other day to day applications including:

- Consumer electronics such as phones, computers, music systems
- Security and Monitoring systems such as burglar alarms, door alarm, etc.
- Home automation such as lighting your house by detecting whistle/clap instead of physically turning the light switch
- Ambient sound recognition and sound level recognition

Fig no:3

*F.FLEX SENSOR:***Flex sensors** are usually available in two sizes. One is **2.2 inch** and another is **4.5 inch**. Although the sizes are different the basic function remains the same. They are also divided based on resistance. There are LOW resistance, MEDIUM resistance and HIGH resistance types. Choose the appropriate type depending on requirement. Here we are going to discuss 2.2inch Flex sensor that is **FS-L-0055**.

FLEX SENSOR terminal resistance changes when it is ben**FLEX SENSOR** is basically a **VARIABLE RESISTOR** whose terminal resistance increases when the sensor is bent. So this sensor resistance increases depends on surface linearity. So it is usually used to sense the changes in linearityt.

Fig no:4

G.MEMS ACCELOROMETER: MEMS is a chip-based technology, known as a **M**icro **E**lectro-

Mechanical **S**ystem. Sensors are composed of a suspended mass between a pair of capacitive plates. When tilt is applied to the sensor, the suspended mass creates a difference in electric potential. The difference is measured as a change in capacitance.

A MEMS sensor provides the convenient features available with any other sensor line, but you don't need to concern yourself with space constraints. MEMS utilizes very compact micro machine components so small that each sensor can fit into the palm of your hand. They have an IP67 seal and since the operating temperature range is -40° to +85°C, they will withstand some intense conditions. While electrolytic sensors have much higher accuracy, some of them can be sensitive to temperature.

These sensors are great solutions to applications that do not demand the highest accuracy such as industrial automation, platform leveling, position control, and pitch and roll measurement. Since they are low cost, you can even save some dough on your next big project

The MEMS fabrication needs many techniques which are used to construct other semiconductor circuits like oxidation process, diffusion process, ion implantation process, low-pressure chemical vapor deposition process, sputtering, etc. Additionally, these sensors use a particular process like micromachining.

MEMS Sensor Working Principle:

Whenever the tilt is applied to the MEMS sensor, then a balanced mass makes a difference within the electric potential. This can be measured like a change within capacitance. Then that signal can be changed to create a stable output signal in digital, 4-20mA or VDC.These sensors are fine solutions to some applications which do not demand the maximum accuracy like industrial automation, position control, roll, and pitch measurement, and platform leveling.

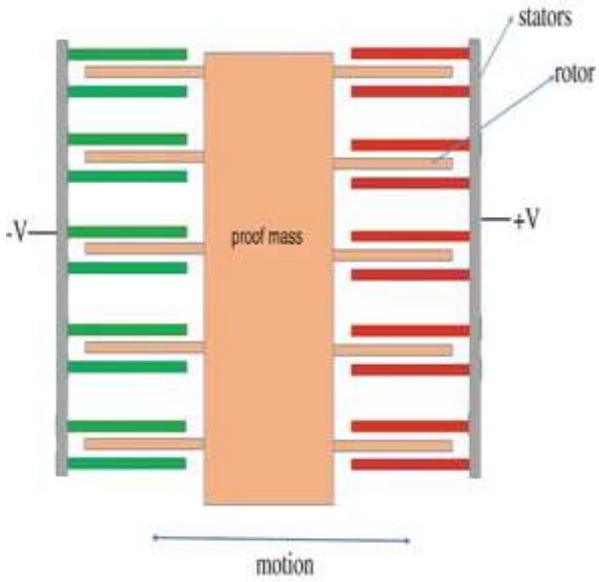


Fig no:5

H.BUZZER: A **buzzer** or **beeper** is a signaling device, usually electronic, typically used in automobiles, household appliances such as a microwave oven, or game shows.

It most commonly consists of a number of switches or sensors connected to a control unit that determines if and which button was pushed or a preset time has lapsed, and usually illuminates a light on the appropriate button or control panel, and sounds a warning in the form of a continuous or intermittent buzzing or beeping sound. Initially this device was based on an electromechanical system which was identical to an electric bell without the metal gong . Often these units were anchored to a wall or ceiling and used the ceiling or wall as a sounding board. Another implementation with some AC-connected devices was to implement a circuit to make the AC current into a noise loud enough to drive a loudspeaker and hook this circuit up to a cheap 8-ohm speaker. Nowadays, it is more popular to use a ceramic-based piezoelectric sounder like a Son alert which makes a high-pitched tone. Usually these were hooked up to "driver" circuits which varied the

ISBN: 978-93-91303-04-04

pitch of the sound or pulsed sound on and off.

Fig no:6

I.GSM: GSM (Global System for Mobile communications) is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800 MHz bands. Some countries in the Americas use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated.

The rarer 400 and 450 MHz frequency bands are assigned in some countries, where these frequencies were previously used for first-generation systems.

GSM-900 uses 890–915 MHz to send information from the mobile station to the base station (uplink) and 935–960 MHz for the other direction (downlink), providing 124 RF channels (channel numbers 1 to 124) spaced at 200 kHz. Duplex spacing of 45 MHz is used. In some countries the GSM-900 band has been extended to cover a larger frequency range. This 'extended GSM', E-GSM, uses 880–915 MHz (uplink) and 925–960 MHz (downlink), adding 50 channels (channel numbers 975 to 1023 and 0) to the original GSM-900 band. Time division multiplexing is used to allow eight full-rate or sixteen half-rate speech channels per radio frequency channel. There are eight radio timeslots (giving eight burst periods) grouped into what is called a TDMA frame. Half rate channels use alternate frames in the same timeslot. The channel data rate is 270.833 kbit/s, and the frame duration is 4.615 ms.

Fig no:7

Fig no:8

J.GPS: The **Global Positioning System (GPS)** is the only fully functional Global Navigation Satellite System (GNSS). The GPS uses a constellation of between 24 and 32 Medium Earth Orbit satellites that transmit precise microwave

ISBN: 978-93-91303-04-04

signals, which enable GPS receivers to determine their location, speed,. GPS was developed by the United States Department of Defense. Its official name is **NAVSTAR-GPS**. Although NAVSTAR-GPS is not an acronym, a few backronyms have been created for it. The GPS satellite constellation is managed by the United States Air Force 50th Space Wing.

Global Positioning System is an earth-orbiting-satellite based system that provides signals available anywhere on or above the earth, twenty-four hours a day, which can be used to determine precise time and the position of a GPS receiver in three dimensions. GPS is increasingly used as an input for Geographic Information Systems particularly for precise positioning of geospatial data and the collection of data in the field.Precise positioning is possible using GPS receivers at reference locations providing corrections and relative positioning data for remote receivers. Time and frequency dissemination, based on the precise clocks on board the SVs and controlled by the monitor stations, is another, use for GPS. Astronomical observatories telecommunications facilities and laboratory standards can be set to precise time signals or controlled to accurate frequencies by special purpose GPS receivers.

Similar satellite navigation systems include the Russian GLONASS (incomplete as of 2008), the upcoming European Galileo positioning system, the proposed COMPASS navigation system of China, and IRNSS of India.

Following the shooting down of Korean Air Lines Flight 007 in 1983, President Ronald Reagan issued a directive making the system available free for civilian use as a common good. Since then, GPS has become a widely used aid to navigation worldwide, and a useful tool for map-making, land surveying, commerce, scientific uses, and hobbies such as geocaching. GPS also provides a precise time reference used in many applications including scientific study of earthquakes, and synchronization of telecommunication networks.

Fig no:9

ISBN: 978-93-91303-04-04

K.LCD: A liquid crystal display (LCD) is a thin, flat display device made up of any number of color or monochrome pixels arrayed in front of a light source or reflector. Each pixel consists of a column of liquid crystal molecules suspended between two transparent electrodes, and two polarizing filters, the axes of polarity of which are perpendicular to each other. Without the liquid crystals between them, light passing through one would be blocked by the other. The liquid crystal twists the polarization of light entering one filter to allow it to pass through the other.

A program must interact with the outside world using input and output devices that communicate directly with a human being. One of the most common devices attached to an controller is an LCD display. Some of the most common LCDs connected to the contollers are 16X1, 16x2 and 20x2 displays. This means 16 characters per line by 1 line 16 characters per line by 2 lines and 20 characters per line by 2 lines, respectively.

Many microcontroller devices use 'smart LCD' displays to output visual information. LCD displays designed around LCD NT-C1611 module, are inexpensive, easy to use, and it is even possible to produce a readout using the 5X7 dots plus cursor of the display. They have a standard ASCII set of characters and mathematical symbols. For an 8-bit data bus, the display requires a +5V supply plus 10 I/O lines (RS RW D7 D6 D5 D4 D3 D2 D1 D0). For a 4-bit data bus it only requires the supply lines plus 6 extra lines(RS RW D7 D6 D5 D4). When the LCD display is not enabled, data lines are tri-state and they do not interfere with the operation of the microcontroller.

RESULT :-

The prototype of the Women security system in below Figure. The signals from temperature, flex, MEMS accelerometer, and sound, pulse rate sensors are detected successfully and send to Arduino. When four out of five above sensors crosses their threshold values the buzzer buzzes and the values are displayed on LCD as shown in below figure.

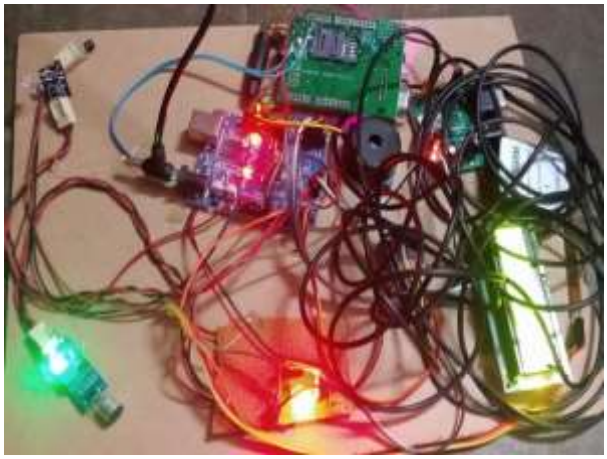


Fig :- prototype System.

ISBN: 978-93-91303-04-04

Fig :- Threshold values of the System.

CONCLUSION :-

This project is all about the existing applications for women security and comes out with an innovative idea for security and protection for women and more research is possible with introducing smart technology where people and objects form a network. This will help to solve them technologically with compact equipment and ideas. Using screaming alarms and also alerting the emergency contacts by sending the messages with the location is helpful for women's security. This system can overcome the fear that scares every woman in the country about her safety and security.

FUTURE SCOPE :-

For example as the school children safety are major concerns for parents as well as school management due to the recent incidents of child crimes like children missing, abuse etc. The modules used monitor the child safety when they are travelling in school buses. Once they reached the school the device gets deactivated by school authority and message send the parents that, "The child reaches the school safely". Hence, the advance technology makes the system more robust and reliable. As the new modules provide the Power and Computing Technologies IEEE [ICCPCT] 2016 functionality which enhance the safety and security.

REFERENCES :-

[1] Dr.Velayutham.R, Sabari.M, Sorna Rajeswari.M,"An Innovative Approach for women [5] http://www.atmel.com/Images/Atmel-42735-8-bit-AVR -Microcontroller- ATmega328-328P_Summary.pdf.

[2] Dhole, "Mobile Tracking Application for Locating Friends Using LBS", International journal Innovative research in computer and Communication engineering, vol: 1, Issue: 2, April 2013 [4] B.Chougula, "Smart girls security system," International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 4, April 2014.

.[3] Shaik Mazhar Hussain, Shaikh Azeemuddin Nizamuddin, Rolito Asuncion, Chandrashekar Ramaiah, Ajay Vikram Singh "Prototype of an Intelligent System based on RFID and GPS Technologies for Women Safety" 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Sep. 7-9, 2016.

[4]children's security Based Location Tracking System" 0n International Conference on Circuit,

[6] Prof.A.Maharajan "A survey on women's security system using GSM and GPS"- International Journal of Innovative Research in Computer and Communication Engineering Vol 5,Issue 2,Feb-2

Supervising Privacy And Security In Cashless Society Through Block-Chain Technology

R. Sivaiah [1]P. Sai Mounika[2] K. Sri Varsha[3] CH. Sushma[4]G. Shalini[5]
Associate Professor[1], UG Scholar[2, 3, 4, 5]
[1, 2,3,4,5]Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

Abstract – Cashless society describe the economicstate *whererefinancial* transactionsare notconductedwith money in theform of physical banknoteorcoinsbut rather through thetransfer of digital information (usuallyan electronic representation of money) between the transacting parties. To provide privacy and securityforsuchtypeof transactions we provide some solutions inour project.We developed three pronged solutionssuch as using randomized technique for creating arandom credit cardnumbergiving proper education about online transactions and using block chain technology for higher privacy.

Keywords –Cashless Society,Privacy, DataSecurity,Block-chain Technology, Credit Cards.

1. INTRODUCTION

Cyber security or Informationsecurity, computer security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware,software, or electronic data, as well as from the disruption or misdirection of the service they provide. The field is becoming increasinglysignificantdue to the increasedrelianceon computer systems, theInternet andwireless network standardssuch as Bluetooth and Wi-Fi, and due tothe growth of "smart "devices including smartphones, televisions, and the various devices that constitutethe "Internetof things". Owning to its complexity, both in terms of politicsand technology, cybersecurity is also one of the major challenges in the contemporary world.

Cashless society is an economic state where alltransactions are performed withoutphysicalmeans of currency, such ascoins or paper bills. Fora cashless system,privacyis a crucial component in need of evaluations. IncreasingPrivacy isand will continue to bea necessary undertaking in a cashless society. A majority ofusersare unaware of what kind of data isbeing collected aboutthemandhowthat data is being used. We thoughtthe whole paperhas realized theneed for improving privacy, and we propose todosowith a threepronged solution. First, promoting propereducationabout data collection and privacywill help people realize the needfor increased privacy.Second, a randomized credit card system willhelp preventunwantedparties from collecting sensitiveandpersonalinformation aboutpeople. Three, blockchainwill prove to be a powerful authentication tool. Securitywillbedrastically improvedthroughthe introductionor these three approaches. Users will have more knowledge about the systems they are using, hackers will have an exceedingly difficulttime fooling the blockchain system, and data willbe difficultto associate with specific people.

A blockchain is a growing list of records, called blocks, that arelinkedtogetherusing cryptography. Each block contains a cryptographic hash of the previous block, atimestamp, and transaction data (generally represented as a Merkle tree). The timestamp proves that the transaction data existed when the block was published in order to get into its hash. Blocks contain the hash of the previous block, forming a chain,with each additional blocks reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given blockcannot be altered retroactively without altering all subsequent blocks.Blockchains are typically managed by a peer-to-peer network for use as a publicly distributed ledger, where nodes collectively adhere to a protocolto communicate and validate new blocks. Although

ISBN: 978-93-91303-04-04

blockchain records are not unalterable as forks are possible, blockchains may be considered secure by design andexemplify a distributed computing system withhighByzantine faulttolerance. This proposed work prepares for thebest privacy and security for the user. Our new ideas are consisting of three solutions

1.Educating the people so that they know how a transaction is going to be done and by that how a hacker can hack there data and how they can use the data.

2.Whenever user request for a credit card a randomized techniquewillbeused to generate a random credit card number for each individual. So that the privacy will be allotted to the user.

3.A blockchain technology will be used to store every transaction. As the blockchain technology stores data in theform of blocks the unauthorized users may find it difficult to stole theuser data details. Hence, we also provide security to the user data.

2. RELATED WORK

2.1.Carry Your Credit in Your Pocket': The Early History of the Credit Card at Bank of America and Chase Manhattan

Drawing from newly available archival material, this article explores the early history of one of today's most ubiquitous financial instruments, the bank credit card. It focuses on the managerial decisions that led to the implementation and development of charge card programs at the two largest American banks of the late 1950s and early 1960s. Even though the initial performance of the two programs was comparable, top management at each bank ultimately adopted different business strategies. The differences resulted from managers' contrasting interpretations of the appropriate market for the credit card, interpretations formed within the context of two distinct banking cultures.

2.2. The rise of big data policing: surveillance, race, and the future of law enforcement

In a high-tech command centre in downtown Los Angeles, a digital map lights up with 911 calls, television monitors track breaking news stories, surveillance cameras sweep the streets, and rows of networked computers link analysts and police officers to a wealth of law enforcement intelligence.

This is just a glimpse into a future where software predicts future crimes, algorithms generate virtual "most-wanted" lists, and databanks collect personal and biometric information. The Rise of Big Data Policing introduces the cutting-edge technology that is changing how the police do their jobs and shows why it is more important than ever that citizens understand the far-reaching consequences of big data surveillance as a law enforcement tool.

2.3.Blockchain: Blueprint for a New Economy

Bitcoin is starting to come into its own as a digital currency, but the blockchain technology behind it could prove to be much more significant. This book takes you beyond the currency ("Blockchain 1.0") and smart contracts ("Blockchain 2.0") to demonstrate how the blockchain is in position to become the fifth disruptive computing paradigm after mainframes, PCs, the Internet, and mobile/social networking.

Author Melanie Swan, Founder of the Institute for Blockchain Studies, explains that the blockchain is essentially a public ledger with potential as a worldwide, decentralized record for the registration, inventory, and transfer of all assets—not just finances, but property and intangible assets such as votes, software, health data, and ideas.

Topics include:

- Concepts, features, and functionality of Bitcoin and the blockchain
- Using the blockchain for automated tracking of all digital endeavours
- Enabling censorship? Resistant organizational models
- Creating a decentralized digital repository to verify identity
- Possibility of cheaper, more efficient services traditionally provided by nations
- Blockchain for science: making better use of the data-mining network
- Personal health record storage, including access to one's own genomic data
- Open access academic publishing on the blockchain

3. PROPOSED WORK

ISBN: 978-93-91303-04-04

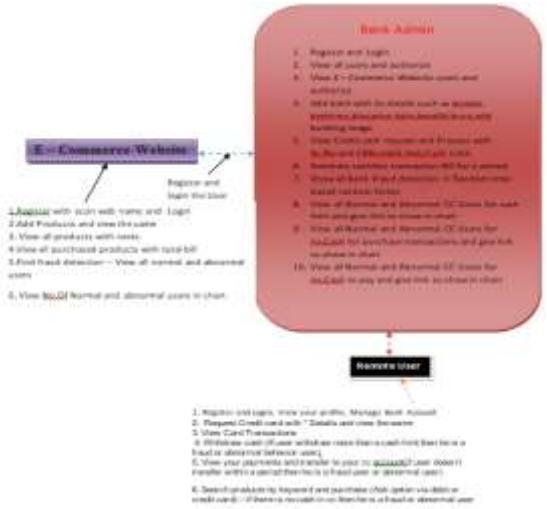


Fig 1: Architecture of Proposed Work

As illustrated in Fig.1 there are three entities in our system: Bank Admin, E-commerce User, User.

3.1 Bank Admin:

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as View all users and authorize, View E – Commerce Website users and authorize, Add bank with its details such as ,View Credit card request and Process with ,Generate card transaction Bill for a period, Show all Bank Fraud detection in Random-tree-based random forest ,View all Normal and Abnormal CC Users for cash limit and give link to show in chart, View all Normal and Abnormal CC Users for no.Cash for purchase transactions and give link to show in chart, View all Normal and Abnormal CC Users for no.Cash to pay and give link to show in chart.

3.2 E-commerce User:

In this module, there are n numbers of users are present. Transport Company user should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Add Products and view the same ,View all products with ranks, View all purchased products with total bill ,Find fraud detection ,View all normal and abnormal users ,View No.Of Normal and abnormal users in chart.

3.3 User:

In this module, there are n numbers of users are present. User should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like View your profile, Manage Bank Account, Request Credit card, View Card Transactions ,Withdraw cash, View your payments and transfer to your cc account, Search products by keyword and purchase ,View all purchased products.

4. METHODOLOGY

In this section, we present the detailed design of our scheme such as Randomized credit card numbers, Blockchain, Implementation

4.1 Randomized Credit Card Numbers

In order to prevent stores and businesses from collecting information about their customers, randomized card numbers can be used. If a customer wants to purchase a product through E-commerce sites they firstly need to have a account in any bank. The user must be authorized by the Bank Admin, then only he can login to that particular Bank website.

The randomized card system would behave similar to a VPN (Virtual Private Network) used for Wi-Fi connectivity. When a mobile device is searching to connect to a Wi-Fi signal, without using VPN, it sends out it's real IP address (Internet Protocol address) . On the other hand, a VPN allows for the mobile device to send out a proxy IP address, then authenticate the network, then give out it's real IP address. The randomized credit card system will consist of a primary account number which is developed by using the randomized technique. So that the random number will be assigned as credit number. When an account holder wants to check their transaction history, they can log into their bank's app or website and check their purchases in real time.

4.2 Blockchain

Another system that all levels of government will need to set in place will be a nationalized blockchain network, which will handle tracking transactions in a secure and private manner. According to Melanie Swan's Blockchain: Blueprint for a New Economy, blockchain operates as a public ledger of all transactions [8].

ISBN: 978-93-91303-04-04

The blockchain will have complete information related to each transaction and the data of each person involved in said transaction. Such technology is more secure than other record-keeping systems. Blockchain's ability to track in real-time allows for the elimination of error handling, which also allows for improved traceability. Such a feat would first need to be built by the collective efforts of developers, engineers and designers. Regulations and operators/maintainers can be established through lawmakers initially passing laws that address who will be operating and maintaining the secure blockchain network and moving the financial aspects of life to the network.

4.3 `Implementation

In order for the public to accept a randomized credit card system, users must either have incentive to switch accounts or no need to switch at all. Incentives to switch bank accounts could be influenced by a publicly accepted need for increased privacy. If the randomized credit card system is made into a standard, then every bank can adopt and implement it for their users. This task will not be simple but would provide the best possible outcome for users, which would be more privacy and minimal hassle. Regarding blockchain, the previously listed features will provide increased privacy and security to users to those living and working in the United States. To successfully roll out such changes to the modern financial system, education and public outreach will be essential. Focusing on the privacy and security aspects concerning a cashless society, this stage is aimed to prepare future members for a life after cash. A public awareness campaign would emphasize gaining and improving upon knowledge and under-standing of current privacy laws and other practices regarding finances. This policy-oriented approach would primarily focus on pre-emptive privacy and security while increasing technological literacy throughout the population. Pre-emptive privacy can be defined as client-side decisions which have a positive effect on the level of privacy and/or security of their data (before implementing strategies like blockchain and other forms of encryption). In 2019, there were 1,473 data breaches, with 164,683,455 records containing sensitive data released .

5. RESULT

This project identified the need for privacy & security in cashless society. Here, the results that are observed in the project.

5.1 Bank Admin Page

Fig 5.1 Bank Admin Page

Description: This is the Bank admin login page. The bank admin can login by using the credentials or if he/she is new they can register by filling details.

5.2 E-commerce Login Page

Fig 5.2 E-commerce login Page

Description: This is E-commerce login page. The E-commerce admin can login by using the credentials. If they are new they can register.

5.3 User Login Page

Fig 5.3 User Login Page

ISBN: 978-93-91303-04-04

Description: This is User login page. He can login by giving correct credentials. If he/she is new then they have to register after bank admin authorize them then only they can login to the site.

5.4 Random Credit Card Numbers

Fig 5.4 Random Credit Card No

Description: After creating an account ser can request for a credit card for future purchases. Bank admin will issue a random credit card number to the user.

6.CONCLUSION

A cashless society poses risks for its members because data and metadata about their transactions are being collected and used. Our group has found the idea of a cashless society to involve many systemic complexities. Within the complex system, opportunities arise to implement Sometimes the best solution to a problem is the culmination of multiple approaches. Spreading information to the general public helps people learn about the systems they are using and allows for them to make informed decisions. Blockchain helps promote privacy and security through its authentication process. Randomized credit cards help users keep their account numbers private. All three approaches are effective ways of adapting to a dynamic currency system. By the proposed system we raised the standards for privacy and security in the cashless society. As user will be aware of the online transactions and they can identify the abnormal usage of their account. While, the bank admin can identify the normal and abnormal users so that they can unauthorize the abnormal users. It will be hard to breech the data by unauthorized persons.

7. REFERENCES

[1] “Bitcoin - Open Source P2P Money.” n.d. Accessed December 12, 2019.https://bitcoin.org/en/.

[2] Wolters, Timothy. ”‘Carry Your Credit in Your Pocket’: The Early History of the Credit Card at Bank of America and Chase Manhattan.”Enterprise& Society 1.2 (2000): 315-54. Print.

[3] Mercer, Christina. n.d. “History of PayPal: 1998 to Now.” Techworld.Accessed December 12, 2019.https://www.techworld.com/picturegallery/business/history-of-paypal-1998-now-3630386/.

[4] Meadows, Donella H., and Diana Wright. Thinking in Systems: a Primer. Chelsea Green Publishing, 2015.

[5] Andrew Ferguson, The rise of big data policing: surveillance, race, and the future of law enforcement,” New York; New York University Press,2017.

[6] “The Rise of Big Data Policing — TechCrunch.” n.d. Accessed February 5, 2020. https://techcrunch.com/2017/10/22/the-rise-of-bigdata-policing/.

[7] Symanovich, Steve. “What Is a VPN?” Official Site,us.norton.com/internetsecurity-privacy-what-is-a-vpn.html.

[8] Swan, M. (2015). Blockchain: Blueprint for a New Economy. Sebastopol,CA: OReilly Media, Inc.

[9] 2019 Data Breaches - Identity Theft Resource Center. (2020). Retrieved27 March 2020, from https://www.idtheftcenter.org/2019-data-breaches/

[10] ”Leverage Points: Places To Intervene In A System.” The Academy for Systems Change.N. p., 2020.Web. 3 Feb. 2020.

[11] ”What’s New In The 2019 Cost Of A Data Breach Report.” SecurityIntelligence.N. p., 2020.Web. 6 Feb. 2020.

[12] Arthur, W. (2018, March 23). Lawsuits may be key to tighter US data privacy rules.

[13] Arthur, W. (2018, March 23). Lawsuits may be key to tighter US data privacy rules. Retrieved March 26, 2020, fromhttps://dailybrief.oxan.com/Analysis/DB230635/Lawsuits-may-bekey-to-tighter-US-data-

IoT Based Health Monitoring System

P. Nagendra Kumar[1]R.Jayakeerthi[2] Ch. SaiSriDurga[3]A. Supraja[4]M. Kavya[5]
Associate Professor[1], UG Scholar[2, 3, 4, 5]
[1, 2,3,4,5]Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

ABSTRACT

Nowadays Health-care systems have been developed rapidly with the advancements in science and technology. Due to the evolution of IoT, many health care systems have been developed based on IoT technology. Patients are facing a problematic situation of unforeseen demise due to the specific reason of heart problems and attacks which is because of non-monitoring of the health condition of patients. This system is developed specifically for monitoring the health condition of patients and informing their health-related factors to their concerned doctors and loved ones. This system makes use of different sensors such as temperature sensor, pulse oximeter, vibration sensor in combination with Wi-Fi module for tracking patient's health conditions and movements and passing the information to the concerned doctors to make specific actions when the measured parameters show abnormality. Through this system, time-to-time monitoring of health condition of patient is measured with different timestamps and passed to the concerned doctors, which in turn enables the doctors to save the lives of patients in critical conditions.

KEYWORDS

IoT, Health care system, Sensors, Wi-Fi module

1.INTRODUCTION

During this present pandamic situation taking care of our loved ones is becoming difficult, this monitoring of patietns health condition can be made easy by using Internet of Things (IoT). Due to present living conditions, continuous monitoring of human health is necessary. For the remote health diagnosis system, health monitoring methods through technology is the key factor.In general patient health monitoring and diagnosis, patients should consult the doctor physically and has to give all the information through the physical checkup. Doctor needs Blood Pressure (BP), Body Temperature (BT), Pulse rate etc for initial analysisor for constant monitoring of patient or it may not be possible to consult doctor physically. It is difficult to contact the Doctor due to their present living conditions, poor economic status, and due to scarce transport facilities, lack of adequate time and other human problems. Some of the rural or urban people are in high risk and may require the continuous monitoring of their health conditions [5,8].

Oxygen (O_2) is one of the most important elements needed to withstand ourlife. The life of the human bodydepends on the amount of oxygen levels present in the human body. The protein hemoglobin, found in red blood cells, bounded to O_2 that delivers 98% of oxygen to cells is known as Oxy hemoglobin (HbO_2). Theoxygen saturation (SpO_2) is the percentage of HbO_2 in arterial blood. This calculation may help to the blood circulation and life span of the human life. In the beginning, SpO_2 wasmeasured by taking samples of blood and measuring Oxygen levels directly. This method was incapable to deliver real-time measurements.This measuring technique made it impossible for SpO_2 to be recognized as an important measure of wellness until a non-invasive method of measuring SpO_2 in real-time was established. In this work we focus on smart health to people health through the development of a sensor hardware circuit, app is developed to both the patient and the doctor for one-to-one communication [2,9]. In this process, Bluetooth also plays a vital role in data transmission between patient, hardware circuit and the communication device. Finally compared the measured information with the existing devices is validated. It can be extended with the help of wireless sensor networks and cognitive radio spectrum sensing techniques for data transmission globally[10,11].

2.LITERATURE SURVEY

R. Paradiso, G. Loriga, and N. Taccini proposed a paper [1] on A wearable health care system based on knitted integrated sensors in 2005. A comfortable health monitoring system named WEALTHY is presented. The system is based on a textile wearable interface implemented by integrating sensors, electrodes, and connections in fabric form, advanced signal processing techniques, and modern telecommunication systems. Sensors, electrodes and connections are realized with conductive and piezoresistive yarns. The sensorized knitted fabric is produced in a one step process. The purpose of this paper is to show the feasibility of a system based on fabric sensing elements. The capability of this system to acquire simultaneously several biomedical signals (i.e., electrocardiogram, respiration, activity) has been investigated and compared with a standard monitoring system. Furthermore, the paper presents two different methodologies for the acquisition of the respiratory signal with textile sensors. Results show that the information contained in the signals obtained by the integrated systems is comparable with that obtained by standard sensors. The proposed system is designed to monitor individuals affected by cardiovascular diseases, in particular during the rehabilitation phase. The system can also help professional workers who are subject to considerable physical and psychological stress and/or environmental and professional health risks.

A. Pantelopoulos and N. Bourbakis proposed a paper [2] on A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis in 2010. The design and development of wearable biosensor systems for health monitoring has garnered lots of attention in the scientific community and the industry during the last years. Mainly motivated by increasing healthcare costs and propelled by recent technological advances in miniature biosensing devices, smart textiles, microelectronics, and wireless communicatoins, the continuous advance of wearable sensor-based systems will potentially transform the future of healthcare by enabling proactive personal health management and ubiquitous monitoring of a patient's health condition. These systems can comprise various types of small physiological sensors, transmission modules and processing capabilities, and can thus facilitate low-cost wearable unobtrusive solutions for continuous all-day and any-place health, mental and activity status monitoring.

A. Benharref and M. Serhani proposed a paper [3] on Novel cloud and SOA-based framework for E-Health monitoring using wireless biosensors in 2014.Various and independent studies are showing that an exponential increase of chronic diseases (CDs) is exhausting governmental and private healthcare systems to an extent that some countries allocate half of their budget to healthcare systems. To benefit from the IT development, e-health monitoring and prevention approaches revealed to be among top promising solutions. In this paper, they proposed a framework to collect patients' data in real time, perform appropriate nonintrusive monitoring, and propose medical and/or life style engagements, whenever needed and appropriate. The framework, which relies on service-oriented architecture (SOA) and the Cloud, allows a seamless integration of different technologies, applications, and services. It also integrates mobile technologies to smoothly collect and communicate vital data from a patient's wearable biosensors while considering the mobile devices' limited capabilities and power drainage in addition to intermittent network disconnections. Then, data are stored in the Cloud and made available via SOA to allow easy access by physicians, paramedics, or any other authorized entity.

LaPlante, PA, Kassab, et all proposed a paper [5] on Building caring health care systems in the Internet of Things in 2018.The nature of healthcare and the computational and physical technologies and constraints present a number of challenges to systems designers and implementers. In spite of the challenges, there is a significant market for systems and products to support caregivers in their tasks as the number of people needing assistance grows substantially. In this paper, they presented a structured approach for describing Internet of Things (IoT) for healthcare systems. They illustrated the approach for three use cases and discuss relevant quality

issues that arise, in particular, the need to consider caring as a requirement.

Annam batti, Assad Ali Siyal, Adeel Mehdi, Huma Shah, Hinesh Kumar, Muhammad Ali Bohyo proposed a paper [6] on IoT based remote patient health monitoring systemin 2018.This paper focuses on the development of a novel, rapid and cost-effective tele-monitoring architecture based on an Arduino device hardware system. The prime goal was to design a prototype that could serve as a reliable patient monitoring system, so that healthcare professionals can monitor their patients in real-time, who are either hospitalized in critical conditions or unable to perform their normal daily life activities. In this paper they monitored ECG, saturated oxygen levels and temperature of the patient and transmit the data using Telemetry-viewer, an open-source java programming-based software application.This prototype framework would be helpful to perform real-time tele-monitoring which will ultimately lead to better diagnosis and treatment of remote patient community.

3.PROPOSED WORK

The main objective of the proposed system is to monitor the patient's health condition effectively in real time. Here we use sensors to monitor the patient's health condition and a Node MCU ESP8266 Wi-Fi module to transfer the data to the remote areas through internet. The sensors we used here are the pulse oximeter MAX30100 which is an intergrated sensor used to monitor both pulse rate and saturated oxygen level, DS18B20 temperature sensor which is used to measure accurate temperature and it is a water proof sensor such that we can even measure temperatur of sensor even in wet conditions like sweating and it is an one wire interface which makes connections easy, also we used an SW-420 vibration sensor to monitor the patients condition, it reads the vibration of the sensor and notifies if the vibrations are beyond the sensitivity level and it is also used as a fall detection if more vibrations are recorded. All these sensors are connected according to the following circuit diagram.

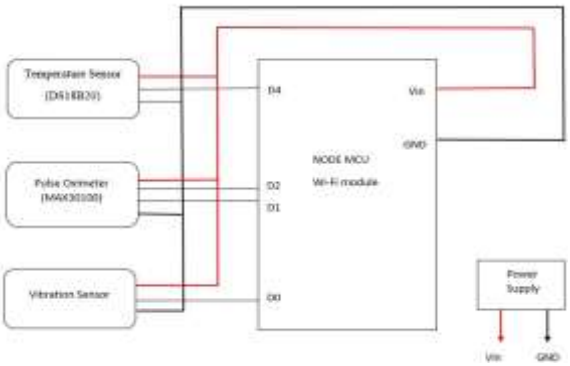


Fig1: Circuit Diagram

The three sensors used are digital sensors such that these sensors are connected to the digital pins of the Here all these sensors are connected by using a Node MCU ESP8266 Wi-Fi module which has a microcontroller within. After connecting the components as per the circuit, we have to dump the code and the code is written in Arduino IDE platform and by selecting the port in the IDE we can dump the code by using the usb cable connected to the system and the Wi-Fi module used. Every sensor requires some power supply here MAX30100 pulse oximeter and vibration sensor SW-420 requires 5V of power and the temperature sensor requires 3.3V of power supply here we used resistors to control the power supply to the temperature sensor and an external power supply is supplied through Node MCU Wi-Fi module.The data that is monitored from these senosrs is transferred to the app environment using Wi-Fi module. The application environment we used here is a blynk application which is a user friendly. Blynk application is the best platform to deal with the IoT projects. Through blynk apllication we can make sure that the data is accessed by the authorized user and the real time monitoring of the patient's health is done effectively through this application.

4.RESULTS

Step1: Code is dumped and the components are connected according to the circuit and given power supply such that the whole system when connected is visible as follows.

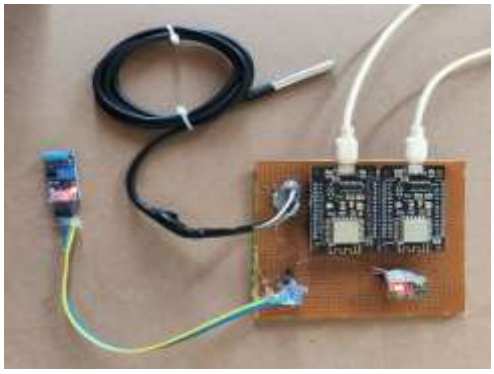


Fig 2: Sytem after connected

Step2: Make sure the internet connection is connected to the Node MCU wi-fi modules in the system inorder to send data to the blynk application.

Step3: when the internet is connected to the system and sensors are connected to the patient we can monitor the temperature, pulse and saturated oxygen levels of the patient in blynk application.

Fig 3: Monitoring patients health through blynk application

Step4: When the patient is suffering from fits, heavy vibrations are produced such that these vibrations are monitored by the SW-420 vibration sensor and an alert message is send to the blynk application notifying a fall detection.

Fig 4: Alert message in blynk application

Step5:Hence, the basic health condition of the patient like temperature, pulse, saturated oxygen level and fall detections are effectively measured and monitored with the help of this system using IoT.

5.CONCLUSION

A new approach for remote measurement and monitoring of the human body parameters based on a wireless sensor network has been presented. The proposed design will be able to effectively measure and monitor human body parameters mutually. This health monitoring system uses sensors, Wi-Fi standard wireless communication protocol for data transfer between the sensors node to the IoT cloud environment, which will allow monitoring of all human body parameters on IoT platform effectively. By using this system, we can monitor the patient's temperature, pulse, saturation oxygen levels and can get an alert message when patient fell down through which we can effectively and efficiently monitor the remote patient's health condition.

6.REFERENCES

[1]. R. Pardiso, G. Loriga and N. Taccini ''A wearable health care system based on knitted integrated sensors'' 2005.

[2]. A. Pantelopoulos and N. Bourbakis ‘‘A survey on wearable sensor-based systems for health monitoring and prognosis’’,” IEEE Trans. Sys., Man, and Cybernetics vol. 40, no. 1, pp. 1–12, Jan 2010.

[3]. A. Benharref and M. Serhani ‘‘Novel cloud and SOA-based framework for e-Health monitoring using wireless biosensors’’ 2014.

[4]. Amr Elsaadany, Amr Sedky and Noor Elkholy ‘‘A triggering mechanism for end-to-end IoT eHealth system with connected ambulance vehicles’’ 2017.

[5]. LaPlante, PA, Kasab ‘‘Building caring health care systems in the Internet of Things’’, IEEE Systems Journal, vol. 12, no. 3, 7862194, pp. 3030-3037, 2018.

[6] Annam batti, Assad Ali Siyal, Adeel Mehdi, Huma Shah, Hinesh Kumar, Muhammad Ali Bohyo “IoT based remote patient health monitoring system”in 2018

[7] Joel J.P.C Rodrigues, Dante Borges De Rezende Segundo, Heres Arantes Junueira, Murilo Henrique Sabino, Rafael Maciel Prince, Jalal A1-Muhtadi, Victor Hugo C. DeAlbuqerque, “Enabling Technologies for the Internet of Health Things” Access IEEE, Vol. 6, pp. 29-13141, 2018.

[8] N. L. Laplante; P. A. Laplante; J. M. Voas,"Stakeholder Identification and Use Case Representation for Internet-of-Things Applications in Healthcare," IEEE Systems Journal, Sept. 2016.

[9] S. Babu, M. Chandini, P. Lavanya, K. Ganapathy, and V. Vaidehi, “Cloud-enabled remote health monitoring system,” in Int. Conf. on Recent Trends in Inform. Tech. (ICRTIT), July 2013, pp. 702– 707.

[10] T. Jagannadha Swamy, S. Avasarala, T. Sandhya, and G. Ramamurthy, “Spectrum sensing: Approximations for eigenvalue ratio-based detection,” in Computer Communication and Informatics (ICCCI), 2012 International Conference on, pp. 1 –5, Jan. 2012.

[11] Swamy, Tata Jagannadha; Prasad, K. V. S.V. R.; Ramamurthy, Garimella, “Novel Energy Efficent Dynamic Routing Protocol for Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science. Sep/Oct2014, Vol. 5 Issue 7, p9- 15

.

Secure and Efficient Dynamic Verifiable Database Scheme in Cloud Based EHR System

Dr. M. Mathan Kumar[1] CH. Harika[2] B. Manjulatha[3] P. Varshitha[4] K. Reema singh[5]
Associate Professor[1], UG Scholar[2, 3, 4, 5]
[1, 2,3,4,5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

Abstract Electronic health record (EHR) is a system that collects patient's digital health information and shares it with other healthcare providers in the cloud. Meanwhile, with the rise of IoT, more low-performance terminals are deployed for receiving and uploading patient data to the server, which increases the computational and communication burden of the EHR systems. The verifiable database (VDB), where a user outsources his large database to a cloud server and makes queries once he needs certain data. To improve efficiency, most existing VDB schemes utilize proof reuse and proof updating technique to prove correctness of the query results. However, it ignores the "real-time" of proof generation. In this project, we propose a publicly verifiable shared updatable EHR database scheme that supports privacy-preserving and batch integrity checking with minimum user communication cost.

Index Terms- Electronic Health Record (EHR), Verifiable Data Base (VDB), Privacy Preserving, Data Integrity, Auditing

Introduction

With the explosive increase of global information, the cloud service industry has been developing unprecedentedly. Many cloud service providers are rushing to cloud launch service platforms and products such as Amazon, GOOGLE, Alibaba, Microsoft etc. As a concrete and high-quality application example of cloud storage, the cloud-based electronic health record (EHR), which is a system that collects the patient's digital health information, is being vigorously promoted by many organizations.

Users actually give up the ultimate control over the EHR's. This brings the security challenges for example, the cloud sever may return the incorrect results various reasons, such as malfunctioning cloud equipment's and hacker's attack. So it returns the serious consequences in medical system. To verify the server responses correctly each time introduced the Verifiable Data Base (VDB).

In this when a client can query the server the item (a message) at position I, the server returns the stored message at this position along with the proof that it is correct answer. The patient EHR's up-loaded to the cloud can be shared among different medical institutions to help patients get better treatment, help scientific researchers to carry out disease analysis and research, and help public health departments predict, detect and potentially prevent the outbreak of epidemic diseases, etc.

The main aim of this project is to propose a publicly verifiable shared updatable EHR database scheme that supports the privacy preserving and batch integrity checking with minimum communication cost, we modify the existing Functional Commitment (FC) scheme for the VBD design and concrete FC under the computational assumptions.

II. Literature Survey

Wei L, Wu C, Zhou S proposed a method "Efficient verifier-local revocation group signature schemes with backward unlinkability" in the year 2009.

Dan B, Shacham H proposed a method called "Group signatures with verifier-local revocation" in the year 2004.

J. Yuan, S. Yu proposed a method "Efficient public integrity checking for cloud data sharing with multi-user modification" in the year 2014.

J. Sun, B. Zhu, J. Qin, J. Hu, and Q. Wu proposed a method "Confidentiality Preserving Publicly Verifiable Computa- tion" in the year 2018.

X. Chen, J. Li, X. Huang, et al proposed a method "New Publicly Verifiable Databases with Efficient Updates" in the year 2015.

W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao proposed a method "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium" in the year 2017.

III. Proposed System

Our research focuses on the security and efficiency of large database storage, such as EHR. According to the characteristics of EHR system, two aspects of security deserve our attention, namely, the server response correctness and the data storage integrity. In order to deal with above problems, we use a new tool called Functional Commitment (FC) and design a publicly verifiable updatable database scheme based on functional commitment supporting privacy-preserving integrity auditing and dynamic group operation. Our construction has fewer parameters and is more efficient than the original scheme.

Our scheme is applicable for large-scale data storage with minimum user communication cost. The scheme preserves data privacy from the auditor by using a random masking technique and the sparse vector is used for sampling auditing.

System Architecture

There are 4 modules in our project i.e, TP Auditor, Cloud Server, Patient and Doctor.

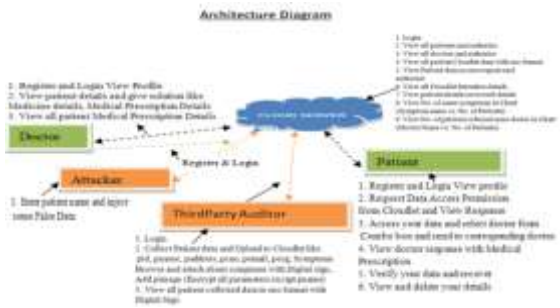


Fig: Architecture

Third party Auditor: In this module, the wearable device Collect Patient data and Upload to Cloud like pid, pname, paddress, pcno, pemail, ppulse, pecg, psymptoms, browse and attach about symptoms with Digital sign, add pimage (Encrypt all parameters except pname) and view all patient collect data in enc format with digital sign.

Cloud Server: The Cloud server manages which is to provide data storage service for the wearable devices and also View all patients and authorize and view all doctors and authorize, View all patient Cloud data with enc format, View Patient data access request and authorize, View all Cloud Intruders details and View patient details recovered details, View No. of same symptoms in Chart (Symptom name vs. No. Of Patients), View No. of Patients referred same doctor in Chart (Doctor name vs. No. of Patients).

Patient: In this module, the patient Register and Login, View profile, Request Data Access permission from cloud and view Response, Access Your data and select doctor from combo box and send to corresponding doctor and View doctor response with medical prescription, verify your data and recover and view and delete your details.

Doctor: The doctor is the one who will perform the following operations such as Register and Login, View Profile, View patient details and give solution like Medicine details, Medical prescription details, View all patient Medical prescription details.

IV. Results

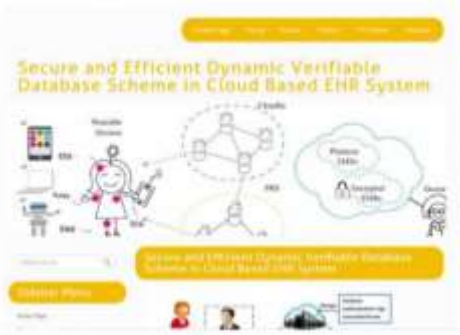


Fig 1: Home Page

Description: Home Page consists of CLOUD, DOCTOR, PATIENT, TP AUDITOR and ATTACKER. Here, it shows the title of the project.

Fig 2:
Login Page for Cloud

Description: In this page, we need to fill the credentials for Cloud login.

Fig 3:
Cloud Profile

Description: Cloud Profile Contains a Cloud Menu in which it can View All Patients and Authorize, View All Doctors and Authorize, View All Patient Cloud Data, View Patient Data Access Request and Authorize, View Patient Recovered Details, View No. of Same Symptoms for the Patients and View No. of Patients Referred to the Same Doctor.

Fig 4:
View All Patients and Authorize

Description: In this page, it will view all the patient details such as Id, Image, Name, Full Details of the Patient and Status of the Patient.

Fig 5:
View Patient Data Access Request and Authorize

Description: In this page, it will view all the patient details such as Id, Name, Requested Date of the Patient and the Status.

Fig 6:
View Patient Recovered Details

Description: In this page, it will view all the patient details who recovered from an attack.

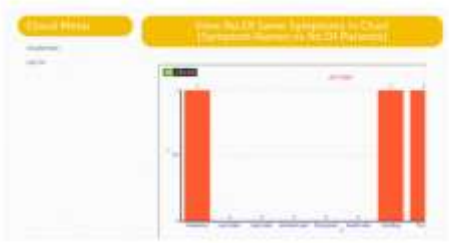


Fig 7:
View No. of Same Symptoms in Chart

Description: In this page, it will show the bar graph indicating Symptoms on X-axis and No. of Patients on Y-axis who are attacked for the same symptoms.

Fig 8: TP Auditor Login

Description: In this page, we need to fill the credentials for TP Auditor login.

Fig 9: TP Auditor Profile

Description: TP Auditor Profile contains Device Menu which consisting of Collect Patient Data and Upload to Cloudlet, and View All Patients Collected Data fields.

Fig 10: Collect Patient Data and Upload to Cloudlet

Description: In this page, it will collect the patient data and upload to cloud.

Fig 11: Doctor Login

Description: In this page, we need to fill the credentials for doctor login.

Fig 12: Doctor Profile

Description: Doctor Profile contains Doctor Menu which consisting of Doctor Profile, View Patient Details and Give Solution and View All Patient Medical prescription fields.

Fig 13: Patient Medical Prescription Details

Description: In this page, it will show the medical prescriptions details of the patient such as Image, Name, Contact Number, E-Mail, Address, Pulses, ECG, etc.

Fig 14: Patient Login

Description: In this page, we need to fill the credentials for Patient login.

Fig 15: Patient Profile

Description: Patient Profile contains Patient Menu which consisting of Patient Profile, Request Data Access Permission From Cloudlet, Access Patient Data and Send to Doctor, View and Delete Patient Details fields etc.

Fig 16: Attacker Login

Description: In this page, we need to fill the patient name to inject the false information.

V. Conclusion

The concept of verifiable database is a great tool for verifiable EHR storage. However, proof reuse and the technique of proof updating by the server to improve system efficiency fails to achieve data integrity checking. In this work, we propose a novel updatable VDB scheme based on the functional commitment that supports privacy-preserving integrity auditing and group member operations, including join and revocation. Our VDB scheme achieves the desired security goals without incurring too much computational increase and provides minimum communication cost for the terminal with limited performance.

VI. References

[1] Wei L, Wu C, Zhou S. efficient verifier-local revocation group signature schemes with backward unlinkability. Chinese Journal of Electronics, 2009, e90-a(2):379- 384.

[2] Dan B, Shacham H. Group signatures with verifier-local revocation. Acm Conference on Computer & Communications Security 2004.

[3] Chaum, David, and T. P. Pedersen. Wallet Databases with Observers. International Cryptology Conference on Advances in Cryptology 1992.

[4] Official Website of The Office of the National Coordinator for Health Information Technology (ONC). (2004). Available:https://www.healthit.gov/.

[5] Canada Health Info way (2001). Available:https://www.infowayinforoute.ca/en/.

[6] J. Sun, B. Zhu, J. Qin, J. Hu, and Q. Wu. "Confidentiality-Preserving Publicly Verifiable Computation", International Journal of Foundations of Computer Science, Vol. 28, No. 06, pp. 799-818, 2018.

[7] X. Chen, J. Li, X. Huang, et al. "New Publicly Verifiable Databases with Efficient Updates". IEEE Transactions on Dependable & Secure Computing, vol. 12, no.5, pp. 546-556, 2015.

[8] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium", Journal of Network and Computer Applications, vol. 82, pp. 56–64, 2017.

DIABETES PREDICTION USING MACHINE LEARNING BASIC AND ENSEMBLE ALGORITHMS – PERFORMANCE VISUALIZATION OF REALTIME DATASET.

P.Chandrakala[1] M. Yathisha Lakshmi[2] S.Lohitha[3] Ch. Lakshmi Priya[4] T. Niveditha[5]Assistant Professor[1], UG Scholar[2, 3, 4,5]

[1, 2, 3, 4,5] Department of CSE, Geethanjali Institute of Science and Technology,Nellore, Andhra Pradesh.

***Abstract*—**Nowadays Diabetes is one of the most rapidly growing diseases which makes the biggest contribution to morbidity and mortality worldwide. Diabetes is a group of metabolic disorders defined by high blood glucose levels over a prolonged period. Although this disease is familiar as a hereditary disease, many people are suffering from this disease without having a family background. If diabetes is not in control, the level of glucose goes up and it may cause damage to small vessels in the human body which appear most often in the nerves, feet, eyes even in the heart and kidneys. To get rid of these issues, it is very crucial to predict diabetes at an early stage. Hence, we have decided to do research on diabetes prediction using Some basic and ensemble Machine Learning algorithms. In this study, we have used five popular Machine Learning algorithms called AdaBoost, Bagging, Random Forest, Logistic Regression, and Support Vector Machine. To train and test the algorithms we have collected real-time information of both diabetic and non-diabetic people. The dataset contains 768 instances with 8 unique risk factors. By taking that dataset we will predict diabetes and visualize algorithms performance using F1 scores and get to know which algorithm gives a precise prediction of diabetes.

Keywords-Machine Learning, Classification, Prediction, Adaboost, Bagging, Random Forest, Logistic Regression, Support Vector Machine.

I. INTRODUCTION

Diabetes is a metabolic disease, which causes high blood sugar due to less amount of insulin in the blood. The insulin hormone makes the sugar to move from blood into the cells of human body to be stored or used for energy. With diabetes, human body either doesn't make enough insulin or can't effectively use the insulin which is made. In general, the symptoms of high blood sugar result in frequent urination, feeling thirsty, increased hunger. If it is not medicated, it will lead to severe complications like cardiovascular disease foot sores, and eye blurriness. This may lead to death. When there is a rise in sugar level of blood, it is referred to as prediabetes. Prediabetes isn't therefore great than the traditional worth. Diabetes has been one of the fastest spreading diseases in the present world. According to statistics, by the end of 2017, approximately 425 million people aged between 20 to 79 years were having diabetes and it is estimated that this number will rise to 629 million before 2050. By 2015, 30.2 million or 9.4% of Americans were affected by diabetes, among them, 1.25 million were children. Every year 1.5 million newly affected Americans are joining in this list. Among the matured people in the top five South-East Asian countries, Bangladesh was the second on the list with 5.2 million diabetic patients in 2013. It is estimated that this number will rise to 8.20 million in 2037. So, it is clear that diabetes has been a universal problem and it's high time to find out the best practical solution for diabetes prediction.

Machine Learning (ML), is the field of Data Mining and the study of algorithms where these types of problems can be solved using ML approaches and sample datasets.

The motive of our work is to analyze diabetes patients' datasets to recognize diabetes accurately using three ML algorithms, AdaBoost, Bagging, and Random Forest (RF).

II. LITERATURE SURVEY

Ayman Mir et al have performed an analysis to predict diabetes disease using ML techniques on big data of healthcare. They used several ML algorithms such as Naive Bayes, Support Vector

Machine (SVM), Random Forest and Simple CART. The dataset contains 9 attributes with having both numerical and nominal values. The obtained accuracy for Naive Bayes is 77%, SVM is 79.13%, RF is 76.5%, and Simple CART is 76.5%. Another research performed for the purpose of indicating the critical features for predicting diabetes. The algorithms have been used in this research are Logistic Regression (LR), SVM and RF. In the analysis, researchers found RF as the best algorithm to predict diabetes which gave 84% accuracy.

Deepika Verma and Nidhi Mishra conducted a study to identify DM by using a dataset on Naive Bayes, J48, Sequential Minimal Optimization (SMO), MLP, and Reduces Error Pruning Tree (REP-tree) algorithms and they found SMO to give 76.80% accuracy on diabetes dataset .

D. Dutta, D. Paul and P. Ghosh published a paper called Analyzing Feature Importance for Diabetes Prediction using Machine Learning .This paper discovered what are the critical elements for the reason for diabetes. Variable and feature choice have turned into the focal point of much research in regions of utilization for which datasets with tens or a huge number of factors are accessible.

Another research team S. Manna, S. Maity, S. Munshi and M. Adhikari analyze the diabetes prediction as The classification and predictive analysis algorithm to predict the important factors for the cause of diabetes and discussed how the predictive model can be implemented in the cloud environment to make a model non-temporal, which will be helpful to find, probability of a person getting a diagnosis of Diabetes in future

N.Sneha and Tarun Gangil proposed method aims to focus on selecting the attributes that available in early detection of diabetes using predictive analysis. Algorithms implemented are as follows: Naïve Bayes, random forest, decision tree. Study proves that naïve Bayesian has accuracy of 82.30%.

Another research team as M. Raihan, Muhammad Muinul Islam, Promila Ghosh, Shakil Ahmed Shaj, MubtasimRafid Chowdhury, SaikatMondal, Arun More proposed a method A Comprehensive Analysis on Risk Prediction of Acute Coronary Syndrome Using Machine Learning Approches Acute Coronary Syndrome (ACS) is liable for the sudden death. The originator of tachycardia is a drug addiction, hyperpiesia polygenic disorder, and lipidemia.
The precision and recall for AdaBoost are 0.741; 0.75 and for Bagging 0.755; 0.763 respectively.

III. PRESENT WORK

The present work focuses on ensemble machine learning algorithms as well as basic machine learning algorithms as shown in the figure below.
The algorithms we used for comparison are Bagging, Adaboost, Random Forest, Support Vector Machine, and Logistic Regression. By this, we will get to know which algorithm produces higher F1 scores and is used for the prediction of diabetes.
So, in our study, a comparison of different machine learning algorithms reveals which algorithm best suits diabetic prediction.

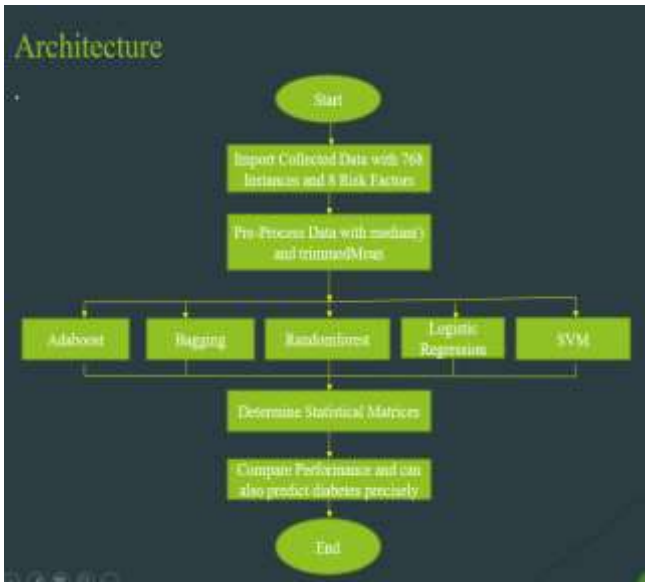


Fig1 Architecture of diabetes prediction

3.1 Dataset Collection

The dataset contains seven hundred and sixty-eight instances and nine unique factors. The dataset features are:

- Number of pregnancies
- Glucose level
- Blood Pressure

- Body Mass Index (BMI)
- Skin fold thickness in mm
- Insulin value
- Hereditary factor-Diabetes Pedigree function
- Age of patient in years

Percentage split option is provided for training and testing of data. Out of 768 instances 80 % is used for training and 20% isused for testing.

3.2 Pre-processing

Pre-processing refers to the transformations applied to our dataset before providing the dataset to the algorithm/model. The Data Preprocessing technique is used to convert the raw data into an understandable data set. In other words, whenever the information is gathered from various sources it is collected in raw format that isn't possible for the analysis. Fig 1 Shown below data preprocessing.
The collected dataset had a number of missing information. We used the median function to manage those missing information and sometimes we may also use trimmedMean() to drop a certain percentage of the minimum and maximum observations and take the mean of the rest scores in the dataset.

Fig2 Preprocessing Steps

3.3 Training Data and Test Data

The training dataset in Machine Learning is used to train the model for carrying out plenty of actions. Detailed features are fetched from the training dataset to train the model. These structures are therefore combined into a prototype. Therefore, if the training set is labeled correctly, then only the model will be able to obtain something from the features. So, for testing the model such type of data is used to check whether it is predicting correctly or not. The ratio of training and test data in our dataset is 4:1.

3.4 Application of algorithms

3.4.1 Adaboost:

The AdaBoost algorithm is short for "Adaptive Boosting" which is a Boosting technique that is used as an Ensemble Method in Machine Learning. It mainly works on the principle where learners are grown sequentially. In this, Boosting is used to reduce bias as well as the variance for supervised learning.

It makes n number of decision trees during the training phase of data. As the first model is made, the record which is incorrectly classified during the first model is given more priority. Among all, only these records are sent as input for the second model.

The process will go on until the number of trees we set to train is reached.

3.4.2 Bagging:

Bagging also called as bootstrap aggregation is an ensemble machine learning algorithm designed to improve the stability and accuracy of machine learning algorithms.

It is used in statistical classification and regression.

Bootstrap =sampling of data

Aggregation =combining the models

Base model = Low bias and High varianceRandom Forest is an ensemble machine learning algorithm. It contains a number of decision trees on various subsets of the given dataset. In this process the final prediction is done by taking the majority voting from all the models. The greatest number of trees in the forest leads to higher accuracy and prevents the problem of over-fitting.

3.4.4 Support Vector Machine

Support Vector Machine" (SVM) is a supervised machine learning algorithm that can be used for both classification or regression challenges. However, it is mostly used in classification problems.

In the SVM algorithm, we will plot each data item as a point in n-dimensional space (where n is number of features you have).

Then, we will perform classification by finding the hyper-plane that differentiates the two classes very well.

Support vectors are simply the nearest data points of the hyper plane.

3.4.5 Logistic Regression:

Logistic regression is a supervised Machine Learning algorithms, which is used for classification problems.
This algorithm is used for predicting the categorical dependent variable using a given set of independent variables.
It gives the probabilistic values which lie between 0 and 1.The value of the logistic regression must be between 0 and 1, which cannot go beyond this limit, it forms a curve like the "S" form. The S-form curve is the Sigmoid function or the logistic function.
That is used to map the predicted values to probabilities. threshold value, which gives the probability of either 0 or 1.
Such as values above the threshold value tends to 1, and values below the threshold value tends to 0.

3.5 Determining statistical Matrices:

3.5.1 Precision:

The precision can be defined as the number of TP(True Positive) upon the number of TP '+' number of FP(False Positive). False positives are cases where the model is incorrectly tagged as positive that are actually negative.

$$\text{Precision} = \frac{TP}{TP+FP}$$

5.2 Recall:

The recall can be defined as the number of true TP(True Positive)separated by the TP'+'FN (False Negative).

$$\text{Recall} = \frac{TP}{TP+FN}.$$

3.5.3 F1 Score:

F1, a function defined for Precision and Recall. F1 Score is needed when you want to seek a balance between Precision and Recall and if there is an uneven class distribution (more number of actual negatives).

$$F1 = 2*\frac{Precision*Recall}{Precision + Recall}$$

3.5.4 Accuracy:

Accuracy is defined as the percentage of correct predictions over the total number of predictions for the test data.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}.$$

3.6 Performance Analysis

After taking the input dataset, the model will predict the data by applying the ML algorithms and provide the best result in the form of classification factors like precision, recall, F1 score and accuracies to predict the best algorithm that will give a precise result of realtime dataset.

IV. RESULTS AND ANALYSIS

The system is developed using Python language with necessary libraries. We have implemented this by using five machine learning basic and ensemble algorithms on the dataset for diabetes prediction. The below figure shows the comparison of F1 scores of all the five algorithms and It clearly states that Logistic Regression with Tuning model gives highest F1 score which best suits to reach the motive of our project.

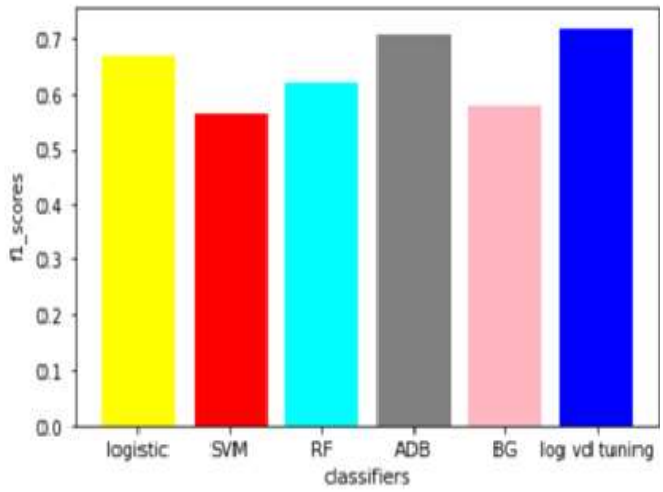


Fig: Comparison of F1 scores of all five algorithms

Algorithms	Accuracy	F1 scores
Logistic Regression	0.8181	0.667
Support Vector Machine	0.7594	0.574
Random Forest	0.8051	0.681
Adaboost	0.8116	0.707
Bagging	0.7727	0.578

Table1: Accuracies and F1 scores of all algorithms

The comparison between Logistic Regression, Support Vector Machine, AdaBoost, Bagging and Random Forest algorithms have been shown in Table1 based on F1 scores and Accuracies of each algorithm.

V. CONCLUSION

Though we have met some significant limitations, we have finished the study flourishingly with our expected outcomes. At the beginning stage, we faced several problems. For example, collection of real time data was one of the main problems and there were a number of missing information. But we have filled up the missing information by using Machine Learning techniques. Among the five algorithms we used, Logistic Regression gave the best performance than all other algorithms used. So, the Logistic Regression with tuning algorithm is used to predict diabetes of real time patient test reports precisely.

VI. REFERENCES

[1] "9 Symptoms of Type 1 & Type 2 Diabetes: Complications, Causes & Diet", Medicine Net, 2019. [Online]. Available: https://www.medicinenet.com/diabetes mellitus/article.htm. [Accessed: 05- Jul- 2019].

[2] "International Diabetes Federation - What is diabetes", Idf.org, 2019. [Online]. Available: https://www.idf.org/aboutdiabetes/what-isdiabetes. html. [Accessed: 08- Jul- 2019].

[3] "Statistics about Diabetes", Diabetes.org, 2019. [Online]. Available:https://www.diabetes.org/resources/statistics/statistics-about-diabetes. [Accessed: 10- Jul- 2019].

[4] R. Hira, M. Miah and D. Akash, "Prevalence of Type 2 Diabetes Mellitus in Rural Adults (¿ 31years) in Bangladesh", Faridpur Medical College Journal, vol. 13, no. 1, pp. 20-23, 2018. [Accessed 16 July 2019].

[5] "Machine Learning - Definition and application examples", Spotlightmetal.com, 2019. [Online]. Available:https://www.spotlightmetal.com/machine-learning–definition-andapplication-examples-a-746226/. [Accessed: 17- Jul- 2019].

[6] A. Mir and S. Dhage, "Diabetes Disease Prediction Using MachineLearning on Big Data of Healthcare", in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018.

[7] D. Dutta, D. Paul and P. Ghosh, "Analysing Feature Importances for Diabetes Prediction using Machine Learning", in 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2018.

[8] M. Raihan, Muhammad Muinul Islam, Promila Ghosh, Shakil Ahmed Shaj, MubtasimRafid Chowdhury, SaikatMondal, Arun More, "A Comprehensive Analysis on Risk Prediction of Acute Coronary Syndrome Using Machine

Learning Approaches“, in 2018 21st International Conference of Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2018, pp. 1 - 6.

[9] D. Kinge and S. Gaikwad, “Survey on data mining techniques for disease prediction”, International Research Journal of Engineering and Technology (IRJET), vol. 05, no. 01, pp. 630-636, 2018. [Accessed 21 July 2018].

[10] S. Manna, S. Maity, S. Munshi and M. Adhikari, “Diabetes Prediction Model Using Cloud Analytics”, in 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 2018.

[11] D. Verma and N. Mishra, “Analysis and prediction of breast cancer and diabetes disease datasets using data mining classification techniques ”, in 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 2017.

[12] W. Xu, J. Zhang, Q. Zhang and X. Wei, “Risk prediction of type II diabetes based on random forest model”, in 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, India, 2017.

[13] H. Emblem, “When to use a Trimmed Mean”, Medium, 2018. [Online]. Available: https://medium.com/@HollyEmblem/when-to-usea-trimmedmean-fd6 aab347e46. [Accessed: 24-Jul-2019].

[14] “TrimMean function R Documentation”,Rdocumentation.org. [Online]. Available:www.rdocumentation.org/packages/sscore/versions/1.44.0/topics/trimMean. [Accessed: 25-Jul-2019].

[15]“Median”,RDocumentation,2019.[Online]. Available:https://www.rdocumentation.org/packages/stats/versions/3.5.2/topics/median. [Accessed: 01- Aug- 2019].

[16] H. Kandan, “Bagging the skill of Bagging(Bootstrap aggregating).”, Medium, 2018. [Online]. Available:https://medium.com/@harishkandan95/bagging-the- skill-of-baggingbootstrap-aggregating-83c18dcabdf1. [Accessed: 04- Aug-2019].

[17] Brownlee, J. (2016). Master Machine Learning Algorithms. 1st ed.pp.137-138.

[18] “How Random Forest AlgorithmWorks in Machine Learning”, Medium,2019. [Online]. Available: https://medium.com/@Synced/how-randomforest-algorithm-works-in-machine-learning-3c0fe15b6674. [Accessed:06- Aug-2019].

[19] “What is a False Positive Rate?”,Corvil, 2019. [Online]. Available:https://www.corvil.com/kb/what-is-a-false-positive-rate. [Accessed: 07-Sep- 2019].

Rivacy Preserving And Verifiable Data Sharing Schema Using Cp-Abe And Blockchain Technology In Vehicular Social Networks

V. Bharathi[1] D. Vidya Reddy[2] N. Pravallika[3] K. Mounika[4] T. Venkata Sukanya[5]
Associate Professor[1], UG Scholar[2, 3, 4, 5]
[1, 2, 3, 4, 5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

Abstract –vehicular social networks (VSN's) maintain various kinds of services such as traffic chiefs, road prosperity, and sharing data In any case, its immense extension and dynamic association structure presents new security challenges. In standard CP-ABE plans, access procedure is taken care of and yielded by the cloud, which needs legitimacy due to centralization. In this project, we propose a secured and obvious one-to-various data sharing intended to deal with the above issue. We use blockchain to record the passageway system, recognizing customer self-insistence and cloud non-repudiation. We propose a convincing arrangement for self-certification. Meanwhile, considering the tricky information associated with the passageway methodology, we propose a methodology hiding plan. Our arrangement also maintains data renouncement when a vehicular customer doesn't meet requirements to share the data in VSNs.

Index terms – CP-ABE, Vehicular Social Network, data revocation.

I. INTRODUCTION

Vehicular uncommonly selected association (VANET) is a capably changing environment pursues to arrange data sharing distant capacity to the vehicles. A conclusive goal of VANET is to give the ubiquitous accessibility among drivers and explorers all over town [1]. A VSN includes a social occasion of individuals who may have typical interests, tendencies or necessities in a setting of transient and spatial closeness. The customers in VSNs may share some tricky data, similar to course, parking space, driver's information, and so forth Meanwhile, in view of VSN's dynamic association structure, data putting away and multi-hop transmission are essential for sharing data. Regardless, the data may be spilled in these two cycles, so much that, security confirmation is crucial in VSNs [2-5].

To guarantee security, scramble the data preceding sharing. A make way is to scramble the data with the public keys of other vehicular customers, which disastrously is inefficient for one-to-various data sharing. Furthermore, access control is in like manner central in data sharing [6-11]. For example, the head of a taxi association needs to share private voice message to male taxi drivers whose ages are near 25 years old. He essentially needs to portray a passageway control procedure: [male]∧[taxi driver]∧[more than 25 years old], then the customers satisfying the passageway system can get to the data.

To handle the security issue in standard CP-ABE, we need to recognize scattered induction control. Blockchain is an emerging decentralized plan and flowed enlisting perspective key Bitcoin and other computerized monetary forms, and has actually pulled in genuine thought from fluctuating foundations [13]. The essential credits of blockchain are decentralization, straightforwardness, self-rule and non-changing [14]. It's anything but's a record, which records trades between two get-togethers. At the point when recorded, the trades can't be adjusted, so much that, we can use blockchain to handle the issue in regular CP-ABE. We can record the passage control methodology on the blockchain to recognize customer self-affirmation and cloud non-repudiation.

In this endeavor, we propose an ensured and clear data sharing arrangement in VSNs, which relies upon both CP-ABE and blockchain. In our arrangement, we use CP-ABE to recognize one-to-various data sharing. Meanwhile, we use blockchain to record the passageway technique of the data, recognizing customer self-endorsement and cloud non-disavowal. Moreover, considering

the handling limits of the VSNs center, we use a fruitful procedures for certificating.

II. LITERATURE SURVEY

VSNs

In 2006, the possibility of vehicular relational associations was first proposed in Massachusetts Institute of Technology. Moreover, the instructors similarly encouraged a structure named Flosser, which was used to split data between driving partners. From here on out, numerous motor associations, similar to GM and BMW, put social sharing modules into their vehicle structures. Regardless, it's anything but an issue of how to construct casual association normally in VANETs. Lequerica et al. proposed a procedure for building relational association reliant upon IP Multimedia Subsystem and Machine and Machine capacities. In 2019, Cheng et al. [8] proposed trust evaluation in VSNs reliant upon Three-Valued Subjective Logic.

CP-ABE

In 2004, Sahai and Waters [9] proposed a plan named fluffy personality based encryption (FIBE). Information proprietor could divide information between the clients who have a specific arrangement of traits. Bethencourt et al. [6] set forward the principal CP-ABE conspire, which permitted an information proprietor to execute access control by setting up access strategy.

In unscrambling stage, the significant calculation overhead was moved to the cloud worker supplier. Yang et al. [10] proposed to sign each property with the form number, and when some trait was repudiated, information proprietor just refreshed the variant number contained in quality mystery keys and sent them to the lawful clients.

Blockchain

In 2008, the blockchain advancement was proposed by Satoshi Nakamato . The primary justification for this advancement is to offer a response for the twofold spending issue. Blockchain is an emerging decentralized plan and passed on enrolling perspective secret Bitcoin and other cryptographic types of cash, and has actually pulled in heightened thought from changing foundations . The crucial traits of blockchain are decentralization, openness, freedom and non-modifying [7].

III. PRESNT WORK

Our protected and verifiable data sharing structure subject to blockchain in VSNs contains six substances: consortium blockchain members (CBMs), a cloud expert association (CSP), trademark trained professionals (AAs), an overall confirmation authority (CA), a blockchain and data customers (DUs).

CBMs are data owners, and can describe access control plans to finish up who can get to, and send the mixed data to the CSP. Meanwhile, CBMs need to affirm that the ciphertext are gotten precisely by the CSP. AA embraced by an overall unique person help, is at risk for perceiving DUs and creating DUs' characteristic mystery keys inside its association region. Then it sends all the trademark secret keys and relating customer's character uid to the CSP.CA is a totally trusted in overall validation master in the structure.

The blockchain is used to regulate the CSP.

In our system, we use consortium blockchain, whose people are genuine vehicular customer. To prevent toxic attackers, we use Practical Byzantine Fault Tolerance (PBFT) understanding estimation.

DUs are data requesters who are supported by overall extraordinary characters uids. Before getting to data, they can watch that their

qualities satisfy the relating access system through the blockchain.

IV. RESULTS

User Login Page:

Fig: User Login

Description: This is the user login page whereuser can login and can insert or extract data.

Attribute Authority Login Page:

Fig: Attribute Authority login page**Description:** Request consumer should satisfy the attribute authority login by their user id and password.

Data Owner Registration Form:

Fig: Data Owner R

egistration Form

Description: Data Owner registers to the cloud by submitting their personal information.

Data Owner Upload File:

Fig: Data Owner Upload File

Description : Data Owner uploads their files using public key by defining access policy.

Data Consumer Registration Form:

Fig: Data Consumer Registration Form

Description: Data Consumer needs to register to cloud before accessing the data.

Public Key Verification:

Fig: Public Key Verification

Description : The public key of the data consumer is verified to the public key given by the data owner in their access policy.

V. CONCLUSION

In this project, we have proposed a secure and verifiable data sharing scheme in VSNs, which is based on both CP-ABE and blockchain. In our scheme, we have developed CP-ABE to realize one-to-many data sharing. Meanwhile, we have also developed blockchain to record the access policy of the data, realizing user self-certification and cloud non-repudiation. Considering the computing capabilities of the VSNs node, we have proposed an effective scheme for certificating. We have designed a policy hiding scheme to hide the

sensitive information included in the access policy. Our scheme also supports data revocation when a vehicular user no longer wants to share the data on the cloud. In the future, we will research on how to reduce the time of reaching consensus.

VI. REFERENCES

[1] L. Fan, and Y. Wang. "Routing in vehicular Ad Hoc networks: A survey." IEEE Vehicular Technology Magazine, vol. 2, no. 2, pp. 12-22, 2007.

[2] J. Wu et al., "FCSS: Fog computing based content-aware filtering for security services in information-centric social network." 1-1, 2017.

[3] K. Zhang, X. Liang, J. Ni, K. Yang, and X. Shen. "Exploiting social network to enhance human-to-human infection analysis without privacy leakage." IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 607-620, 2018.

[4] H, Ren, et al., “Querying in internet of things with privacy preserving: challenges, solutions and opportunities." IEEE Network, vol. 32, pp. 144-151, 2018.

[5] L. Guo, et al., "A secure mechanism for big data collection in large scale internet of vehicle." IEEE Internet of Things Journal, vol. 4, pp. 601-610, 2017.

[6] Y. Yong, and F. Y. Wang. "Blockchain: The state of the art and future trends." Acta AutomaticaSinica., vol. 42, no. 1, pp. 481-494, April. 2016.

IOT BASED ON-THE-FLY VISUAL DEFECT DETECTION IN RAILWAY TRACKS

RajaKullayi Reddy Y [1] Roopa Sri N [2] Tasleem S [3] Vamsi Krishna P [4] Pavan Kalyan K [5]
Assistant Professor [1], UG Scholar [2,3,4,5]
[1,2,3,4,5] Department of ECE, Srinivasa Ramanujan Institute of Technology, Anantapur, Andhra Pradesh.

Abstract :

Railway transportation requires constant evaluation and timely maintenance to ensure public safety. Periodic manual inspections are tedious and expensive, but the accuracy of defining deformation also depends on the skills and performance of the personnel during the inspection. Robots can be transported by rail to hard-to-reach areas and controlled from the control room to speed up inspections. This document transports a robot on a railway track. The robot includes an infrared sensor for detecting broken tracks and an ultrasonic sensor for detecting constraints. The framework provides image management of the environment, while analyzing the distributed data storage as part of the decommissioned railway image and constraining it to 36 inches. Track defective tracks and visible obstacles, as well as images of abandoned tracks via GPS and the cloud. Then these areas are verified, and full-time managers can conduct more conservative assessments without having to check many areas (not all areas).

1. INTRODUCTION

In transportation frameworks, wellbeing and unshakable quality are the fundamental factors that are constantly being addressed, especially in railroad transportation frameworks. Early inspection systems take railroad safety seriously to ensure a safe journey. Railway disruptions could be assessed by human personnel.In any case, not only is this time-consuming but the precision is second to none as not all interruptions are visible to independent eyes Railroad match in Qatar. Line route evaluations. This interest requires inspection systems that continuously assess the conditions on all roads in Qatar and issue quick maintenance warnings in order to avoid accidents. Throughout the trip, mechanized inspection systems have proven to be a response for faster inspection and assistance. Such elevator designs are standard in their ability to find breaks in the train tracks, similar to the area of the break, and help the caregiver to reach and fix the break in less time. Actions that apply developments in artificial vision to recorded chronicles; or mechanical airplanes, which are robotic structures sent by railways that sense breaks with ultrasonic or infrared sensors. Plan-based courses of action consume an optimal way of removing and separating photos from recorded pearls, and mechanical plans are limited in their ability to unambiguously break using sensors without generating results or images Working a novel motorized structure is proposed that includes a robot that performs the evaluation by a non-hazardous investigation method that depends on visual inspection and the ability to disseminate information containing images. Only abandoned train tracks and robot boundary within the 3-inch range. Railway Defects Abandoned railways are divided into two core parts: internal defects and surface defects. These blemishes can be in the head, weld, or base portion of the splint. The most noticeable defects that appear on railroad tracks are known as RCF (Rolling Contact Fatigue), which are caused by grinding, are high-speed railroad lines. Another standard deformation plan is the one that results from the local climatic conditions and the peculiarities of the facility. High temperatures and humid weather, such as in Qatar, cause heat fixation and wrinkles, also called sun wrinkles, on train tracks. Distortions such as broken train tracks or sun tides are more critical than free balance or advancing vegetation.

2. EXISTING SYSTEM

Rail route Track Inspection Methods

The railway inspection method is based on a contact called non-destructive testing (NDT) or a non-contact voting method based on lost or long-term images of the railway. The following are various examples:

• Contact-based (NDT):

- Ultrasonic testing: This strategy can detect significant internal defects, but not surface and near-surface deformations.

- Eddy current testing: this procedure is based on objection fields; therefore, like MFL, this technique can detect surface defects but cannot distinguish significant inward deformations. To remedy this inadequacy, crossover schedules are available that combine ultrasound and eddy current evaluations.

- Acoustic Emission Testing: This technique is common on steel railways where it is used to separate turning from breakage and total events similar to breakage control.

• Contact-less:

- Visual inspection: This system is the best strategy for uncovering surface defects. It is based on fast cameras that take photos of the train tracks, which are discussed with the back room after confirming the plan of the images received; consequently, it is sensible and productive but requires more computation time. After reviewing that amount of documents, we closed down to start a company that would provide better social standards in a financially smart way of railway break identification and deterrent detection.The strategy uses infrared sensors and ultrasonic sensors and offers numerous advantages over the conventional method.

3. LITERATURE SURVEY

The current normal call structure is based on verbal and telephone calls as a compromise with train route dynamics. Due to the most obvious human obstacles in this field, misunderstandings of information or searching for corresponding relationships have greatly increased. This misunderstanding may lead to unacceptable train missions and eventually train accidents. It should also be noted that the collision avoidance gadget system does not exist because it has nothing to do with the current serious promises of railways. You also need to establish two clear coordination lines between the train and the controlled area or station.

Railway Track

Track-caused crashes are usually achieved through careful screening. Since the track will wear out due to train traffic, the track can form a somewhat disproportionately well-used plan. Disproportionate wear and tear on the track can cause intermittent truck movement, which is called "truck chase". Chasing trucks may be one of the excuses for accidents. The splint breaks smoothly and is easy to be found. The lane departure indicator lights up at the top of the signal, indicating that the lane has been destroyed. When there is no train in the clip. The gatekeeper must investigate. One possible explanation is a perfect railroad interruption. To detect broken rails later, a signal connection welded or bolted to the highest point of the rail must be used. Conquer the lanes and create a continuous track chain.If the splint is only broken or there is an inner hole, the splint will not remember that it has nothing, but the broken splint will continue to generate force to a certain extent. More terrifying and more real. When a train catches fire at the previous crack, the track usually breaks under load.

Break Detection Using LED-LDR

The criterion-related to detectable tear testing is LDR capability. In the proposed plan, the LED is placed next to the rail and the LDR is placed on the other side. Driven Light is not available during normal uninterrupted operation. t falls on the LDR, so the LDR resistance is very high. Therefore, when the LED light falls on the LDR, the LDR resistance will drop, and the magnitude of the drop depends on the power of the scene light. As a result, when the light emitted by the LED deviates from its path due to an interruption or interruption, the LDR value will suddenly drop. This change in resistance indicates that there is a break or something that is almost the same. The rails are severely deformed. In order to detect the current device location when an interruption detection event is about to occur, GPS payees are used, and the limitation is to obtain the current perimeter and length data. s The received information is transmitted via GSM modem. The GSM modem transmits the received information to GPRS, and at the time it compactly showed a certain space on the congested railway. The suggested configuration of the railway area structure includes ARM7 controller, GPS, GSM, LED - LDR Gathering, and GPRS, DC motor.

Savvy Railway Crack Defect Detection

This structure is divided into three parts: microcontroller, IR module, and Zigbee module. The infrared sensor is used to detect when the path is broken. An infrared (IR) transmitter is a type of LED that produces infrared bands and is commonly referred to as an infrared transmitter. The emitted light is captured by the infrared collector on the adjacent side. The emitter and the IR collector must be the same and adjacent to each other so that the transmitted light can directly fall on the authority. Exodus.

4. PROPOSED SYSTEM

The main goal is to distinguish gaps in the trackbed and detect obstacles when driving through the track to avoid accidents and train collisions. This model provides an economically wise solution to the use of infrared sensors to detect broken rails. And a set of ultrasonic sensors that can track specific areas of the faulty track, and then teach them to close the control room through text messages to save many lives. In this proposed structure, we use Raspberry Pi as the microcontroller. The proposed framework consists of an ultrasonic sensor for detecting limits and an infrared sensor for detecting interruptions. L293D motor controller is used to control DC motors. The Raspberry Pi controller is used to control the operation of the sensor and transmit data through the GSM module, which can send messages to any interrupt or interceptor sent to the point where the SMS of the base station is identified. The GPS module is used to obtain the accurate latitude and longitude position of the fault track. Therefore, the proposed framework is competent and skilled. The square outline of the recommended frame is shownbelow

Microcontroller

A microcontroller is an independent unit that can perform functions independently without any prerequisites for additional hardware (such as I/O ports and external memory). The microcontroller core is the center of the processor. Connect to a PC or TV monitor and use a standard console and mouse. The SD card built into the circuit board is like a Raspberry Pi hard drive. It is USB controlled, and the video quality can be connected to ordinary RCA TVs, more modern monitors, and even TVs with HDMI connections. Raspberry Pi has several advantages:

1. Low cost (~$35).

2. Minimize the large payload on the board.

3. Installed Ethernet, Wi-Fi, and Bluetooth, a large number of GPIOs, powered by USB, etc.)

4. Compatible with Linux and Python (making it easy to create applications)

IR Sensor

Infrared (IR) innovations apply to various detectors and controllers. The infrared heater is a translucent diode (LED). Different types of infrared LEDs are identified by their grouping and special properties (such as optical power, frequency, and response). An infrared receiver is also called a sensor because it can detect the frequency and terrible emission of light from infraredmanufacturers.

Infrared receivers are indicated by optical reflections, constellations, unusual devices (such as circular light channels), wide observation points, and the skyline from there. Remote applications, especially in the areas of discovery and management. The infrared transmitter emits infrared rays. If there is an interruption in the track of the railway line, the infrared collector will not receive the emitted infrared, so that this can be recognized by the interruption.

Ultrasonic Sensor

An ultrasonic sensor is an electronic device that detects the distance to an object by emitting ultrasonic waves and converts the reflected sound into an electrical signal. Ultrasonic waves travel faster than detected sounds (such as sounds that can be heard by humans). It consists of two standard components: transmitter (using piezoelectric gems to make sound) and receiver (detecting sound after it reaches and leaves the target). Sensors and objects, the sensor estimates the time elapsed before the sound from the transmitter touches the collector.

Camera

The camera is used to take pictures of trains. The captured images are sent to the cloud along with track location details, and railway authorities can access these images and location details for railway maintenance.

Global Positioning System(GPS)

Fig. 3. GPS Module SIM28M [7]

The Global Positioning System (GPS) is a heading structure that uses satellites, authority, and calculations to synchronize area, speed, and time data for air, sea, and land travel. GPS consists of three proprietary parts called parts that are coordinated to provide information about the area. The Global Positioning System (GPS) was developed to enable military and non-military customers to pinpoint geographic areas. By using global satellites to send information, you can check the distance between and along these lines, and GPS can help you find the possible increase in the range and length of cracks or detectable obstacles.

L293D

L293D is a standard 16-pin motor driver. As the name suggests, it is mainly used for engines. The L293D is configured to only run two DC motors continuously; in addition, the strokes of the two motors can be controlled independently of each other. Therefore, if you have a working voltage of 36V and a working current of less than 600mA, the motor needs to be powered by a mechanized circuit,

such as an operational amplifier, a 555 clock, a progressive input, and even a micrometer roller. For example, Arduino, PIC, ARM, etc., this IC is your right choice. The use of IC in the L293D motor controller is very basic. As far as H-Bridge is concerned, please understand for the time being that the H interface is a device used to start the motor clockwise and counterclockwise.

DC Motor

A DC motor is any type of rotating electric machine that tracks the conversion of direct current to mechanical energy. The most common type depends on the force transmitted by the attractive field. In a wide range of DC motors, there is any type of internal tools, electromechanical or mechanical. For electronic devices that change the direction of the current in the motor part from time to time, DC motors are the most widely used motor type because they can fill the existing DC power dissipation system for lighting. The speed of a DC motor can be controlled in a wide range by using a standard AC voltage or by changing the current intensity in its field winding. Small DC motors are used in tools, toys, and cars. The motor may wear out anywhere through direct current. Lightweight brushed motors for machines and equipment with minimal power. From now on, larger DC motors are used to drive, lift and lift electric vehicles and drive steel mills. In the proposed framework, DC motors are used for the wheels of the robot.

5. METHODOLOGY

The strategy shown here includes the use of sensors to detect faulty tracks and send the data via SMS to the next control center when the faulty track is detected. In this module, we use two specific data sources: infrared and ultrasonic sensors. The ultrasonic transducer emits ultrasonic waves, hits the element, and then returns. When there is an obstacle, the ultrasonic beam will be reflected. Use the formula to test distance = (time to reach a significant level * speed of sound (340 m)/S) to measure distance. The infrared sensor works according to the intensity of light falling on the sensor. The kit properties of the two sensors are common. When the test training exceeds the specified estimated value, it will stop and determine the distance and length of the faulty route through the GPS module, and send it to the base station through the GSM modem.

6.CONCLUSION

The proposed framework allows you to distinguish breaks and seizures on the track. Comparing the proposed structure with traditional positioning technology has many advantages, including the lowest cost, low workload, rapid identification without manual intervention, and shorter inspection time. With this model, we can certainly avoid train collisions and accidents to save many living souls.

7.REFERENCES

[1]Er.Kunduru Umamaheswari and Er.Polepogu Rajesh, " An Arduino based Method for Detecting Cracks and Obstacles in Railway Tracks" International Journal of Electronics, Electrical, and Computational System ISSN 2348-117X Volume 6, Issue 4 April 2017.

[2]N.Karthick, R.Nagarajan, S.Suresh, and R.Prabhu, "Execution of Railway Track Crack Detection and Protection" International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 6 Issue 5 May 2017.

[3] Mr. Shridhar Doddmani, "An Inspection System for Detection of Cracks

Design And Analysis Of Novel Architecture For Signed Carry Save Multiplication

Y Madhusudhana [1] P Divya Sai Teja [2] G Harini [3] M Sai Prashanth [4]B. Nafees Anjum [5]

Assistant Professor[1], UG Scholar[2, 3, 4,5]

[1, 2, 3, 4,5] Department of ECE, Srinivasa Ramanujan Institute of Technology, Ananatapur, Andhra Pradesh.

Abstract—

The most important unit in every electronic device was the arithmetic and logic unit. Throughout the current development, it requires an efficient algorithmic operation like Multiplication and Addition in order for an arithmetic and logic unit towards being relevant. In digital signal processing, artificial intelligence, neural networks, and machine learning, multiplication is perhaps the most crucial function. The VLSI field relies upon on area, power and latency of something like the performance with electronic devices. There in functioning of it's own multiplication operation, the digital signal processing (DSP) significantly influenced. Simultaneous performance enhancement like deferral, power, space and energy efficiency was indeed a problem and is tough to attain. In this respect, it is suggested to provide an effective carry save multiplier (CSM) using the modified square root carry select adder (MSCA) for both the addition of vectors as well as the improved full adder (IFA) instead of a traditional full adder. Its critical path delay (CPD), power, area, power delay (PDP) and area delay (ADP) product for that suggested CSM range were 16x16 multipliers.

20. 1. INTRODUCTION

Energetic Effectiveness Minimization with practically every electronic system and notably mobile devices such as smart phones, tablets and gadgets are among the main design objectives. This reduction with a low performance cost (speed) is widely sought. These Digital Signal Processing Blocks (DSP) were crucial components for many multimedia applications of such portable devices. That computational heart among these blocks is indeed the arithmetical logical unit in which the majority of arithmetic operations in such DSP systems involve multiplication. In order to enhance the processor effectiveness, its development of multiplier speed and energy performance plays an important role. Several DSP cores incorporate algorithms enabling video and image processing, in which the end outputs are either human-made pictures or movies. Which enables us to employ approximations towards speed/energy efficiency improvement? That is because human people are restricted in their perceptive ability to see a picture or video. Besides the use of image and video processing, additional areas weren't crucial to the system's functioning in relation to the accuracy of arithmetic operations. That designer has the capacity to make trade-offs between accuracy, speed and energy usage by using approximation computation. Apart from circuit, logic and architecture levels including algorithms and sound layers, the approach of something like the arithmetic may be accomplished at numerous design abstraction levels. Approximation may be carried out using many strategies, such as permitting timing breaches and methods involving function estimate or a combination of those ways. A variety of approximate arithmetic blocks like supplements and multipliers were proposed at various design levels inside the field of function approximation techniques. We are focusing on offering a low-energy high-speed but approximation multiplier for error-resistant DSP applications. The suggested, area-efficient approximation multiplier is designed by changing the usual algorithm-level multiplication technique using round input values.

2. LITERATURE SURVEY

A reduced complexity Wallace multiplier reduction

Wallace high-speed multipliers uses supplies and half-adders throughout this reduction step. That amount of partial product bits is not reduced by half adders. Thus, the decrease in multiplier difficulty

will result in a minimization of half adders. An amendment to the decrease in Wallace is proposed to guarantee that the delay is identical to the standard decrease in Wallace. The improved reduction approach significantly decreases the number of 50% suppliers; configurations with 80 percent less than typical Wallace high speed multipliers provide that very little growth in the no. of complete suppliers.

Low-cost and high performance 8 X 8 booth multiplier

That article displays an improved power/delay/area radix-4-8 Booth multiplier. That parallel structure has been used to add partially encoded products seems to be the primary improvement for delay reduction. An enhanced Boot encoder, an optimised B2C design as well as A one-square root carrier-select adder with a carrier-look adder logic improves further to reduce multiplier delay. The design reduced power consumption by 26.6%, area consumption by 15%, and data arrival time by 25.6% compared to comparable designs previously reported. In Synopsys CMOS 32 nm together all suggested circuits have been developed and synthesised.

A reduced complexity wallace multiplier reduction, by R. S. Waters and E. E. Swartzlander.

Wallace high-speed multipliers employ full adders & half adders throughout their decreasing phase multipliers. The amount of partial product bits is not reduced by half adders. Thus, the decrease in multiplier complexity would result in a minimization of half adders. An amendment to the decrease in Wallace is proposed to guarantee that the delay is identical to the standard decrease in Wallace. The improved reduction approach significantly decreases the number of 50% suppliers; implements with 80% less than typical Wallace multipliers provide a very little growth in the number of complete suppliers.

D.R.Kelly, B.J.Phillips, and S.Al-Sarawi, "Approximate signed binaryinteger multipliers for arithmetic data value speculation," in Proc. Config. Design Archit. Signal Image Process:

Speculation of both the arithmetical data value boosts the processor pipeline's output by speculative performance, based on early arrival of such an approximate result, in dependence on the operating system. Approximation propagators compute a product quicker than an accurate propagator and there is a linked likelihood that now the product approximately is right. This article offers the concept of a family with usage in a specular data channel with signed approximately multipliers. A 32 TSMC Artisan 180nm SAGE-XTM cell Library-synthesized signed TSMC multiplier was 20% quicker than a full-adder tree multiplier, with such an error probability of around 14% for benchmarking applications.

K.Y.Kyaw, W.L.Goh, and K.S.Yeo, "Low-power high-speed multiplier for error-tolerant application," in proc. IEE int. config. Electron Devices solid state circuits:

A new paradigm of design is offered which includes precision as just a design criterion. The bottleneck of traditional digital IC design methodologies, with precision as design parameters, may be pushed through to increase power consumption and speed performance. This goal is to meet the requirement for high-efficiency, low-powered, continuously increasing sequential components.

3. CONVENTIONAL CARRY SAVE MULTIPLIERS

The carrying save multiplier method is based upon that form below. During the first step AND phases generate the partial product matrix This carry save multiplier method is based mostly on form below. During first phase, AND stages generate this same partial product matrix.

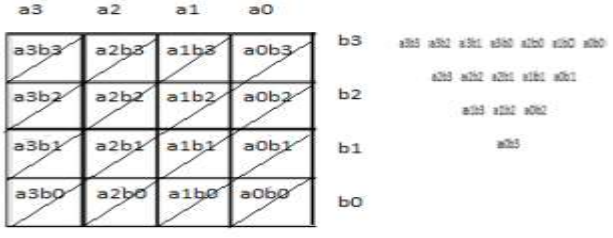


Fig. 14x4 Carry save Algorithm

Steps involved in carry save multipliers Algorithm

Multiply every bit (i.e. - AND) from one argument, producing N outcomes, by each bit of each other.

These wires carry varying weights, based on the area of both the multiplied bits.

Reduce below two complete layers with adders maximum partial products. Group into two numbers those wires, then add a standard adder to them. Product conditions produced by the gathering of AND gates.

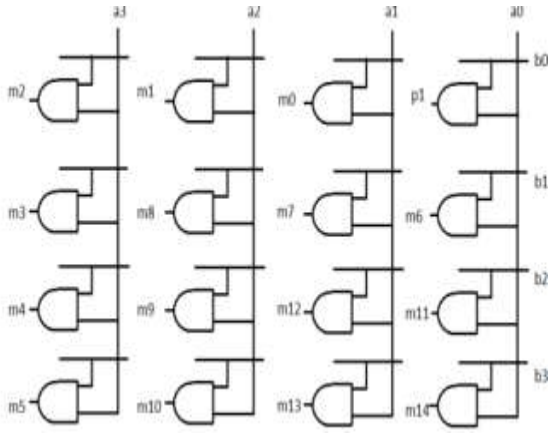


Fig 2 Product terms generated by a collection of AND gates.Carry save Tree Multiplier Using Ripple Carry Adder

Carry Adder is indeed the approach used to add extra adds to the and executable chain to just be carried out. Therefore many adders are employed in the adder. You may use numerous complete adders for the addition of multiple-bit integers to form a logical circuit. Every complete adder enters a Cin that is the preceding adders Cout. This kind of adder is an adder inside the ribs, as each piece is fed to another complete adder. Figures 9 to 11 illustrate the design suggested to use the RCA CARRY SAVE algorithm Take three values of the very same weight and provide them in a complete adder as that of the input. This outcome is an equal weight output wire. At the first step, a partial product was acquired following propagation. With 3 wires, every data are received and added by adders, although with two next data in the very same phase, each phase is carried. Partial products using the same technique decreased to two layers of complete adders. Over the last phase, the same rib carry technique is used, thereby achieving product conditions p1 to p8.

4.IMPLEMENTATION OF MODIFIED CARRY SAVE MULTIPLIER

The updated transmission save multiplier technique is built on the current matrix. During the first step AND phases generate the partial product matrix

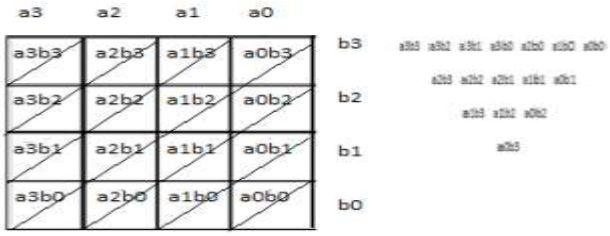


Fig.2 4x4 carry save Algorithm

Steps involved in MODIFIED CARRY SAVE MULTIPLIER Algorithm

Multiply evey bit (i.e. - AND) from one argument, producing N outcomes, from each bit of one another. These wires carry varying weights, These multiplied bits vary depending on the location. Reduce the amount from partial products into two full layers using adders.Group every wires throughout 2 numbers, then add a standard adder to them. A series of AND gates generates the product words.

The amended CSM will be produced with the following tactics included.

1. The conventional full adder (FA) structure was substituted by the improved full adder (IFA).

2. That conventional vector-merging adder(CVMA) is substituted by the suspension and energy efficient MSCA.

Improved Full Adder

A traditional complete adder depicted in Fig 5a might display the sum (S) and the carry(Co) outputs

$$S = (A \oplus B) \oplus C_{in} \quad (9)$$

$$C_o = AB + (A \oplus B)C_{in}. \quad (10)$$

In Fig. 5 b you can see improved full adder (IFA) employing logic degradation and booly duration sharing. The total (Si) and the transportation (Cio) IFA outputs may be shown

$$S_i = (((A + B)(AB)')' \oplus C_{in})' \quad (11)$$

$$C_{io} = ((AB)'((A+B)C_{in})')'. \quad : \quad (12)$$

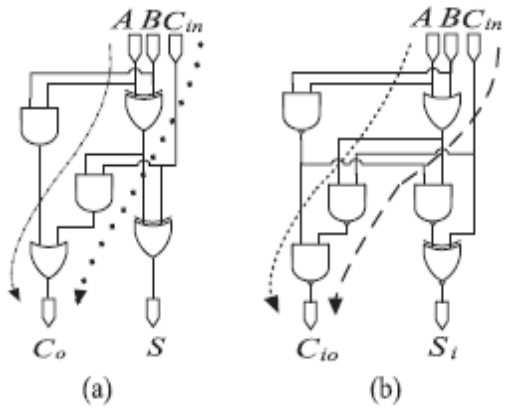


Fig.3.Conventional full adder (b) Improved full adder.

Exactly 6 complex logic (XOR and XNOR) gates are available to the proposed MCSM. This suggested multiplier's 18 logic doors are reversed gates along of the critical route. The critical route length has thus been

PROPOSED SYSTEM

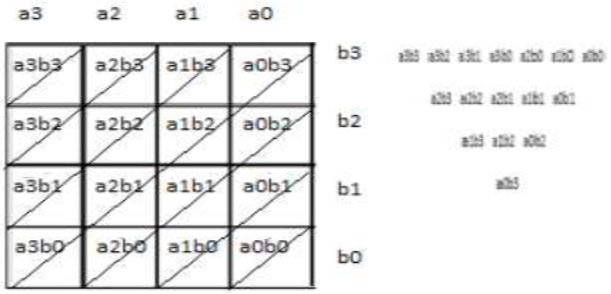


Fig.2 4x4 carry save Algorithm

Steps involved in MODIFIED CARRY SAVE MULTIPLIER Algorithm

Multiply evey bit (i.e. - AND) from one argument, producing N outcomes, from each bit of one another. These wires carry varying weights, These multiplied bits vary depending on the location. Reduce the amount from partial products into two full layers using adders. reduced. The AND gates for both beginning rows (except for A0B0) are replaced with NAND gates throughout order to significantly increase speed. In accordance with this adjustment, likewise the design of half an adder (HA0) has been altered. In order to assure a NAND-XNOR combination rather than AND–XOR combination is the Half-Adder (HA1) along the crucial route. The CSLA modified square root was made of three adder segments was using to add vector merging. A next parts comprise each of the adder parts of both the MSCA.

1. CPG: This block to carry propagate and generate(CPG) spreads and generate functions.

2. NCC: The nand carry chain(NCC) generates 2 carry rows one for input carry, Cin = 0 and the other for Cin = 1.

3. CS: One of the two potential carriers based on the carry input may be picked from the carry choice block.

4. SG: The block SG creates the final amount.

5. MCG: Module carry generation (MCG) block generates module end carry.

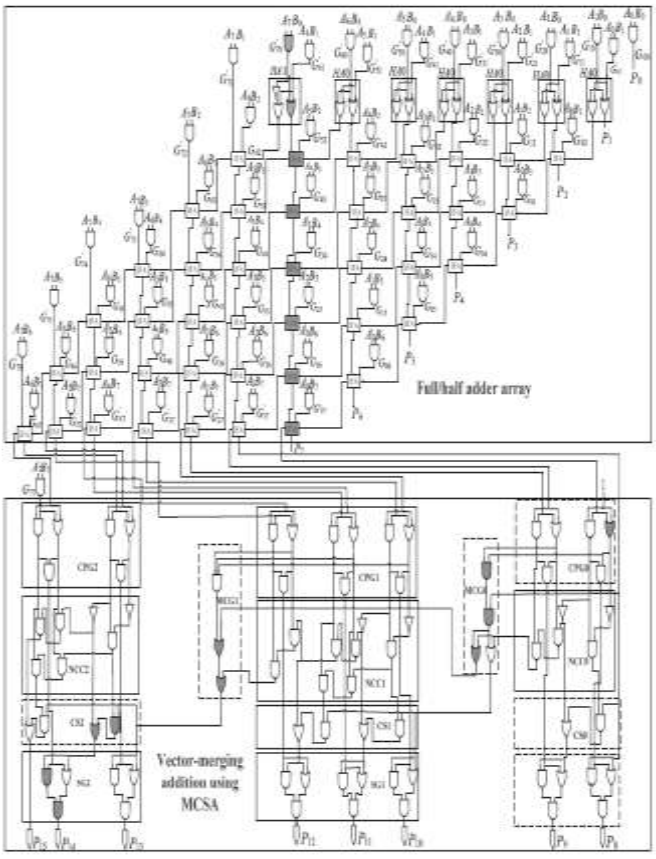


Fig. 4. An 8 x 8 Modified carry save multiplier showing critical path. The logic elements along the critical path are highlighted.

5. SIMULATION RESULT OF MULTIPLIER:

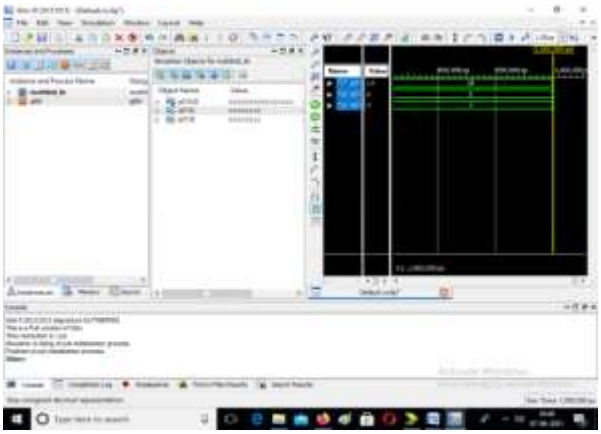


Fig 5 Simulation Result of Multiplier

Here we can give the inputs as A=6, B=3 then the final output is 14.

6. CONCLUSION

A delay, power, area and energy efficient carry save multiplier is presented. Precise critical path analysis of carry save multiplier was done and derived the critical path delay as a function of number of full adders and logic gates. Remarkably improved performance in terms of majority of the performance metrics is achieved through the use of improved full adder and modified square root CSLA. The structural simplicity and regularity of the full adder/ half adder array of the proposed CSM is improved through the use of IFA. The carry generation delay, area and power of the IFA is improved through the use of NAND-NAND chain in place of AND-OR chain along the carry generation and propagation path. The final vector-merging addition using modified square root carry select adder (MCSA) further improves the speed.

7. FUTURE SCOPE

In our daily lives, this multiplier performs a very significant function. The multipliers will play an important role in the advancement. With additional carry save additives, the pace of both the multipliers is enhanced, look ahead, etc. Rounding patterns are designed depending on the necessary precision and various strategies for compression. With future, better technologies may minimise the area & delay.

REFERENCES

[1] M. Alioto, “Ultra-low power VLSI circuit design demystified and explained: A tutorial,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 59, no. 1, pp. 3–29, Jan. 2012.

[2] V. Gupta, D. Mohapatra, A. Raghunathan, and K. Roy, “Low-power digital signal processing using approximate adders,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 32, no. 1, pp. 124–137, Jan. 2013.

[3] H. R. Mahdiani, A. Ahmadi, S. M. Fakhraie, and C. Lucas, “Bio-inspired imprecise computational blocks for efficient VLSI implementation of soft-computing applications,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 57, no. 4, pp. 850–862, Apr. 2010.

[4] R. Venkatesan, A. Agarwal, K. Roy, and A. Raghunathan, “MACACO: Modeling and analysis of circuits for approximate computing,” in Proc. Int. Conf. Comput.-Aided Design, Nov. 2011, pp. 667–673. [5] F. Farshchi, M. S. Abrishami, and S. M. Fakhraie, “New approximate multiplier for low power digital signal processing,” in Proc. 17th Int. Symp. Comput. Archit. Digit. Syst. (CADS), Oct. 2013, pp. 25–30.

[6] P. Kulkarni, P. Gupta, and M. Ercegovac, “Trading accuracy for power with an underdesigned multiplier architecture,” in Proc. 24th Int. Conf. VLSI Design, Jan. 2011, pp. 346–351.

[7] D. R. Kelly, B. J. Phillips, and S. Al-Sarawi, “Approximate signed binary integer multipliers for arithmetic data value speculation,” in Proc. Conf. Design Archit. Signal Image Process., 2009, pp. 97–104.

[8] K. Y. Kyaw, W. L. Goh, and K. S. Yeo, “Low-power high-speed multiplier for error-tolerant application,” in Proc. IEEE Int. Conf. Electron Devices Solid-State Circuits (EDSSC), Dec. 2010, pp. 1–4.

[9] A. Momeni, J. Han, P. Montuschi, and F. Lombardi, “Design and analysis of approximate compressors for multiplication,” IEEE Trans. Comput., vol. 64, no. 4, pp. 984–994, Apr. 2015.

[10] K. Bhardwaj and P. S. Mane, "ACMA: Accuracy-configurable multiplier architecture for error-resilient

Design of Surface Plasmon Resonance In Gap Waveguides

Adarsh S K[1], Saida S[2], Manoosha G[3], Sai Keerthi S[4], Anantha Vishnu k[5]
Assiatant Professor[1],UG Scholars[2,3,4,5]
[1,2,3,4,5]Department of ECE, Srinivasa Ramanujan Institute of Technology,Anantapur, Andhra Pradesh

Abstract - In this work, the modal analysis and power coupling analysis of gap plasmon wave guides for use in optical sensing applications is presented. The power coupling analysis is carried out by using Lumerical FD TD simulation tool. The structure consists of Silver (Ag) metallic wave guides separated by a very small gap distance in the range of less than 100nm on glass substrate. Two separate Ag- metallic arms attached to the metallic waveguides at the center of the structure is used as nano antenna which acts as an electromagnetic wave sensor. The pro pagation constant of the metallic electrodes used as optical nano antenna to sense the light from Gaussian light beam is analyzed with respect to variations in width of Ag- metallic arms. The optical light beam is illuminated in the direction normal to propagation direction in metallic waveguides. The optical nano antenna is used to couple the optical beam into air gap present between me tallic waveguides. The power coupling analysis is carried out at 1550nm for variations in numerical aperture (NA) of optical source. The modes are coupled to the air gap and results in 4.8% to

12.17 % of o ptical power coupling by using high numerical aperture optical beam. Such structures can be effectively used to solve light coupling problem in SPR based gap waveguides and can be used in many more optical sensing applications.

Index Terms - Plasmons; Surface plasmon resonance (SPR); Nano-antenna; Gap- waveguides; power coupling.

I. INTRODUCTION

Bio-sensors that rely on rapid and portable screening techniques have been of interest to identify harmful toxins for food safety or to detect chemical or biological agents that could be used in bio-terrorism. The predictable advantage bio-sensors offer over many other bio-physical techniques is that it is label-free, chemical or radio labeled tags, eliminating the need for fluorescent.

Surface plasmon resonance is the resonant oscillations of conduction electrons at the interface between metal and dielectric material.Surface plasmon resonance (SPR) is generally occurs at metal surfaces (typically gold and silver). when an incident light beam strikes the surface at a particular angle. The SPR phenomenon results in a graded reduction in intensity of the reflected light Depending on the thickness of a molecular layer at the metal surface.

Plasmon generation means when a light incident on the surface of the glass substrate.

The light strikes the glass substrate and generates the localized resonant oscillation (i.e., hot carriers) at the same time plasmons are generated at the surface of the gold coated glass substrate.Plasmons are locally generated evanescent waves at the interface between metal and dielectric material. In this paper the structure of the optical device consists of Silver (Ag) metallic waveguides separated by very small gap distance in the order of less than 100nm.

I. MODELING AND SIMULATION SETTINGS

A. Design of Gap Plasmon Waveguides

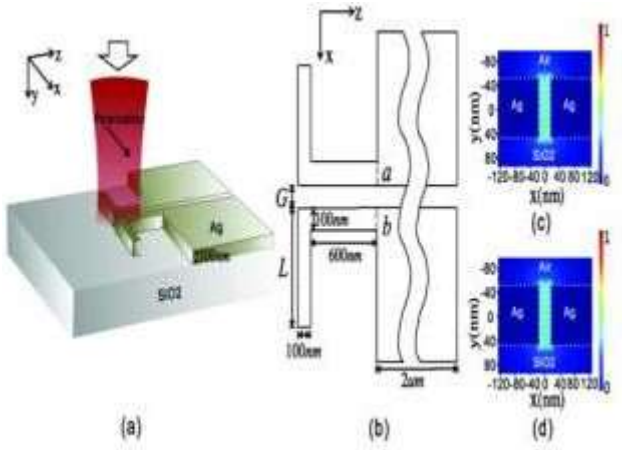


Fig: General block diagram of SPR based gap waveguide with vertical polarization

Fig. 1. 3D view of Gap Plasmon Waveguide with air gap

Fig .1 shows the structure of gap plasmon waveguide. It consists of dielectric layer which acts as a substrate which is shown in blue color and two Ag (Silver) metallic waveguides (shown in red color) separated by air gap on top of glass substrate.

The gap plasmon waveguides shown in fig1 is excited by two metallic (Ag) arms which acts like optical nano-antenna and serves as optical coupler. Each electrode is connected to edge of waveguide at the center The height of two electrodes which forms a nano antenna is calculated using equation (1). Nano antenna couples the optical light beam from source to the center (air gap) of gap plasmon waveguides and is discussed in detail in section III

$$h \leq \lambda/4 \qquad \text{------(1)}$$

The operating wavelength is selected at 1550nm. The height of the two metallic arms is calculated using equation

(1) and is chosen to be 200 nm. The effect of antenna width results in variations in propagation constant of the optical light confined to the gap plasmon waveguides and is discussed in section III.

B. Simulation settings

The Lumerical mode solution is used to analyze modal analysis and Lumerical finite difference time domain (FDTD) is used to analyze power coupled from optical source to gap plasmon waveguide using nano antenna structure. The vertically polarized Gaussian optical beam is used as a light source as shown in Fig 2.

In simulation optical power monitor is used to collect the power coupled at the air gap between plasmonic waveguides and the variation in coupled power is analyzed as a function of numerical aperture of the optical source and is discussed in section III.

II. RESULTS AND DISCUSSIONS

A. Modal Analysis

Modal analysis of plasmon waveguides with air gap shown in Fig 1 is carried out by using Lumerical mode solution simulation tool. Modes are searched near the highest and lowest refractive index of the structure shown in Fig 1 at the wavelength of 1550nm. It results in multiple modes for the structure. Fig 4, shows the TM mode confinement in the gap surface plasmon waveguide. Plasmonics modes confined to the air gap are found and its TE mode confinement at the gap is shown in Fig 5.

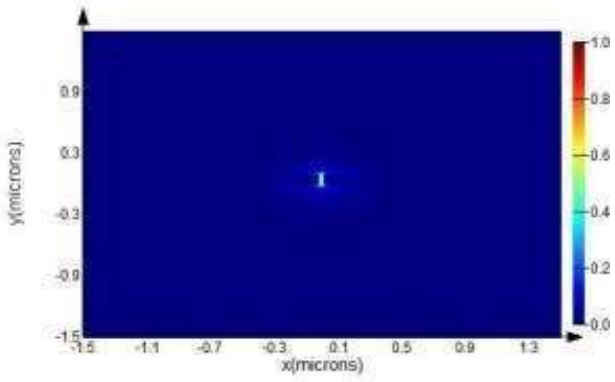


Fig.3 Mode coupling in gap

A.Power Coupling Analysis

The power analysis is carried out as a function of

numerical aperture of the optical source and propagation constant of the gap plasmon waveguides is determined for different widths of nano antenna (two Ag-electrodes which forms the nano- antenna) by using Lumerical FDTD simulation tool. The width of the antenna is varied from 50nm to 150nm. The effect of width on real value of the refractive index is shown in Fig 5. It is found that the effective index of the structure is 1.81 at 50nm and it is 1.68 when the width is 150nm.

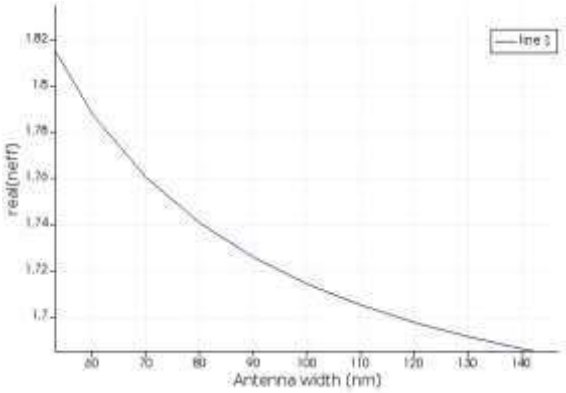


Fig. 6. Effect of Antenna width on a real value of refractive index of gap plasmon waveguide

Fig.7 shows percentage of power coupled at air gap between two plasmon waveguides shown in Fig 1. It shows that
4.8 % to 12.17 % of the incoming light is coupled into the gap surface plasmon waveguide by using optical source with 0.5 NA and 0.9 NA respectively. Fig.5 concludes that using high NA light beam and optical nano antenna results in a better confinement of light within the air gap present between two metal electrodes (waveguides) and such waveguides can find many more applications in surface plasmon resonance (SPR) based optical sensing applications.

III. CONCLUSION

In this work surface gap plasmon waveguide structure is modeled and is excited by using two metal electrodes having length very much less than quarter wavelength which acts as nano antenna. An efficient method of coupling light from high NA source to gap plasmon waveguides is presented and coupled power is analyzed with respect to variations in NA of the optical source. The modal analysis is carried out by using Mode solution and clearly demonstrates the modes are confined at the gap and coupled mode propagation constant is found to be varied from 1.81 to1.68 for 50nm to 150nm sweep in antenna width. Power coupling analysis is carried out by using finite difference time domain simulation tool. This model gives optimum way to couple light into the gap surface plasmon waveguide. This work also gives the coupling efficiency of upto 12.17% by using high numerical aperture source (NA=0.9) with vertical polarization.

The simulated coupling efficiency result obtained in this paper gives an improvement of 26.05% compared to results obtained in Jing Wen et al., Excitation of plasmonic gap waveguides by nanoantennas [12]. Such structures can be effectively used to solve light coupling problem in SPR based gap waveguides and can be used in many more optical sensing applications.

IV. ACKNOWLEDGMENT

We would like to express our sincere gratitude to the Management, Principal of Srinivasa Ramanujan Institute of Technology, Anantapur for the facilities provided and their support. Also we would like to thank the Head of department Electronics and Communication Engineering and our guide Adarsh sir for their encouragement and support.

REFERENCES

21.

[1] Jianjun chen, chengwei sun & Xiaoyong Hu “Nanoscale optical devices based on surface plasmon polaritons ”. Chinese Science Bulletin volume 59, pages2661–2665 (2014).

[2] Badrinathan , Dinesh ,”Waveguide Design Strategies for Surface Plasmon Resonance” IJARIIE-ISSN(O)-2395-4396, Vol-5 Issue-2 2019.

[3] Jing Wen, Sergei Romanov, and Ulf Peschel, "Excitation of plasmonic gap

waveguides by nanoantennas," 13 April 2009 / Vol. 17, No. 8 / OPTICS EXPRESS 5925-5932

[4] Savitha, K. S. Rao and P. Sharan, "Detection of oncological cell for breast cancer by using SPR technology," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 2747-2749.

[5] M. Nafari and J. M. Jornet, "Modeling and Performance Analysis of Metallic Plasmonic Nano-Antennas for Wireless Optical Communication in Nanonetworks," in IEEE Access, vol. 5, pp. 6389-6398, 2017, doi: 10.1109/ACCESS.2017.2690990.

[6] K. Bremer, J. Walter, M. Rahlves, T. Scheper and B. Roth, "Optical SPR sensor designed for smartphones," 2017 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC), 2017, pp. 1-1, doi: 10.1109/CLEOE-EQEC.2017.8087218.

[7] K.Sharma, R.Jha and B.D. Gupta, "Fiber-Optic Sensors

Based on Surface Plasmon Resonance: A Comprehensive Review," in *IEEE Sensors Journal*, vol. 7, no. 8, pp. 1118-1129, Aug. 2007, doi: 10.1109/JSEN.2007.897946**.**

[8] Ruoxi Yang, Zhaolin Lu, "Subwavelength Plasmonic Waveguides and Plasmonic Materials", International Journal of Optics, vol. 2012, Article ID 258013.

Deep Learning and Bot Notification Services in Green House Farming of Tomato

SaiSumi D, Supraja P, Vignesh G, ShashidharReddy M

Department of ECE, Srinivasa Ramanujan institute of technology, Anantapur, Andhra Pradesh.

ABSTRACT:

The early disease monitoring and detection system. To provide a smart farming solution, this paper proposed with a bot notification on tomato growing stages. The tomato dataset was obtained from Shin chi Agri Green, the tomato greenhouse. The training and testing of the deep learning model to detect the fruit/tomato proposal region. Then, the detected regions were classified into 6 stages of fruit/tomato growth using the visible wavelength as a feature in SVM classification with the weight accuracy of 91.5%.Tomato/fruits development can be divided into different stages like Green, Breaker, Turning, Pink, Light Red and Red. There are several environmental conditions, such as temperature, moisture, water and nutrients, and lights, which have effect on fruit development. Finally detected reasons of images to further contribute the study to detect and classify the tomato diseases appearing either on fruit or tomato sections.

INTRODUCTION:

These days, tomato creation and utilization becomes progressively more extensive. Numerous farming investigates have been carried out to improve the nature of tomatoes. Shin chi Agri-Green is one of the tomato nurseries that carried out advances to screen the states of development on tomatoes. Nonetheless, controlling and checking these development factors is vital to create great quality harvests and to stay away from any terrible conditions prompting a strange development. By utilizing the deep learning techniques, we can give the water and required supplements at required levels at perfect time which will improve the yield of the harvest and the pi-cameras are used to capture the images to monitor the growth of organic products or the tomato areas. Moreover the deep learning techniques and notification system supports the cultivators in early detection of growing stages of tomatoes and the diseases which are appearing to the crop.

EXISTING SYSTEM

Green House farming has variety of options to cultivate the crops in the field, yet the cultivation of crops and harvesting of crops is done in old and traditional manual Way which may lead to improper management, in turn leading to reduction in the yield of crop. The composition of monitoring system for agricultural purpose included the use of aurdino, Raspberry Pi, cloud services and LINE Bot. For data collection pi-cameras are used to detect the physical conditions by sensing different parameters and this data is transferred to the cloud after processing. An API bot notification server then displays this information on the display syste**m** through user's interaction.

PROPOSED SYSTEM:

Pi-Camera takes the periodic snapshots and the dataset provides a data storage and data analytics. It stores the data and analyzes the data like color and growth of the fruit. Image processing, Machine learning and Deep learning techniques are used in extracting and categorizing the tomato fruit into various growth stages. This information was integrated with a notification platform to send notifications to Slack from Mat lab software via Incoming Web hooks integration. With Slack we can easily send analyzed data from Mat lab and with a Bot API platform we can provide a workspace where the user can get notifications of the data obtained from camera nodes and growth monitoring of fruits.

Block Diagram

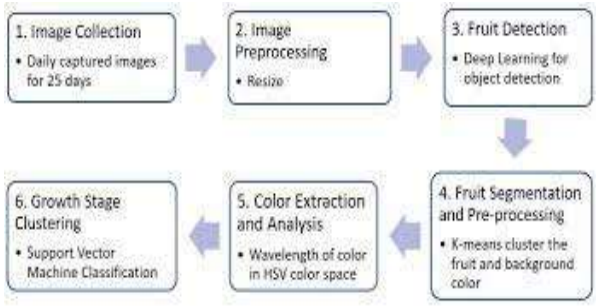


Fig.1: Proposed Methodology of Tomato Growth Analysis

Analyzing the growth of tomatoes, we combined the methods of deep learning, image processing showing in the above fig.1 and it also includes image collection, pre-processing and four main analyses to be considered:

1. Deep Learning for object detection:

Deep learning is an artificial neural network with hidden layers. The learning algorithm finds the best way to represent data through optimizations where the features are automatically extracted. Our images captured from the real field include background such as leaves, and soil where it is challenged to differentiate the fruit section out of the background. So, we proposed Faster Region-Convolution Neural Network to examine the bunch of proposals by a classifier for checking the occurrence of fruit regions. Our goal is to detect the fruit regions, then crop them from the background section. The detected results will be used in classification of growth stages.

2. K –means clustering:

The recognized districts from profound learning were pre-handled for eliminating the excess foundation of uninterested segment. For an essentially pre-bunching, we determined K equivalents 2 in request to group 2 sections: leafy foods area where a large portion of the pictures included just 2 tones. In this way, K-Means algorithm can be applied here.

3. Color Extraction:

The images of segmented regions were converted to hue plane scaled from 0 to 360 degree in Hue-Saturation-Value (HSV) color space. Then, we extracted the features of the visible light wavelength from 530 nm to 620 nm. This range defines color of green, yellow, orange and red respectively.

4. Support Vector Machine:

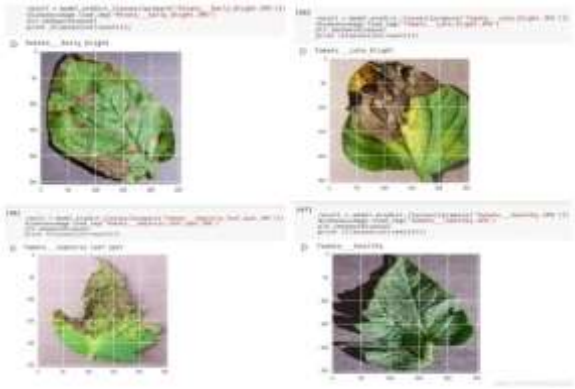
Finally, we use the extracted features of visible wavelength to classify the ranges of wavelength to 6 stages of tomato growth as shown in fig.2 using Support Vector Machine (SVM).

WORKING

The image is preferably taken from the plant. Dataset Images are the ones that are taken and stored already in the database for comparison. The images to be detected cannot be compared directly to the dataset images, as that may mislead the process of the detection system. The images are processed with a series of feature extraction mechanisms and are then segmented to determine the affected portion of the leaf to be compared using the CNN Classifier. Then results are used to detect and classify the tomato plant disease and suggest a suitable solution to the farmers as a precautionary step. The steps that are done are pre-processing, feature extraction for both the input image and dataset images to increase the accuracy level of prediction. The notification system gives access to this analyzed data for the user and gives timely updates and alerts for the user about the growth conditions and the requirements of nutrients and water and also displays about the diseases appearing on the fruit.

REULTS

The project “Deep Learning and Bot Notification services in Green House Farming of Tomato” was designed based on Deep Learning techniques along with image processing which control by using the convolution neural networks.



CONCLUSION

With the help of deep learning algorithms and neural networks, machines can be taught to see and interpret images in the way required for a particular task. Progress in the implementation of Deep Learning based image processing is impressive and opens a wide range of opportunities in fields from agriculture used to recognize and characterize the diseases showing up either on leaf or on organic products respectively.

FUTURE SCOPE

This proposed system considers the leaf of the plant to detect the diseases of that crop. It will be more convenient if other parts of the crop such as roots, stem, branches etc. which increases the detection accuracy more than current one. Also image categorization will also be done to check whether the given leaf is of preferred category or not. If a model provided with input other than leaf image then also it shows some name of diseases for it.

REFERENCES

[1] K. Yosuke, I. Masahiro, O.Nobuhiro, and I. Hiroshi, “Development of “IoTOMATO” that is an agriculture monitoring system by using chat bot,” FIT2017, proceeding of IPSJ and IEICE, vol. 4, pp 229-230.

[2] G. T. Vishal and G. Mohit, “Arduino based tomato ripening stages monitoring system,” IJIRSET, vol. 7, pp. 530-536, January 2018.

[3] S. Narut, T Panwadee, S. Panu, and R. Preesan, “An agricultural monitoring system: field server data collection and analysis on paddy field,” ISCIT, 2014, pp. 597-601.

[4] W. Patrick and M. Medhat, “Early powdery mildew detection system for application in greenhouse automation,” Comput. Electron. Agric. 127, 2016, pp. 487-494.

[5] D. Halil, O. G. Ece, and K. Murvet, “Disease detection on the leaves of the tomato plants by using deep learning,” 6 th International Conference on Agro-Geoinformatics, 2017.

[6] F. Alvaro, Y. Sook, C. K. Sang, and S. P. Dong, “A robust deeplearning-based detector for real-time tomato plant diseases and pests recognition,” Sensors, vol. 17. No. 9, p. 2022, April 2017.

[7] R. S. Redmond, W. J. James, R. T. Kelly, A. Desa, C. M. Hafalina, and T. Sima, “Review of optimum temperature, humidity, and vapor pressure deficit for microclimate evaluation and control in greenhouse cultivation of tomato: a review,” International Agrophysics, vol. 32, no. 2, pp. 287–302, January 2018.

THIRD EYE FOR BLIND USING ULTRASONIC SENSOR AND HEALTH MONITORING

D. Maruthi Kumar[1], Brunda.J[2], Kalpana .M[3], Sandhya. L[4], Eswar Sai Rahul Reddy. K[5]

Assistant professor[1], UG Scholars[2,3,4,5]

[1, 2, 3, 4,5] Department of ECE, Srinivasa Ramanujan Institute of Technology, Anantapur, A.P

Abstract: The "Third Eye for blind using ultrasonic glove and health monitoring" is intended to assist blind people in overcoming their visual impairment. When conducting daily duties, the visually handicapped experience a number of difficulties. The development of practical solutions to assist the visually impaired is gaining popularity. The proposed solution is developing an ultrasonic glove which detects the obstacle and alerts the user to change his direction of movement through a voice module. This glove is also designed for health monitoring. It continuously monitor their pulse rate and body temperature using heart rate sensor and LM35. When a user falls, a MEMS sensor detects it, and a message is delivered to the concerned person via the GSM module.

Keywords: Ultrasonic Glove, voice module, LM35, Heart Rate Sensor, MEMS Sensor, GSM Module.

I.INTRODUCTION

The ability to see is one of the most important aspects of human physiology. Our senses of sight is crucial to our understanding of our surroundings. From the research provided by the WHO, there are around 285 million individuals who are visually impaired, with 39 million of them blind (WHO). Furthermore, 90% of visually handicapped people live in developing countries. The first tool for blind people was a walking stick, but the main disadvantage is that it requires training before use. With technological advancements, it is now possible to discover a solution that allows visually impaired people to travel freely both indoor and outdoor environment.

The key qualities of this project are that it is beneficial to both visually impaired and elderly people. Obstacles such as vehicles and stones in outdoors and stairs, walls, and furniture in the indoors are identified and alerted to the user via the speech module. Sensors like the LM35 and the pulse sensor are used to continuously monitor body temperature and heart rate. The MEMS sensor detects a person's fall, and a message is delivered to the individual concerned via the GSM module.

II.EXISTING SYSTEM

The smart stick was created with obstacle detection and navigation. Infrared, ultrasonic, and water sensors were used. This project also makes use of a GSM module and GPS. The stick's position and navigation are detected via GPS. If the blind person is in danger, the GSM module can send a notification to the concerned person. The power source for the system is a 9V battery. The Arduino Uno microcontroller ATmega328P is used in this system. This system has a GSM module that allows it to call in an emergency. When the distance between the visually impaired person and the obstacle is reduced, the intensity of beep sound rises. When an obstruction is recognised, a spoken warning message is delivered through earphone. Obstructions such as downhill stairs, holes, and other obstacles can also be detected by this technology. The fundamental disadvantage of this method is that it cannot be folded.

III.PROPOSED SYSTEM

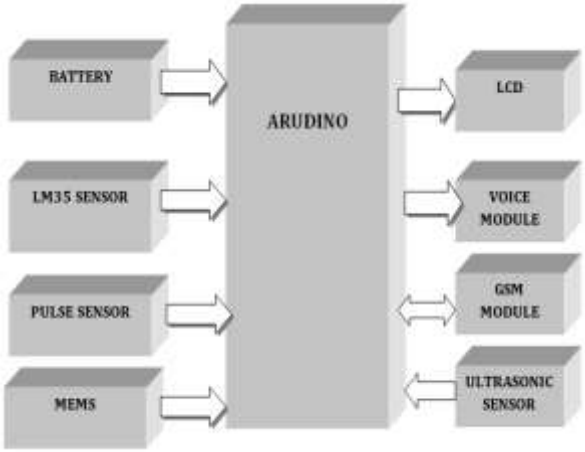
Blind Glove is an innovative glove designed for blind people for navigation in indoor and outdoor environment.

Our proposed system first uses ultrasonic sensors to detect obstacles using ultrasonic waves. When the obstacle is detected then sensor passes data to the microcontroller, the microcontroller calculates distance between the blind person and obstacle.

Pulse sensor will detect the heart beat of blind person, If pulse is abnormal then it will be send message to microcontroller. If the pulse detected in the sensor is higher than normal level then microcontroller executes the code the microcontroller sends a signal to voice module and send sms through gsm.

Temperature sensor will detect the temperature of blind person, If temperature is abnormal then it will be send message to microcontroller. If the temperature detected in the sensor is higher than normal level then microcontroller executes the code the microcontroller sends a signal to voice module and send sms through gsm.

Mems sensor will detect the falling of blind person, If mems is abnormal then it will be send message to microcontroller. If the value detected in the sensor is higher than normal level then microcontroller executes the code the microcontroller sends a signal to voice module and send sms through gsm.



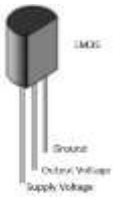
BLOCK DIAGRAM DESCRIPTION

1. LM35:

The LM35 series of precision integrated-circuit temperature sensors have an output voltage that is proportional to the temperature in Celsius (Centigrade). It measures the temperature of range -55 to 150°C. Figure of LM35 is shown below(fig1)

2. Pulse sensor:

Knowing your heartbeat rate is extremely important when exercising, researching, and so forth. However, calculating the heartbeat rate might be difficult. The pulse sensor, sometimes known as a heartbeat sensor, is utilised to solve this problem. This is a plug-and-play sensor that is primarily developed for Arduino boards. We can get quick and accurate heartbeat readings by utilising this circuit. This circuit can be used in mobile applications with a current of 4mA and a voltage of 5V.



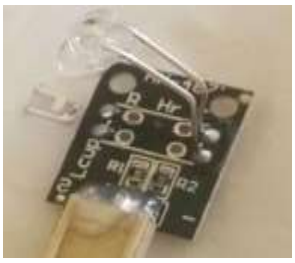


Fig1. LM35 *Fig2: Pulse sensor*

3. MEMS Sensor: The Acronym of MEMS is Micro Electro-Mechanical System. MEMS inertial sensors are low-cost, high-accuracy inertial sensors that are employed in a wide range of industrial applications. This sensor is based on the micro-electro-mechanical-system, which is a chip-based technology. These sensors are used to detect and measure external stimuli such as pressure, after which it responds to the pressure that is sensed using some mechanical mechanism.

Fig3: MEMS

4. Ultrasonic Sensor: Ultrasonic sensor is used to measure the distance by sending ultrasonic waves and receives the reflected wave when this waves hits the obstacle. This sensor has 4 pins they are, VCC, Trigger, Echo and Ground. It's theoretical measuring distance is 2 to 450 cm and practical measuring distance is 2 to 80cm.

Fig4: Ultrasonic Sensor

5.GSM Module: GSM stands for global system for mobile communication. Following commands are used

- ❖ AT : For serial interfacing.
- ❖ ATD : used to Dail.
- ❖ ATA : Used to Answer.
- ❖ ATO : Used to return to the online data set.
- ❖ AT+CMGS : Used to send SMS.
- ❖ AT+CMGL : To view list of SMS messages.
- ❖ AT+CMGR : To read SMS messages.

Fig5: GSM

6. Voice Module: APR33A3 voice module is used in this project. It provides high quality recording and playback audio at 8KH sampling rate with 16 bit resolution. It has 8 channels to record 8 voices. It has built in audio recording microphone amplifier.

Fig6: APR33A3 voice module

7. LCD : LCD(Liquid crystal display) is a flat panel display that operates primarily with liquid crystal. LCDs have wide range of applications and it is the most commonly connected device to any microcontroller.

Fig7: LCD module

8. Arduino UNO: It is a widely used open source microcontroller board based on microchip ATmega328P which is developed by Arduino.cc. It has 14 digital pins and 6 analog pins. It is programmed by using Arduino IDE. It is powered by using 9V battery or external USB cable. Among 14 digital pins 6 pins are used for PWM output. It has 32KB flash memory, clock speed is 16MHz.

Fig8: Arduino UNO

IV.EXPERIMENTAL RESULTS

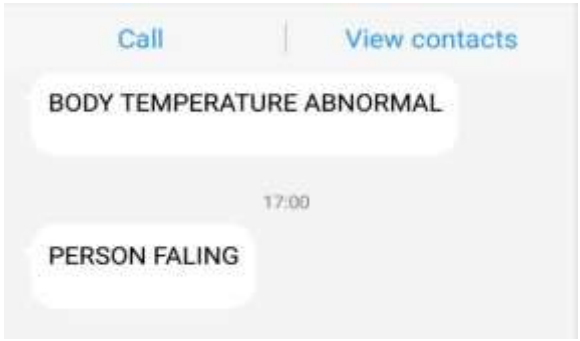


Fig9: Message is sent during Abnormal Condition

Fig10: Temperature, pulse rate, distance displayed in lcd

T: Temperature in ˚C

P: Pulse rate

X, Y: Axis in mems sensor

26 is distance measured by Ultrasonic sensor in centimeters(cm)

When the obstacle is closer system alerts the user to change his direction through voice module.

V.CONCLUSION

The project's goal of designing and implementing a Smart Glove for the blind has been entirely realised. This glove serves as a foundation for future generations of assistive gadgets that will enable the vision impaired travel securely both indoors and outdoors. It is both efficient and cost-effective. It performs well when identifying obstructions within 3 metres. This system provides a low-cost, dependable, portable, low-power, and robust navigation solution with a quick response time. It is lightweight and simple to operate. When the individual's health is in danger, the lm35 and pulse rate sensor are used to send a GSM message to the concerned person. Continuous health monitoring is done by using lm35 and heartrate sensor by GSM message is sent to concerned person when the person is in risk. Finally this device is not only useful for visually impaired but also for elder persons.

VI.REFERENCES

[1]. Ultrasonic Distance Meter by Md Arefi and Mollick published in International Journal of Scientific and Engineering Research in March 2013.

[2]. Ultrasonic stick for blind by Agarwal, Kumar and Bhardwaj, published in International Journal of engineering and computers in April 2015.

[3]. Voice operated outdoor navigation system for blind people by Koleey and Misra, published in International journal of emerging trends and technology in 2012.

[4]. Smart stick for visually impaired: Obstacle detection, artificial vision, and real-time help via GPS by S. Dhambare and Sakare published in National Conference of Information and Communication Technology in 2011.

[5]. A smart walking stick is an electronic aid for visually impaired people by Hazzaz, Ranasaha, Sayemul Islam.

[6]. Assistive infrared sensor based smart stick for blind people by Ayat Nada, A. Fakhar and Ahamed FSaddiq.

Facial and Voice Recognition-Based Security System to The Door

HarshiniT, Pavan K, Praveena B, Mounika S, Rubeena S, Pradeep M, Venkata Poushika B, and RaghuManoj G , Srinivasa Ramanujan Institute of Technology, Andhra Pradesh, 515701, Rotarypuram, Ananthapuramu, India

ABSTRACT

The principle topic of our task is to give security to the entryway by utilizing a facial and voice acknowledgment based framework. our framework will catch the essence of the individual who needs to open the entryway and afterward it contrasts the caught face and the beforehand put away face in the information base in the event that it is coordinated, the individual can go to the second step of the check assuming the face isn't coordinated, the picture of the unapproved individual will be shipped off the higher specialists mail id by utilizing IoT.Assuming the face is coordinated, the individual will go into the second step confirmation then the individual needs to provide voice orders through the voice module.If the voice order got by the voice module is coordinated with the recently put away voice orders then the second step check is effective. On the off chance that the voice order isn't coordinated, SMS is shipped off the higher specialists utilizing the GSM module. Then, at that point he needs to enter the secret word this is the last advance of check assuming the entered secret key isn't right, SMS will be shipped off higher specialists in the event that the entered secret word is right, the entryway will open.

Keywords: Face recognition, voice recognition, Keypad, GSM module, Door lock module.

Introduction:These days, such a lot of are going throughcrucialsafetyproblems; Thule, they wantan incredibly pre-organizednow no longer many. Surveillance and safetystructures. Nevertheless, this safetymachinefinally tumbles because ofthriller key hacking or encoded or unscrambled information. In this way, to cope with such problems and to make surethe safety of the doorway biometric structures like face confirmation, iris confirmationare used. Among those Face discovery System is greater useful and clean to do moreover, it moreover perceived the unauthenticated characterwith out their understanding. Already the facial confirmationchanged intoachieved with the assist of PCA and LDA calculations. Howeverthere are numerouslimitationsto those calculations. The vitaldifficulty of the PCA calculation is that it's milesmuch lesstouchy to distinctive getting preparedinformationexperience and it's miles in like way computationally exorbitant with excessive time complexity.

The chief issue of the LDA calculation is just in case there's any selection within the gift or during any condition in a similar image the speech act of bumble rate is extended. A structure may be controlled and detected remotely/subsequently with the assistance of Windows IoT ten. Hence, the system is formed with Windows IoT 10 which may beat the shortcomings of the PCA (Principal half investigation) and LDA (Linear discriminant examination). Direct discriminant examination discourse is that the most worthy limit. changed speaker affirmation (ASR) structures acknowledge folks utilizing the articulations. contingent the chance of the application, speaker recognizing verification or speaker affirmation systems can be shown to figure either in text-ward or text-free modes. The essential objective of this security system is to confirm the prosperity of the access by perceiving unauthenticated folks and exploitation voice affirmation.

Literature Survey:

[1]Anilk.Jain "Longitudinal Study of Automatic Face Recognition", The two mystery premises of changed face confirmation are uniqueness and lastingness. This paper reviews the perpetual quality property by keeping an eye out for the going with: Does go facing attestation breaking point of top level constructions debase with sneaked past time among picked and question face pictures? Given that this is legitimate, what is the speed of decay w.r.t. the sneaked past time? While past evaluations have revealed defilements assessment, no formal certain assessment of giant degree longitudinal information has been driven. We direct such an assessment on two mugshot enlightening assortments, which are the best facial creating educational assortments thought to date the degree that couple of subjects, pictures per subject, and spent events. Blended impacts break faith models are applied to certified similarity scores from best in class COTS face matches to measure everyone

mean the speed of progress in true blue scores over the long haul, subject-express impulse, and the impact develop enough, sex, race, and face picture quality. Longitudinal assessment shows that in spite of diminishing certifiable scores, 99% of subjects can, in any case, be seen at 0.01% FAR up to around 6 years sneaked past time, and that age, sex, and a race just indistinguishably influence these models. The method familiar here ought to with be on occasion repeated to pick age-invariant properties of face insistence as bleeding edge makes to even more plausible region facial creating.

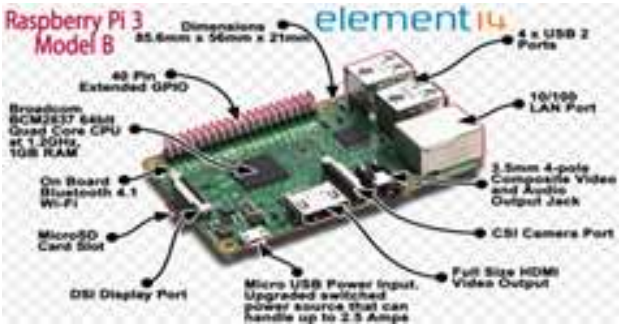
[2] **Navaf Yousef almudhahka and Mark S. Nixon, "Programmed Semantic Face Recognition",** Ongoing improvement in perception structures has animated exploration in sensitive biometrics that engage the unconstrained affirmation of human appearances. Relative fragile biometrics show common affirmation execution than unmitigated sensitive biometrics and have been the point of convergence of a couple of assessments which have included their ability for affirmation and recuperation in constrained and unconstrained conditions. These assessments, regardless, just would in general defy affirmation for recuperation using human-delivered attributes, offering an ice breaker about the believability of thusly making comparable names from facial pictures. In this paper, we propose a method for the adjusted near naming of facial delicate biometrics.Plus, we research unconstrained human face affirmation using these moderately sensitive biometrics in a human-stamped display (and the opposite way around). Using a subset from the LFW dataset, our investigations show the reasonability of the modified period of close to facial names, highlighting the normal extensibility of the best approach to manage other face affirmation circumstances and greater extents of characteristics.

[3] **HteikHtar Lwin, Aung SoeKhaing, Hla Myo Tun "Programmed Door Access System Using Face Recognition",** This paper explains that how self-administering vehicles will act while opening the entrances with the help of face affirmation. There are different ways to deal with open entrances with the most insightful way yet facial affirmation will be generally secure as two people can never have similar appearances. This framework is using PCA (Principal Component Examination) which is used for facial affirmation, to genuine the supported individual for the vehicle.

Proposed system:

In the proposed system, we are providing high-security system to the door by three-step verification. When a person wants to open the door of the room then the camera which is integrated with a Raspberry Pi captures the image of the person then the captured image is verified with the previously stored images in a Raspberry Pi SD card if both the images are not matched then the image of an unauthorized person will be sent to the owner mail I D by using SMPT protocol Otherwise he will enter into next step that is voice recognition now the person has to give command if the given command and voice of the person is matched with the previously stored voice commands in the voice module then he will enter to the final step of verification that is password entering step otherwise SMS will be sent to the owner by using GSM module. Finally, if the password is correct, the door will open, otherwise, a message will be sent to the owner.

Block diagram of the proposed system:

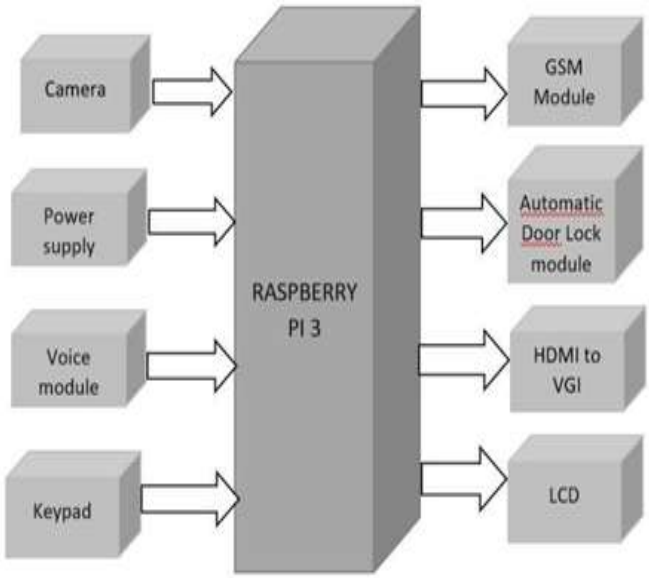


Components used in the Proposed System:

1.Camera

A digital digicam is an optical devicethat's used to get a photograph. At their all matterstaken into consideration basic, cameras are constant boxes (the digital digicam body) with pretty opening (the outlet) that awards mild in to get a photograph on a mild-sensitivefloor (commonly photographic movie or a wellknown sensor). Cameras have exclusivestructuresto manipulate how the mild falls

onto the mild-sensitivefloor. Focal shines shine the mildgetting into the digital digicam, the dimensions of the outletmay beprolonged or restrictedto present for all intents and functionsmild permission to the digital digicam, and a display screenshapealternatives the quantity of time the phototouchyfloor is familiar with the mild. The licensedphotographdigital digicam is the imperativedevicewithinside theelectricity of pictures and regardedphotosis probably imitated up straightaway as a bit of the instance of pictures, automatic imaging, photographic printing. The comparative innovative fields withinside thetransferringphotographdigital digicamlocation are movie, videography, and cinematography.



2.Power Supply

Reference to a wellspring of electric force. The framework that provisions electrical energy to yield burden or gathering of burden is called power supply unit.This segment is needed to change over AC signal to DC signal.

3.Voice Recognition Module

Voice Recognition Module is a restricted fundamental control talking insistence board. It's anything but's a speaker-subordinate module and supports up to 80 voice orders. Any strong could be pre-pared as solicitation. Clients need to set up the module first before seeing any voice demand. Voice orders are dealt with in one goliath get-together like a library. Any 7 voiced solicitations in the library could be brought into recognizer. It recommends 7 orders are powerful meanwhile. Particulars of Voice attestation module.

1) Voltage: 4.5-5.5V
2) Current: <40mA
3) Digital Interface: 5 V TTL level UART interface
4) Analog Interface: 3.5 mm mono-channel intensifier connector + collector pin between face
5) Recognition exactness: 99% (under ideal environment)
6) Support most outrageous 80 voice orders, with each voice 1500 ms
7) Maximum 7 voice orders practical at same time
8) Easy Control: UART/GPIO
9) User-control General Pin Output

4.Keypad

A keypad is a bunch of catches organized in a square that typically bears digits and different images however not a total arrangement of sequential letters.

5.GSM Module

GSM (Global System for Mobile interchanges) is a mobileular organization, which means thatmobileulartelephones interface with it throughseeking out cells withinside thebrief area. GSM networks paintings in 4numerous recurrence ranges. Most GSM networks paintingswithinside the 900 MHz or 1800mhz groups.

RASPBERRY PI

The Raspberry Pi three is the contemporary interpretation of Raspberry Pi. It additionally encourages the toughdisplay and Wi-Fi speed. The version has numerousequalspecifications as its original, regardless, it brings the rate of the processor as much as 1.4GHz. Not honestly Processor butfurthermore the corporation is in addition upheld upon this version. The versionfurthermore has a Micro USB connection for strengthwithinside the middle, a full-sized HDMI port, and a valid framework sound and composite video yield at the right.

HDMI to VGA

This HDMI to VGA Adapter permits you to consistently streams content from HDMI gadgets like Apple TV, furthermore, other HDMI-fit gadgets to your projector, old screen, or other VGA show.
It likewise incorporates an additional sound link to carry sound to your VGA gadget.
VGA associations just convey visual data. The included sound link guarantees your substance shows up complete with sound.

Liquid Crystal Display

LCD is a slim, level presentation gadget. The working voltage of this LCD is 4.7V-5.3V.
Comprised of monochrome pixels showed in front of the light source. A Most regular gadget connected to a miniature regulator.

Future Scope

In the proposed security structure, face assertion with Windows IoT 10 is gotten along with the voice certification framework for thriving reasons. Facial and voice attestation both are making improvements, with the assistance of these advances we can develop different things. Different calculations are made on the embodiment of confirmation, yet they have different weights. Google API is one of the fit frameworks in voice insistence which eats up less an ideal opportunity to change over any message into demand an embraced.

Conclusion

The proposed system almost gives twofold security because of a mix of face affirmation with Windows IoT 10. Thusly, the face acknowledgment system with the help of windows IoT 10 improves the security of the room without-out permitting unapproved individuals to enter it. Expecting someone endeavors to open the entryway, then, at that point the photograph of the unapproved individual will be shipped off the higher specialists. The voice affirmation is moreover used for the prosperity of secure the room. In this manner, the proposed structure is particularly valuable, effective for getting the room from unapproved individuals.

References:

[1] Automatic Door Unlocking System Using Face Recognition:https://thestempedia.com/project/automatic-door-unlocking-system-using-face recognition/amp/
[2] Face Recognition Door Lock System using Raspberry Pi:
https://iotdesignpro.com/projects/face-recognition-door-lock-system-using-raspberry-pi
[3] Voice Recognition System and it is Working Operation:
https://www.elprocus.com/voice-recognition-security-system/
[4]Facial and Voice Recognition Based Security and Safety System in Car:
https://ieeexplore.ieee.org/document/9197886
[5] Home Security System and Door Access Control Based on Face Recognition: https://www.irjet.net/archives/V4/i3/IRJET-V4I385.pdf
[6] How to build a face detection and recognition system:
https://towardsdatascience.com/how-to-build-a-face-detection-and-recognition-system f5c2cdfbeb8c
[7] Facial Recognition Technology Guide: https://www.techfunnel.com/information technology/facial-recognition-technology/
[8] Facial Recognition using Deep Learning:
https://www.cronj.com/blog/face-recognition-facial-recognition/

Advanced Robot For Defence Applicaion Using Iot

N.C.Bhavitha, C.Ramya, K.Navyasree, P.Malini, SK.Md.Dhahaseem
Dept. Of Ece ,Audisankara College Of Engineering For Women,A.P

Abstract::A robot isa mechanical or virtual arti ficial agent. In practice, it is usually an electro-mechanical system which, by its appearance or movements, conveys a sense that it has intent or agency of its own. The word robot can refer to both physical robots and virtual software agents, but the latter are usually referred to as Robots. There is no consensus on which machines qualify as robots, but there is general agreement among experts and the public that robots tend to do some or all of the following: move around, operate a mechanical arm, sense and manipulate their environment, and exhibit intelligent behavior, especially behavior which mimics humans or animals.

This project is built with Arduino UNO micro controller; this project is housed on a robot base, which moves forward, backward, left and right, this robot base is mounted with an inductive metal detector. When any metal is detected on its way, then a high signal is sent to the micro controller which switches

ON the buzzer. The entire robot
controlling is done through the wifi module and the monitoring of robot movements is done through the website using IOT.

Intrroduction :In today's world, robotics is fastest growing and very interesting field. ROBOT has various input and output to sense the environment and take appropriate action. It has an infrared sensor which is used to sense the obstacles coming in between the path of ROBOT, Camera to capture the pictures of the environment and actuator like motors, grippers and arms to perform actions. With the development and research of technology, scientist has come up with invention of military robots. This makes soldier's life more secure on war field. Military robots are used to perform various risky task like monitor war field, diffuse live unexploded bombs, detect landmines and shoot enemies. Nowadays, many countries take the helps of these robots to take dangerous jobs. These military robots appointed with the integrated systems like sensors, gripper, weapons, cameras and actuators. based purpose of robot it comes in different shapes and features.

The robot is basically electro-mechanical machine or device that is controlled either by computer program or with electronic circuit to perform variety of physical tasks. With the gradual development in technology scientists come up with new ideas and inventions of robots. In the today's life robot are becoming indispensible part of human life [1]. The robotic technology also provides automation in hospital, office and factory. Besides automation this technology also used in Defense forces, Entertainment, Space exploration, Security systems and many dangerous mission execution[3]. As the terror is always remains India's first enemy so, the robots are going to use for saving human life. Countries like India are still facing and confronting with regular threats from terrors. Both Kashmir and Mumbai terror attacks have consummated that as far as possible the future of warfare will be handle by robot and unmanned machines to to protect human life [3]. Currently, the Indian Army has Daksh Military robot to combat in battle field. As the technology proliferate rapidly in automation field by incorporating Military Robots as Soldiers in war field to reduce grievance and demise in war fields [2]. DTMF is known as Dual Tone Multi Frequency which is generated by cell phone when any key is pressed. When any key is pressed then it made connection between the tones of Row and Column which generate dual tone frequency. This dual tone is used to determine which key is pressed [4]. In defense areas, Robot are usually miniature in size so they are enough capable to enter in tunnels, mines and small holes in building and also have capability

to survive in harsh and difficult climatic conditions for life long time without causing any harm [2]. Military robots were designed from last few decades. But still there are some problems in earlier developed military robots.

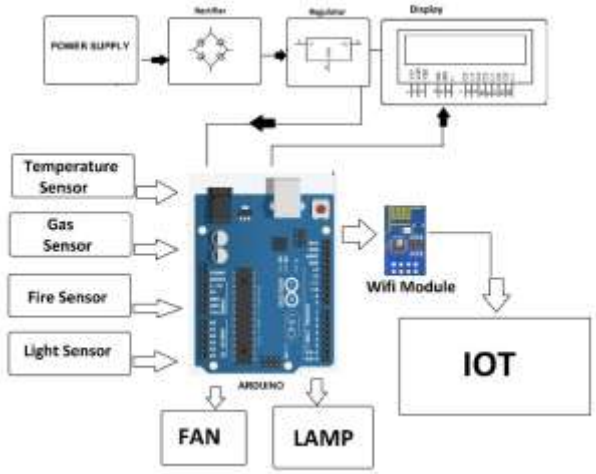


FIG. 1 BLOCK DIAGRAM

HARDWARE REQUIREMENTS

- ARDUINO UNO
- ULTRASONIC SENSOR
- ESP8266 WIFI MODULE
- LASER GUN
- L293D DRIVER CIRCUIT
- POWER SUPPLY
- DC MOTOR
- LCD
- PROXIMITY SENSOR (METAL DETECTOR)
- BUZZER.

ARDUINO UNO

The Arduino Uno is a microcontroller board based on the ATmega328. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button.

It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter

ULTRASONIC SENSOR

An Ultrasonic sensor is a device that can measure the distance to an object by using sound waves.

It measures distance by sending out a sound wave at a specific frequency and listening for that sound wave to bounce back. By recording the elapsed time between the sound wave being generated and the sound wave bouncing back, it is possible to calculate the distance between the sonar sensor and the object.

ESP8266 WIFI MODULE

ESP8266 wifi module is low cost standalone wireless transceiver that can be used for end-point IoT developments.ESP8266 wifi module enables internet connectivity to embedded applications. It uses TCP/UDP communication protocol to connect with server/client

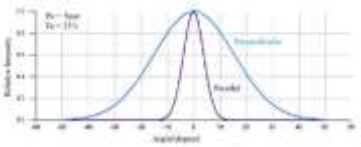
LASER GUN

Characteristics Curves

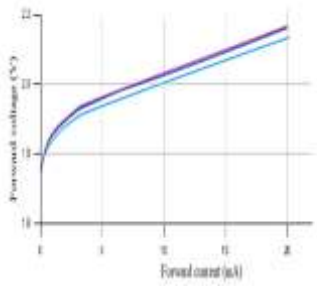
1. Temperature Effect on Operation of Laser Diode

This graph is between Optical output power v/s forward current. It's clear from the graph that laser output will only be visible if obtained above the threshold value of the laser diode. Before the threshold value the output of the laser diode is zero. After the threshold value the output of laser diode increase with slightly increase in forward voltage. The **effect of temperature in the operation of Laser Diode** is shown in graph below:

2. Laser Beam Divergence in parallel and perpendicular plane

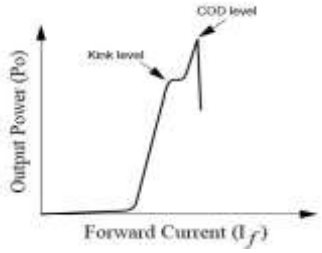


3. Forward voltage v/s Forward current



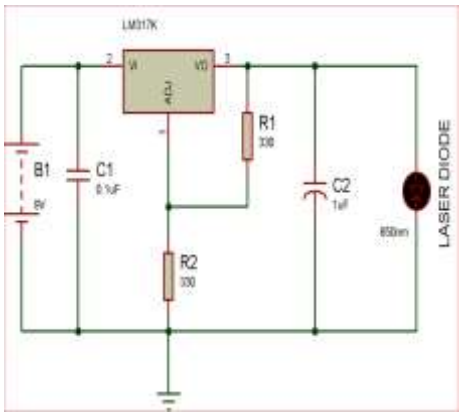
4. Output Power v/s Forward Current

If the direction of moving current is forward and the output is continuously increasing, after the kink level the laser face a sudden breakdown which is the COD (Catastrophic Optical Damage) level. At this level due to high optical density the crystal at the face of diode melts. At the time of manufacturing of Red lasers a special care is taken to avoid surge like static electricity and increase in current, because in red laser the oscillation is occur with the low power of 2 to 3 mW even after the breakdown. As the element is damaged the laser gets damaged or not able to work.



How to use a Laser Diode?

If we want to operate a **Laser diode** then we must have **laser diode driver circuit**. As it helps in limiting current then supply it to laser diode. A laser diode can only work properly with the help of this circuit, if we directly connect it to the supply, because of having more current it will damage and if the value of current is low then the laser diode will not operate. Laser Diode driver circuit helps in providing a correct value of current to operate the laser diode. For making a laser diode driver circuit we need a few no. of components like resistor, capacitor and a voltage regulator IC.



The first capacitor in the circuit filter the High-frequency noise from the DC supply. The second capacitor works as power load balancer used to filter the fluctuating signals of output voltage and a voltage regulator IC is used to provide a fix output voltage and we can adjust the output voltage by changing the value of resistor. You can use a potentiometer instead of resistor (R2) to adjust the intensity of laser light.

L293D DRIVER

The L293 and L293D are quadruple high-current half-H drivers. The L293 is designed to provide bidirectional drive currents of up to 1 A at voltages from 4.5 V to 36 V.

The L293D is designed to provide bidirectional drive currents of up to 600-mA at voltages from 4.5 V to 36 V. Both devices are designed to drive inductive loads such as relays, solenoids, dc and bipolar stepping motors, as well as other high-current/high-voltage loads in positive-supply applications.

BUZZER

A buzzer or beeper is a signaling device, usually electronic, typically used in automobiles, household appliances such as a microwave oven, or game shows.

It most commonly consists of a number of switches or sensors connected to a control unit that determines if and which button was pushed

or a preset time has lapsed, and usually illuminates a light on the appropriate button or control panel, and sounds a warning in the form of a continuous or intermittent buzzing or beeping sound.

SOFTWARE REQUIREMENTS

- ARDUINO IDE
- C-LANGUAGE

SOFTWARE DESCRIPTION

Arduino Software (IDE)

The Arduino Integrated
Development Environment -
or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino and Genuine hardware to upload programs and communicate with them.

CONCLUSION

When we consider military robots today, there has been a huge development as compare to those robots used in earlier times. Today, military ground robots & unmanned vehicles are used worldwide. However, the significant growth of the current military robots comes as the nature of combat changes in every region while the globally integrated enterprise replaces nationalistic dominance. It can be said that military robot automation of the defense process is the next wave of military evolution. This proposed system gives an exposure to design a simple robot that can be used to do multifunction in defense. Manual control is also employed to control the robot from the control room which is located far away from the border area. The system uses non-commercial WIFI module for wireless communication since this provides access to the as-yet unpublished specifications and permission to create products for market using the specifications. Our system is aimed towards the wifi module up to 300 meters distance. In future we can increase the distance depending on our necessities. The proposed system is focusing on the welfare infantry to minimize the causalities to a great extent. This also helps on remote bomb detection and also we can moniter the surroundings through the camera in web page.

REFERENCES

1. Robotic Systems Joint Project OfficeUnmanned Ground Systems Roadmap by Materiel Decision Authority (MDA): Macro USA, McClellan, CA, February 2012.

2. RF Controlled Terrorist Fighting Robot By Abhinav Kumar Singh., NilayaMitashShanker., Anand Prakash Yadav, International Journal of Computer Science & Communication, vol. 1, No. 1, January-June 2010, Pp. 109-112.

3. 7 th Sense: A Multipurpose Robot For Military by L.Srinivasavaradhan., G.Chandramouli., Mr.A.G.Maniprashanna MEMSTECH'2009, 22-24 April, 2009, Polyana - Svalyava (Zakarpattya), Ukraine.

4. Continued testing of the Cannon Caliber electromagnetic Gun System (CCEMG) By: M.D. Werstc.E. Penneyt.J. Hotzj.R. Kitzmiller, 9th EML Symposium, Edinburgh, Scotland, May 1998. 5. IEEE Transactions on Magnetics, Vol 35, No. 1, January 1999, and Pp. 388- 393.

6. Landmine Detection Technologies to Trace Explosive Vapour Detection Technique, C.Kapoor1 and G.K. Kannan, Defense Science Journal, Vol. 57, No. 6, November 2007, Pp. 797- 810, 2007, Desidoc.

7. Analysis And Design of Human-Robot Swarm Interaction in Firefighting By Amir M.Naghsh., JeremiGancet., AndryTanoto., Chris Roast Proceedings of the 17th IEEE International Symposium on Robot and Human Interactive Communication, TechnischeUniversitätMünchen, Munich, Germany, August 1- 3, 2008.

8. Ocari: Optimization of Communication for Ad Hoc Reliable Industrial Network stuan Dang* PhD Member IEEE. 9. Catherine Devic* Et Al***EDF (Electricité De France) R&D – Step. 10. Department of control Systems & Information Technologies Group France 1-4244-9701-0/06/$20.00 © 2008 IEEE.

11. http://www.Robotnik.Es/Automation/Productos/Agvs/Robotnikp01-E.Html

12. http://www.armyofrobots.com

13. http://www.microcontroller.com.

14. www.microchip.com/pic

Covid-19 Future Forecasting Using Time Series Machine Learning Models

V. Gayatri [1] J. Bhavani[2] P. Bhavana[3] P. Divya[4] S. Meghalavani[5]
Associate professor[1], UG Scholars [2,3,4,5]
[1, 2, 3, 4, 5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

ABSTRACT

Machine learning (ML) based forecasting mechanisms have proved their significance to produce outcomes to improve the decision making on the future course of actions. This study demonstrates the capability of Time Series ML models to forecast the number of upcoming patients affected by COVID-19 which is presently considered as a potential threat to mankind. In particular, Time Series Forecasting Models have been used in this study to forecast the number of confirmed and active cases of COVID-19. The dataset used in this study has been obtained from prsindia.org website. Algorithms such as Moving averages, Auto Regressive, ARIMA, SARIMA and Exponential smoothing models have been used in this study. The types of predictions are made by each of the models, such as the number of newly confirmed and active cases in the next 10 days for all over India. Algorithms are evaluated using parameters such as R^2score, MAE, MSE, and RMSE. The results produced by the study prove that it is a promising mechanism to use these methods for the present scenario of the COVID-19 pandemic.

KEYWORDS: Covid-19, Machine Learning, Forecasting, Time Series, Moving Averages, Auto Regressive**.**

I. INTRODUCTION

Artificial Intelligence (AI) may be a science of machines to duplicate the behavior of humans. Machine Learning (ML) is that the subset of AI that focuses on getting machines to form decisions by feeding them with data. ML is that the field of study that provides the pc the power to find out without being explicitly programmed. ML focuses on the event of computer programs which will access the info and use it to find out it. Here Learning is often done by Memorization - Accumulation of facts also called Declarative Knowledge and by Generalization - Deduce new facts from old facts also called Imperative Knowledge. One of the many areas of ML is forecasting, various ML algorithms are utilized in this area to guide the longer term course of actions needed in several application areas including forecasting weather, diseases, and stock exchange prices.

This study aims to supply a forecast model for the spread of novel corona virus, also referred to as SARS-CoV-2, named as COVID-19 (Corona virus Disease of 2019) by the World Health Organization (WHO). COVID-19 currently a significant threats to human life everywhere the planet. Thousands of latest people are reported to be positive a day from countries across the planet. The virus spreads primarily through person to person physical contacts, by respiratory droplets, or by touching the contaminated surfaces. The foremost challenging aspect of its spread is that an individual can possess the virus for several days without showing symptoms. The forecasting is completed on the amount of latest Confirmed and Active cases for the approaching next 10 days.The study is predicated on ML models like Auto Regressive (AR), Moving Averages (MA), Auto Regressive Integrated Moving Average (ARIMA), Seasonal Auto Regressive Integrated Moving Average (SARIMA), Exponential Smoothing (ES).The learning models are trained using the COVID-19 patients dataset provided by prsindia.org website. Models are evaluated using evaluation metrics like MAE (mean absolute error), MSE (mean square error), RMSE (root mean square error), R^2 score (R-squared score).

II. MATERIALS AND METHODS

A. DATASET

The aim of this study is that the future forecasting of COVID-19 spread that specialize in the amount of latest positive cases. The dataset utilized in this study has been obtained from the prsindia.org website. The folder contains daily statistic summary tables, including the amount of confirmed cases, active cases, deaths, and recoveries. All data are from the daily case report then updated with the frequency of 1 day.

B. MACHINE LEARNING MODELS

Time Series Forecasting Models are utilized in this study to forecast the threatening factors of COVID-19. Time Series defined as a sequence of observations taken sequentially in time. Five Time Series models are utilized in study for forecasting number of confirmed and active cases.

1. Auto Regressive (AR)

2. Moving Averages (MA)

3. Auto Regressive Integrated Moving Average (ARIMA)

4. Seasonal Auto Regressive Integrated Moving Average (SARIMA)

5. Exponential Smoothing (ES)

1. AUTO REGRESSIVE (AR)

An Auto Regressive (AR) model predicts future behaviour supported past behaviour. It's used for forecasting when there's some correlation between values during a statistic and thus the values that precede and succeed them. This system is often used on statistic where input variables are taken as observations at previous time steps, called lag variables. In model, we will predict the worth for subsequent time step (t+1) given the observations at the last two time steps (t-1 and t-2). As a regression model, this is often ready to look as follows:

$$X(t+1) = b0 + b1*X(t-1) + b2*X(t-2)$$

The regression model uses data from the same input variable at previous time steps; it's mentioned as an Auto Regression (regression of self).

2. MOVING AVERAGES (MA)

Calculating a moving average involves creating a replacement series where the values are comprised of the standard of raw observations within the first statistic .A moving average requires that you simply specify a window size called the window width. This defines the quantity of raw observations used to calculate the moving average value. The "moving" part within the moving average refers to the actual fact that the window defined by the window width is slid along the statistic to calculate the standard values within the new series.

3. AUTO REGRESSIVE INTEGRATED MOVING AVERAGES (ARIMA)

ARIMA explains the given statistic data supported its own past values, that is, its own lags and therefore the lagged forecast errors, in order that equation are often wont to forecast future values. A typical notation is used of ARIMA(p,d,q) .The parameters of the ARIMA model are as follows-p: the quantity of lag observations included within the model, also called the lag order. q: the amount of times the raw observations are differenced, also called the degree of differencing. d: the dimensions of the moving average window, also called the order of moving average.

4. SEASONAL AUTO REGRESSIVE INTEGRATED MOVING AVERAGES (SARIMA)

SARIMA or Seasonal ARIMA is an extension of ARIMA that explicitly supports univariate statistic data with a seasonal component. It adds three new hyper parameters to specify the Auto Regression (AR), differencing (I) and moving average (MA) for the seasonal component of the series, also as a further parameter for the amount of the seasonality. The notation for an SARIMA model as follows: SARIMA (p,d,q)(P,D,Q)m. The parameters of the ARIMA model are as follows-p: Trend auto regression order, d: Trend difference order and q: Trend moving average order. P: Seasonal auto regression order, D: Seasonal difference order, Q: Seasonal moving average order, m: the quantity of sometime steps for one seasonal period.

5. EXPONENTIAL SMOOTHING (ES)

Exponential smoothing forecasting methods are same therein a prediction may be a weighted sum of past observations, but the model explicitly uses an exponentially decreasing weight for past observations. Past observations are weighted with geometrically decreasing ratio.

New Base=Prev Base -α (Demand -Prev Base) Where New Base represents future predicted value, Prev Base represents Current Predicted Value, Demand represents Actual or fluctuations

occurred in Current values and Alpha is Smoothing Constant whose value ranges from 0 to 1.

C. EVALUATION METRICS

Models are evaluated using evaluation metrics like MAE (mean absolute error), MSE (mean square error), RMSE (root mean square error), R^2 score (R-squared score).

1. MEAN ABSOLUTE ERROR (MAE): The mean absolute error is often a mean on test data between the model predictions and actual data where all individual differences have equal weight.

2. MEAN SQUARE ERROR (MSE): Mean square error takes the space of knowledge points from the regression curve and squaring them. The smaller mean squared error shows the closer you're to finding the road of best fit.

3. ROOT MEAN SQUARE ERROR (RMSE): Root mean square error are often defined because the variance of the prediction errors. RMSE is thus a measure of how concentrated the particular data points are round the best.

4. R-SQUARED SCORE: The metric measures the connection strength between the variable and regression models on a convenient 0 – 100% scale. The high R^2 score shows the goodness of the trained model.

III. METHODOLGY

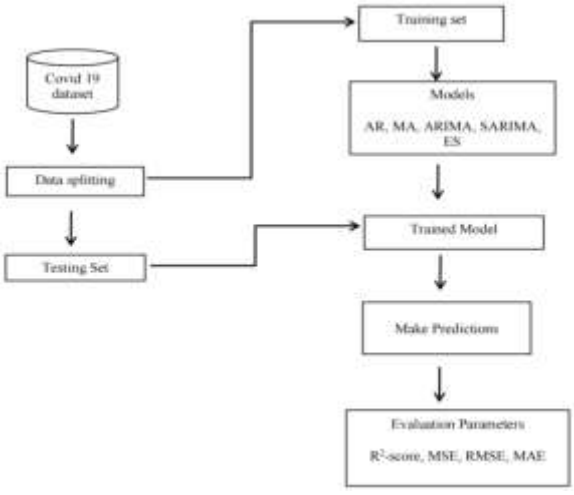


Figure 1: Workflow

The dataset used in this study has been taken from prsindia.org website. The dataset has been divided into training set and testing set. Models such as AR, MA, ARIMA, SARIMA, ES have been trained on days and then make predictions for newly confirmed and active cases for the upcoming ten days. Models have been evaluated using evaluation metrics such as MAE (mean absolute error), MSE (mean square error), RMSE (root mean square error), R^2 score (R-squared score) and reported in the results.

IV.RESULTS

In this study, develop a model for the longer term forecasting of number of Confirmed and Active cases of Covid-19 infected patients.

A. **Confirmed cases future forecasting** The study performs the predictions on number of confirmed cases and consistent with the results SARIMA model works well in forecasting the data where as ES model performs worst during this scenario.

ALGORITHMS	MSE	RMSE	MAE	R^2 SCORE
AR	11353297514.570	106551.854	99688.315	0.8905
MA	4091844134.436	63967.524	44352.569	0.9605
ARIMA	28020600488.628	167393.550	129873.863	0.7298
SARIMA	1827147600.116	42745.147	31033.899	0.9823
ES	52176328485.517	228421.384	226682.413	0.4969

Table 1: Models performance on future forecasting of Confirmed cases

For all the below figures, red line indicates predictions, blue line indicates original data.

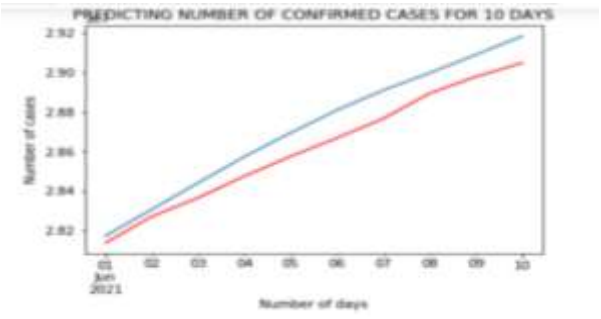


Figure 2: New infected confirm cases prediction by AR for 10 days.

Figure 3: New infected confirm cases prediction by MA for 10 day.

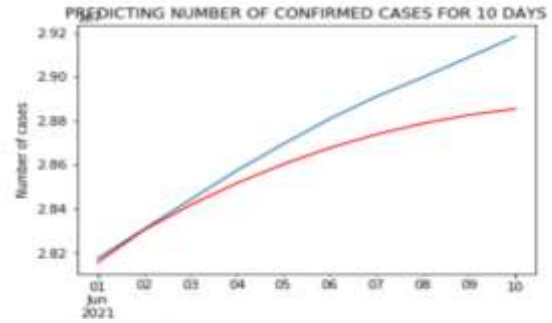


Figure 4: New infected confirm cases prediction by ARIMA for 10 days

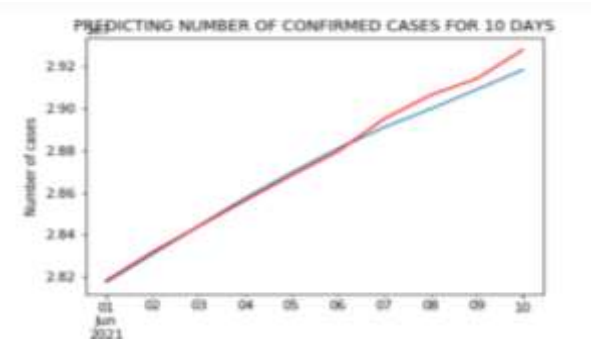


Figure 5: New infected confirm cases prediction by SARIMA for 10 days

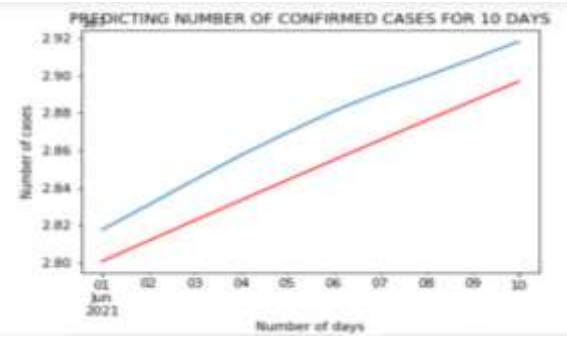


Figure 6: New infected confirm cases prediction by ES for 10 days

B.Active cases future forecasting

The study performs the predictions on number of active cases and according to the results AR model works well in forecasting the data where as ES model performs worst in this scenario.

ALGORITHMS	MSE	RMSE	MAE	R^2 SCORE
AR	752511138.509	27431.936	24476.639	0.9860
MA	2644472706.703	51424.437	43045.942	0.9508
ARIMA	1761047145.178	41964.832	41232.254	0.9672
SARIMA	1173539320.136	34256.960	30077.297	0.9781
ES	9451633766.631	97219.513	89837.685	0.8242

Table 2:Models performance on future forecasting of Active cases

For all the below figures, red line indicates predictions, blue line indicates original data.

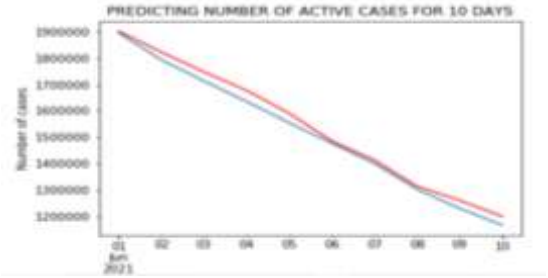


Figure 7: New infected active cases prediction by AR for 10 days

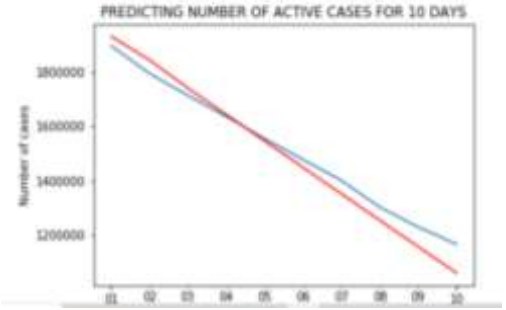


Figure 8: New infected active cases prediction by MA for 10 days

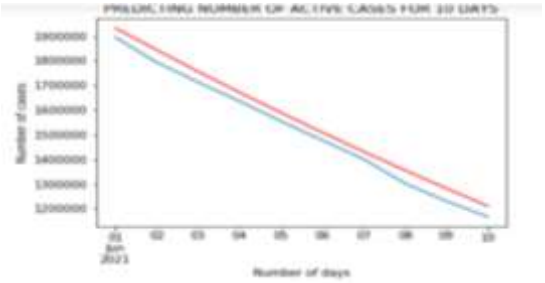


Figure 9: New infected active cases prediction by ARIMA for 10 days

Figure 10:New infected active cases prediction by SARIMA for 10 days

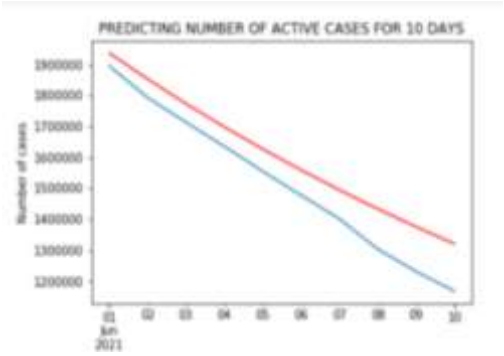


Figure 11: New infected active cases prediction by ES for 10 days

V. CONCLUSION

The precariousness of the COVID-19 pandemic can ignite a huge global crisis. In this study, an ML-based prediction system has been proposed for predicting the danger of COVID-19 outbreak. The system analyses dataset containing the day-wise actual past data and makes predictions for confirmed and active cases for the ten days using statistic Machine Learning Algorithms. From the results seen in Table 1 &2, SARIMA algorithm works well in predicting the amount of Confirmed cases and AR algorithm works well in predicting Active Cases from 1st June 2021 to 10th June 2021, whereas ES algorithm couldn't perform the predictions in comparison to other algorithms. The result indicate that the ML models utilized in this study benefit the forecasting task making the way towards the usability of the study and future research of the similar nature.

VI. REFERENCES

1. G. Bontempi, S. B. Taieb, and Y.-A. Le Borgne, ''Machine learning strategies for time series forecasting,'' in *Proc. Eur. Bus. Intell. Summer School*. Berlin, Germany: Springer, 2012, pp. 62–77.

2. E. Cadenas, O. A. Jaramillo, and W. Rivera, ''Analysis and forecasting of wind velocity in chetumal, quintana roo, using the single exponential smoothing method,'' *Renew. Energy*, vol. 35, no. 5, pp. 925–930, May 2010.

3. R. Kaundal, A. S. Kapoor, and G. P. Raghava, ''Machine learning techniques in disease forecasting: A case study on rice blast prediction,'' *BMC Bioinf.*, vol. 7, no. 1, p. 485, 2006.

4. C. Willmott and K. Matsuura, ''Advantages of the mean absolute error (MAE) over the root mean square error (RMSE) in assessing average model performance,'' *Climate Res.*, vol. 30, no. 1, pp. 79–82, 2005.

5. X. F. Du, S. C. H. Leung, J. L. Zhang, and K. K. Lai, ''Demand forecasting of perishable farm products using support vector machine,'' *Int. J. Syst. Sci.*, vol. 44, no. 3, pp. 556–567, Mar. 2013.

6. H. Asri, H. Mousannif, H. A. Moatassime, and T. Noel, ''Using machine learning algorithms for breast cancer risk prediction and diagnosis,'' *Procedia Comput. Sci.*, vol. 83, pp. 1064–1069, Jan. 2016.

DEVELOPMENT OF MEDICAL TREATMENT SYSTEM USING NON-DETERMINISTIC FINITE AUTOMATA

Dr. Nagendra Kumar P [1] Saketh Damodara [2] Vishnu Vardhan C[3] Abdul RaqeebSk [4] Lokesh Pokala [5]
Associate Professor[1], UG Scholar[2, 3, 4,5]
[1, 2, 3, 4, 5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

Abstract:

In this paper, we propose a security saving clinical treatment system using non-deterministic restricted automata (NFA), from now into the foreseeable future suggested as P-Med, planned for distant clinical environment. P-Med uses the nondeterministic progress typical for NFA to deftly address clinical model, which joins ailment states, treatment methods and state propels achieved by applying different treatment methodologies. A clinical model is encoded and moved to cloud to pass on telemedicine organization. Using P-Med, patient-driven end and treatment can be made on-the-fly while getting the mystery of patient's illness states and treatment idea results. Also, another insurance saving NFA evaluation system is given in P-Med to get a private match result for the appraisal of a mixed NFA and an encoded instructive assortment, which keeps an essential separation from the ambling internal state progress confirmation. We show that P-Med recognizes treatment procedure proposition without assurance spillage to unapproved parties. We lead wide tests and examination to evaluate the capability.

Index terms – Data Confidentiality, NFA, Cloud, IoT.

1. INTRODUCTION

The developing of people and normality of progressing sicknesses have exacerbated various social issues. Far away finding and therapy systems, which use information advancement to give accessible, pragmatic, and high-quality clinical consideration benefits indirectly, can be passed on to moderate a bit of the issues. Such a structure makes it serviceable for continued with treatment in a home environment and grows patient adherence to clinical proposition [1]. The clinical Internet of Things (m-IoT) expects a fundamental part in distant clinical end and treatment by sending far off wearable (or implantable) sensors on a patient to accumulate the vital signs and physiological data [2], [3]. The noticed physiological limits are transported off facility for clinical investigation, which supplies rich longitudinal prosperity records than the brief illness depiction. Using the bare essential checking data, specialists can improve a much representation for the patient and recommend treatment, early intervention and medicine change that are amazing for disease recovery.

The indispensable factor for the exactness of far-off clinical assurance and treatment is the specialist's capacity and master insight. A clinical model is arranged according to practical and quantifiable insight to give clinically supportive information about the course of the illness as time goes on and direct express meds for the condition, which accepts a basic part in dealing with the therapy communication and giving cost rate clinical benefits organizations.

Restricted automata (FA) [4] is one of the standard progressions that can be used to address clinical models. Differentiated and the stream graph or square layout-based model, a FA-based clinical model appreciates the advantage of regularized depiction, versatility in ailment state evaluation and extraordinary expansibility [5], [6]. FA can be organized into two sorts: deterministic restricted automata (DFA) and nondeterministic restricted automata (NFA). The articulation "deterministic" in DFA suggests that it can simply head out to each state thusly (for instance for some given information); "nondeterministic" in NFA infers it can make a trip to different states immediately. Thusly, DFA can be seen as a phenomenal example of NFA; NFA is astonishing to address the nondeterministic state advances and allows void string input (- move), which is more sensible. NFA is an able exhibiting instrument and proper to various fields before long, for instance, common language dealing with, program lexer, and clinical showing. NFA-based clinical models have been used in clinical consideration noticing [5], [6], assurance and treatment of diseases [7], contamination genome acknowledgment [8].Due to the extraordinary openness, accessibility and

staggering estimation limit of cloud, NFA-based clinical models can be moved to a cloud stage to make assurance decisions and propose the treatment methodologies on-the-fly as shown by understanding's physiological data that are checked by mIoT. For instance, a technique could monstrously improve patients' clinical benefits, decrease cost, and redesign the precision of finding in view of its inclination of quantitative assessment. Regardless of the tremendous benefits that can be brought by the far-off assurance and therapy advancement, clinical benefits providers and patients are hesitant to accept it without adequate security and security protections [9]. Since an incredible NFA-based clinical model is every now and again saw as the authorized development and focus earnestness of a clinical establishment, one of the guideline challenges is to get the insurance of the model and severely limit it from divulgence during on the web clinical advantages. Of course, it is required in various domains to guarantee the mystery of patients' prosperity states and keep them from unapproved access. What's more, treatment systems for patients are incredibly sensitive and ought to be kept mystery by the cloud stage or some other pariah.

In this paper, we propose an assurance shielding clinical treatment system using NFA-based clinical model, later on insinuated as P-Med. In a clinical model, the disease states are imparted as the NFA states; an illness state progress achieved by an accommodating intervention is conveyed as a NFA state change; the assortment of medicinal responses is imparted by exploring the nondeterministic typical for NFA. To get the insurance of the clinical model, the NFA-based model is encoded and before it is moved to a cloud specialist for far off clinical advantage. To perform security saving decision and treatment, a patient exchanges their new (e. g. a couple of long stretches of) sickness states in encoded construction to the cloud specialist which performs computations over mixed data.

2. BACKGROUND WORK

A cloud and IoT based ailment assurance framework is proposed in [2] to analyze the data made by clinical IoT contraptions and anticipate the conceivable infection with its level of earnestness. Soft standard based neural classifier is utilized in [3] to construct a cloud and IoT based flexible clinical benefits application for noticing and diagnosing the infections. A continuous patient-driven application is created in [6] to help the treatment of post-discharge patient by a discrete event dynamic system. A clinical decision genuinely strong organization is arranged in [7] to manage the treatment of patients with gestational diabetes, which uses restricted automata to choose the patient's metabolic condition and produce treatment change ideas. These plans recognize web-based finding and treatment subject to plaintext clinical data, where security saving part isn't given. The security concerns should fundamentally be considered to thwart the possible openness of the tricky clinical data and end/treatment result. Yang et al. [24] put forward a lightweight distinguishable arrangement for securely sharing electronic prosperity records, which guarantees the insurance of clinical data. The AI techniques are introduced in secure clinical consistent and finding. An assistance vector machine and Paillier homomorphic encryption based clinical decision sincerely steady organization was arranged in [32], which requires various rounds of correspondence between the specialist and clinician in the assurance.

A security ensuring on the web clinical pre-end framework was suggested in [33] subject to nonlinear bit support vector machine, which utilizes multi-party self-assertive covering and polynomial absolute techniques. Lin et al. [34] utilized legitimate clinical data of patients to get ready irregular neural associations (RNN), and the pre-arranged RNN model made perceptive end decisions. The arrangement proposed in [34] use Paillier homomorphic encryption to set up the clinical benefits model, and bilinear mixing systems to confirm message. Zhang et al. [35] presented a security saving contamination assumption structure reliant upon single-layer perceptron learning and discretionary grids estimation, which consolidates affliction learning stage and gauge stage. An insurance saving different layer neural association was arranged in [36] to help clinical decision, and a safe piecewise polynomial calculation show was proposed to fit the non-straight inception work.

Modified drug may analyze the DNA information of the patient to make end and treatment decisions. Blanton et al. [40] assembled a security saving rethought error resilient DNA search plot through careless evaluation of restricted automata, where the innate test configuration is tended to as a restricted automata and the DNA course of action is considered as the data. During the test cycle, both the model and DNA game plan are kept secret. Keshri et al. [41] presented a mechanized procedure for Epileptic Spike disclosure in Electroencephalogram (EEG), and the system handiness was shown with DFA. Lewis et al. [23] solidified DFA and data disclosure development in data mining TV-tree to construct a phase to discover epileptiform development from Electroencephalograms (EEG), which could expect the interictal spikes inside upheaval to be the pointers of the clinical start of a seizure. Mohassel et al. [42] arranged a reckless DFA evaluation plot with application to get DNA configuration organizing. Selva Kumar et al. [43] utilized DFA to see the cholesterol assimilation with the recognize and reject states and proposed a checking framework subject to DFA, which is used to improve the decisive methodologies and standard treatment in cholesterol metabolic issues. Sasakawa et al. [8] suggested a careless evaluation system for NFA reliant upon homomorphic encryption with secure circuit appraisal procedure, which is appropriate to insurance protecting disease genome area. In any case, the course of action requires diverse correspondence changes between NFA holder and genome data holder.

3. PROPOSED SYSTEM

A. System Model

P-Med consists of five entities (fig 1): key generation center (KGC), cloud platform (CP), computing service provider (CSP), hospitals and patients.

- KGC is a trusted party, and tasked to distribute the public/secret keys and grant authorizations (1).
- Hospital designs medical models for distinct diseases. Without loss of generality, we consider just one medical model per hospital in our description. After encryption, a hospital outsources its own encrypted medical model to CP (2).
- Patient is monitored by mIoT. If patient needs diagnostic and treatment service, the encrypted illness states are sent to CP (3) to issue a query. After the result is returned, patient recovers it using the secret key (5).
- CP has powerful storage and computation capability, tasked to provide storage service for hospitals and respond on the medical query from the patients. CSP provides online calculation service. Upon receiving a patient's query, CP and CSP interactively execute the outsource computing protocols to find the best encrypted treatment procedures (4).

Fig 1: System design

Implementation Algorithm

- In this paper to protect the personal documents we adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES).
- AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

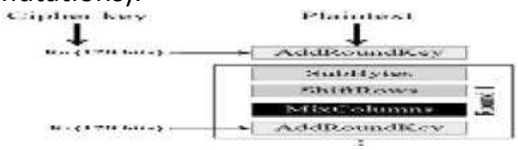


Fig. 2: AES Overview

4. RESULTS

Fig. 3: Home page

Fig. 4: Hospital uploads a report

Fig. 5: Key entry page at doctor or patient

Fig. 6: Database at Cloud Server

Fig. 7: Patients' report

5. CONCLUSION

In this endeavor, we proposed a secured clinical end and treatment framework named as P-Med that can be used to endorse treatment methods to the patients as shown by their illness states. The clinical model in P-Med is fabricated ward on NFA, encoded and moved to cloud. The patient submits reformist a couple of long stretches of mixed mIoT data to give a question and get the top-k best treatment recommendations using secure assurance computation. An ensured affliction state match show is moreover arranged in P-Med to achieve quantitative secure connection between's the state in clinical model and patient's disorder express that are seen by mIoT.

6. REFERENCES

[1] Young K, Gupta A, Palacios R. Impact of telemedicine in pediatric postoperative care. Telemedicine and e-Health. 2018 Dec 5.

[2] Verma P, Sood S K. Cloud-centric IoT based disease diagnosis healthcare framework[J]. Journal of Parallel and Distributed Computing, 2018, 116:27-38.

[3] Kumar P M, Lokesh S, Varatharajan R, et al. Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier[J]. Future Generation Computer Systems, 2018, 86: 527-534.

[4] Sipser M. Introduction to the theory of computation (3rd Edition). Cengage Learning (2013).

[5] Gambheer H. Design safety verification of medical device models using automata theory[D]. California State University Channel Islands, 2016.

[6] Alkhaldi F, Alouani A. Systemic design approach to a real-time healthcare monitoring system: reducing unplanned hospital readmissions[J]. Sensors, 2018, 18(8): 2531.

[7] Caballero-Ruiz E, et al. A web-based clinical decision support system for gestational diabetes: Automatic diet prescription and detection of insulin needs[J]. International Journal of Medical Informatics, 2017, 102: 35-49.

Implementing an Efficient Data Privacy Scheme using Deep Packet Inspection in Cloud

K. Sukeerthi[1] V. Bhargav[2] G. Sumanth[3] Sk.Sultan4 E. Nikhil Teja[5]
Assistant Professor[1], UG Scholar[2, 3, 4, 5]
[1, 2,3,4,5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh

ABSTRACT

Nowadays the traffic is redirected to the public cloud, so some threats like information leakages, such as packet payload and inspection rules, arouse privacy concerns of both middlebox owner and packet senders.To address the concerns, we propose an efficient verifiable deep packet inspection (EV-DPI) scheme with strong privacy guarantees. Specifically, a two-layer architecture is designed and deployed over two non-collusion cloud servers. To improve the efficiency, only fast symmetric crypto-systems, such as hash functions, are used. Large-scale dataset (millions of packets) is tested to obtain the key performance metrics. The experimental results demonstrate that EV DPI not only preserves the packet privacy, but also achieves high packet inspection efficiency.So the Enterprises choose middlebox in order to acquire rich computational and communication resources.

KEYWORDS

Cloud Computing, Network function outsourcing, Middlebox, Privacy-preserving.

---

1. INTRODUCTION

Middlebox is network equipment that supports a wide spectrum of network functions for enterprise networks. For instance, a middlebox can provide firewall, load balancer and deep packet inspection (DPI) services. It is a computer networking device that transforms, inspects, filters, and manipulates traffic for purposes other than packet forwarding. Nowadays, some of the modern middlebox services are delay sensitive. Moreover, it is also challenging to offer high efficiency facing with the explosion of traffic volume. For instance, DPI is a typical delay sensitive network function. One of its key performance metrics is the packet throughput within a certain period of time. Thus, to achieve high efficiency, the most appealing solution is outsourcing the DPI service to the cloud platform.The below figure shows the overview of the two non collision servers.As shown in Fig. i, the proposed system consists of four entities to capture the typical scenarios of the cloud assisted middlebox. The gateway (GW) is the administrator of the internal network. It is responsible for key management and DPI rule generation. At the system initialization phase, GW outsources the encrypted DPI rule set to the middlebox. Afterwards, all the packets sent from the internal network will be gathered by GW. The payload of each packet should be encoded for privacy protection. At last, the encoded packets are redirected to middlebox (MB). The MB is implemented by two non-collusion cloud servers. One is token filtering server (TFS) and the other is rule matching server (RMS). Note that, MB can be instantiated by two real or virtual cloud servers. The external server provides various services to the users of internal network that could be file storage, e-mail, web and so on.Various benefits can be acquired with the assistance of the cloud servers.

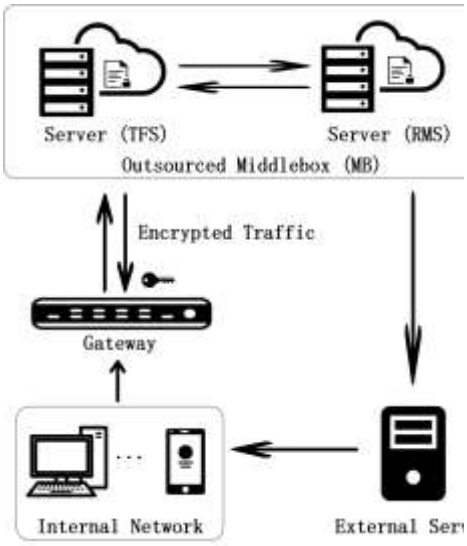


Fig 1: System Overview

First, powerful computation and communication capabilities are provided, which makes it feasible to support efficient DPI over large-scale traffic volume. Second, for the owner of middlebox, diverse DPI functions can be customized to meet the new requirements without purchasing additional hardware. Third, the heavy burden of the daily management of DPI system is released. In addition, the advanced DPI functions, such as machine learning based malware detection, can be efficiently supported by cloud computing. Consequently, significant attentions have been paid to the outsourcing of DPI for cloud-assisted middlebox. Unfortunately, the DPI outsourcing also introduces several security and privacy concerns. In specific, the network traffic has to be redirected to the cloud for inspection. As a result, an important privacy concern is the exposure of packet payload. For example, the personal information of enterprise employees is inevitably disclosed to the cloud server if without any protection. The cloud service provider may even attempt to analyze the private contents for economic interest. Moreover, the passing packets may contain sensitive information that relates to commercial secrets of an enterprise. If these kinds of information are leaked to the cloud or any competitor, serious losses may be caused. Unfortunately, it is usually difficult to process DPI directly over ciphertext domain. Therefore, it is challenging and urgent to design a privacy-preserving DPI scheme over cloud platform.Which done verification and filtering independently because of two non-collusion cloud servers

2. RELATED WORKS

In this section, we give a brief review of previously proposed schemes that are closely related to this paper. Considerable amount of works is presented towards diverse secure and privacy-preserving network functions for outsourced middleboxes. Roughly, they can be divided into two categories. The privacy-preserving DPI schemes [1] can inspect the packet payload and the secure header matching schemes can detect the packet header. And all the works [2] explore diver functions over ciphertext domain. We also discuss the topic of searchable encryption used in the second layer of EV-DPI. Moreover there are some previously proposed schemes which are as follows.

Privacy-preserving DPI:

Symmetric key based schemes: The first privacy-preserving DPI scheme named as BlindBox is proposed in [1]. BlindBox provides a definition of the threat model and the system model to lay a foundation of this topic. It assumes that there are two connections between the packet sender and the receiver. One is the traditional TCP connection and the other is a virtual connection used for payload inspection. The payload is firstly tokenized and then encrypted using AES. And the DPI rules are obfuscated using garbled circuit [4]. Yuan et al. [5] utilize broadcast encryption [6] to control the membership of the network. Thus, all the authorized users can share the same encrypted DPI rules. They also leverage Cuckoo hash to fast filter the passing tokens. Yuan et al. [7] also explore another important issue that is the verification of the DPI execution results. In [7], the verification technique ringer [2] is adopted. The authors extend the basic scheme to support multiple middle boxes, which has the potential to support service function chain. Lan et al. directly use searchable encryption scheme without any modification to implement privacy preserving DPI. Thus, it may suffer from higher packet latency. Recently, Guo et al. [8] achieve dynamic DPI over two non-collusion cloud servers, which allow the middle box to update

the encoded DPI rules. The system and threat models of this scheme are similar to EV-DPI. EV-DPI has not only improved the efficiency, but also provided fine-grained result verification. Public key based schemes: The first public key based privacy-preserving network function outsourcing scheme is presented by Melis et al. The somehow homomorphic encryption (BGN) is used to support additive and one-time multiplicative homomorphic operations over the ciphertext domain. Our previously proposed scheme [10] also utilize BGN to process DPI and machine learning based malware detection. Similarly, Fan et al. [3] also leverage homomorphic encryption to support DPI as well as malware detection. Recently, a scheme based on decryptable searchable encryption named as BlindIDS is presented by Canard [9]. BlindIDS allows the packet receiver directly decrypt the received tokens to verify that whether the tokens are generated and encrypted correctly.

Secure header matching:

The first secure header matching is proposed by Lan et al. The authors design a new algorithm named as PrefixMatch to support the prefix matching over cipher text domain. Prefix Match is implemented and is proved to be quite efficient. Guo et al. convert the header matching problem into privacy preserving range query over cipher text domain. The numerical ranges in the rules are encrypted using order-revealing encryption (ORE). The right cipher text of ORE can achieve semantic secure under chosen plaintext attack. Guo et al. [8] also leverage ORE to support stateful firewall, which lays a foundation for the real deployment of header matching based network functions.

Searchable encryption:

As pointed out by Lan et al., searchable encryption (SE) can be adopted to support privacy preserving DPI. Moreover, the recent advancement of secure range query shows that SE can also be adapted to support semantic secure and efficient range query. Thus, we argue that the SE techniques have the potential for processing the diverse outsourced network functions. SE was originally designed for keyword search over ciphertext domain. With the fast development of this area, many useful properties such as multi-keyword search, conjunctive keyword search and even privacy preserving machine learning are supported. In this paper, we adapt the scheme presented to implement the second layer of EV-DPI. the information leakage of the intermediate search result (result pattern) is formalized and concealed.

3. PROPOSED WORK

In this paper, we have proposed an efficient verifiable deep packet inspection (EV-DPI) scheme with privacy preservation. EV-DPI can well support the verification over final and intermediate inspection results. Both inspection and verification protocols are able to preserve the privacy of packet payload and confidentiality of DPI rules. We have demonstrated the high performance of EV-DPI through extensive experiments and compared the results with the existing scheme. In the future, we will explore the blockchain techniques and learning-based approach to secure diverse outsourced middlebox services.

we propose an efficient verifiable deep packet inspection scheme (EV-DPI) with privacy protection over two non-collusion cloud servers.

• EV-DPI adapts fast symmetric encryption primitives to support privacypreserving DPI.

• EV-DPI also achieves inspection result verification using Cuckoo hashing.

• The verification and DPI can be processed independently.

4.METHODOLOGY

In these section, we present the detailed view of system and describes the work flow of it, And the phases as follows

System initialization: Gateway generates an encoded filter, an encrypted rule set, and uploads them to Token filtering server (TFS) and Rule matching server (RMS), respectively. All the secret keys will be generated and distributed to TFS and RMS. To support the verification of the inspection results, GW also constructs two encoded hash tables and uploads them to TFS and RMS.

Packet processing: GW tokenizes the payloads of packets sent from the internal network. Each token is then encoded. Afterwards, encoded tokens along with the packets are redirected to MB for DPI process.

Token filtering: This is the first layer of EV-DPI. Upon receiving the encoded tokens, TFS fast filters out all the matched tokens. If there is no toke matched, the traffic should be transmitted to the external server. Otherwise, TFS and RMS will collaboratively conduct exact rule matching. Note that, TFS should generate the verification object for each token to prove the execution correctness.

Rule matching: This is the second layer that returns the final inspection result. RMS needs to determine whether each rule is exactly matched or not. During the matching process, RMS may interact with TFS. If any rule is matched, RMS will trigger the pre-defined actions. RMS also needs to return the result to GW for further detection. Otherwise, the packet should be forwarded as usual. It is also needed for RMS to generate the verification objects.

Verification: TFS and RMS each maintains a verification space. They are used to store the verification objects. The size of the verification space is decided by GW. And GW can verify the returned results at any time. The verification only involves GW. TFS and RMS are unaware of when and which packet is verified.

5. RESULTS

The implementation involves various steps. They are:

- Owner
- Gateway
- Middlebox
- Consumer

Owner:

Description: In this module, owner has to register and login to the system. Since there are multiple owners so we use registration.He/she can upload files to the cloud server. These files can be send to the gateway and performs the DPI , generate token and send to the middle box. It verifies the matching rules and stored. The owner can view the file information stored in cloud and then logouts.

Gateway:

Description: The gateway is administrator of the internal network.It is responsible for key management and DPI rule generation. At the system initialization phase, gateway may login and it outsources the encrypted DPI rule set to the middlebox. Afterwards, all the packets sent from the internal network will be gathered by gateway. The payload of each packet should be encoded for privacy protection and then logouts.

MiddleBox:

Description: The encoded packets are redirected to middlebox. It is implemented by two non-collusion cloud servers. One is token filtering server (TFS) and the other is rule matching server (RMS). Note that, MB can be instantiated by two real or virtual cloud servers.

Consumer:

Description: the consumer is a end user. He/she can register and login to the system.He/She can view the files stored in cloud server ,Dowload the files and then logouts.

6. CONCLUSION

In this paper, we have proposed an efficient verifiable deep packet inspection (EV-DPI) scheme with privacy preservation. EV-DPI can well support the verification over final and intermediate inspection results. Both inspection and verification protocols are able to preserve the privacy of packet payload and confidentiality of DPI rules. We have demonstrated the high performance of EV-DPI through extensive experiments and compared the results with the existing scheme. In the future, we will explore the blockchain techniques and learning-based approach to secure diverse outsourced middlebox services.

7.REFERENCES

[1] J. Sherry, C. Lan, R. A. Popa, and S. Ratnasamy,“ BlindBox: Deep packet inspection

over encrypted traffic," in Proc. of ACM SIGCOMM, 2015, pp. 213–226.

[2] C. Wang, X. Yuan, Y. Cui, and K. Ren, "Toward secure outsourced middlebox services: Practices, challenges, and beyond," IEEE Network, vol. 32, no. 1, pp. 166–171, 2018.

[3] J. Fan, C. Guan, K. Ren, Y. Cui, and C. Qiao, "SPABox: Safeguarding privacy during deep packet inspection at a middlebox," IEEE/ACM ToN, vol. 25, no. 6, pp. 3753–3766, 2017.

[4]E.M.Songhori,S.U.Hussain, A. Sadeghi, T.Schneider,F.Koushanfar,"TinyGarble: Highly compressed and scalable sequential garbled circuits," in Proc. of IEEE S&P, May 2015, pp. 411–428.

[5] X. Yuan, X. Wang, J. Lin, and C. Wang, "Privacy-preserving deep packet inspection in outsourced middleboxes," in Proc. of IEEE INFOCOM, 2016, pp. 1–9.

[6] T. V. X. Phuong, G. Yang, W. Susilo, and X. Chen, "Attribute based broadcast encryption with short ciphertext and decryption key," in Proc. of ESORICS, 2015, pp. 252–269.

[7] X. Yuan, H. Duan, and C. Wang, "Bringing execution assurances of pattern matching in outsourced middleboxes," in Proc. of IEEE ICNP, 2016, pp. 1–10.

[8] Y. Guo, C. Wang, and X. Jia, "Enabling secure and dynamic deep packet inspection in outsourced middleboxes," in Proc. of ACM SCC, 2018, pp. 49–55.

[9] S. Canard, A. Diop, N. Kheir, M. Paindavoine, and M. Sabt, "BlindIDS: Market-compliant and privacy-friendly intrusion detection system over encrypted traffic," in Proc. of ACM AsiaCCS, 2017, pp. 561–574.

[10] H. Li, H. Ren, D. Liu, and X. Shen, "Privacy-enhanced deep packet inspection at

Efficient Data Migration Model and Key Agreement Scheme for Peer-to-Peer Cloud

Shaik.Asiff[1] Sd.Sumayya Muskan[2] P.Greeshma[3] N.Rajeswari[4] P.Veena Vahnika[5]

Associate Professor[1], UG Scholar[2, 3, 4, 5]

[1, 2, 3, 4, 5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

Abstract - Cross-cloud data migration is one of the prevailing challenges faced by mobile users, which is an essential process when users change their mobile phones to a different provider. However, due to the insufficient local storage and computational capabilities of the smart phones, it is often very difficult for users to backup all data from the original cloud servers to their mobile phones in order to further upload the downloaded data to the new cloud provider. To solve this problem, we propose an efficient data migration model between cloud providers and construct a mutual authentication and key agreement scheme for peer-to-peer cloud. The proposed scheme helps to develop trust between different cloud providers and lays a foundation for the realization of cross- cloud data migration.

Keywords - Cloud computing, data migration, authentication, key agreement.

I.INTRODUCTION

People are now increasingly relying on hand-held devices such as smart phones, tablet etc., in an unprecedented number. It is worthy of note that one individual may own and use multiple smart devices. It is also common for people to recycle their smart devices quite frequently, given the fact that new arrivals characterize more attractive inherent features from a variety of manufacturers.

When people opt to use a new smart device from a different manufacturer, the data stored in the cloud server of the previous smart device provider should be transferred to the cloud server of the new smart device provider. One of the common ways of accomplishing this transfer is to log onto the original cloud server, download the data onto the smart terminal devices, log onto the new cloud server, and finally upload the data to the new server. As shown in Fig. 1, this process is very inefficient and tedious.

To this end, it is essential to develop a more efficient and secure way of data transfer from one cloud server to another. An ideal data migration model that can transfer user data directly between cloud servers is shown in Fig. 2. Such a model often imposes compatibility issues, since different cloud service providers characterize diverse user functions, mutual distrust and security risks in the process of data transmission, which make this ideal data migration model difficult to implement.

A few researches have attempted to overcome such data migration issues in the recent past. For example, in 2011, Dana Petcu [6] argued that the biggest challenge in cloud computing is the interoperability between clouds, and proposed a new approach for cloud portability. Binz et al. [7] proposed a cloud motion framework that supports the migration of composite applications into or between clouds. In 2012, Shirazi et al. [8] designed a scheme to support data portability between cloud databases.

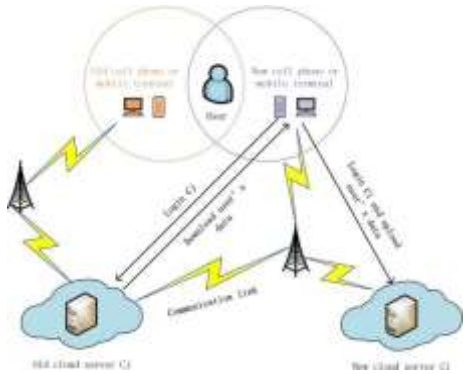


Fig. 1. Original data migration model

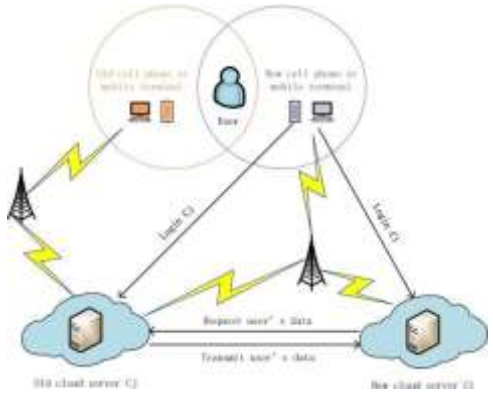


Fig. 2. Ideal data migration model

A. *Our Motivations*

First, we realized that the study of data migration across cloud platforms has very important practical significance. The data migration issues between clouds has many unresolved potential problems. Existing efforts in the context of cloud data migration has obvious pitfalls that restrains their efficiencies. This is to say, further research into the context of cloud data migration is an important and timely necessity, especially to facility quicker and ease data transfer between the cloud servers after users change their smart phones. Secondly, in reality, trustworthiness among multi-clouds cannot

be easily achieved, particularly applications involving sensitive data transfers characterize more security constraints. For instance, achieving mutual authentication, building communication key securely and protecting the data transfer from potential attacks are some concerns to mention. Herein, authentication and key agreement mechanism can be an effective way to solve these problems. ultimately to facilitate easy and secure data transfer between multi-clouds.

B. *Our Contributions*

To our knowledge, this is the first authentication and key agreement scheme for peer cloud servers.

· We propose a peer-to-peer cloud authentication and key agreement (PCAKA) scheme based on anonymous identity to solve the problem of trust between cloud servers. Based on the Advanced Encryption Standard (AES), our scheme can establish secure session keys between cloud service providers to ensure session security.

· The novelty of our scheme lies in the fact that it eliminates the need for trusted authority (TA) and simplifies operations while maintaining security. In our scheme, the cloud servers enable the data owners in need of the data migration services to act as trusted third authority, so that they can verify each other and establish trusted session keys after each of the involved users performs some computation independently.

· Our scheme uses server anonymity to protect the privacy of service providers and users. It is worthy of note that both the two cloud servers involved in the migration process use anonymous identities for mutual authentication and key agreement. This strategy not only protects the identity privacy of the cloud service providers, but also makes it impossible for the involved cloud service providers to gain unnecessary information such as the brand of the old and new mobile phones belonging to the users respectively. Thus, our methodology maintains the privacy of the users by not revealing his/her personal choice.

· Our scheme provides identity traceability to trace malicious cloud servers. If the cloud service providers exhibit any errors or illegal operations in the service process, users can trace back to the real identity of the corresponding cloud server based on the anonymous identity.

II.RELATED WORK

In order to realize data sharing in the cloud, a few schemes have used proxy re-encryption techniques [9]–[13]. For ex- ample, Liang and Cao

[9] proposed a property-based proxy re-encryption scheme to enable users to achieve authorization in access control environments. However, Liang and Au [10] pointed out that this scheme does not have Adaptive security and CCA security features. Sun et al. [12] introduced a new proxy broadcast repeat encryption (PBRE)

scheme and proved its security against selective cipher text attack (CCA) in a random oracle model under the decision n-BDHE hypothesis. Ge and Liu [13] proposed a broadcast agent encryption (RIB- BPRE) security concept based on revocable identity to solve the key revocation problem. In this RIB-BPRE scheme, the agent can undo a set of delegates specified by the princi- pal from the re-encryption key. They also pointed out that the identity-based broadcast agent re-encryption (RIB-BPRE) schemes do not take advantage of cloud computing, thus causes inconvenience to cloud users.

Liu et al. [14] proposed a secure multi-owner data sharing scheme for dynamic groups in the cloud. Based on group signature and dynamic broadcast encryption technology, any cloud user can share their data anonymously with others. Yuan et al. [15] proposed a cloud user data integrity check scheme based on polynomial authentication tag and agent tag update technology, which supports multi-user modification to resist collusive attack and other features. Ali et al. [16] proposed a secure data sharing cloud (SeDaSC) method using a single encryption key to encrypt files. This scheme provides data confidentiality and integrity, forward and backward access control, data sharing and other functions. Li et al. [17] proposed a new attribute-based data sharing

scheme to assist mobile users with limited resources based on cloud computing.

Authentication and key agreement is a method that enables both parties to secretly calculate the session key on a public channel, which have been widely studies [18]–[31]. As early as 1993, Maurer [18] proposed that only a difference in the received signals helps achieving perfect cryptographic security, regardless of the enemy's computing power. But they have not considered the advantage of legitimate communicants. Suffices for achieving perfect cryptographic security, regardless of the enemy's computing power. Lu and Lin [19] proposed a medical key negotiation scheme based on patient symptom matching. However, He et al. [32] pointed out that Lu's scheme does not provide an identity tracking and resistance modification function and further proposed a cross-domain handshake scheme applicable to medical mobile social net- work and developed an android app for experimental analysis. Later, Liu and Ma [20] found that He et al.'s scheme does not resist replay attack.

Tsia and Lo [21] proposed an efficient distributed mobile cloud computing service authentication scheme with multiple functions such as user anonymity. Irshad and Sher [23] improved the protocol of Tsia [21] to make the scheme suitable for practical deployment in different wireless mobile access networks. However, Jia and He [33] pointed out that Tsia et al.'s scheme does not offer resistance to impersonation at- tacks and man- in-the-middle attacks. Moreover, Irshad et al.'s scheme does not support perfect forward privacy. Amor and Abid [24] proposed a mutual authentication scheme for fog users and fog servers under the condition of user anonymity. Mahmood et al. [26] proposed an anonymous key negotiation protocol for smart grid infrastructure that enables smart meters to connect anonymously to utilities. But Wang and Wu [31] pointed out that Amor et al.'s protocol cannot resist stolen verifier attacks and Mahmood et al.'s protocol cannot resist man- in-the-middle attacks and impersonation attacks.

III.PROPOSED WORK

To this end, it is essential to develop a more efficient and secure way of data transfer from one cloud server to another. For that, we propose a peer- to-peer cloud authentication and key agreement (PCAKA) scheme based on anonymous identity to solve the problem of trust between cloud servers. The novelty of our scheme lies in the fact that it eliminates the need for trusted authority (TA) and simplifies operations while maintaining security. Here we are using Advanced Encryption Standard (AES).

Our scheme can establish secure session keys between cloud service providers to ensure session security. Our methodology maintains the privacy of the users by not revealing his/her personal choice

IV.RESULT

Fig. 3. Home Page

Home Page Consists of Mobile Terminal, User Login, Cloud Server. In User Login we migrate data from one cloud server to other cloud server, In Mobile Terminal we can see from which cloud to cloud the data has been migrated.

Fig. 4. Data Migration

The Data will be migrated securely from one cloud to another cloud, this secure data migration is the result of the project.

V.CONCLUSION

This project proposed a novel scheme to transfer user data between different cloud servers based on a key agreement protocol. The advantages of our scheme are proved from three aspects: security performance, calculation costs and communication costs. Our proposed scheme can efficiently solve the primary problem of trust during data migration between cloud servers and further can provide anonymity for the identity of cloud servers. On the premise of protecting the privacy of cloud service providers, our proposed scheme indirectly protects the privacy of users. In addition, the identity traceability provided by our proposed scheme also enables users to effectively constrain the cloud service providers.

As a future work, we plan to explore and develop a protocol that allows multiple users to share data across different cloud servers, with the motivation of enhancing the efficiency of data sharing among multiple users.

REFERENCES

[1] C. I. network information center, "The 44th china statistical report on internet development,"http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201908/P020190830356787490958.pdf, 2019.

[2] B. Li, J. Li, and L. Liu, "Cloudmon: a resource-efficient iaas cloud monitoring system based on networked intrusion detection system virtual appliances," Concurrency and Computation: Practice and Experience, vol. 27, no. 8, pp. 1861–1885, 2015.

[3] J. Cui, H. Zhou, H. Zhong, and Y. Xu, "Akser: attribute- based key- word search with efficient revocation in cloud computing," Information Sciences, vol. 423, pp. 343–352, 2018.

[4] J. Cui, H. Zhong, W. Luo, and J. Zhang, "Area-based mobile multicast group key management scheme for secure mobile cooperative sensing," Science China Information Sciences, vol. 60, no. 9, p. 098104, 2017.

[5] J. Cui, H. Zhou, Y. Xu, and H. Zhong, "Ooabks: Online/offline attribute- based encryption for keyword search in mobile cloud," Information Sciences, vol. 489, pp. 63–77, 2019.

[6] D. Petcu, "Portability and interoperability between clouds: challenges and case study," in European Conference on a Service-Based Internet. Springer, 2011, pp. 62–74.

[7] T. Binz, F. Leymann, and D. Schumm, "Cmotion: A framework for migration of applications into and between clouds," in 2011 IEEE International Conference on Service-Oriented Computing .

A **Secure and Efficient Cloud Data Transfer and Deletion Using Counting Bloom filter**

Ms. N. Sivanagamani[1] M. Karthik [2] Md. Shareef [3] M. Vamsi Krishna Savarkar [4] Sk. Althaf[5]
Associate Professor[1], UGScholar[2,3,4,5]
[1,2,3,4,5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh

ABSTRACT - Now a days due to the development of cloud storage, an increasingnumberofdataownersprefer to outsource their data to the cloud server,whichcangreatlyreducethelocal storage overhead. Because different cloud service providers offer distinct quality of data storage service, e.g., security, reliability, access speed and prices, cloud data transfer has become a fundamental requirement of the data owner to change the cloud service providers. Hence, how to securely migrate the data from one cloud to another and permanently delete the transferred data from the original cloud becomes a primary concern of data owners. To solve this problem, we construct a new counting Bloom filter- based scheme in this paper. The proposed scheme not only can achieve secure data transfer but also can realize permanent data deletion. Additionally, the proposed scheme can satisfy the public verifiability without requiring any trusted third party.

Keywords - Cloud storage, Data deletion, Data transfer, Counting Bloom filter, Public verifiability.

INTRODUCTON

Computing paradigm, connects large-scale distributed storage resources, computing resources and network bandwidths together[1,2]. By using these resources, it can provide tenants with plenty of high-quality cloud services. Due to the attractive advantages, the services (especially cloud storage service)have been widely applied [3,4], by which the resource-constraint data owners can outsource their data to the cloud server, which can greatly reduce the data owners' local storage overhead [5,6]. According to the report of Cisco [7], the number of Internet consumers will reach about 3.6 billion in 2019, and about 55 percent of them will employ cloud storage service.

Because of the promising market prospect, an increasing number of companies (e.g., Microsoft, Amazon, Alibaba) offer data owners cloud storage service with different prices, security, access speed, etc. To enjoy more suitable cloud storage service, the data owners might change the cloud storage service providers. Hence, they might migrate their outsourced data from one cloud to another, and then delete the transferred data from the original cloud. According to Cisco [7],the cloud traffic is expected to be 95% of the total traffic by the end of 2021, and almost 14% of the total cloud traffic will be the traffic between different cloud datacenters. Foreseeably, the outsourced data transfer will become a fundamental requirement from the data owners' point ofview.

To realize secure data migration, an outsourced data transfer app, Cloudsfer[8], has been designed utilizing cryptographic algorithm to prevent the data from privacy disclosure in the transfer phase. But there are still some security problems in processing the cloud data migration and deletion. Firstly, for saving network bandwidth, the cloud server might merely migrate part of the data, or even deliver some unrelated data to cheat the data owner[9].Secondly, because of the network instability, some data blocks may lose during the transferprocess.

Meanwhile, the adversary may destroy the transferred data blocks[10]. Hence, the transferred data may be polluted during the migration process. Last but not least, the original cloud server might maliciously reserve the transferred data for digging the implicit benefits. The data reservation is unexpected from the data

owners' point of view. In short, the cloud storage service is economically attractive, but it inevitably suffers from some serious security challenges, specifically for the secure data transfer, integrity verification, verifiable deletion. These challenges, if not solved suitably, might prevent the public from accepting and employing cloud storage service.

1. RELATEDWORKS

Secure and efficient fine-grained data access control scheme in cloud computing

By combining cloud computing and Peer-to-Peer computing, a P2P storage cloud can be formed to offer highly available storage services, lowering the economic cost by exploiting the storage space of participating users. However, since cloud severs and users are usually outside

the trusted domain of data owners, P2P storage cloud brings forth new challenges for data security and access control when data owners store sensitive data for sharing in the trusted domain. Moreover, there are no mechanisms for access control in P2P storage cloud. To address this issue, we design a ciphertext-policy attribute-based encryption (ABE) scheme and a proxy re- encryption scheme. Based on them, we further propose a secure, efficient and fine-grained data Access Control mechanism for P2P storage Cloud named ACPC[1]. Our security analysis demonstrates that ACPC is provably secure.

A. New algorithms for secure outsourcing of modular exponentiations

With the rapid development of cloud services, the techniques for securely outsourcing the prohibitively expensive computations to untrusted servers are getting more and more attention in the scientific community. Exponentiations modulo a large prime have beenconsidered the most expensive operations in discrete- logarithm-based cryptographic protocols, and they may be burdensome for the resource-limited devices such as RFIDtags or smartcards. Therefore, it is important to present an efficient method to securely outsource such operations to (untrusted) cloud servers. In this paper, we propose a new secure outsourcing algorithm[2] for (variable-exponent, variable-base) exponentiation modulo a prime in the two un trusted program model. Compared with the state-of-the-art algorithm, the proposed algorithm is superior in both efficiency and check ability.

Based on this algorithm, we show how to achieve outsource-secure Cramer- Shoup encryptions and Schnorr signatures. We then propose the first efficient outsource-secure algorithm for simultaneous modular exponentiations.

B. Privacy-preserving outsourced classification in cloud computing

Classifier has been widely applied in machine learning, such as pattern

recognition, medical diagnosis, credit scoring, banking and weather prediction. Because of the limited local storage at user side, data and classifier has to be outsourced to cloud for storing and computing. However, due to privacy concerns, it is important to preserve the confidentiality of data and classifier in cloud computing because the cloud servers are usually untrusted. In this work, we propose a framework for privacy- preserving outsourced classification[3] in cloud computing (POCC). Using POCC, an evaluator can securely train a classification model over the data encrypted with different public keys, which are outsourced from the multiple data providers. We prove that our scheme is secure in these mi-honest model.

C. Next generation cloud computing: New trends and research directions

The landscape of cloud computing has significantly changed over the last decade. Not only have more providers and service offerings crowded the space, but also cloud infrastructure that was traditionally limited to single provider data centers is now evolving. In this paper, we firstly discuss the changing cloud infrastructure and consider the use of infrastructure from multiple providers and the benefit of decentralising computing away from data centers. These trends have resulted in the need for a variety of new computing architectures that will be offered by future cloud infrastructure.

These architectures are anticipated to impact areas, such as connecting people and devices, data-intensive computing, the service space and self-learning systems. Finally, we layout a roadmap of challenges that will need to be addressed for realising the potential of next generation cloud systems.

2. PROPOSEDWORK

The main aim of this project to propose a new counting Bloom filter-based scheme in this proposed. The proposed scheme not only can achieve secure data transfer but also can realize permanent data deletion. Additionally, the proposed scheme can satisfy the public verifiability without requiring any trusted third party.

- In this work, we study the problems of secure data transfer and deletion in cloud storage, and focus on realizing the public verifiability.
- Then we propose a counting Bloom filter-based scheme, which not only can realize provable data transfer between two different clouds but also can achieve publicly verifiable data deletion.

- If the original cloud server does not migrate or remove the data honestly, the verifier (the data owner and the target cloud server) can detect these malicious operations by verifying the returned transfer and deletion evidences.

4. RESULTS

The implementation involves various steps. They are:

- Dataowner
- Cloudserver
- ProxyServer
- End user

Dataowner:

Fig: Data owner login page

Fig: Data owner Home page

Description: This is Data Owner Login Page; in this page admin can login and check the user details.

Description: This is the data owner Home page, in this page admin can login and check the user details and data owner details and file request details, Data owner can purchase VM, upload the data, and Transfer the data.

Cloud server

Fig: Cloud server home page

Description: This is the cloud server login page; in this page admin can login and check the user details, data owner details, data sharing request details and download or view file details.

Description: This is cloud provider home page; in this page admin can check the user details, data owner details, threshold details, view end users and view all the transaction details, view attacker details.

Proxy server:

Fig: Proxy server Home page

Description: This is Proxy server home page in this page admin can View transfer details, View work load, view proxy files and view all the transaction details.

End user

Fig: End user login page

Fig: End user Home page

Description: This is user login page; in this user login page user can login and check the user details and download or view data details.

Description: This is user home page, in user home page user can login, request file, view file response, download file.

5. CONCLUSION

In cloud storage, the data owner does not believe that the cloud server might

execute the data transfer and deletion operations honestly. To solve this problem, we propose a CBF-based secure data transfer scheme, which can also realize verifiable data deletion. In our scheme, the cloud to which the data has been transferred can check the transferred data integrity, which can guarantee the data is entirely migrated. Moreover, the cloud from where the data has transferred should adopt CBF to generate a deletion evidence after deletion, which will be used to verify the deletion result by the data owner. Hence, the cloud from where the data has been transferred cannot behave maliciously and cheat the data owner successfully

6. REFERENCES

[1] C.YangandJ.Ye,"Secureandefficient fine-grained data access controlscheme in cloud computing", Journal of HighSpeed Networks, Vol.21, No.4, pp.259–271,2015.

[2] X. Chen, J. Li, J. Ma, et al., "New algorithms for secure outsourcing of modular exponentiations", IEEE Transactions on Parallel and Distributed Systems, Vol.25, No.9, pp.2386–2396,2014.

[3] P. Li, J. Li, Z. Huang, et al., "Privacy-preserving outsourced classification in cloud computing", Cluster Computing, Vol.21, No.1, pp.277–286,2018.

[4] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions", Future Generation Computer Systems, Vol.79, pp.849–861,2018.

[5] W. Shen, J. Qin, J. Yu, et al.,"Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage", IEEE Transactions on Information Forensics and Security, Vol.14, No.2, pp.331– 346,2019.

[6] R. Kaur, I. Chana and J. BhattacharyaJ, "Data deduplication techniquesfor efficient cloud storage management: A systematic review", The Journal of Supercomputing, Vol.74, No.5, pp.2035–2085, 2018.

IMPROVED SECURITY USING FOG BASED ENCRYPTED CONTROL SYSTEM

R. Sivaiah[1]P.Naveen Kumar Reddy [2]M.Prudhvi[3]Ch. Muniraja [4]J.C. vinodkumar [5]
Assistant Professor [1], UG Scholar[2,3,4,5],[1,2,3,4,5] Department of CSE,
Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

Abstract – This paper encourages a dimness preparing based mixed control structure in a utilitarian present day setting. The made structure conceals controller gains and signals over correspondence joins using multiplicative homomorphic encryption to thwart tuning in attacks. Exploratory endorsement avows the credibility of position servo control for the motor driven stage with the made system to the extent execution degradation, limit assortment, and taking care of time. The made system procures its dauntlessness whether plant limits change or not even after the controller gains and signals are mixed. In addition, despite the way that planning time ends up being longer by extending an imperative length of encryption, debasement of control execution is further developed meanwhile.

Index terms – cloud computing, Fog Computing, Controller, Homomorphic encryption.

---

1. INTRODUCTION

Cloud-based control systems, in which controlled contraptions are related with a correspondence association to be noticed and controlled in the cloud, are getting reputation. Control as a Service (CaaS) for auto control, a cloudbased control thought, was proposed. The makers introduced RobotControl as a Service. This thought similarly recognizes higher-layer control (e.g., development preparing for) mechanical robots. Rapyuta assisting RoboEarth is Platform as a Service (PaaS) for cloud progressed mechanics applications. The essential advantage of these designs lies in their further evolved flexibility, adaptability, and efficiency over customary coordinated systems.

Of course, lower-layer control (e.g., servo control of actuators) very neighborhood execution, and a cloud designing isn't sensible for such control by virtue of latencies between controlled devices related with the cloud. This issue can be tended to by fog enrolling, which is a decentralized figuring plan with a moderate layer called fog. Murkiness enrolling based control structures diminish correspondence concede and hold the potential gains of cloud-based control systems, that is, the controller shouldn't be presented locally, and directors can remotely screen the plant condition and adequately change the control law. In addition, the fog aggregates and cleans dirty data to help assessment in the cloud.Dimness figuring offers various anticipated benefits, especially for ceaseless applications, notwithstanding the way that security and insurance issues in the fog persist like the occurrence of the cloud. Attacks on computerized real systems, for instance, coordinated control structures, are more hurting than attacks on information systems considering the way that real structures candirectly impact certifiable conditions. Enemies can sneak around, assault, and contort the structure if wellbeing endeavors have not been done sufficiently.

The makers checked the threats of regulators by authentic attacks, which meddle with controller gains. It is fundamental to muddle controller gains and to camouflage signals from the attacks.

Encoded control, a mix of cryptography and control theory, is a promising methodology to chip away at the security of control systems by decreasing perils of tuning in attacks. Snoopping attacks intend to take information of control structures to execute more outrageous attacks, for instance, zero components attacks, later on. In encoded control structures using ElGamal encryption, which is multiplicative homomorphic encryption, control inputs are resolved in ciphertext from mixed controller limits, mixed sensor data, and a mixed reference without unscrambling. Also, mixed control can be applied for the recognizable proof of replay attacks and

controller or sign defilement attacks. The encoded control system with Paillier encryption, which is added substance homomorphic encryption was proposed. The makers outfitted the sign covering method with totally homomorphic encryption. Homomorphic encryption is utilized as a wellbeing exertion in control systems, as demonstrated already. In any case, it's hard to tangle the controller limits with added substance homomorphic encryption since duplication between two data can't be executed in ciphertext. Besides, added substance and totally homomorphic encryptions require incalculable computational resources for homomorphic action. Thusly, these encryption plans are not sensible for lower-layer control of mechanical systems.

2.BACKGROUND WORK

a. Rapyuta:Acloud robotics platform

In this paper,we present the arrangement and execution of Rapyuta, an open-source cloud progressed mechanics stage. Rapyuta helps robots with offloading powerful computation by giving got flexible figuring conditions in the cloud. The figuring conditions in like manner license the robots to conveniently get to the RoboEarth data storage facility. In addition, these figuring conditions are immovably interconnected, preparing for association of mechanical gatherings. We furthermore portray three typical use cases, some benchmarking and execution results, and two proof-of-thought appearances. Note to Practitioners - Rapyuta grants to re-proper a couple or the sum of a robot's introduced computational cycles to a business worker ranch. Its essential differentiation to other, similar frameworks like the Google App Engine is that it is expressly altered towards multiprocess high-information transmission mechanical innovation applications/middlewares and gives an overall filed open-source execution that can be changed to cover a huge arrangement of mechanized circumstances.

rethinking of for all intents and purposes the sum of the current 3000+ ROS packages out of the compartment and is viably extensible to other mechanized middleware. A pre-presented Amazon Machine Image (AMI) is given that licenses to dispatch Rapyuta in any of Amazon's worker ranch right away. Once dispatched, robots can check themselves to Rapyuta, set up something like one got computational conditions in the cloud and dispatch the best centers/measures. The enlisting conditions can in like manner be discretionarily connected with develop equivalent preparing models on the fly. The WebSocket-based correspondence show, which gives composed and unique correspondence frameworks, licenses ROS based robots, yet also projects and mobiles phones to connect with the climateRapyuta's figuring environmental factors are private, secure, and improved for data throughput. In any case, its show is in colossal part directed by the lethargy and nature of the association affiliation and the introduction of the worker ranch. Further developing execution under these goals is regularly significantly application-express. The paper shows an outline of execution headway in an aggregate steady 3-D arranging application. Other target applications fuse shared 3-D arranging, task/handle organizing, object affirmation, restriction, and teleoperation, among others.

b. Fundamental issues in networked control systems

This paper gives an investigation on showing and hypotheses of organized control systems (NCS). In the underlying section, showing of the different kinds of defects that impact NCS is discussed. These imperfections are quantization botches, pack dropouts, variable reviewing/transmission extends, variable transmission deferrals, and correspondence impediments. Then proceeds in the second area a demonstration of a couple of hypotheses that have been applied for controlling organized structures. These speculations include: input delay structure approach, Markovian system approach, traded structure approach, stochastic system approach, hurried system approach, and perceptive control approach. In the last part, some general issues in NCS including decentralized and scattered NCS, cloud control structure, and co-plan of NCS are evaluated.

c. Fog computing and its role in the Internet of Things

Fog sorting loosens up the Cloud Computing perspective to the edge of the association, accordingly engaging another assortment of

employments and organizations. Describing qualities of the Fog are: a) Low latency and region care; b) Wide-spread geological flow; c) Mobility; d) Very tremendous number of centers, e) Predominant piece of distant access, f) Strong presence of streaming and ceaseless applications, g) Heterogeneity. In this paper we battle that the above characteristics make the Fog the fitting stage for different essential Internet of Things (IoT) organizations and applications, to be explicit, Connected Vehicle, Smart Grid, Smart Cities, and, when everything is said in done, Wireless Sensors and Actuators Networks (WSANs).

3. PROPOSED WORK

Fig. 1 delineates an idea of the haze processing based control framework with a Public cloud. Organization An administrates a cloud framework and gives a stage to work the higher-layer control. Organization B, C, and D oversee mist associated with the cloud and one another. Organization B and C might be parts of Company D, and they intend to control gadgets, which incorporate a few actuators and are possessed by each organization. An administrator sends undertakings for the higher-layer control to an application in the cloud. The application creates reference signs to carry out the errands and moves them to the haze. The haze chooses the info signals from the reference signs and sensor information of the gadgets continuously. Furthermore, the mist handles working information and moves them to the cloud. The cloud stockpiles the information and pictures them with a web interface for the administrator.

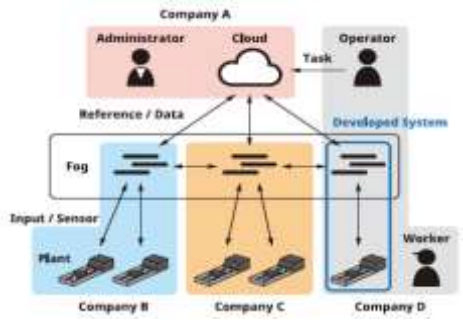


Fig. 1. Concept of the fog computing-based control system with the public cloud.

Architecture

This paper centers around fostering the mist registering based control framework inside the blue casing found in Fig. 1. Fig. 2 shows the organization design of the created framework. We utilize PCs for a mist processing climate and the interface between a controlled gadget and the organization. The PCs are associated with L2 switches, which thusly are associated with a L3 switch through an Ethernet link. Furthermore, according to the necessities of a legitimate organization, the two PCs are introduced in a similar VLAN.

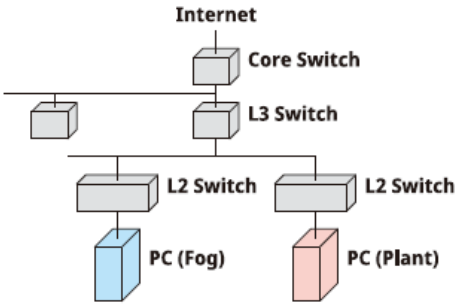


Fig. 2: Network architecture of the developed system.

Fig. 3 outlines the cooperation in the made system using the made C library. The plant-side PC obtains a current circumstance from the spinning encoder through the counter board and the servo speaker. Then, the plant-side PC changes over the current position, reference data, and controller states, which are twofold precision floating point data, into various exactness entire numbers by using Round. The changed over data are encoded by Enc, and they are transported off the murkiness side PC. The fog side PC picks a control commitment to ciphertext from the mixed data and encoded controller limits by using Mult. In addition,

the fog side PC returns the ciphertext of the control commitment to the plant-side PC. The plant-side PC unravels the ciphertext by using Dec+, and thereafter, inputs a request voltage into the servo intensifier through the D/A board. Note that Gen should be executed to get an essential pair before the recently referenced infrequent control measure, and the mixed controller limits should be set early.

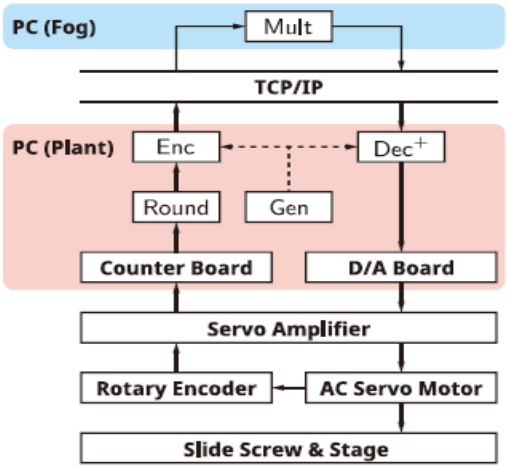


Fig. 3: Control flow of the developed system.

Implementation Modules

Worker:

User is the owner of data. Privacy, disaster recoverability, modification detection of user's data is ultimate goal of this project.

Fog server:

Fog server is trusted to user. User relies on fog server with his data. Close proximity of fog devices to the user, robust physical security, proper authentication, secure communication, intrusion detection ensures fog server's reliability to the user.

Cloud Server*:*

Cloud server is considered as *honestbutcurious*. This means that cloud server follows the Service Level Agreement (SLA) properly, but has an intention to analyze user's data. Conversely, cloud server may pretend to be good but acts as a potential adversary. In that case, cloud server may modify data in order to forge as original data. Similarly, cloud server may hide/loss the data resulting in permanent data loss of the user. Furthermore, hardware/software failure may result in data modification or permanent loss as well.

4. RESULTS

Fig.1:Homepage

Fig.2: Cloud home page

Fig.3:Company details

Fig.4:Worker details

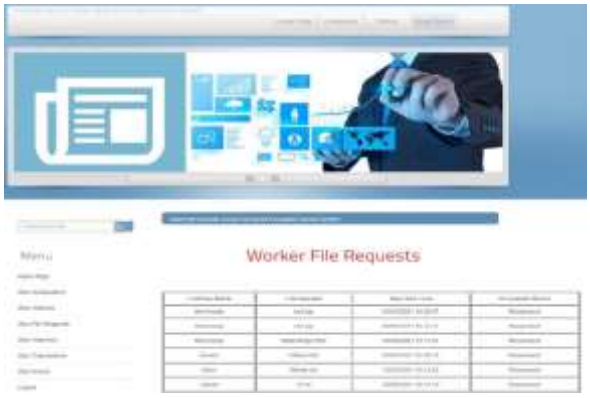


Fig.5: worker Request files

Fig.6: Attacker details

Fig.7: Transaction details

5. CONCLUSION

This project encourages an ensured fog figuring based control structure, which fills in as the fundamental execution of a mixed control system in a genuine current setting. The controller gain and signals are covered up against enemies. The made structure is hard to tuning in attacks and prevents zero components attacks. Thus, the controller encryption technique canbe used as another section of defend all around for mechanical control systems.

6.REFERENCES

[1] Y. Xia, “Cloud control systems,” IEEE/CAA J. AutomaticaSinica, vol. 2, no. 2, pp. 134–142, Apr. 2015.

[2] H. Esen, M. Adachi, D. Bernardini, A. Bemporad, D. Rost, and J. Knodel, “Control as a service (CaaS): Cloud-based software architecture for automotive control applications,” in Proc. Int. Workshop Swarm Edge Cloud, Seattle, WA, USA, 2015, pp. 13–18.

[3] A. Vick, V. Vonásek, R. Pˇeniˇcka, and J.Krüger, “Robot control as a service towards cloud-based motion planning and control for industrial robots,” in Proc. Int. Workshop Robot Motion Control, Poznan, Poland, 2015, pp. 33–39.

[4] G.Mohanarajah, R.D’Andrea, andM.Waibel, “Rapyuta:Acloud robotics platform,” IEEE Trans. Autom. Sci. Eng., vol. 12, no. 2, pp. 481–493, Apr. 2015.

[5] M. Waibel et al., “Roboearth,” IEEE Robot. Autom. Mag., vol. 18, no. 2, pp. 69–82, Jun. 2011.

[6] B. Kehoe, S. Patil, P. Abbeel, and K. Goldberg, “A survey of research on cloud robotics and

automation," IEEE Trans. Autom. Sci. Eng., vol. 12, no. 2, pp. 398–409, Apr. 2015.

[7] A. Botta,W. de Donato, V. Persico, and A. Pescape, "Integration of cloud computing and Internet of Things:Asurvey," Future Gener. Comput. Syst., vol. 56, pp. 684–700, 2016.

[8] M. S. Mahmoud and M. M. Hamdan, "Fundamental issues in networked control systems," IEEE/CAA J. Autom. Sinica, vol. 5, no. 5, pp. 902–922, 2018.

EARTHQUAKE PREDICTION USING RANDOM FOREST ALGORITHM AND BOOSTING METHOD

V.Gayatri [1]R.Vineesha[2] R.Sai Padmaja[3] Ch.Harshitha[4] K.Harshitha[5]
Associate Professor[1], UG Scholar[2, 3, 4, 5]
[1, 2, 3, 4, 5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

ABSTRACT

Earthquake rate is being increasing and that is leading to property loss, human deaths and also making people homeless. So, this study helps to forecast earthquake location before it occurs with the help of machine learning algorithm. By that the necessary precautions can be taken to save the properties and human lives. By considering the parameters like time, latitude, longitude, magnitude, depth and models like boosting and random forest regressor, the earthquake prediction will be done with a good accuracy.

KEYWORDS: Earthquake, Forecast, Machine Learning, Random Forest.

INTRODUCTION

Earthquakes association with structural damage and loss of life is one that keeps on enduring and thus the focal point of consideration for a many fields, say, seismological research and environmental engineering yet not limited to these. Its significance is stretched out to human life too, for to sustain and to survive. A prediction that can be accurate and relied on is a requisite for all the areas prone to disasters and as well as for locations that have less to none chances. It will get us ready for all the worst possible scenarios and for necessary measures as well that can be taken before hand to solve upcoming crisis.

As the technology is evolving and helping humans for a better and a convenient lifestyle, possibility at saving life is taken up with the help of efficient ML algorithm and data science to give accurate forecast. Machine Learning is a subset of Artificial Intelligence. It permits the system to adapt to a behavior of a particular kind based on its own learning and possess the ability to improve itself naturally solely from experience without any explicit programming, human mediation or help.

Initialization of a machine learning process starts with feeding an honest quality data-set to the algorithm(s), so as to build a ML prediction model. Algorithms perform knowledge discovery and statistical evaluation, determining patterns and trends in data. Selection of algorithms relies on data and on the task that requires automation. Target of project is foreseeing catastrophic events and improving the manner in which we react to them. Great forecasts and admonitions spare lives. A be aware of an drawing close calamity may be issued properly in advance of time because it will assist in lowering each loss of life incidence and structural loss. Machine gaining knowledge of algorithms assemble varieties of predictive models, Regression and Classification models. Each of them procedures records in a one of a kind way. Concerned gadget uses regression version whose center concept is forecasting a numerical value.

LITERATURE SURVEY

Roxane Mallouhy, Chady Abou Jaoude, Christophe Guyeux, and Abdallah Makhoul proposed a paper[1] on foremost earthquake occasion prediction the usage of numerous system gaining knowledge of algorithms withinside the Year 2019. At least primary classes of earthquake prediction exist: Short-time period predictions and forecast ones. Short time period earthquake predictions are made hours or days in advance, even as forecasts are expected months to years in advance. The majority of research are accomplished on forecast, considering the records of earthquakes in precise nations and areas. In this context, the middle concept of this paintings is to are expecting while an occasion is assessed as poor or wonderful main earthquake via way of means of making use of extraordinary system gaining knowledge of algorithms. Eight distinct algorithms were implemented on a actual earthquake dataset, namely: Random Forest, Naive Bayes, Logistic Regression, Multilayer Perceptron, AdaBoost, K-

nearest neighbors, Support Vector Machine, and Classification and Regression Trees.

Wanjiang Han, Yuanlin Gan, Shuwen Chen, and Xiaoxiang Wang proposed paper [2] on take a look at on earthquake prediction version on visitors catastrophe statistics with inside the yr 2020. This paper collects statistics at the harm to the visitors device resulting from earthquakes in China with inside the beyond decades, and makes use of KNN set of rules, SVM set of rules, logistic regression set of rules, naive Bayes set of rules and selection tree set of rules to teach the statistics, after which set up earthquake prediction models. The paper introduces the manner of preprocessing, modelling, evaluation, and visualization of catastrophe statistics. An earthquake disaster inversion model based on traffic data has been established, which can predict the earthquake intensity based on the relevant data provided by the traffic department.

The prediction accuracy is relatively accurate, which is very helpful for earthquake prediction and rescue operations. Yash Garg, Arpit Masih, and Utkarsh Sharma proposed a paper [3] on predicting bridge damage during earthquake using machine learning algorithms in the year 2021. The more the magnitude of the earthquake, the more is the damage. During an earthquake, the mobility of the smooth soil receives augmented and due to the fact maximum of the bridges are constructed on smooth soil, there are even greater possibilities of the bridge behaving like a deliver with inside the sea.The balance of the bridges is the maximum vital undertaking to keep away from all disasters. Many bridges disintegrate at some stage in earthquake due to the fact their mobility and sustainability can't stand the importance of the earthquake. In this paper, the technique proposed to are expecting whether or not a bridge will preserve harm or now no longer after an earthquake through the use of elements like importance of the earthquake, distance to epicenter of the bridge, bridge type, fabric used to make bridge and plenty of greater, the use of many type algorithms like Logistic Regression, Decision Tree, Random Forest, XGBoost, and KNN.

A.Shameem Ansar and S.Sudha proposed a paper on Prediction of earthquake triggered the use of deep mastering fashions with inside the 12 months 2020. Earthquakes are one of the main elements of a landslide.

Over the beyond ten years, damages resulting from earthquakes in human settlements are discovered to be increasing. Recently, landslide prediction the usage of Radial Basis Function of Support Vector Machine with an accuracy of 91.2% is reported. With landslide prediction probability, there are possibilities: a landslide prevalence or non-prevalence. In both cases, the prediction might be accurate or fake. In the primary case, fake prediction ought to bring about lack of human existence and property, even as accurate prediction is valuable. But with inside the latter case, fake prediction may want to cause human stress & strain, luxurious catastrophe prevention measures and so on, whilst accurate prediction is appreciable. Hence, to decrease losses it's miles important to expect the landslide accurately. With this intention, prediction algorithms with excessive accuracy are developed. Landslide prediction the usage of device gaining knowledge of strategies consisting of Naive Bayes, Logistic Regression, Support Vector Method, and Random-wooded area are proposed.

The accuracy suggested with the aid of using those strategies is low and so prediction the usage of deep gaining knowledge of strategies consisting of Convolutional Neural Network and Recurrent Neural Network is attempted. Performance measures of these methods are evaluated using the three pillars of binary classification namely accuracy, precision and recall.

Risul Islam Rasel, Nasrin Sultana, G.M.Azharul Islam, Mahfuzul Islam, and Phayung Meesad proposed a paper [5] on Spatio-Temporal Seismic Data Analysis for Predicting Earthquake in the year 2019. Earthquake prediction concerns specifying the earthquake's occurrence time, location, latitude, longitude, and intensity level. The determination of factors for the next earthquake happening in a region is very hard, almost impossible because earthquake occurrence depends on many things, such as changes in global warming, underground seismic wave, underground explosions, and underground rocks colliding, etc.

But, nowadays, many types of research have been done around the world to build an earthquake warning system which upon detection of an earthquake provides a real- time warning to the neighbouring regions that might be affected. In this study, only the Spatio-temporal seismic data of Bangladesh is analyzed to propose an earthquake prediction model using the probabilistic assumption of the next earthquake happening in and around the Bangladesh region. The experimental dataset contains 100 years of a historical earthquake happening records in and around Bangladesh from the year 1918 to 2018 and this data is collected from Bangladesh Meteorological Department's (BMD) climate division.

PROPOSED WORK

In this project, the proposed work is implemented as per the following steps. **Step-1:** Removing the unneccessary data from dataset.

The required data fields of project are: latitude,longitude,time,magnitude and depth.

Step-2: Divide dataset into two subsets Which are training set and testing set.

Step-3: By using random forest regression and boosting algorithms the dataset will be executed with accuracy of 87%.

Random Forest Regression

A Random Forest is an ensemble method able to acting each regression and class duties with the usage of more than one choice bushes and a way referred to as bootstrap and aggregation, normally referred to as bagging. The fundamental concept at the back of that is to mix more than one choice bushes in figuring out the very last output as opposed to counting on man or woman choice bushes. Random Forest has more than one choice bushes as base studying models.

We randomly carry out row sampling and characteristic sampling from the dataset forming sample .Datasets for each model. This component is referred to as Bootstrap. A Random Forest operates through building numerous choice timber at some stage in education time and outputting the suggest of the instructions because the prediction of all of the timber.

BOOSTING: Theterm"boosting" is used to describe a family of algorithms which are able training the Random Forest Regression model on the whole dataset convert weak models to strong models. Boosting incrementally builds an ensemble by training each model with the same dataset but where the weights of instances are adjusted according to the error of the last prediction.

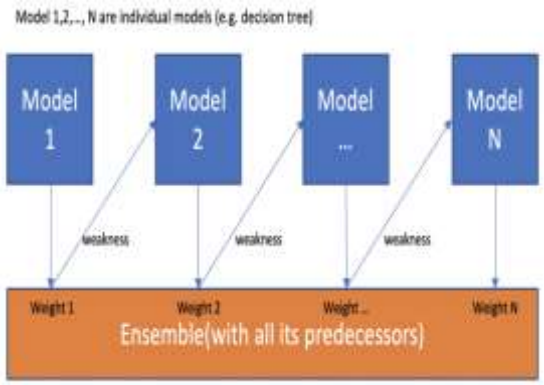
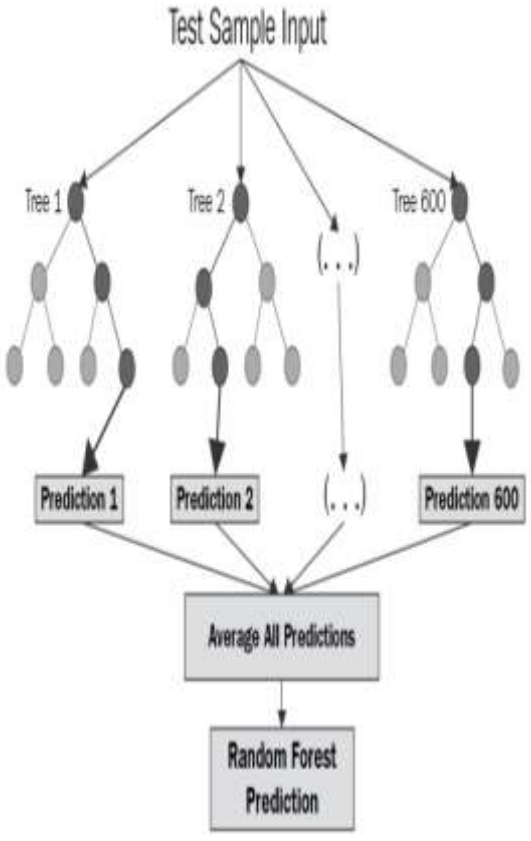
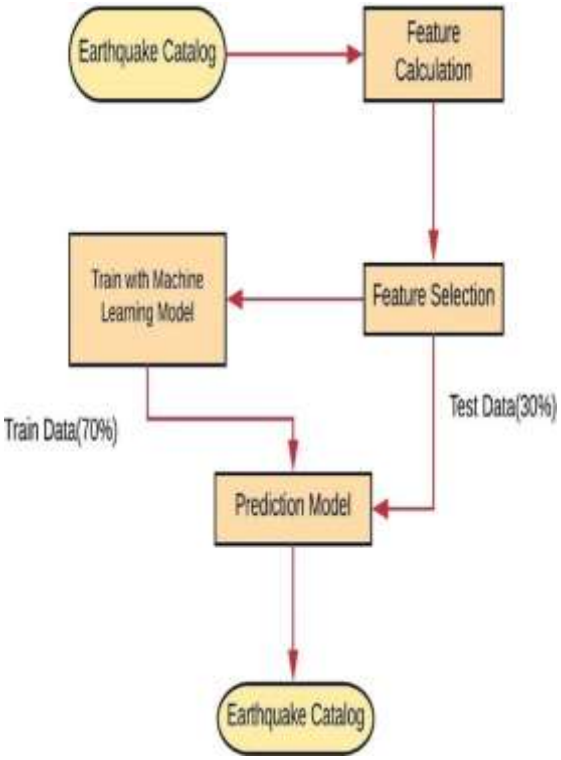


Fig 1: Random-Forest

METHODOLOGY





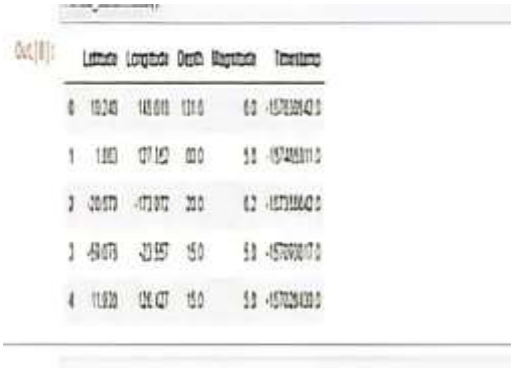


Fig 2: Boosting

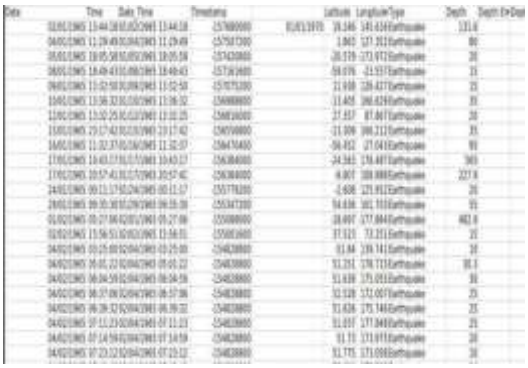


Fig 3 : Work flow

The dataset used in this study has been taken from the year 1965 to 2016 which consists of 23412 samples. The dataset has been divided into training set and testing test. From the whole data,80% will be considered for training purpose and 20% will be considered for testing purpose.

Fig 4: Dataset

Models like random forest regressor and boosting are used in this prediction.

RANDOM FOREST REGRESSION IMPLEMENTATION:

• Initially, import the libraries and dataset.

• Identify dependent and independent variables.

• Split the dataset into the Training set and Test set.

• Training the Random Forest Regression model on the whole dataset.

• Predicting the Test set results.

RESULTS

In this study, earthquakes are predicted with the help of random forest and boosting algorithms.

Fig 5: Data fields

Initially,the required data fields will be taken and unncessary data will be omitted from dataset. On this data ,the algorithms will be implemented and visualize it in the form of a pictorial representation of the affected areas with the help of matplot library.

In the below picture, the blue dots represent the earthquake prone areas in the map.

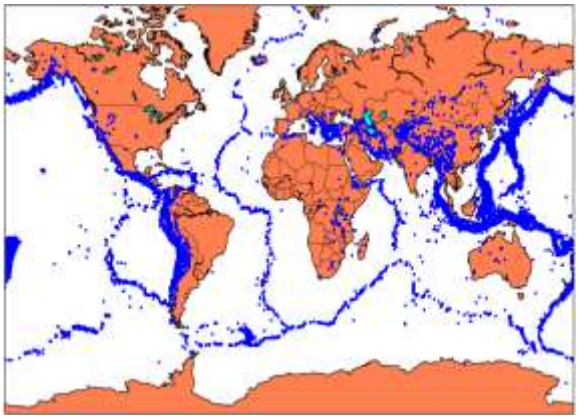


Fig 6: Data Visualization

Finally, by using the random forest regressor and boosting algorithm, accuracy of 87% is achieved to predict earthquakes.

CONCLUSION

The integration of seismic activity with machine learning technology yields efficient,significant result and can be used to predict earthquakes widely, here the usage of boosting and random forest regressor models is to predict the earthquakes in future which leads to the accuracy of 87% . Therefore, it improves the accuracy when compared the other works of prediction.

REFERENCES

[1] Wenrui Li, Nishitha Narvekar, Nakshatra Nakshatra, Nishitha Raut, Birsen Sirkeci, and Jerry Gao "Seismic Data Classification Using Machine Learning"2018.

[2] Roxane Mallouhy, Chady Abou Jaoude, Christophe Guyeux, and Abdallah Makhoul "Major Earthquake event Prediction using various machine learning algorithms" 2019.

[3] Risul Islam Rasel, Nasrin Sultana, G.M.Azharul Islam, Mahfuzul Islam, and Phayung Meesad "Spatio-Temporal Seismic Data Analysis for Predicting Earthquake: Bangladesh Perspective"2019.

[4] Anmol Gaba, Arnab Jana, Rahul Subramaniam, Yash Agrawal, and Merin Meleet "Analysis and Prediction of Earthquake Impact-a Machine Learning approach" 2019.

[5]Mario Maya and Wen Yu "Short-term prediction of the earthquake through Neural Networks and Meta-Learning 2019**.**

[6]Kuldeep Chaurasia, Samiksha Kanse, Aishwarya Yewale, Vivek Kumar Singh, Bhavnish Sharma and B.R.Dattu "Predicting Damage to Buildings Caused by Earthquakes Using Machine Learning Techniques" 2019.

[7]Wanjiang Han, Yuanlin Gan, Shuwen Chen, and Xiaoxiang Wang "Study on Earthquake Prediction Model Based on Traffic Disaster Data" 2020.

[8]Shameem Ansar.A and S.Sudha "Prediction of Earthquake Induced Landslide Using Deep Learning Models" 2020.

[9] Md. S AI Banna, Kazi Abu Taher, M.Shamim Kaiser, Mufti Mahmud, Md.Sazzadur Rahman, A.s.m. Sanwar Hosen, and Gi Hwan Cho "Application on Artificial Intelligence in Predicting Earthquakes: State-of-the-art and Future Challenges" 2020.

[10] Yash Garg, Arpit Masih, and Utkarsh Sharma" Predicting Bridge Damage during Earthquake Using Machine Learning Algorithms" 2021.

Bitcoin Price Prediction Using Machine Learning Techniques

T. Prasanth1 O. Sujay Kumar2 N. Varshith Kumar 3 G. Mahesh 4SK. Wajid5
Associate Professor1, UG Scholar2, 3, 4, 5
1, 2, 3, 4, 5 Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh.

Abstract— Crypto currencies are one of the forms of digital currencies which operates on a blockchain database, and they resemble stock market. The stock market is influenced by many risky factors. crypto currencies also involve many factors as like the stock market. Bitcoin is a variant of crypto currency and the bitcoin market is volatile because its pricing trends do not follow any consistency. Even considering all its cons there is a lot of potential in the future of bitcoin. Bitcoin is an investment opportunity like stock market but investors are encountering difficulties while investing because of its volatile nature, so in this project we aim to predict the price of bitcoin using different machine learning algorithms. The collection of algorithms varies from less complex linear regression to more complex LSTM neural networks along with historical price of bitcoin dataset which consists of 9 features and recorded over the last

9 years on daily basis. The predicted price trends will help investors to make decisions while investing on bitcoin.

Keywords:

Crypto Currency, Stock Market, Block Chain, LSTM

1.INTRODUCTION

Day by day the exponential growth of internet users along with the data they have to deal with triggers to emerging new technologies. Crypto currency is one of such technologies where digital currency is used instead of conventional currency. within short span-new variants of crypto currencies are started to emerge, one of such a kind is the Bitcoin where its existence dated back to 2009 by Satoshi Nakamoto. Bitcoin is a decentralized digital currency where it uses block chain data base for transactions. In a centralized currency system, everything is controlled by government but in case of bitcoin no one holds the power to control. It is a digital currency that was created in January 2009 which offers the promise of lower transaction fees than traditional online payment mechanisms and, unlike government-issued currencies, it is operated by a decentralized authority. The unique thing about bitcoin is its price will change daily because of the factors like political, economic and interest of the bitcoin miners in local and global level. Bitcoin price has recorded a new all-time high in 2021which is

65,000 USD. we can able to draw a close resemblance with stock market to bitcoin market. The research done to predict the stock price have been going on for decades, but most prediction models fail to predict the stock price precisely because of more features, sources and signal to noise ratio. The common approach for this problem is to use machine learning algorithms and to train them on historical stock price data set. Due to the close resemblance of bitcoin with stock price the machine learning models can be used to predict the price of bitcoin. Machine learning models include less complex linear regression, polynomial regression, random forest etc.; along with more complex neural networks like LSTM can be used.in predicting the prices of complex data like stock price and bitcoin price LSTM is the widely popular model, LSTM is defined as long short-term memory where LSTMs are explicitly designed to avoid the long-term dependency problem. Remembering the certain information for long periods of time is practically their behavior in default, not something they are struggling to learn! Recurrent neural networks will be in the form of a chain of repeating modules of a neural network. In standard RNNs, the repeating module will have a structure which is very simple, such as single tanh layer. The pricing of bitcoin will depend on demand and supply, there are limited number of bitcoins existed in the market. If the demand for the bitcoin is more the price of bitcoin will raise because of limited nature the demand for bitcoin will increase if the investors prefer to buy bitcoin, the buyers use the bitcoin for various commercial

purposes which will also increases the usage of bitcoin This ultimately results in scaling of bitcoin usage in many applications. The above things are possible with bitcoin price prediction.

2. LITERATURE SURVEY History of bitcoin

It is a digital currency that was created in January 2009 which offers the promise of lower transaction fees than traditional online payment currencies, it is operated by a decentralized authority. The bitcoin system is a collection of computers that all run bitcoin's code and store its block chain. A block chain is a thought of as a collection of blocks. In each block is a collection of transactions. Because all the computers running the block chain has the same list of blocks and transactions, and can transparently see these new blocks being filled with new bitcoin transactions, no one can cheat the system. Bitcoin is existed in the market as a form of digital currency since 2009, in recent times the bitcoin got all the attention it deserves from both investors and miners.it results a surge in bitcoin price to a new all-time high.it may grab the attention of investors, but the market of bitcoin in volatile and uncertain to maintain a consistency in its price .it will remain as an obstacle not only for investment. Also, for the future of digital currency, it halts the progress of integration of digital currency to other applications which turn the attention away from public. The above problem can be addressed with bitcoin price prediction.

Bitcoin price prediction methods

There are many methods that are used to predict the price of bitcoin, in [7] authors discussed the approach to predict bitcoin price using multivariate linear regression in these methods they had predicted the highest and lowest prices of cryptocurrencies in this model they have used multiple independent variables to predict the dependent variables in the data set.

In [15] the authors have used Bayesian regression for Latent source model to predict bitcoin price and they have proposed a strategy to for trading bitcoin which can doubles the investment in less than 60 days.

The Bitcoin price market closely resembles with Stock market so the references for price prediction approach of bitcoin can be drawn from stock market prediction models In[16] the authors have used the LSTM network to predict the future price of stock market using historic price data and they achieved 55 percent average accuracy many price prediction models of bitcoin uses references from stock market price prediction models because of similar nature like volatility ,resemblance of features in data set, inconsistencies, noise.

In [1] the authors have used LSTM cells to predict bitcoin price and achieved the RMSE vale 288 in their prediction.

3. PROPOSED SYSTEM

Approach

The ml algorithms which are used to predict fewer complex data like linear, polynomial, Bayesian regressions and SVM, random forest, ARIMA algorithms along with more complex neural networks like LSTM (long short-term memory) which are relatively better at predicting complex data are used. We want to test the efficiency of ml algorithms for prediction even we are aware of the fact that LSTMs are best to do the job.

$$\tilde{c}_t = tanh(w_c[h_{t-1}, x_t] + b_c)$$
$$c_t = f_t * c_{t-1} + i_t * \tilde{c}_t$$
$$h_t = o_t * tanh(c^t)$$

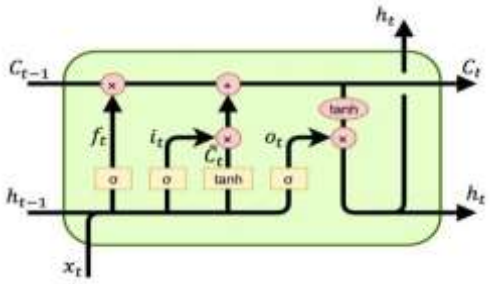
Where ct represents cell state at time stamp t,c~ represents candidate for cell state at time stamp ,ht indicate final output. In this project different variants of LSTM cells are used to attain the best result they are single layer LSTM with single feature, multiple features as an input and Two-layer LSTM with single feature as an input and LSTM GRU model with single feature as an input.

About GRU

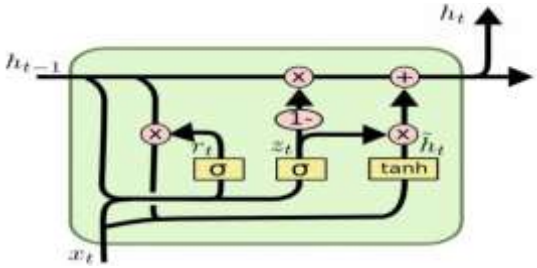
GRU is related to LSTM as both are utilizing a different way in gating information to prevent vanishing gradient problem. The GRU controls the flow of information like the LSTM without using a memory unit. It exposes the full hidden content without any control. GRU is relatively

new, and from my perspective, the performance is on par with LSTM, but computationally more efficient. GRU is easier to modify because of less complex nature than LSTM which grant more freedom for tweaking to achieve performance gains

h_t , C_t indicates hidden layer vectors, x_t for input vector, b_f , b_i , b_c , b_o for bias



vector, W_f , W_i , W_c , W_o for parameter matrices. , $\tanh$ for activation functions.



h_t indicates hidden layer vectors., for input vector, b_z , b_r , b_h : bias vector. W_z , W_r , W_h : parameter matrices, , $\tanh$: activation functions.

The below block diagram indicates the steps involved in the Prediction model.

Data set description

For the price prediction we have used historical data set of bitcoin ranges from 2012-2020, available in Kaggle.com which is an extracted data from coinmarketcap.com. The size of this dataset is 292MB and has historical price of Bitcoin. The dataset consists of 4727777 rows and

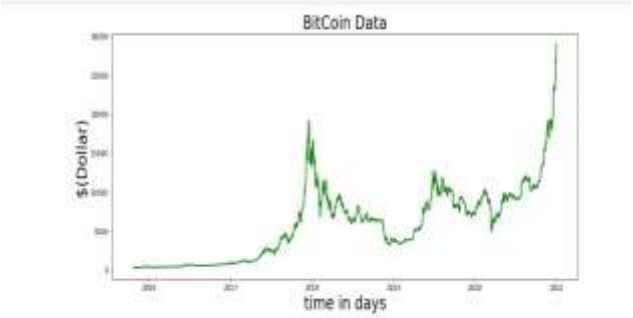
8 columns. each column represents a feature of the bitcoin dataset like Time stamp, High, Low, Open, Close, Volume (BTC), Volume (Currency), Weighted price. The purpose of choosing this dataset is to study the trends of bitcoin price.

Out[2]:

	Timestamp	Open	High	Low	Close	Volume_(BTC)	Volume_(Currency)	Weighted_Price
4727767	1609372260	28836.97	28848.97	28807.76	28826.52	2.051917	59173.965272	28838.379450
4727768	1609372320	28825.49	28844.25	28816.09	28816.09	0.172410	2980.457100	28837.207539
4727769	1609372380	28814.36	28822.71	28800.80	28808.00	1.529671	44079.572351	28814.411845
4727770	1609372440	28808.08	28832.79	28800.00	28831.35	2.036450	58675.679644	28812.732950
4727771	1609372500	28806.07	28825.58	28800.11	28810.08	0.667591	2517.799882	28810.597267
4727772	1609372560	28801.47	28829.42	28795.64	28829.42	0.995227	27804.572129	28806.429798
4727773	1609372620	28829.42	28863.98	28829.42	28857.06	2.398821	69332.350629	28846.441863
4727774	1609372680	28858.49	28900.52	28850.49	28862.82	2.466598	71232.784464	28879.855326
4727775	1609372740	28910.54	28911.52	28867.80	28881.30	7.332773	211870.912860	28893.695821
4727776	1609372800	28893.21	28928.48	28893.21	28928.48	5.757679	166448.788123	28908.166861

Experimental result

The entire data in the dataset is pre-processed to fill the missing data using mean. After the pre-processing step the trend of the bitcoin price is plotted. The below figure shows x_t the actual trends of the bitcoin price after loading the dataset to the machine learning models. σ



For those ml algorithms which are used in this experiment i.e., Linear, Polynomial, Bayesian regressions along with Random Forest, SVM, Arima and for single layer LSTM neural network the entire data set is split into 80-20 ratio for

training and testing, and the entire data in the dataset is used for the experiment for two-layer LSTM and GRU neural networks only small chunk of data is to be used for training and testing rather than using entire data in the dataset like above ml algorithms for better results. We want to train our model on the data from January 1, 2016 until August 21, 2017 and to test the model on the data from August 21, 2017 until October 20,

2017.For all the algorithms except LSTM single layer multi feature Date is the independent feature that is used as an input to predict dependent feature that is weighted price. For measuring the result RMSE (root mean square error) is used as a metric, RMSE is calculated as the square root of the mean of the squared differences betweenactual outcomes and predictions. Squaring each error forces in which the values need to be positive and the square root of the mean squared error returns the error metric back to original units for comparison. The smaller RMSE value indicate the better performance of the algorithm.

Testing

To ensure the values to be more accurate we performed testing on various scenarios before finalizing the results. For ml algorithms we have used different segments of dataset for training and testing to search for the best result, for neural networks we have combined the parameters like epoch and cell count of the algorithm along with different segment of dataset to get the best result. Based on the below table the GRU model with EPOC value-50 and cell count of 256.

CELL	EPOCH	RMSE
256	50	116
256	100	145
256	200	191
256	300	132
256	400	152
256	500	175

The below figure shows the result from the prediction using GRU neural network with epoch

50 and 256 cells which combination have least RMSE value of all the algorithms, from the above graph actual price indicates the data present in the data set and the predicted price indicates the predicted price using the algorithm.

4. CONCLUSION

With the vision for the future of digital currency in mind, we aim to present an insight into the trends of the bitcoin prices, being an inconsistent and volatile market(cryptocurrency) by predicting bitcoin prices .With limited literature availability of bitcoin price prediction using machine learning we presented a wide variety of machine learning algorithms for price prediction with their efficiencies, with this the investors in bitcoin market can able to get an idea on the trends of bitcoin pricing for the next few days and they can able to make a decision on their investments.Finally we conclude that LSTM GRU model has given the best accuracy which is better than the previous models with RMSE value of 116.

5. REFERENCES

[1] Ferdiansyah, siti hajar othman, Deris Staiwan "A LSTM-Method for Bitcoin Price Prediction: A Case Study Yahoo Finance Stock Market" Universitas Bina Darma, Indonesia and University Teknologi, Malaysia.

[2] S. Hochreiter and J. Schmidhuber, "Long

short-term memory," Neural Comput., vol. 9, no.

8, pp. 1735– 1780, 1997.

[3] A. Judmayer, N. Stifter, K. Krombholz, and E. Weippl- "Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms," Synth. Lect. Inf. Secur. Privacy, Trust, 2017.

[4] S. Nakamoto and others, "Bitcoin: A peer-to-peerelectronic cash system," 2008.

[5] H. Jang and J. Lee on "An Empirical Study on Modeling and Prediction of Bitcoin Prices With Bayesian Neural Networks Based on the given Blockchain Information," IEEE ACCESS, 2018.

[6] J. Brownlee, “Time series prediction with lstm recurrent neural networks in python with keras,” Available Mach. com, p. 18, 2016.

[7] R. Mittal, S. Arora, and M. P. S. Bhatia on “Automated Cryptocurrencies Prices Prediction By Using Machine Learning,” 2018.

[8] F. Reid and M. Harrigan, “An Analysis of Anonymity in the Bitcoin System”, Proceedings of IEEE International Conference on Privacy, Security, Risk, and Trust, pp. 13181326, 2013.

[9] J. B. Heaton, N. G. Polson, and J. H. Witte, “Deep learning in finance,” CoRR, vol. abs/1602.06561, 2016. [Online]. Available: http://arxiv.org/abs/1602.06561

[10] K. Chen, Y. Zhou, and F. Dai on “A lstm-based method for stock returns prediction: A case study of china stock market,” in Big Data (Big Data), 2015 IEEE International Conference on, Oct 2015, pp. 2823–2824.

[11] O. H. Luca Di Persio on “Artificial neural networks approach to the forecast of stock market price movements,” nternational Journal of Economics and Management Systems, vol. 1, pp.158–162, 2016.

BREAST CANCER DIAGNOSIS USING MACHINE LEARNING TECHNIQUES

T. Prasanth[1],G.Bharathi[2],K.Lalitha Hansika[3], MD.Anees Sultana[4], D.keerthana[5]
Assistant Professor[1], UG Scholar[2, 3, 4, 5]
[1, 2,3,4,5]Department of Computer Science and Engineering
Geethanjali Institute of Science and Technology,Nellore,
Andhra Pradesh.

ABSTRACT–A tumor that arises in the tissues of the breast is known as Breast cancer. Most of the women are found to be cancerous and it is a reason for large number of death cases in women around the world. In this paper, relative analysis of machine learning techniques are proposed for the prediction of breast cancer. A lot of researchers have been done research on breast cancer diagnoses and prognoses, where accuracy rate varies for different situations, tools and datasets being used in each technique. Our main aim is to relatively analyze different existing machine learning techniques such asSupport Vector Machine, Logistic Regression, K-Nearest Neighbor and Naïve Bayes in search of most appropriate model, which is used to hold up the large dataset with good precision of prediction. Our key purpose of this analysis is to study all the earlier researches that are being used for prediction of breast cancer on machine learning algorithms.

KEYWORDS:
Breast Cancer, Prediction, Tumor, Relatively Analyze, Tissues, Machine Learning Techniques

1.INTRODUCTION

In this present era, breast cancer is one of the most poisonous and wide-ranging disease that causes death in massive number of women around the world. Where it is the second largest disease which is leading cause of women death [1]. There areseveral machine learning [2] algorithms that are being used for breast cancer prediction. Our aim is to find out the most preferable and appropriate algorithm for the prediction of breast cancer. Breast cancer is initiated through malignant tumors, and it occurs when rapid increase in growth of cell got out of control [3]. The abnormal growth of fatty and fibrous tissues in breast, that becomes the cause of breast cancer. The tumors are spreaded by cancer cells that leads to cause different types of cancer. The different types of breast cancer [4] arises when affected cells and tissues spread throughout the body. The first type of breast cancer is Ductal Carcinoma In Situ (DCIS)that usually occurs when abnormal cells spread outside the breast and it is recognized as the Non-Invasive cancer [5]. Invasive Ductal Carcinoma (IDC) [6] is the second type of breast cancer and is also recognized as Infiltrative Ductal Carcinoma [7]. When the abnormal cells spread out all over the breast tissues, this type of cancer occurs and IDC cancer is generally found in men [8]. The third type of breast cancer is Mixed Tumor Breast Cancer (MTBC)which is also recognized as Invasive Mammary Breast Cancer [10]. Abnormal duct cell and lobular cell causes such kind of cancer [10]. Lobular Breast Cancer (LBC) [11] isfourth type of cancer which occurs inner side of the lobule and increases the possibility of other invasive cancers. Fifth type of breast cancer is Mucinous Breast Cancer (MBC) [12] that arises because of invasive ductal cells, it is also recognized as Colloid Breast Cancer. It emerge when the abnormal tissues spread all over the duct [13]. Last type of cancer is Inflammatory Breast Cancer (IBC) that causes bump and reddening of breast. This type of cancer starts to appear, whenthe lymph vessels block in break cell as it is a fast growing breast cancer [14].

2. LITERATURE SURVEY

Y.Khourdifi and M. Bahaj presented a paper [2]in the year 2018, on“Applying optimum machine learning algorithms for breast cancer classification and prediction”. The main goal of this study is to predict breast cancer, where it is the second largest disease which is leading cause of women death, and with prior detection and prevention can decrease the risk of death dramatically, using more than a few machine-learning algorithms.

F.K. Ahmad and N.Yusoffpresented a paper [4]in the year 2013, on“Breast cancer types are put in

order based on fine needle aspiration biopsy data using random forest classifier".Random forest is a classifier built based on the grouping of decision trees and has been known to perform well in comparison to other machine learning techniques.

Y. Lu, J. Y. Li, Y. T. Su, and A. A. Liu presented a paper [3]in the year 2018, on"A review for detecting breast cancer in medical images". In this paper, we make known about some commonly used medical imaging methods for breast cancer diagnosis, and based on them we examine some newly proposed approaches for detection of breast cancer with computer vision and machine learning techniques. In conclusion, we compare and analyze the performance of detection for different methods on histological images and mammograph images respectively.

D. Delen presented a paper [15] in the year 2009,on"Analysis of cancer data: a data mining approach".In this study, they used three well liked data mining techniques (decision trees, artificial neural networks and support vector machines) along with that most commonly used statistical analysis technique logistic regression to develop prediction models for prostate cancer survivability.

3. PROPOSED SYSTEM

In this proposed system we designed a model for the prediction of unseen data which gives the good expected result in both the training and testing steps. Generally machine learning process consist of three main strategies such as pre-processing, features selection or extraction and classification. The core part is feature extraction in machine learning process and actually helps in the prediction of cancer. The proposed learning schemes improve the performance. It will predict cancer accurately.

Implementing Modules

Load Dataset : In this stage, we load the dataset into program and data is extracted from.csv file. This data can be analyzed and best features are extracted to preprocess the data.

Preprocessing : In this stage ,for the given data set, there are quite a few 'NA' values which are filtered in python. Moreover, as the data set consists of numeric data, we use robust scaling, which is quite similar to normalization, but it instead uses the inter quartile range whereas normalization is something which normalization shrinks the data in terms of 0 to 1.

Split Dataset : After pre-processing stage, the given dataset can be separated into two parts in 80, 20 ratio. The first part is called training part and second part is called test part. The training part of the data is used to train the classifier that we are used implement in this project, and the test part of data is used to verify the prediction accuracy of the used classifiers.

Graphical Analysis : In this stage of the Implementation user can get the clear picture analysis of the breast cancer issues. Various factors take into consideration for the graph analysis, plot the charts like pie graph, bar chart and so others.

Implementing Algorithms

In this proposed system we have used Support Vector Machine algorithm, Logistic Regression algorithm, K-Nearest Neighbor algorithm and Naive Bayes algorithm, through which we acquired maximum 96% accuracy in the prediction of breast cancer detection.

The system architecture diagram is shown as below:

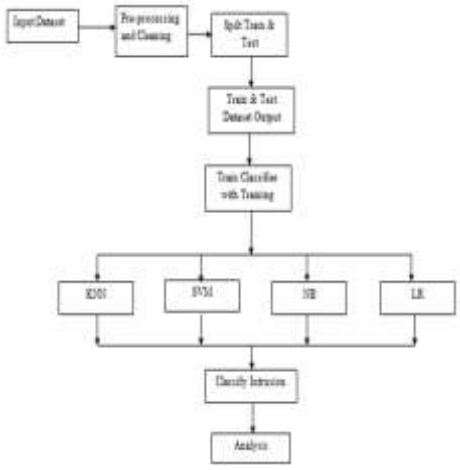


Figure 1: System Architecture Diagram

Support Vector Machine (SVM) is one of the popular Supervised Learning algorithm. It is used for Classification problems in Machine Learning. SVM algorithm creates the best line which can

usually separates n- dimensional space into classes so that the new data point is easily categorized in future. This best decision boundary is so-called a hyper plane. By using Support Vector Machine algorithm, we got 0.94 of accuracy.Logistic Regression is also one of the popular Machine Learning algorithm, which is based on the Supervised Learning technique. Logistic regression estimates the output of a categorical dependent variable.By using Logistic Regression algorithm, we obtained0.96 of accuracy .K-Nearest Neighbor (KNN) algorithm stores all the available data and sorts a new data point based on the resemblance. By this K- NN algorithm when ever new data emerge it is easy to classify into a well suite category.By using K-Nearest Neighbor algorithm, we obtained 0.94 of accuracy.Naïve Bayes is a supervised learning algorithm, which is based on Bayes theorem and used for answering the classification problems. Naïve Bayes is a probabilistic classifier such that it predicts on the basis of the probability of an entity. By using Naïve Bayes algorithm, we obtained 0.94 of accuracy.

4. RESULTS

1. Predicting breast cancer diagnosis using Support Vector Machine algorithm results are shown below:

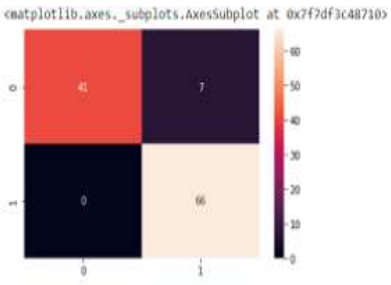


Figure 2: By Using Support Vector Machine Algorithm

2. Predicting breast cancer diagnosis using Logistic Regression algorithm results are shown below:

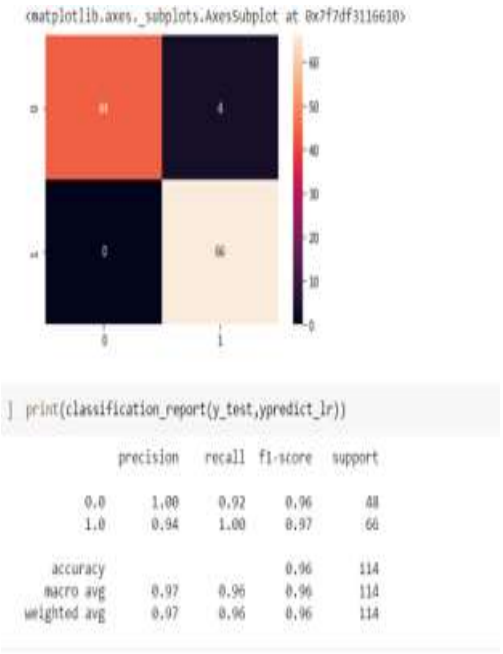


Figure 3: By Using Logistic Regression Algorithm

3. Predicting breast cancer diagnosisusing K-Nearest Neighboralgorithm results are shown below:

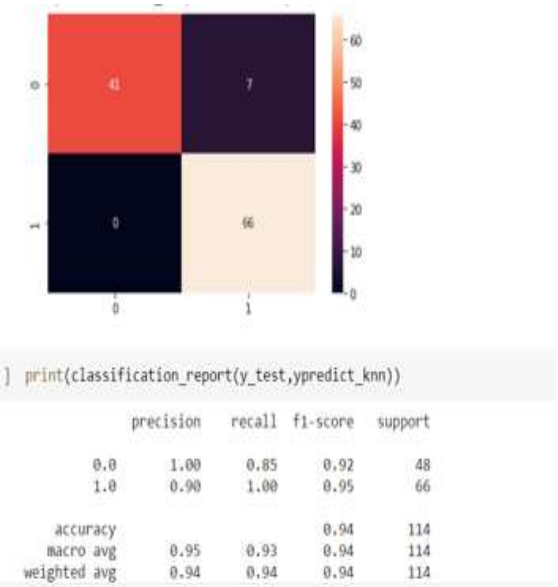


Figure 4: By Using K- Nearest NeighborAlgorithm

4. Predicting breast cancer diagnosisusing Naive Bayes algorithm results are shown below:

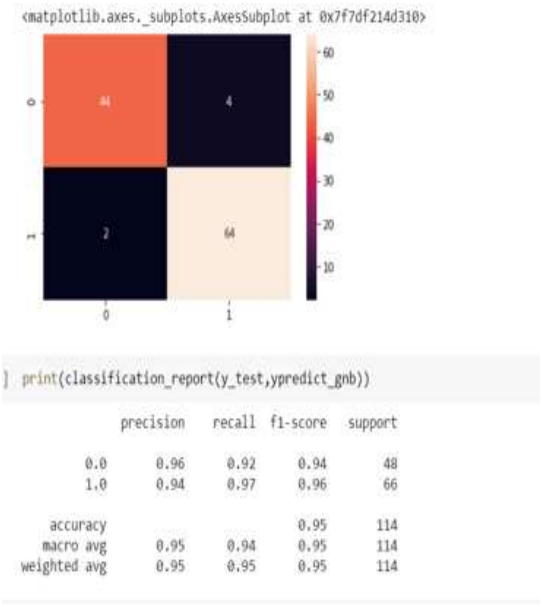


Figure 5: By Using Naive Bayes Algorithm

Algorithm	Accurate Value
Support Vector Machine	0.94
Logistic Regression	0.96
K-Nearest Neighbor	0.94
Naïve Bayes	0.95

5.CONCLUSION

In this paper we have studied different machine learning algorithms for breast cancer prediction. Our main attention is to treasure out the most appropriate algorithm that can estimate the occurrences of breast cancer in effective manner. The main resolution of this review is to highpoint all the earlier studies of machine learning algorithms that are being used for breast cancer estimations. The study of this paper is started from the types of breast cancer, studied papers have been reread to get some important information about the major types, signs and cause of breast cancer.The results obtained show that Logistic Regression has better accuracy with 96% than remaining algorithms in predicting breast cancer.

6.REFERENCES

[1] Y.-S. Sun et al., "Risk factors and preventions of breast cancer," International journal of biological sciences, vol. 13, no. 11, p. 1387, 2017.

[2] Y. Khourdifi and M. Bahaj, "Applying best machine learning algorithms for prediction and classification of breast cancer," in 2018 International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS), pp. 1–5, IEEE.

[3] Y. Lu, J. Y. Li, Y. T. Su, and A. A. Liu, "A review of breast cancer detection in medical images," in 2018 IEEE Visual Communications and Image Processing (VCIP), pp. 1–4, IEEE.

[4] F. K. Ahmad and N. Yusoff, "Classifying breast cancer types based on fine needle aspiration biopsy data using random forest classifier," in 2013 13th International Conference on Intellient Systems Design and Applications, pp. 121–125, IEEE.

[5] R. Hou et al., "Prediction of upstaged ductal carcinoma in situ using forced labeling and domain adaptation," IEEE Transactions on Biomedical Engineering, 2019.

[6] A. R. Chaudhury, R. Iyer, K. K. Iychettira, and A. Sreedevi, "Diagnosis of invasive ductal carcinoma using image processing techniques," in 2011 International Conference on Image Information Processing, pp. 1–6, IEEE.

[7] S. Pervez and H. Khan, "Infiltrating ductal carcinoma breast with central necrosis closely mimicking ductal carcinoma in situ (comedo type): a case series," Journal of medical case reports, vol. 1, no. 1, p. 83, 2007.

[8] D. L. Page, W. D. Dupont, L. W. Rogers, and M. Landenberger, "Intraductal carcinoma of the breast: follow up after biopsy only," MDPI Cancers, vol. 49, no. 4, pp. 751–758, 1982.

[9] A. B. Tuck, F. P. O'Malley, H. Singhal, and K. S. Tonkin, "Osteopontin and p53 expression are associated with tumor progression in a case of synchronous, bilateral, invasive mammary carcinomas," Archives of pathology and laboratory medicine, vol. 121, no. 6, p. 578, 1997.

[10]B. Lee et al., "Efficacy of the multidisciplinary

tumor board conference in gynecologic oncology: a prospective study," Medicine, vol. 96, no. 48, 2017.

[11] S. Masciari et al., "Germline e-cadherin mutations in familial lobular breast cancer," Journal of medical genetics, vol. 44, no. 11, pp. 726–731, 2007.

[12] A. Memis et al., "Mucinous (colloid) breast cancer: mammographic and us features with histologic correlation," European journal of radiology, vol. 35, no. 1, pp. 39–43, 2000.

[13] A. Gradilone et al., "Circulating tumorcells (ctcs) in metastatic breast cancer (mbc): prognosis, drug resistance and phenotypic characterization," Annals of Oncology, vol. 22, no. 1, pp. 86–92, 2010.

[14] F. M. Robertson et al., "Inflammatorybreast cancer: the disease, the biology, the treatment," CA: a cancer journal for clinicians, vol. 60, no. 6, pp. 351–375, 2010.

[15] D. Delen, "Analysis of cancer data: a data mining approach," Expert Systems, vol. 26, no. 1, pp. 100–112, 2009.

IMAGE DEHAZING ALGORITHM USING DARK CHANNEL PRIOR AND MORPHOLOGICAL RECONSTRUCTION

Lavanya.B, B. Suresh Babu, Indu. B, Krishna Sree Bhavya. N , Naveen Kumar. K
Department Of ECE, Srinivasa Ramanujan Institute Of Technology,
Rotarypuram, Ananthapuram, 515701, Andhra Pradesh, India.

Abstract: Surveillance, remote sensing, and autonomous navigation are just a few of the applications that use outdoor photos. The biggest problem with these kinds of photographs is that they're so small. Image gets degraded by the effects of pollution which are fog, smog, water drops etc. For the input of computer vision systems, this form of deterioration must be eliminated. The majority of cutting-edge research, The goal of dehazing techniques is to improve estimates. Transmission maps, often known as depth maps, are also a type of transmission map. The transmission maps are important because they have a direct impact on the transfer of information. In connection to the picture restoration's quality. This research proposes a novel restoration algorithm based on the use of a single image to lessen the impact of pollution on the environment. Using the metrics, the acquired experimental results are reviewed and compared qualitatively and quantitatively with those of other dehazing algorithms. The peak signal-to-noise ratio, as well as the structural similarity index; The proposed approach is found to be effective based on these measures. When compared to the recently launched version, it has enhanced performance a strategy.

Index Terms:Image Dehazing, Dark Channel Prior, Morphological reconstruction, color channel Estimation, Image Sharpening

1. Introduction:

When the outdoor images are captured we can get noise depending on the light scattering occurred during the time of capturing. The noise may include hue shifts, haze or any kind of disturbance in the picture.The main cause of noise in the picture is due to tha change in the atmospheric light while capturing.

These dehazing algorithms may take single image or more than one image to dehaze. But when we need dehaze the image by using the multiple images it becomes difficult task to have more than one image. So we go for algorithms having only one image and process it for getting dehazed image.

Now here we propose a method which uses the morphological reconstruction to make the picture more visible without noise. These images are the single images that can be modified to the original image without haze.

This paper is arranged as follows. Section II gives the brief literature review of previous works done regarding this work. Section III gives an overall theorical background used. Section IV is all about Proposed Technique description and implementation. The results obtained are compared with different algorithms and given in Section V. Conclusion of the work is given in Section VI.

2. EXISTING SYSTEM

ICA (Independent Component Analysis) is a statistical and computational methodology for uncovering hidden or underlying features in data.If all components are independent, ICA can be used to find the independent components or sources.

In the 1980s, ICA was introduced as a new approach for separating data or signals. Although ICA is a relatively recent data analysis approach, its foundations have been in place for quite some time. There is a huge demand for algorithms which use single images for the processing. Haze is addressed via independent component analysis which estimates the albedo in the collected picture.

The term albedo refers to the amount of light that is reflected rather than absorbed when it strikes a surface. Something that seems white reflects the majority of the light it receives, whereas something that seems black absorbs the majority of the light it receives, suggesting a low albedo.

The extension of principle component analysis is ICA (PCA). PCA is a type of data analysis that decorrelates and maximizes data variance. Because the resulting principal components are still

dependent, this methodology cannot be used to isolate the sources. ICA is a nonlinear PCA variant. Sources must be as independent as possible in order to achieve greater source separation.The separation procedure must account for all higher order correlations in order to make the signals independent.

In the ICA methods we use the correlations which are more complex and time taking. But in the morphological reconstruction we get quality output. This process is less complex compared to ICA.Now we can justify that morphological reconstruction is the effective process than the ICA.

3. FRAMEWORK FOR PROPOSED SYSTEM:

The proposed methodology for reducing haze in an image is built around principles like air scattering, DCP, and morphological restoration

3.1.Model of Atmospheric Scattering

In the obtained image, Fig. 1 demonstrates how environmental pollution causinghaze could damage a scene. Below equation describes the mathematical model that corresponds to it.

$I(\chi)=J(\chi)t(\chi)+A(1-t(\chi))$

Where

I(χ) = Intensity of Output image

J(χ)= Intensity of Scene capture by camera

t(χ)= Transmission

A = color vector of atmospheric light

Transmission of information $t(\chi)=e^{-\beta d(\chi)}$

3.2. Dark channel prior

We knowthat every image has RGB channels in it. Now DCP analysis makes images without haze and of natural type. This is achieved by taking the low -intensity pixel in the image and making it close to 0.

The Dark channel prior of the image can be given as:

$$I^{\text{dark}}(\chi) = \min_{C\in R,G,B}\left(\min_{y\in\Omega(\chi)}(I^c(y))\right)$$

Hence,DCPisexpressedby

$I^{dark}(\chi)\rightarrow 0$

We can see that the image is dehazed, but the main drawback here is the computational complexity. So here we propose a method which is the combination of the DCP and morphological reconstruction.

3.3.MORPHOLOGICAL RECONSTRUCTION

The morphological reconstruction is the process of decreasing haze in the images by preserving the important features of the image.This approach uses mainly two kinds of methods which are erosion and dilation. We can reconstruct the image by using the opening and closing operations which are the combinations of erosion and dilation.

3.4.Erosion of the grayscale image:

The erosion of the grayscale image can be given by:

$$[\varepsilon_B(I)](\chi) = \min_{s\in S} I(\chi+s)$$

3.5.Dilation of the grayscale image:

The dilation of the grayscale image can be given by:

$$[\delta_B(I)](\chi) = \max_{s\in S} I(\chi+s)$$

3.6.MORPHOLOGICALRECONSRUCTION:

Geodesic dilation and erosion are used to describe morphological reconstructions.

3.7.Geodesic dilation:

Thegeodesic dilation ofthe marker image with respect to the mask image in grayscale pictures is defined by

$\delta^{(1)}(I)=\delta^{(1)}(I)\wedge F$

When marker image and mask image are both the same size, the intensity relationship I ≤F is established. '∧' is the operator minimum.

$\delta g^{(n)}(I)=\delta g^{(1)}[\delta g^{(n-1)}(I)]$

with$\delta G^{(0)}(I)=I$.

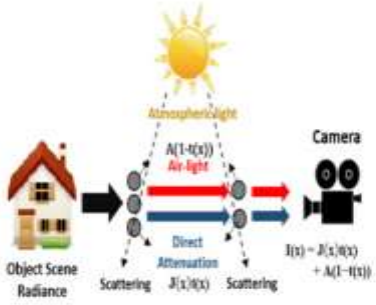
3.8.Geodesic erosion:

We can perform the geodesic erosion operation by using the formula:

$\varepsilon g^{(1)}(I)=\varepsilon g^{(1)}(I)\vee G$

3.9.Dilation Operation:

We can perform the dilation operation by using the



formula:

$Rg^{\delta}(I)=Rg^{(i)}(I)$

We can consider the system reached stability if:

$\delta g^{(i)}(I)=\delta g^{(i+1)}(I)$

3.10.Erosion Operation:

We can perform the erosion operation by using the formula:
$Rg^{\varepsilon}(I) = \varepsilon g^{(1)}(I)$
Stability is achieved when
$\varepsilon_g^{(i)}(I) = \varepsilon_g^{(i+1)}(I)$.

3.11.Opening and Closing by Reconstruction:

The opening operation is performed by the dilation followed by the erosion. The closing operation is performed by the erosion followed by the dilation. In each phase we perform the erosion and the dilation operations for the objects which are exceeded by structuring element. Now the closing and opening operations can be given by:

$$\gamma_R^{(n)}(I) = R_I^{\delta}\left[\varepsilon^{(n)}(I)\right]$$
$$\phi_R^{(n)}(I) = R_I^{\varepsilon}\left[\delta^{(n)}(I)\right]$$

4.PROPOSED SYSTEM:

In terms of morphological erosion, the dark channel depicted in (3) can be stated as:

$$I^{dark}(\chi) = \left[\varepsilon_S\left(\min_{C\in R,G,B}(I^C(y))\right)\right](\chi)$$

The atmospheric light of the RGB image with a height of h and a width of w pixels is given by:

$$A = max\sum_{C=1}^{3} I^C\left(\arg\max_{\chi\in(0.1\%*h*w)}\left(I^{\text{dark}}(\chi)\right)\right)$$

To produce dark-channel values between zero and one, the picture I () is normalised in relation to ambient light A, as shown by

$$I_N(\chi) = \frac{I(\chi)}{A}$$

We can define the minimum channel as:

$$I^{min}(\chi) = \min_{C\in R,G,B}(I_N^C(y))$$

We can compute the transmission map as:

$$t_1(\chi) = 1 - I^{min}(\chi)$$

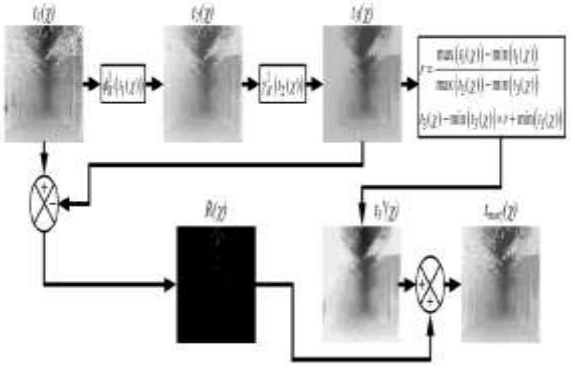


Fig. 4. Morphological process.

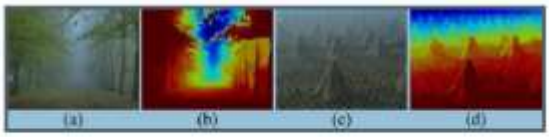


Fig. 5. Examples of transmission maps generated by the proposed algorithm, where (a) (c) are the input images and (b) (d) are the respective transmission maps.

Each stage of the proposed morphologic model is depicted in Figure 4.
The process of improving the first transmission, which involves the usage of
S which is a square structural element.Closing by rebuilding is conducted in the first stage as follows:

$$t_2(\chi) = \phi_R^1(t_1(\chi))$$

Over the picture structuring element, this technique removes little dark elements.Later, a reconstruction of the aperture is carried out as follows:

$$t_3(\chi) = \gamma_R^1(t_2(\chi))$$

This process removes little things that are more visible than others.Its size is smaller than that of S, and it exists in a smaller context. These objects are saved by

$$R(\chi) = t_1(\chi) - t_3(\chi)$$

The intervals of the image $t_3(\chi)$ are changed to the $t_1(\chi)$ and the values are stored in $t_3'(\chi)$.

Now, we get the output image $t_{\text{morf}}(\chi)$:

$$t_{\text{morf}}(\chi) = t_3'(\chi) + R(\chi)$$

Finally, the scattering model is applied to the

transmission map tmorf (χ) and the ambient light A is added to extract the ImageJ(χ) without haze.

$$J(\chi) = \frac{I(\chi) - A}{t_{\text{morf}}(\chi)} + A$$

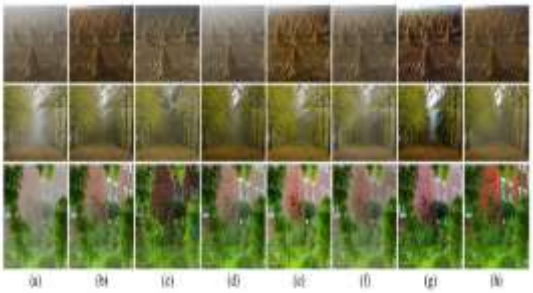


Fig. 6. Comparison of recovered outside scene without haze. (a) Input images, the results from (b) He et al. [15], (c) Tarel et al. [18], (d) Gibson et al. [30], (e) Kim et al. [31], (f) Zhu et al. [23], (g) Berman et al. [24], and (h) proposed algorithm.

TABLE I

OBTAINED RESULTS FROM PSNR ANALYSIS

Images	He et al. [15]	Tarel et al. [18]	Gibson et al. [30]	Kim et al. [31]	Zhu et al. [23]	Berman et al. [24]	Proposed algorithm
Bikes1	20.7	8.3	15.5	16.2	12.7	20.1	17.4
Rock2	12.9	11.8	14.0	19.2	13.8	16.0	14.3
Trees2	18.9	16.1	17.4	15.0	16.9	19.5	**18.0**
Church	19.1	17.2	17.9	18.7	17.2	16.6	**18.4**
Couch	19.9	15.9	20.9	19.1	18.8	12.3	**19.1**
Dolls	18.7	16.9	18.6	16.1	21.1	11.9	**18.0**
Flower1	20.1	16.5	17.8	18.9	18.8	17.6	**19.4**
Flower2	14.8	14.1	15.4	16.2	16.5	15.1	**14.7**
Mansion	18.7	16.0	19.1	17.7	20.5	19.2	**18.7**
Moebius	21.9	12.6	17.3	13.0	15.4	21.0	**20.0**
Reindeer	19.4	18.7	16.6	12.0	13.3	20.8	**18.2**
Average	18.7	14.8	17.3	17.0	17.2	17.6	**18.0**

5.EXPERIMENTAL RESULTS:

In this section we compare the qualitative and quantitative results from the proposed system and the ICA. We have used MATLAB software to implement the proposed method on the Intel i3 processor. The mean, entropy and the contrast of the picture are found and are noted in the table format.

TABLE III

COMPUTATIONAL TIME ANALYSIS (SECONDS).

Method	Image Size (pixels)			
	600×400	800×600	1280×720	1920×1080
He et al. [15]	23.35	47.76	97.10	420.98
Tarel et al. [18]	8.13	24.96	111.64	520.02
Gibson et al. [30]	1.19	2.35	4.57	10.43
Kim et al. [31]	0.2	0.3	0.7	1.6
Zhu et al. [23]	0,74	1,31	2,48	5,55
Berman et al. [24]	1,24	2,46	5,12	12,58
Proposed algorithm	**0.02**	**0.04**	**0.06**	**0.14**

These results prove that the proposed system has more advantages than the ICA and other algorithms.

The comparision tables have precise values and are given by:

5.1.Qualitative Comparision:

From figure 6 we can see that the past methods which are used have no higher quality and we can see the proposed system image having higher quality than the other past mthods used.

5.2.Comparison of Quantitative Data:

The PSNR of the image can be given by:

$$PSNR = 10\log_{10}\left[\frac{MAX^2_{I_{HF}(\chi)}}{MSE}\right]$$

$$\text{MSE} = \frac{1}{(w \times h)}\sum_{x=1}^{w}\sum_{y=1}^{h}(J(\chi) - I_{HF}(\chi))^2$$

with width w and height h, respectively, indicating the pixel position χ =(x, y) in the picture The better the picture approximation J(χ), the higher the PSNR value. Here we found the values of mean, entropy and contrast visibility of the picture by using the above formulae.

TABLE II

OBTAINED RESULTS FROM SSIM ANALYSIS

Images	He et al. [15]	Tarel et al. [18]	Gibson et al. [30]	Kim et al. [31]	Zhu et al. [23]	Berman et al. [24]	Proposed algorithm
Bikes1	0.762	0.494	0.644	0.586	0.515	0.643	**0.696**
Rock2	0.805	0.763	0.855	0.886	0.822	0.893	**0.864**
Trees2	0.866	0.795	0.816	0.876	0.829	0.902	**0.839**
Church	0.933	0.774	0.805	0.815	0.826	0.903	**0.901**
Couch	0.874	0.827	0.919	0.842	0.945	0.707	**0.832**
Dolls	0.879	0.802	0.864	0.820	0.964	0.665	**0.846**
Flower1	0.914	0.845	0.842	0.854	0.876	0.870	**0.893**
Flower2	0.806	0.774	0.852	0.811	0.959	0.835	**0.796**
Mansion	0.877	0.782	0.868	0.716	0.949	0.900	**0.836**
Moebius	0.956	0.955	0.781	0.758	0.962	0.960	**0.820**
Reindeer	0.772	0.846	0.676	0.558	0.579	0.739	**0.783**
Average	**0.833**	**0.731**	**0.807**	**0.741**	**0.801**	**0.806**	**0.811**

TABLE IV
MEMORY UTILIZATION (MEGABYTES)

Method	Image Size (pixels)			
	600×400	800×600	1280×720	1920×1080
He et al. [15]	895.5	1792.5	3472.9	8079.9
Tarel et al. [18]	40.3	82.3	159.7	358.7
Gibson et al. [30]	9.3	18.4	70.3	101.2
Kim et al. [31]	53.3	116.3	215.4	468.7
Zhu et al. [23]	16.6	33.1	63.6	142.7
Berman et al. [24]	117.2	234.5	449.9	1012.5
Proposed algorithm	**13.0**	**23.1**	**43.6**	**90.3**

5.3.Evaluation of Time Performance :

Table IV compares the proposed method to the alternatives in Table III in terms of peak memory use.Table IV shows that, in some situations, the suggested strategy uses less memory than all of the other strategies studied, with the exception of Gibson et al. [30].

6.Conclusion:

The pictures we take, have haze and fog in them, which reduces the visibility of the picture. As a result, a number of studies have been conducted. R reducing haze in photos through design and application of algorithms for dehazing. In this sense, the majority of recently published algorithms combine DCP with various strategies aimed at calculating accurate transmission maps quickly. Attempting to maintain image quality at the expense of time for long computations

As a result, the combination of DCP and the morphological reconstruction has less computational complexity than the past algorithms. Hence morphological reconstruction is used to retain significant picture structures at all stages. The amount of time it takes to compute and how much memory it takes up. By the experimental results it has be proven that it consumes less memory and it is dehazing algorithm with high performance.

7.Literature survey:

1.K. He, J. Sun, and X. Tang, “Single image haze removal using dark channel prior,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 12, pp. 2341–2353, Dec. 2011.

Adv: Using Prior , we can directly estimate the thickness of the haze, and recover a high quality haze free image.

Disadv: When scene objects are similar to atmospheric light, the dark channel prior is invalid

2.Q. Zhu, J. Mai, and L. Shao, “A fast single image haze removal algorithm using color attenuation prior,” IEEE Trans. Image Process., vol. 24, no. 11, pp. 3522–3533, Nov. 2015.

Adv: With help of depth maps we can estimate the transmission and restore the scene radiance.

Disadv: Long distances have very low value of scattering coefficient. The dehazing algorithms based on the scattering model are prone to underestimate transmission.

3.W. Wang, F. Chang, T. Ji, and X. Wu, “A fast single-image dehazing method based on a physical model and grey projection,” IEEE Access,vol. 6, pp. 5641–5653, 2018

Adv: This algorithm can restore images to a clear and natural state and quality is ensured.

Disadv: Shadows appears at the edges of the dehazed image.~,%*+$19;85.

DYNAMIC EMBEDDED SYSTEM FOR PRECISION AGRICULTURE

B.Varun Kumar[1]B.Nandini[2]P.Jyothi[3]S.Chandra Sekhar[4]G.M.GowthamiPriya[5]
Assistantprofessor[1],UGScholars[2,3,4,5]
[1,2,3,4,5]Department of ECE, Srinivasa Ramanujan Institute of Technology,Anantapur, AndhraPradesh

ABSTRACT - An embedded system is a combinationn of computer hardware and for a specific function andPrecision agriculture is an approach to farm management that uses latest technologies to ensure that crops and soil receive exactly what they need for optimum health and productivity. At present many countries have shortage of skilled labour in agriculture sector, which affects the growth rate of the developing countries including India which hugely depends on agriculture sector. As the population of India is rising, demand of food is also escalating which leads to higher crop production per hectare. So, to fix these problems farmers should use latest technological advancements for the various agricultural practices like digging, sowing, irrigation etc.The Internet of Things (IoT) can revolutionize the agriculture business from static and manual to dynamic and smart, resulting in higher production with reduced human labour. Precision agriculture and image processing are the primary drivers of agricultural automation.The major goal of this project is to create an embedded system-based precision agricultural robotic vehicle that can be controlled via IoT from an Android phone.The project designed with raspberry pi3 processor which is capable of taking the decision based on situation.The pi camera is used to detect the leaf diseases using image processing technique and activate the buzzer. And the robot consists of water motor and seed drop motor which is controlled by the user from Wi-Fi and also robot consists of plough tool when the robot moves it can be done automatically.

Keywords: Precision agriculture, Internet of Things (IoT), Raspberry Pi 3, image processing, Wi-Fi

I.INTRODUCTION

Generally, all the repetitive agriculture Tasks are being done either by the use of manpower or heavy machinery .Several primitive seed sowing methods such as animal drawn funneling, pipe drilling and drilling using tractor were being used. The above mentioned techniques require labor, a lot of time and energy consumption. Usage of heavy machinery results in exposure to high level noise and vibration affecting the health and work performance of the farmer. The key factors kept in mind during the development of autonomous field robots are:

- Speed
- Energy Efficiency
- Accuracy

By using this robot technology, one can sit in a cool and comfortable place and can accomplish various tasks by just monitoring the robot.

Agriculture is not all about growing crops but also taking care of the crops and preventing it from various diseases and threats. If the plant gets affected it directly affects both man-kind and animal life. Therefore, detection of the disease is an important and urgent task. One of the traditional methods of plant disease detection is by observing the plant with the naked eye, but this doesn't give accurate results as the disease can be microscopic which is not visible to the naked eye. This problem can be solved by automating the monitoring process by use of advanced image processing technique and machine learning.The proposed work aims in making the automated system easily available for the farmers using the device for early detection of disease in the plants.

India is a country whose economy mostly depends on agriculture. Farmers have variety of options to cultivate crops in the field, yet the cultivation of crops and harvesting of crops is done in old and traditional manual way which may lead to improper

management, in turn leading to reduction in the yield. The yield can be increased and quality can be improved by the use of technology.

II .PREVIOUSWORK

A. Smart Irrigation System

Smart irrigation is a synthetic irrigation application that controls the quantity of water by making a decision about where water is needed. It is the most important key in agriculture, which has a great effect on crops' health, cost and productivity. One major aspect of smart irrigation is to avoid the wastage of water since most countries in the world are facing water shortage problems. A smart irrigation system was presented which a Raspberry Pi was used along with two sensors: a soil moisture sensor was used to assess the water level in the soil, while a temperature and humidity sensor was used to display the environmental condition. The Raspberry Pi was connected to these sensors and the water supply system. A mobile application was established for remote monitoring and remote water flow control allowing both manual and automatic water flow control. In automatic mode, water flow was automatically twisted ON/OFF based on the water level of the soil without human interference. In manual mode, the user was bright to monitor the soil moisture level. An alert was generated when the water level of soil was getting below an exact value, and the user twisted it ON/OFF using a mobile application.

B. IoT-Based Irrigation System

In an IoT-based irrigation system using soil moisture sensor controlled by ATMEGA 328P on an Arduino UNO board along with a GPRS module. The data collected from the sensors were sent to the cloud, i.e. Things Speak, where graphs were generated to visualize the data developments. A web gateway was also designed where the farmer was able to check the status of water, if it was ON/OFF. Similarly, a real-time prototype for an irrigation system was presented. Which soil moisture sensors and soil temperature sensors were used to assess the water status, temperature status of the soil. RFID was used to transmit data to the cloud for further data analysis.

III.PROPOSEDMETHODOLOGY

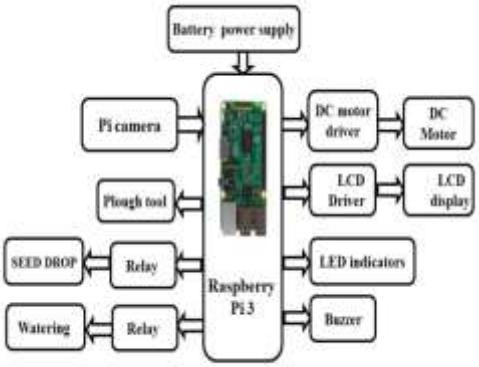


Fig 1: Block diagram of proposed methodology

The design can be implemented with Raspberry pi3 processor it has inbuilt Wi-Fi. The interfaced devices to the raspberry pi3 are Pi camera, DC motors along with l293d motor driver, seed drop, water motor along with relays, Buzzer. To control the robot and agriculture system user need to enable the mobile hotspot which is written into the program and it can access raspberry pi3 through program. So in this way both raspberry pi3 and user mobile connected with same network for communication. Then the user control the robot from remote place through Wi-Fi as well as control the seed sowing, watering system through Wi-Fi by using mobile phone which is interfaced to the relays. Here rely works as a switch to on/off the water, seed motors. Pi camera is . The leaf picture is captured using pi camera which is fed as input to the Raspberry Pi3 processor. The Processor takes duty to test the health of the leaf by using image processing technology and show the disease on LCD module and additionally provide the audible alert through BUZZER if the system detects the leaf disease. And the robot has seed drop, watering structures which manage the consumer from remote place through Wi-Fi by using android cellular phone. And additionally the robotic designed with plough device while the robotic movements closer to the sector it could be executed automatically. To achieve this project, Raspberry Pi3 processor is programmed the use of 'RaspbianOS'.

Fig.2:Prototype of Proposed System

The brief introduction of different modules used in this project is discussed below:

A. Raspberry pi3 processor:

Fig.3: Raspberry pi 3

The full specifications for the Raspberry Pi 3 include:

- CPU: Quad-core 64-bit ARM Cortex A53 clocked at 1.2 GHz.
- GPU: 400MHz VideoCore IV multimedia.
- Memory: 1GB LPDDR2-900 SDRAM (i.e. 900MHz)
- USB ports: 4. 3
- Video outputs: HDMI, composite video (PAL and NTSC) via 3.5 mm jack.
- Network: 10/100Mbps Ethernet and 802.11n Wireless LAN.

B. pi camera:

The camera consists of a small circuit board, which connects to the Raspberry Pi's Camera Serial Interface bus connector via a flexible ribbon cable. The camera's image sensor has a native design of five megapixels and has a fixed focus lens.

Fig.4. pi camera

The Raspberry Pi Camera Module v2 is a high quality 8 megapixel for Raspberry Pi, participating a fixed focus lens. Features of pi camera .Connects to the Raspberry Pi board via a short ribbon cable (supplied) .

C. DC motor:

Fig.5:DC Motor

An electric motor is an electrical device which converts electrical energy into mechanical energy. The simple working principle of a DC motor is: "at any time a current carrying conductor is placed in a magnetic field, it involvements a mechanical force". In this project we are using DC motors to moves the robot.

D. L293d motor driver:

Fig.6: L293d motor driver

This l293d ic works on the basic principle of h-bridge, this motor control circuit allows the voltage to be flowing in any direction. As we know that the supply polarities are change the motor directions are change automatically. Hence, h-bridge circuit using l293d ics are faultless for driving a motor. Single l293d ic contains of two h-bridge circuits

inside which can rotate two dc motors separately. Generally, these circuits are used in robotics due to for controlling the directions of DC motors

E. Seed dropping:

In this project there is also a third motor interfaced to the Raspberry pi through relay controlled by the user through Wi-Fi. When that third motor is rotating the pipe attached to the motor also rotates. There is a hole on the pipe. Only when the hole comes downwards, the seeds drop outwards. We put a funnel in fixed position above the holder arrangement on the pipe. Now when the pipe is rotating, there is point of time at which the hole comes downwards, exactly at that point of time, funnel gets arranged through holder. The seeds in funnel fall down through the hole.

F. Watering:

Here we are interfacing the water motor through relay to the Raspberry pi controlled by the user through Wi-Fi. When the user control the water motor through Wi-Fi, it will receive the raspberry pi and control the water motor accordingly through relay. Here relay works as a switch to on and off the water motor.

G. Plough Tool:

Fig.7.:Plough tool

In this system Plough tool is attached to the robot, so when the robot moves it can be done automatically. G. Relay: Relay is an electromagnetic switch. It consists of a coil of wire nearby a soft iron core, an iron yoke, which provides a low reluctance path for magnetic flux, a movable iron armature, and a set, or sets, of contacts; two in the relay pictured. The armature is hinged to the yoke and mechanically linked to a moving contact or contacts.

H. Relay:

Fig.8:Relay

When an electric current is accepted through the coil, the resulting magnetic field attracts the armature and the following movement of the movable contact with a fixed contact.

IV.RESULTS

Thus embedded system-based precision agricultural robotic vehicle that can be controlled via IoT from an Android phone.Thisdesigned with raspberry pi3 processor which is capable of taking the decision based on situation.The pi camera is used to detect the leaf diseases using image processing technique and activate the buzzer. And the robot consists of water motor and seed drop motor which is controlled by the user from Wi-Fi and also robot consists of plough tool when the robot moves it can be done automatically.

V.CONCLUSION AND FUTURESCOPE

The agriculture robot was proposed based on the automation of agriculture. The proposed method helps the farmers to easily perform their agricultural activities and efficientle af disease detection.Ther obot reduces thes tress and strain suffered by the farmer.Information about the leaf disease was obtained through image processing.This system can be extended using high efficiency GPS receiver and a GPRS module. The GPRS module gives the intimation of the robot vehicle tracking directly on to the predefined web link for tracking the vehicle on Google maps.The project can be extended using memory card using which the traveled path can be stored which helps in storing the tracked path along with speed and time.

REFERENCES

[1] Sunitha .M, "Seeding Robot", The Intl. Conf. on Information, Engineering, ManagementandSecurity2014(ICIEMS2014).

[2] M.Priyadarshini,L.Sheela,"CommandBased dSelf-GuidedDigging and Seed Sowing Rover", International Conference onEngineeringTrendsandScience&Humanities(ICETSH-2015).

[3] Ankit Singh, Abhishek Gupta, Akash Bhosale, Sumeet Poddar,"Agribot:AnAgricultureRobot",InternationalJournalofAdvancedResearchinComputerandCommunicationEngineering Vol.4,Issue1,January2015.

[4] N. FirthousBegum, P.Vignesh, "Design, and ImplementationofPick and Place Robot with WirelessCharging Application",InternationalJournalofScienceandResearch.

SMART DIARY USING ARDUINO & CLOUD APPLICATION

Y. Rajakullayi Reddy[1] A. Pranathi[2] K.Sai Krishna Yaswanth[3] L. Niranjan Reddy[4]
D. Hema Latha[5], Assistant Professor[1],SRIT[2,3,4,5]
[1,2,3,4,5]Department of ECE, Srinivasa Ramanujan Institute of Technology(SRIT) ,Anantapur, Andhra Pradesh

Abstract:

The milk is that the dietary fluid secreted by the mamma of mammals. The top quality milk ought to have higher density and is free from the adulterants. Milk is most commercially oversubscribed artifact each by native vendor's furthermore super markets. but in native square measure as to extend the yield sure adulterants are further which can have an effect on the nutrition quality of milk. Milk adulteration may be a social drawback. It exists each within the backward and advanced countries. Consumption of adulterate milk causes serious health issues and a good concern to the food business. The Country milk producers and shoppers facing drawback to seek out the standard of milk, settle for the honest of value and consumption. thus it's necessary to make sure the standard of milk by measure sort and quantity of adulterants that square measure further to the milk. this can be performed by exploitation combined electronic device instrumental system like Temperature sensor (DS18B20), LDR Module. advanced information sets from these device signals square measure combined with variable statics represents fast and economical tools for classification, discrimination, recognition and identification of adulterants furthermore because the concentration of various compound results in analyze and make sure the quality of milk. This project is enforced exploitation ARDIUNO microchip. All the sensors square measure combined to create compact and versatile system that analyze and classify the standard of milk into totally different grades and eventually output displayed on LCD screen and information of the sensors are sent to the cloud and hold on .From the cloud it'll be sent to the farmers mobile range that temperature, amount of milk, price of the milk supported fat and amount.

Keywords- Arduino,temperature, level,embedded c, fat

INTRODUCTION

In Asian country dairying may be a joint business of Indian farmers is backbone of our country. Milk and its by product square measure valuable nourishing food to kinsmen adulteration milk that effects to the human health thus quality of milk are going to be maintained. Indian farm sector contributes one, 15,970 crores to Indian economy. The standard of mi**lk is** measured exploitation milk o tester thought and different device. The milk with average 3.5 to 4 dimensional is AN smart milk. The adulterated milk is harmful to human health. There's a necessity of adaption of latest technology into this. Here we have a tendency to square measure exploitation Raspberry pi based mostly machine-driven system. this technique reduces the corruption improper maintenance of knowledge then on. Here we have a tendency to live the standard of milk like (FAT, Temperature, SNF) and amount is measured exploitation weighing balance and therefore the details is send to farmers mobile then the info is hold on in cloud. this technique produces the transparency between farmer and farm management.

LITERATURE REVIEW

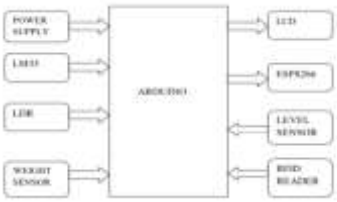
Rupak Chakravarty[1] this paper states blessings of automatic milk assortment station and use of instruments like electronic milkotestometer for correct fat mensuration. Abhishek M. Aware.et.al.[2] this paper states construction of straightforward milk o tester with paired IR semiconductor diode and a phototransistor as a module. The system would be came upon with the receiver and transmitter separated by alittle distance within the given sample. Fat molecules tend to specifically absorb bound bands of IR module. Yadav S.N.et.al. [3] this paper states associate applications of embedded system MILKOTESTER. it's tiny compact embedded in a very single unit, needs less power and live milk parameters like SNF (Solid however Not FAT), FAT, CLR, WEIGHT, PH, with less value.

D.Shekar Goud.et.al.[4] this paper states Implementation of small industry victimi**zation RASPBERRY PI and Rasbian** software system. Dr. G. Rajakumar.et.al.[5] this paper states implementation of IoT based mostly adulteration detec**tion in milk victimization arudino** microcontroller. Dr. D. R. Shende.et.al.[7] this paper states implementation of the system for detection the Standard of milk supported fat and temperature
Displaying these parameters on show LCD Digital Display and caustion to farmers through GSM.

Proposed System

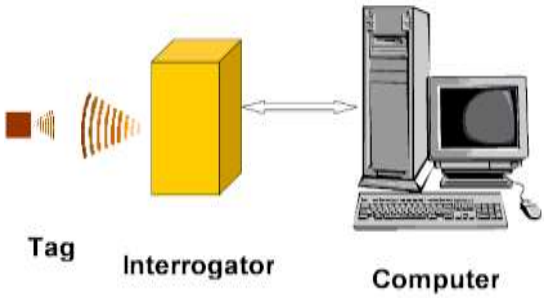
The main objective of milk assortment system is corruption free milk parameter observance and assortment. System checks the fat contents of a milk and amount of milk with the assistance of Fat tester and weight device. For client identification RFID Tags and RFID Reader area unit used.LCD show is employed for displaying the worth. Arduino microchip is employed for dominant and process knowledge**.**

Block Diagram



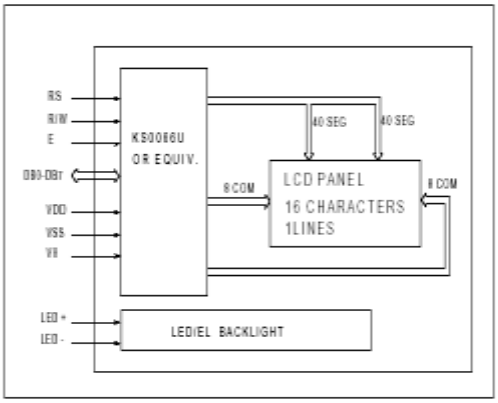
RFID

Radio Frequency Identification reader has two parts one has integrated circuit which is used for storing and processing the information and it can also modulating and demodulating the radio frequency signals coming from radio frequency identification tag. Another one has antenna for transmitting and receiving the radio frequency signals.



LCD

Liquid Crystal Display which is used to display the data from the micro controller .Liquid Crystal Displays are some many types ,here we are using 16*2 display. That means it represents two lines ,each line consists of 16 bits of data In LCD each pixel on screen depends on the Crystal molecule which is placed between two electrodes and polarising filters and which are perpendicular to each other
In LCD's having yellow light source or we can also called reflectors .so that we can easily identify the pixels on the LCD screen.



ESP8266

The Wifi module has a 32 bit processor .This module allows the chip to either function as a wireless adapter to extend the other systems with wifi functionality. This module has 8 general purpose input and output pins and transmitter and receiver pins for serial communication purpose. The wifi module has very low power of 80mhz.programmable memory depends on the module manufactures, but generally esp512kb.

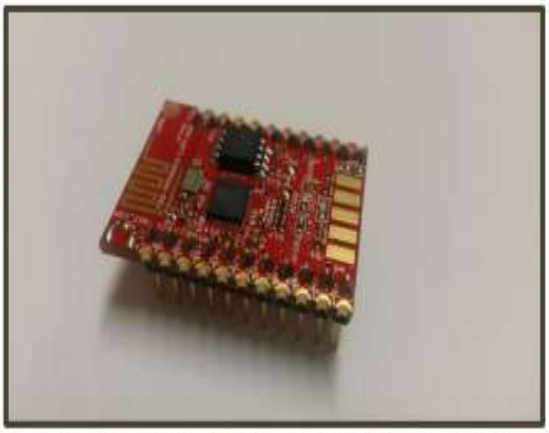
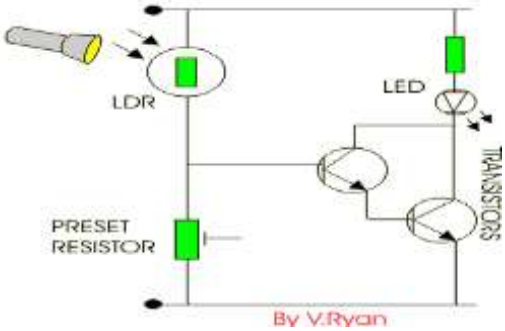


Figure 3.8 Olimex MOD-WIFI-ESP8266-DEV module used in this thesis

LDR

LDR is a variable resistor whose resistance depends on the amount of light falling on it's top. It's like potentiometer. But incase of potentiometer it's output can be changed by turning the screw whereas in LDR resistance changes according to the amount light falling on it's top. Intensity of light falling on LDR is measured in LUX this shows that the resistance of LDR. As amount of light falling on top of LDR increases then it's resistance and vice versa. The below graph shows we have taken amount of light on x-axis and resistance on y-axis. The below graph results as hyperbolic because of this we are calling it as colloidal sensors.



LEVEL SENSOR

In the water level sensor schematic as shown, the level water in the tank . We have to give the input voltage as +5V-12V. The level equal to ‘ZERO' is referred as the tank is empty.. The another in medium level of tank, which slightly above the 'ZERO' label, is given as ‘ONE'. The water level above the 'ONE' checked. The extreme level of the tank is labelled as 'HIGH' and the stage just above the 'ONE' is called as 'LITTLE' stage. Presets STG11, STG22, and STG33 are to be changed so that semiconductors SEM1, SEM3, and SEM5 will be 'ON' as it contacts test sets 'ZERO-ONE', 'ZERO-HIGH', and 'ZERO-LITTILE', separately. Then RES44 guarantees that semiconductor SEM22 is not works' without supply. Additionally, resistors IMP55 and IMP66 guarantee that the semiconductors SEM44 and SEM66 are 'on' without any base voltage. These SW111 and SW222 can be utilized for turn on and turn off, the drain physically, individually.

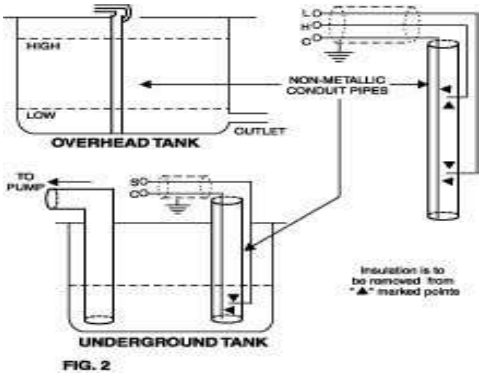
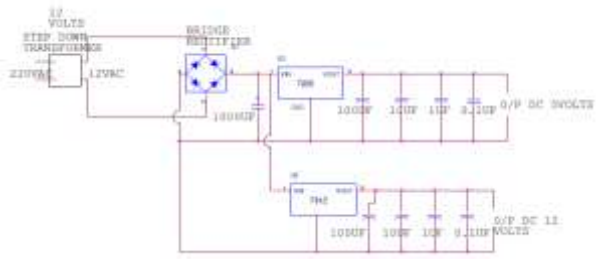


FIG. 2

POWER SUPPLY

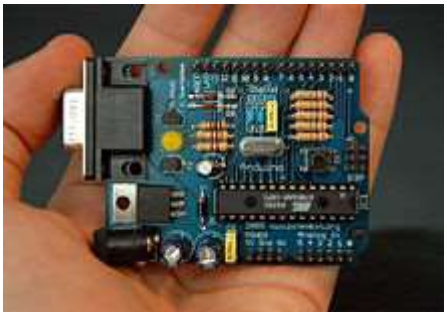
Force supply is a reference to a wellspring of electrical force. A gadget or framework that provisions electrical or different sorts of energy to a yield burden or gathering of burdens is known as a force supply unit or PSU. The term is most ordinarily applied to electrical energy supplies, less frequently to mechanical ones, and once in a while to others This force supply segment is needed to change over AC sign to DC sign and to decrease the plentifulness of the sign. The accessible voltage signal from the mains is 230V/50Hz which is an AC voltage, yet the required is DC voltage(no recurrence) with the plentiful of +5V and +12V for different applications. In this part we have Transformer, Bridge rectifier, are associated sequentially and voltage controllers for +5V and +12V (7805 and 7812) employing a capacitor (1000µF) in equal are associated equally as demonstrated in the circuit chart beneath. Every

voltage controller yield is again is associated with the capacitors of qualities (100µF, 10µF, 1 µF, 0.1 µF) are associated equally through which the comparing output(+5V or +12V) are thought about.



ARUDINO

Arduino microcontroller is a 8 bit microcontroller. It runs on standard 16Mhz frequency. It has inbuilt RC-Phase shift oscillator which it can generate 2-8Mhz frequency in built without crystal oscillator. It can process 8 bits in one time. Things we are using for writing code is open source. It's less expensive. It has voltage regulator and RISC based structure. It's of 16Mhz. It also has voltage regulator which is used to fluctuations in the input voltage. It also has the 32KiloBytes of inbuilt memory and 6 channels inbuilt and 10 ADC pins. ADC pins are used to convert the analog data into digital because arduino only accepts digital values. It is also has the features like I2C, SPI, PWM outputs



METHODOLOGY

1. A supply of 5V is given to the arduino. Once the Radio frequency Identification card is swiped card is browse through Radio frequency Identification reader, the ID and farmers name are showed on Liquid crystal display. After displaying the details of farmers the milk is taken in the test tube.

2. To know the temperature of the milk we can use lm35 temperature sensor which gives value of temperature in Celsius.
3. To check the fat content in the milk we can use LCD and LDR which are placed parallel and between them we can place milk in a test tube when the light from the LCD falls on the milk ,the fat content of the milk scattered the light from lcd to ldr .The light emits from milk to ldr has low than the fat content of milk is low and vice versa.
4. For cow's milk fat price are within the vary of 3.5-4.5 p.c & for buffalo milk fat price are within the vary of 6-7 p.c. If milk fat doesn't fall during this acceptable vary then quantity are given supported fat price.
5. The temperature price and fat p.c of milk are displayed on LCD as well as fat vary. successively it displays the ID of the farmer.
6.To know all the temperature ,level,fat sensor values of milk then we can check the weight of the milk with the help of load cell sensor..
7. Once activity the amount of milk request is completed supported Fat content in milk .
8. once request all details like {Date, Time, Fat, Temperature, quantity} is send to farmer mobile phone and therefore the same information is hold on in cloud.
9. The higher than steps is continual for different farmers once pressing the push button within the board.

RESULT

After swiping the radio frequency identification card the data will be displayed in liquid crystal display as buffalo id, farmers name and place. In liquid crystal display the values of temperature ,fat content ,weight, level are displayed.

wifi module the live data will be send to the cloud

With the help of wifi module the same live data will be sent to farmer mobile through pocket iot app.

CONCLUSION

Here we have a tendency to developed an automatic corruption free milk assortment system within the diary to live the milk parameter by the standard analysis of milk. It provides quality assurance for farmers and customers. this technique additionally calculates the payment victimization numerous sensors. This device is employed in little dairies for that ought to primarily based associate degree fat content within the milk and automatic asking are going to be worn out cloud so manual errors may be reduced.

REFERENCES

1. Abhishek M. Aware1, Ujwala A. Kshirsagar (Belorkar), "Design Of Milkotester For Fat And Clr Measurement Using Arduino Micro controller", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),Vol4, Issue 5, May 2017.pp.13-16. 2. D.ShekarGoud, V.NaveenKumar , "Advanced Handheld Electronic Banking System Using Raspberry Pi", Adavanced Research of Science And Technology(ARJST) 4.1(2017): 276-279.

3. Dr. G. Rajakumar, Dr. T.Ananth Kumar, Dr. T.S. Arun Samuel, Dr. E.MuthuKumaran, "Iot BASED MILK MONITORING SYSTEM FORDETECTION OF MILK ADULTERATION", International Journal of Pure and Applied Mathematics,Volume 118 No. 9 2018, 21-32.

4. Likki Rajeev, P. Suresh Kumar , S. Koteshwara Rao, "Design of Milk Analysis Embedded System for Dairy Farmers" , International Journal Of Advance Technology And Innovative Research,Vol.07,Issue.09, August - 2015, Pages:1678-1681.

5. Dr. D. R. Shende ,Mr. PankajPatil ,Mr. MahadeoMundhe. "Automated Corruption Free Milk Collectionsystem Indairy Farming" ,International Journal of Scientific Research and Review, Volume 7, Issue 6, 2018,pp.478-480.

6..N.Indumathi, K.Vijaykumar. "Wellorganized Milk Distribution Monitoring System based on Internet of Thing's (IoT)", International Research Journal of Engineering and Technology (IRJET),Volume: 05 Issue: 07 , July 2018,pp.589-593.

E MASK DETECTION USING OPENCV AND DEEP LEARNING

D. Gowtham[1] P. Kavyasree[2] C. Ravi Teja[3] G.E.Anusha[4]
P. Jagadeeshwara Reddy[5] Assistant professor[3], UGScholars[1,2,4,5]
Department of ECE, Srinivasa Ramanujan Institute of Technology, Ananthapur, Andhra Pradesh

Abstract— COVID-19 outbreaks are rapidly spreading across the country. It's a disease that's even more damaging, powerful, and dangerous. It spreads between people when a contaminated person comes into contact with an uninfected person. Computer Vision plays a critical role in enhancing government administrations. During this pandemic, little object location is a really difficult undertaking of Computer vision, as it enlists the pair of characterization, furthermore, location underneath of video representation. Contrasted with other item recognition deep neural network showed an accommodating object identification with an unrivaled accomplishment that is Face mask detection. The proposed approach in this paper utilizes deep learning, TensorFlow, Keras, and OpenCV to distinguish face masks. This model can be utilized for well-being purposes since it is very asset-productive to convey. The SSDMNV2 approach utilizes Single Shot Multi-Box Detector as a face locator and MobilenetV2 architecture as a system for the classifier, which is extremely lightweight and can even be used in embedded devices with less computational capacity (like Raspberry Pi) to perform real-time mask detection. Concerning the paper area beneath, we have accomplished that individual who wear face mask or not, it's trained by the face mask images and non-face mask images. We experimented with a data set that is available on various open source platforms. After training the model with various values of batch size and number of epochs, the highest generated accuracy of ~0.99 is achieved whereas the validation loss is 0.0198 and the validation accuracy is 0.9928.

Keywords— MobileNetV2, SSMNV2, OpenCV, TensorFlow

I. INTRODUCTION

Since December 2019, the corona virus epidemic has continued in numerous nations. It all started in Wuhan, China. The World Health Organization (WHO) proclaimed these to be deadly diseases that have spread throughout the globe and had a major impact on 114 countries on March 11, 2020. Every clinical expert, medical service association, and analyst is searching for appropriate immunizations and medicines to defeat this destructive sickness. The infection spreads through the air channel when the contaminated individual sniffles or speaks with the other individual, the water beads from their nose or mouth scatter through the air and influence others nearby. Face Mask Recognition has become a key application as a result of the Covid-19 outbreak, which requires people to wear face veils, keep social distance, and wash their hands with hand sanitizers. During this epidemic, wearing a mask is a basic preventive step and the most essential approach in scenarios where social separation is impossible to maintain. Wearing a veil is fundamental, especially for those individuals who are in more danger of extreme sickness from COVID-19 illnesses. It has been determined that COVID-19 transmits especially among people who are in immediate contact with one another (almost around 6 feet). As a result, the Organization for Research on Epidemiology advised everyone to wear a mask in open areas, especially when other social separation measures are difficult to maintain. Face mask recognition has proven to be a difficult topic in the fields of computer vision and image processing. Face detection has several uses, ranging from snapshot identification to capturing facial expressions, the latter of which necessitates a high level of power and accuracy in detecting the face. This study proposes the SSDMNV2 model for face mask recognition, which uses OpenCV, Deep Neural Network (DNN), TensorFlow, Keras, and MobileNetV2 architecture as an image classifier. SSDMNV2 can figure out the difference between portraits with masks and without masks on the faces. The proposed model will be used in

collaboration with surveillance cameras to recognize faces who are not wearing face masks and so prevent COVID-19 transmission. This work also pays attention to the eradication of many incorrect predictions, particularly in real-world data sets, which have been observed in several other proposed models.

As far as we can determine, the motivation behind this work is to fill in badly designed circumstances in the cutting-edge world by recognizing veils in specific regions where individuals covered or didn't cover their appearances. Somehow, the local area is protected while more influenza stops are dispersed noticeable all around and give hindrances to section into the human body. As a result, the enhanced MobilenetSSD scans the entire human face, as well as small parts of the mouth from the nose to the chin.

II. LITERATURE SURVEY

P. Viola et al.[2] presented a face detection system that can detect faces quickly at a high detection frame rate. Integral image, an efficient classifier using Adaboost learning method, and finally combined a classification into a cascade for background region are the three contributions in their paper. As COVID-19 became a global pandemic many researchers are trying to work about wearing masks[5]. Viola-Jones locator improved Haar's highlights but failed to address current reality difficulties and was influenced by factors such as face brilliance and face direction. It could only recognize adequately bright frontal faces and could not function in a dark setting or with a non-bright face image.

The corona virus's origin and history have been described by X. Liu and S. Zhang [8]. They also discussed on how wearing a mask can protect you from the corona virus, but their research did not include any model or method.

MFDD, RMFRD and SMFRD are three types of mask face datasets described by Z. Wang et al.[6]. Face detection and analysis using deep learning were described by M. Kawulok et al.[9]. Their goals included facial analysis, deceit detection and the prediction of various physiological disorders, among other things. A recognition method based on facial geometry was proposed by Zhen et al.(2011). A model that can detect and recognize a human face was proposed by P. Gupta et al.[4]. They managed to achieve accuracy of 97.05%.

III. EXISTING SYSTEM

You Only Look Once is the shorthand for YOLOV3, where V3 stands for version 3. To recognize multiple objects, the network only looks at the image once. As a result, it's known as YOLO, or You Only Look Once. YOLOv1, YOLOv2, and YOLOv3 are the first three versions of YOLO. The first version introduced a broad architecture, while the second version enhanced the design and used pre-existing object detection to improve the object detection proposal, and the third version strengthened the model infrastructure and workflow even more.

YOLOv3 is a real-time computer vision algorithm that recognizes specific things in streams, live broadcasts, and snapshots. Joseph Redmon and Ali Farhadi developed the first three versions of YOLO. Darknet-19 was utilized as a feature extractor in previous models of Yolov2. It was renamed darknet-53 in yolov3 after numerous modifications and upgrades. The Darknet is a framework for training neural networks implemented in the C programming language that excels at these tasks.

An image is passed into the YOLOv3 model as an input. The image detector examines an image for the coordinates that are present. It generally splits the input into an array and analyses the target object's characteristics from those grids. The characteristics that were identified with a high confidence rate in adjacent cells are combined in one place to provide model output.

IV. EXPERIMENTAL RESULTS FOR EXISTING SYSTEM

The YOLOV3 model is now ready for training after all the arrangement has been per- formed. YOLOv3 employed logistic regression as a loss function, which was different from other networks. The Google Co laboratory was used to train the system because resources were inadequate. About 80% of the data was used for training and the remaining data used for validation. It achieved a 96 percent accuracy after 4000 epochs of training, with an average loss of 0.0730 and a mean average

precision score of 0.96 as shown in the Fig 1.
Our model detects the object more accurately after being trained using data. In addition, the YOLOV3 model was also tested in real-time video and was capable of achieving a rate of 17 frames per second on average.

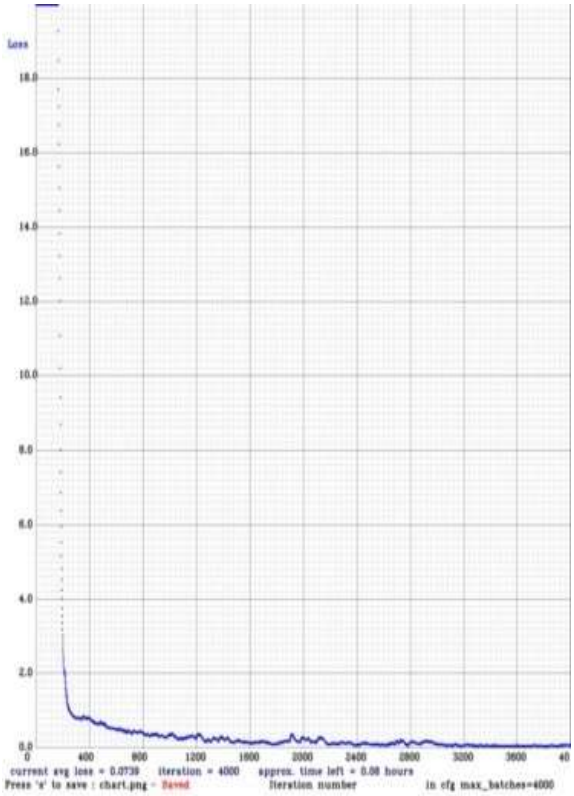


Fig. 1. *Experimental Result of existing system showing Average Loss Curve*

V. PROPOSED SYSTEM

The proposed system works to detect the masked face in this current pandemic situation to play an important role in ordered to stop the spreading of the corona virus from one person to another person. The architecture used in this system is MobileNetV2 architecture. Because mobilenet SSD is an efficient CNN architecture specially designed for embedded applications. So, this system can also be used in devices with less computational capacities.

This system presents a unique mask face detector, which is capable of detecting mask face in any direction or orientation regardless of its arrangement and train it with a proper neural network to get exact results. The input to this system is an RGB image from any orientation to get the output. The system's main function is feature extraction and class prediction of the input images. The feature extraction involves, creating a new image from the existing image, where the newly generated image is more efficient than the existing image. In this, the dataset containing a large number of images is reduced dimensionally to get the required interesting part of an image, by removing the unnecessary features.

After feature extraction is done, the images in the dataset are assigned labels, and these images represent a set of labeled images. The proposed system can detect mask faces from images as well as the live video streams using the webcam. As the image is given as input, it resizes to 224*224 in which feature extraction is performed. By doing feature extraction, background noise is reduced, performs filtering to remove high frequency from the input image. This image is used for training the model. After completing the training it gives the model its accuracy level. The entire process can be simply put into three parts, the first part is preparing the images into a good dataset for training the model, the second part is all about creating the model and training it to get good accuracy, and the third part is to detect mask face, from the images or the real-time video stream using the webcam.

Pseudocode :

```
LoadMobileNETV2,
MobileNetV2(shape=(224,224,3))
AveragePooling2D(pool-size=(7,7)
Flatten()
Dense(128,activation = "relu")
Dropout(0.5)
The final layer has 2 neurons,
Dense(2,activation = "softmax")
```

VI. EXPERIMENTAL RESULT

As Covid-19 is declared as a global pandemic, many researchers are trying to research wearing masks and its protection from the virus. Many of them worked on proposing methods but not implemented them in real-time. Even though there are some methods are available, they are not reliable and do not have alert systems. We experimented with a dataset that is available on

GitHub. Out of all the images, 80% images are used for training the model and 20% of them are used for testing the model.

As we can see in the above image, the validation loss is lower than the training loss, which indicates, fewer signs of overfitting.

After training the model with various values of batch size and number of epochs, the highest generated accuracy of ~0.99 is achieved whereas the validation loss is 0.0198 and the validation accuracy is 0.9928.

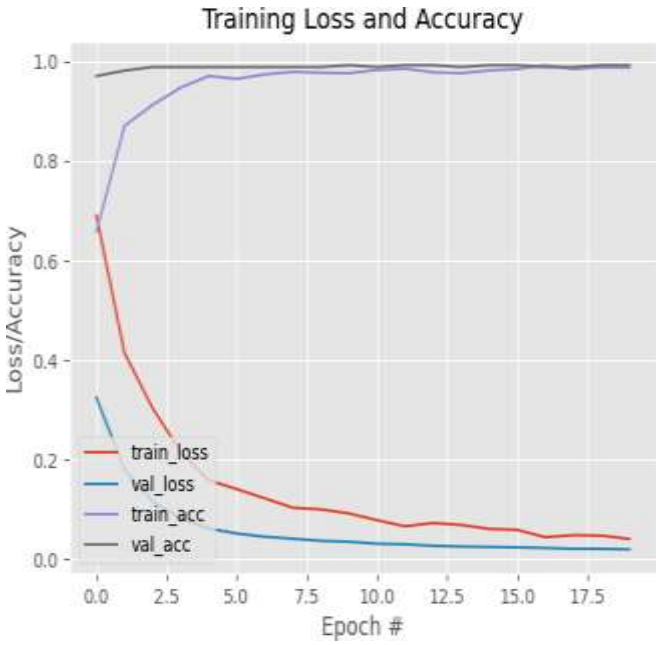


Fig. 2. *Accuracy/Loss Curves*

At the top of our work, our system was able to detect whether a person wearing a mask or not. Here sample output of our system detecting mask and no mask are shown below.

Fig. 3. *Our system detected No mask.*

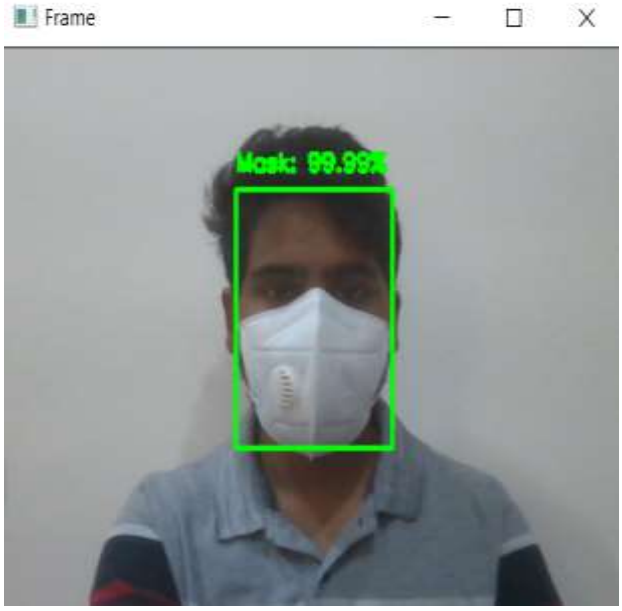


Fig. 4. *Our system detected No mask.*

VII. COMPARATIVE STUDY

TABLE I. Comparative study

S.No.	Comparative Study	
	Proposed System	***Existing System***
1.	In this system, MobileNetV2 architecture	Authors used YOLOV3 in the existing system.

S.No.	Comparative Study	
	Proposed System	***Existing System***
	used.	
2.	Less computational capacity is required.	High computational capacity is required.
3.	This system provides security alerts.	Doesn't have any alert system.
4.	Detection time is less.	Detection time is more than the proposed system.

VIII. CONCLUSION

The proposed system is based on the MobileNetV2 architecture, which was specially developed to implement on the edge devices with less computational capacity, so it will help for the betterment of the surveillance system by detecting the masked face in a secured way. The dataset is readily available for training this model, but it is small, also gives better accuracy. This proposed system delivers a model with higher accuracy and ensured the outcome.

IX. REFERENCE

[1] Altmann, D.M., Douek, D.C., Boyton, R.J.: What policy makers need to know about COVID-19 protective immunity (2020), 10.1016/s0140-6736(20)30985-5;https://dx.doi.org/10.1016/s0140-6736(20)30985-5.

[2] Paul Viola, Michael J. Jones, "Robust real-time face detection". International Journal of Computer Vision 57(2), 137–154 (2004).

[3] Within the lack of chest COVID-19 X-Ray dataset: a novel detection model based on GAN and deep transfer learning, Symmetry, 12(4)(2020), p.651.

[4] P. Gupta, N. Saxena, M. Sharma and J. Tripathi, "Deep Neural Network for Human Face Recognition", MECS, 8 January 2018.

[5] Feng, S., Shen, C., Xia, N., Song, W., Fan, M., J, B.: Cowling Rational use of face masks in the COVID-19 pandemic". Lancet Respirate. Med 8(5), 434–436 (2020).

[6] Z. Wang, et al., Masked Face Recognition dataset and application, arXiv preprint arXiv:2003.09093,2020.

[7] Paris Tests Face-Mask Recognition Software on Metro Riders. Bloomberg.com (2020)

[8] X. Liu, S., Zhang: COVID-19: Face masks and human-to-human transmission. Influenza Other Respirat viruses.

[9] M.Kawulok, M.E. Celebi, B. Smolka(Eds.), Advances in Face Detection and Facial Image Analysis, Springer International Publishing, Cham(2016), pp. 189-248.

Tumor Detection Using K-Means & Fuzzy-C Means Clustering Methods by Image Processing

B. Suresh Babu[1] T.M. Yasaswini[2] S. Pragna[3] G. Poojitha[4] M. Vishnu Vardhan[5]
Assistant professor[1],UG Scholars[2,3,4,5]
Department of ECE, Srinivasa Ramanujan Institute of Technology, Anantapur, Andhra Pradesh

ABSTRACT - This article administer the execution of Basic Calculation meant for recognition of reach and condition of cancer in cerebrum Magnetic Resonance image. Cancer is an unrestrained increase of tissues in any portion of the body. Cancer is of different variety moreover they include various Qualities and dissimilar handling. Since it is recognized, mind tumor is basically genuine and hazardous inside light of its quality in the restricted gap of the intracranial depression (gap shaped within the head). Mainly Exploration in shaped realm shows to facilitate the number of persons who have brain cancer was passed on for the reason that of the certainty of erroneous identification. Usually, Computed Tomography clean or else X-ray with the aim of corresponding keen on intracranial cavity creates a entire portrait of mind. This image is superficially analyzed by the physician intended for discovery and wrapping up of cerebrum tumor. Anyway these approaches designed for locating resist the exact declaration of period and volume of cancer. To keep clear of that, this venture employ PC sustain strategy in favor of splitting up (location) of cerebrum cancer dependent on the blend of two calculations. These practices allow the separation of cancer tissue through exactness and reproducibility equivalent to physical partition. In expansion, it similarly lessens the best chance for assessment. On the way to the conclusion of the interaction the cancer is divided from the Magnetic Resonance picture and its careful location and the contour also determined. The stage of the cancer is exposed dependent on the computation of region determined from the bunch.

Keywords: K – Means, Fuzzy C – Means, Pre-processing, Thresholding, Feature Extraction.

I. INTRODUCTION

The concept of planned mind tumor division is discussed in this study. Typically, the X-ray output or CT filter can reveal the Mind's living structures. The entire cycle is photographed with an X-ray filter in this article. For analysis, the X-ray filter is preferable to the CT check. It has no effect on the body because it does not use radiation. It is also influenced by the attracting field, which is radio wave. For the detection of cerebrum tumors, many types of calculations have been developed. They may, however, have some disadvantages in terms of location and extraction. For division, two calculations are used in this study. As a result, it provides a precise result for tumor division. Tumors arise from the uncontrolled growth of tissues in any part of the body. The tumor could be required or optional. If it's a start, it's considered critical. If a fragment of the tumor spreads to another location and develops on its own, it is referred to as optional. Normally, a brain tumor has an effect on the CSF (Cerebral Spinal Liquid). It is the cause of strokes. Rather than treating the tumor, the doctor treats the strokes. As a result, the tumor's detection is critical for treatment. The lifespan of the person affected by a cerebrum tumor will increase if it can be distinguished at this time. This will increase the lifespan by 1 to 2 years. Tumor cells are usually divided into two types. They are both numerous and harmful. The detection of a hazardous tumor is difficult in the case of a bulk tumor. A 3-D mental representation and a 3-D analyzer are required for the precise identification of the dangerous tumor.

II. PREVIOUS WORK

Roy, et al [1] suggested an analysis on automated brain tumor detection and segmentation from MRI of brain. Brain tumor segmentation was a

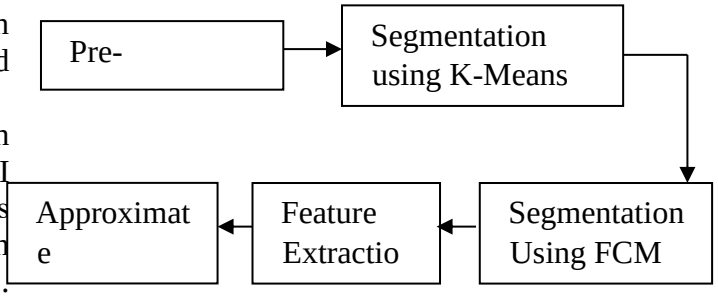
significant process to extract information from complex MRI of brain images. P. Vasuda and S. Satheesh [2] proposed a technique to detect tumors from MR images using fuzzy clustering technique. This algorithm uses fuzzy C-means but the major drawback of this algorithm is the computational time required. A.Mustaqeem, et al [3] implemented an efficient brain tumor detection algorithm using watershed and threshold based segmentation. This research was conducted to detect brain tumors using medical imaging techniques. E-J.Selvakumar,A.Lakshmi,T.Arivoli [4] Although we have achieved many feats in the field of medical imaging, highly accurate segmentation and characterization of tumor abnormalities has continued to be a challenging task for us. The task is mostly made challenging due to the variety in locations, shapes and image intensities of various tumor types. Tumors present can also lead to the deformation of surrounding organs and tissue spaces and may result in necrosis which can eventually lead to the image density change around the tumor [4].

Rajesh C. Patil and Dr. A. S. Bhalchandra et al, in his paper "Brain Tumor Extraction from MRI Images Using MATLAB", they focused on Meyer's flooding Watershed algorithm for segmentation and also presents the morphological operation [5]. R. Preetha and G. R. Suresh et al, 2011, in his paper "Performance analysis of fuzzy C means algorithm in automated detection of brain tumor" they used fuzzy C means clustering for segmentation. That method gives the high computational complexity. FCM shows good performance result in segmented the tumor tissue and accuracy of tumor. Segmentation was identified by applied the SVM classifier [6] Malathi Hong-Long et.al [7], proposed approach by desegregation wave entropy based mostly spider net plots and probabilistic neural network for the classification of Brain MRI. Proposed technique uses two steps for classification one is wavelet entropy based mostly spider net plot for feature withdrawal and probabilistic neural network for classification. The obtained brain magnetic resonance image, the feature extraction was done by wavelet remodel and its entropy worth was calculated and spider net plot space calculation was done. With the assistance of entropy worth classification of probabilistic neural network was calculated. Probabilistic neural network provides a general resolution for pattern classification.

III. PROPOSED METHODOLOGY

The proposed framework has basically four modules: pre-preparing, division, Feature extraction, and estimated thinking. Pre preparing is finished by shifting. Division is done by cutting edge K-implies and Fuzzy C-implies calculations. Highlight extraction is by thresholding lastly, Approximate thinking technique to perceive the tumor shape and position in MRI picture utilizing edge identification strategy. The proposed technique is a blend of two calculations. In the writing review numerous calculations were produced for division. In any case, they are not useful for a wide range of the X-ray pictures.

BLOCK DIAGRAM



PRE-PROCESSING

As per the need of the powerful the pre-preprocessing step converts the picture. It performs separating of clamor and different curios in the picture and honing the edges in the picture. RGB to dark transformation and Re-forming likewise happens here. It incorporates middle channel for commotion expulsion. The prospects of appearance of commotion in current MRI check are extremely less. It might show up because of the warm impact. The principle point of this paper is to distinguish and section the tumor cells. However, for the total framework it needs the interaction of clamor expulsion. For better understanding the capacity of middle channel, we added the salt and pepper clamor misleadingly and eliminating it utilizing middle channel.

A. K-MEAN SEGMENTATION

Segmentation is one of the significant information examination strategies broadly utilized in numerous useful utilizations of arising regions. clustering is the way toward discovering gatherings of objects to such an extent that the items in a gathering will be comparable to each other and not quite the same as the objects in other gatherings. Excellent clusters with high intra-cluster closeness and low between cluster similitude this is a decent clustering strategy. In the k-means calculation at first we need to characterize the quantity of clusters k. Then, at that point k cluster center are picked haphazardly. The distance between the every pixel to each cluster communities are determined. The distance might be of straightforward Euclidean work. Single pixel is contrasted with all cluster communities utilizing the distance formula.

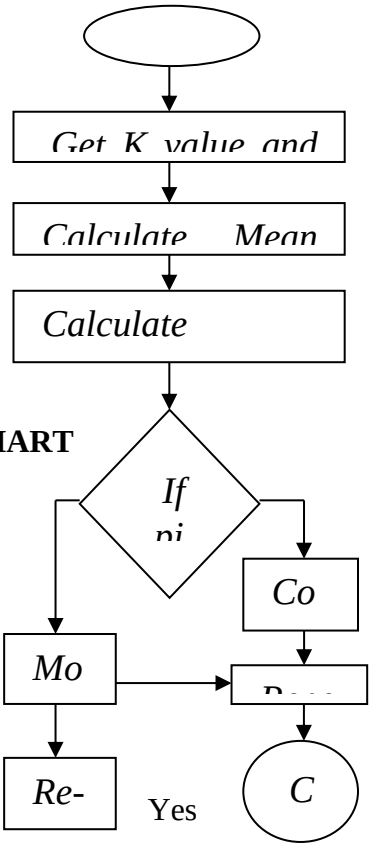


Fig: Flowchart for K-Means Clustering

i. FLOW CHART

i. ALGORITHM OF K-MEAN

1. Give the number of cluster value as k.
2. Arbitrarily pick the k cluster communities.
3. Figure mean or center of the cluster.
4. Figure the distance between every pixel to each cluster center.
5. Assuming the distance is close to the middle, move to that cluster.
6. If not move to next cluster.
7. Re-estimate the center.
8. Repeat the interaction until the middle doesn't move.

iii.MATHEMATICAL REPRESENTATION

Mean is calculated for each cluster using below formula

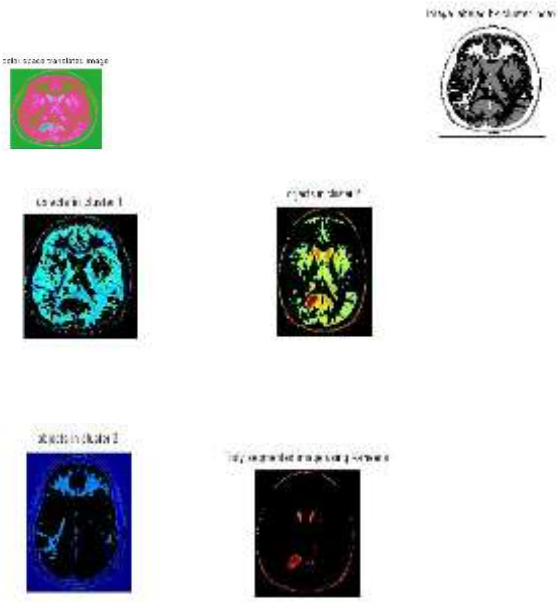
$$M = \frac{\sum x_i}{N_k} \quad ,k = 1, \ldots, K$$

Distance between each pixel and center of cluster is calculated by

$$D(i) = \arg\min \left\| x_i - M_k \right\|^2 \quad , i = 1, \ldots\ldots, N$$

Both steps are to be repeated till mean value convergence.

iv. USING K-MEANS




First image is Gray level image which is converted from input color image. Second image is converted into secondary colors. Fourth, fifth and sixth images are obtained after K-means clustering is applied. Seventh image displays the tumor in image. After thresholding method is applied, eighth and ninth images are obtained. Dilation is applied to image.

B. FUZZY-C MEAN SEGMENTATION

In this, information must be handled by giving the fractional participation worth to every pixel within the picture. The enrollment charge of the fuzzy place is in the scope among 0 to 1. In fuzzy segmentation fundamentally, an entity from single fuzzy set be capable of the same be an entity as of new fuzzy sets in something comparable depiction. For the most part, it is difficult to decide if pixels fit in to an area. It is due to blunt changeover by section borders. Fuzzy segment be done through an iterative enhancement of objective work, through the updatation of the participation capacity and cluster focus. Closer the information highlight the cluster community the additional potential its enrollment towards the specific community. Contrast with K-means, FCM gives better outcomes to covered area also, information point which has a place with at least one cluster. It is turning into a productive exploration region.

MATHEMATICAL REPRESENTATION

Fuzzy segmentation implies clustering of every

information point that has a place with above single cluster. It depends going on dropping the subsequent task.

$$Y_m = \sum_{i=1}^{N}\sum_{j=1}^{C} M_{ij}^{m}\left\|x_i - c_j\right\|^2$$

Where m- one real integer larger than 1,
M_{ij} -level of relationship of x_i within the cluster j,
x_i,_ statistics calculated within d-dimensional,
R_j - d-dimension midpoint of the cluster,
The renew of relationship Mij and the cluster midpoint R_j are given by:

$$M_{ij} = \frac{1}{\sum_{K=1}^{C}\left(\frac{\left\|x_i - c_j\right\|}{\left\|x_i - c_j\right\|}\right)^{\frac{2}{m-1}}}$$

$$R_j = \frac{\sum_{i=1}^{N} x_i . M_{ij}^{m}}{\sum_{i=1}^{N} M_{ij}^{m}}$$

The beyond procedure halts while,

$$\max_{ij}\left\{M_{ij}^{(K+1)} - M_{ij}^{(k)}\right\} < \delta$$

Where
δ= extinction value or unvarying among 0 and 1,
K= quantity of iteration steps.

ii. ALGORITHM OF FUZZY-C MEANS

1. Initialize M=[M_{ij}] matrix, $M^{(0)}$
2. On k-stage: estimate the middle vectors $R^{(k)}$ =[R_j] with $M^{(k)}$

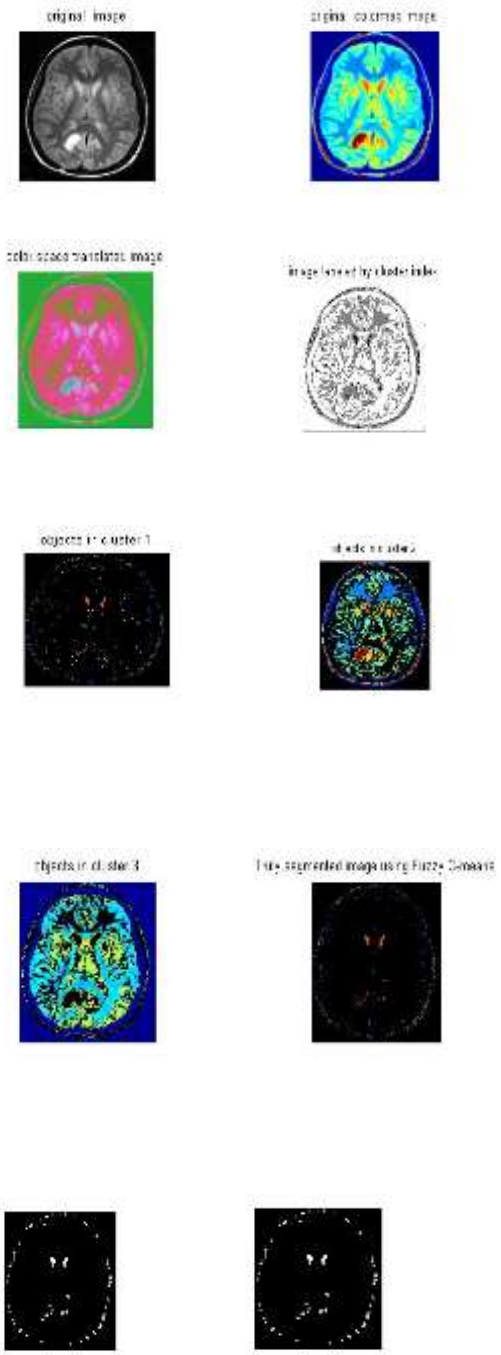
$$R_j = \frac{\sum_{i=1}^{N} x_i . M_{ij}^{m}}{\sum_{i=1}^{N} M_{ij}^{m}}$$

3. Revise $U^{(k)}$, $U^{(k+1)}$

$$M_{ij} = \frac{1}{\sum_{K=1}^{C}\left(\frac{\|x_i - c_j\|}{\|x_i - c_j\|}\right)^{\frac{2}{m-1}}}$$

4. Whether $||M^{(k+1)} - M^{(k)}|| < \delta$, in that case bring to an END; if not revisit toward stage 2.

iii. USING FUZZY-C MEANS



First image is gray scale image which is converted from input color image. It is then converted into secondary colored image. After applying FCM, image is divided into 3 clustered images, where 1 image indicates Tumor part, other indicates Brain part and other indicates background part. Finally, tumor is detected using FCM.

iv. CHARACTERISTIC REMOVAL

The characteristic removal is to take out the groups which illustrate the expected tumor by the FCM result. The removed cluster is specified to the thresholding method. A binary cover is used above the whole picture. This creates the dim pixel turn out to be gloomier as well as fair happen to be intense. During this process, every coefficient is evaluated through the threshold value which is set earlier. If the pixel rate is fewer compared to threshold charge, value is taken as 0. If pixel rate is larger compared to threshold charge, value is taken as 1. The thresholding technique is an adaptive process where merely individual coefficients whose magnitudes are higher than a threshold are preserved inside every mass. Assume a picture 'b' which has k gray stage. Set a threshold rate T which stays in the choice of k. This method is completely based on assessment. Every pixel within the input image 'b' is compared with T. Derived from comparisons, output can be decided. Let amount produced by binary image be 'f',

$$f(N) = \begin{cases} \text{'0', when b (N) <=T} \\ \text{'1', when b (N) >T} \end{cases}$$

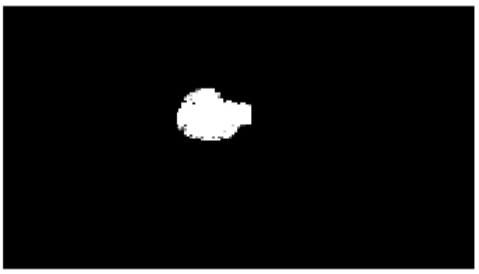


Fig: Extracted image using FCM Segmentation

If there are any cancer tissues that aren't detected by K-Means, they can be identified by using Fuzzy-C Mean.

IV. APPROXIMATE REASONING

During this pace, size or area of swelling is to be considered by using a method called Binarization, i.e., the picture has no more than two values either black otherwise white (0 or 1 respectively). Now 256x256 JPEG representations is a highest picture size. The dual image is able to be characterized as a outline of whole quantity of white and black pixels.

$$image\ , I = \sum_{W=0}^{255}\sum_{H=0}^{255}[f(0)+f(1)]$$

Pixels = Width (W) X Height (H) = 256 X 256
f (0) = colorless pixel (number 0)
f (1) = black pixel (number 1)

$$No\_of\_whitepixe\text{ę}P = \sum_{W=0}^{255}\sum_{H=0}^{255}[f(0)]$$

Where,
P = amount of colorless pixels (thickness*altitude)
1 Pixel = 0.264 mm

Region of tumor can be calculated by using following formula

$$Size\_of\_tumor, S = \left[\left(\sqrt{P}\right)^{*} 0.264\right]$$

Above value will be in mm^2
P= quantity of colorless pixels; W = thickness; H = altitude.

A.ALGORITHM

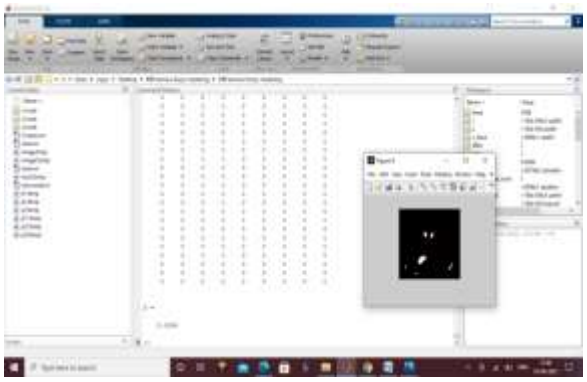
Algorithm for finding out the brain tumor:

i. Initiate the way
ii. Take Magnetic Resonance scanned image of brain in JPEG layout
iii. Confirm if the figure is in necessary arrangement or not, else displays a error
iv. If icon is in RGB design, convert to gray level image, otherwise go to subsequent pace.
v. Locate the border of the gray size figure
vi. Estimate amount of colorless points within picture
vii. Show the tumor volume and area
viii. Stop the process

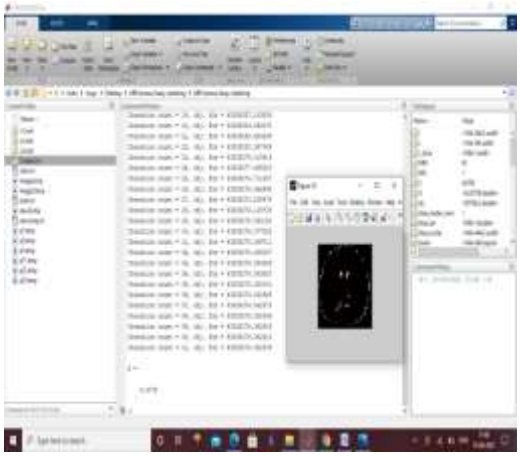
This calculation checks the RGB or gray balance photo; it changes over the picture into twofold figure by means of binarization procedure and identifies the boundary of cancer pixels in the double picture. Likewise this computes the extent of cancer by figuring the quantity of fair pixels (numeral 0) in twofold representation

V. RESULT

EXPECTED OUTCOME USING K-MEAN



EXPECTED OUTPUT USING FUZZY-C MEAN



VI. CONCLUSION AND FUTURE SCOPE

Tumors in brain may be of any type. K-Means algorithm is sufficient for non-cancerous type of

tumor in brain cells. Firstly noise in image if any is removed and noiseless picture is taken as key to the K-Means method and cancer is detected. For exact detection of cancerous type of tumor, Fuzzy-C means segmentation can be applied, and then thresholding is done to the output.

This method gives the accurate results when compared to other proposed methods. 3D slicers could be used in future with MATLAB for assessing the brain in 3D view.

REFERENCES

[1] S.Roy, et al., "A Review on Automated Brain Tumor Detection and Segmentation from MRI of Brain", arXiv preprint arXiv:1312.6150, 2013.

[2] P.Vasuda, S.Satheesh, "Improved Fuzzy C-Means Algorithm for MR Brain Image Segmentation", in International Journal on Computer Science and Engineering(IJCSE), vol. 02, no. 05, pp. 1713-1715, 2010.

[3] A.Mustaqeem, et al., "An efficient Brain Tumor Detection Algorithm using Watershed & Thresholding Based Segmentation", in International Journal of Image, Graphics and Signal Processing, vol. 4, 2012.

[4] IEEE-J.Selvakumar,A.Lakshmi,T.Arivoli;ICAESM, march30,31,2012-" Brain tumor segmentation and its area calculation in Brain MRI images using K-means clustering and fuzzy C-means algorithm."

[5] Rajesh C. patil, A.S. Bhalchandra, "Brain tumor extraction from MRI images Using MAT Lab", IJECSCSE, ISSN: 2277-9477, Volume 2, issue1.

[6] R. Preetha, G. R. Suresh, "Performance Analysis of Fuzzy C Means Algorithm in Automated Detection of Brain Tumor",IEEE CPS, WCCCT, 2014.

[7] Malathi Hong-Long , , "Segmentation C- Means Clustering With Spatial Information For Image Segmentation," Computerized Medical Imaging And Graphics 30 (2006) 9–15.

DESIGN AND IMPLEMENTATION OFSMOKE DETECTOR

A.Seemasadiya[1], Y.Pranavi[2], M.Vannurakka[3], G.Yaswanth[4]
[1,2,3,4] Dept. Of Electronics and Communication Engineering,
Srinivasa ramanujan institute of technology,Anantapuram, Andrapradesh

ABSTRACT:

Fire is the principal reason of wounds asserting valuable lives and things. The synthetic reaction among carbon-basically based absolutely substances in presence of oxygen creates combustible fume delivering a predictable vertical push in temperature and impacts in a hearthplace.The chief characteristics of chimney are it expands dramatically with time. Thus, very much planned recognition of hearth is basic for warding off an outrageous mishap.

The fire of hearthplace keeps on being an outrageous difficulty coming about because of people, and homes are at an unreasonable danger of hearthplace. As of late, people have utilized smoke alerts which least complex have one sensor to find hearthplace. Smoke is transmitted in various desk work in step by step presence. An unmarried sensor is definitely not a reliable way to find hearthplace. With the quick advancement in Internet innovation, people can show their homes distantly to choose the current condition of the house. By consolidating the continuous unique changes of assorted natural components, in contrast with the ordinary smoke alert, the precision and controllability of the hearthplace alert are extended, and the perception of the measurements grants clients to show the room environmental factors extra instinctively. The proposed contraption incorporates a smoke recognition module, a wi-fi discussion module, and keen character and insights perception module. As of now, the assembled ecological insights might be ordered into 4 situations with, is, normal air, water fog, kitchen cooking, and hearthplace smoke. Decreasing the recurrence of miscounts moreover approach improving the security of the person and things of the individual.

In this test, Fire and Smoke area gadget is advanced. It can experience smoke and the upward push in temperature and prepared individual through strategy for techniques for starting ringer besides transport bearings on automated terminal of android telecellsmartphone through wifi module. Fire dangers aren't exceptional. To stay away from hurt from hearthplace wounds, smoke alerts are presented at excessive security places. The gear used is Ardunio Uno, Temperature Sensor, Smoke sensor, Wifi Module and Buzzer. Programming utilized Arduino IDE and V-Terminal utilized as a cell utility. These smoke discoverors find smoke because of the reality the hearthplace wreck related conjure an early caution. This way, sooner than the hearthplace spreads to extraordinary added substances of the building, people might be emptied and countermeasures might be refined right away. In this test besides a smoke alarm has been planned. The smoke alarm progressed all through this test now presently don't altogether summons accessory alert however also turns on assistant sprinkler and a couple distinctive gases(CO2,CF3 BR ,Halon1211) just so smoke could be disposed of or diminished with on the spot activity.

INTRODUCTION

Automatic hearth place alarm can be a gadget designed to hastily discover fires and notify occupant that the constructing changed into ablaze. Every now and again, an overwhelming hearth place occurs by chance from a combustible inventory and hurriedly spreading from a little area to whole building. In this way, the chimney alert has been being used when you consider that the best Fire of London in 1667. There is sort of hearth place caution designs to be had in the commercial center like smoke and warmth finder which may be prepared to work precisely on recognizing a fire. Programmed sprinkler that upheld water-basically based absolutely hearthplace concealment

structures is some other by and large utilized hearthplace insurances contraption in over the top vertical push homes, store parcel and industrial facilities yet at this point not, at this point private house. The sprinkler will dispatch water while the finder detects any smoke and warmth over the limit esteem. The chimney caution will be initiated when the chimney is distinguished. There are not many types of robotized sprinklers that sound for assorted utility. The subtleties at the kind of sprinklers are consistently seen in. Presently a day, hearthplace alert designs have become increasingly more cutting edge and practically extra succesful and reliable. The previous examinations proposes the pristine design to find hearthplace fiasco through method of methods for utilizing a continuous video imaging technique upheld red, unpracticed and blue shading rendition to recognize a genuine hearthplace pervasiveness by means of method of methods for shooting measurements and investigated in PC . Plus, Bahrud by and large proposed to show the substance material of picture caught from a webcam and transferred the image to a site while a sensor recognized. A commonness of chimney. Aside from that, consistent with, the most straightforward hearthplace caution is routinely mounted through method of methods for the utilization ofinternational gadget for cellular (GSM) community. Nonetheless, the ones proposed hearthplace alert constructions in not ready to educate Fire and Rescue Office from the beginning genuine an optimal chance to prevent hearthplace from spreading. it is suggested that during 2016, pretty 6,000 homes in Malaysia have been gotten through technique for strategies for hearthplace yearly and killed in excess of 1,000 lives steady with estimation from Fire and Rescue Department . Steady with, paying little psyche to the presence of hearthplace alert, most direct 18.three you appearance after alarm viably frightened occupants. Because of this the current robotized hearthplace alert isn't by and large crafty sufficient to downsize the fireplace fiasco case.The inhabitants stay obscure that their homegrown is on fire especially when they might be a long way from their home. Besides, the defer of warning to safeguard branch can likewise moreover impacts in hearthplace quick unfurl to various homes. That is consistently even extra significant if the developing burning can be an unreasonable vertical pushed building. Consequently, a mechanized smoke identification device the utilization of Internet of Things (IOT) is proposed. The spotlight of the contraption is that the usefulness of device to advise the inhabitant moreover as Fire and Rescue Department when the chimney is recognized. This can reduce the likelihood of chimney escape, safe guard people and properties.

1. LITERATURESURVEY

For more than written history, hearthplace has been a stockpile of comfort and debacle for the human raceFire is quick, self-keeping up oxidation strategy in the midst of the advancement of warmth and light-weight in different powers. All hearthplace occurrences are routinely partitioned in a couple of techniques depending on the reason for hearthplace episode, anyway broadly there are types of flames, one is natural and distinctive is artifical. Timberland fires will be both due to natural or artifical reasons.

All private and non-private underlying flames are generally artifical., Tamil Nadu on sixteenth July 2004 finished in 93 passings of grade personnel youngsters. Awful hearthplace at thought about one of Kolkata's luxurious medical services offices (AMRI emergency clinic) killed at the very least 89 people in November 2011. The people in question - practically all have been victims in urgent consideration units - choked to death.

It can experience smoke, temperature, flame etc. and ship it to faroff tracking station via GSM to get considered necessary commands for the actuators.

Louie Giglio, Jacques Descloitres, Christopher O. Equity, Yoram J. Kaufman[2] gave an advanced hearthplace recognition set of decides that offers extended affectability to more modest, cooler flames moreover as a widely decline alert charge has been given. The creators utilized the hypothetical reenactment and exorbitant choice Advanced Spaceborne thermionic emanation and Reflection Radiometer (ASTER) scenes to choose the general exhibition in their

arrangement of rules. A sensor local area changed into utilized for genuine presence hearthplace

identification in (Veskoukis, Olma et al. 2007). Every sensor hub changed into prepared with a GPS and a thermometer. The creators suggested that every sensor hub must be snared on a tree with a pinnacle of at the very least three.5m. Since the instrument hubs can likewise be annihilated through method of methods for chimney, a dynamic steering convention changed into proposed. They

inferred that a sensor hub can insight and send measurements extra effectively.Moreover, they deduced that if three nodes display same location, fireplace will lots of correctly be detected. In the paintings accomplished viaway of means of Angayarkanni. K [4], a green woodland detection hired to discover woodland fires from woodland spatial statistics. This technique utilizes spatial insights handling and AI systems for the discovery of flames.The virtual pix are changed to YCbCr shading space, and afterward sectioned to recognize the chimney areas. Lim et al proposed a cutting edge system for private chimney discovery (Lim, Lim et al. 2007). They added metric of span message-apportion (IMR) and assessed their system misuse the IMR metric. They whole that the structure isn't in every case altogether significant for hearthplace-location yet in addition can be executed for a promising circumstance fiasco recuperations. Another paper proposed through method of methods for Joydeb Roy Chowdhury [5], delineates a Fuzzy Rule Based Intelligent Security to find the chimney. This paper, examines the instrument of hearthplace-getting technique, and put into impact through method of
methods for utilizing a chip essentially based absolutely equipment and brilliant hearthplace prevalence programming. The author also did a fluffy guideline fundamentally based absolutely shrewd early hearthplace discovery alert device. The primary caution earlier than the fault without any ambiguity will keep away from the catastrophe in opposition to the fault taking a few preventive measures.

1. HARDWARE

MQ-135

MQ-a hundred thirty five Module sensors has decrease conductivity in easy air. When the goal flammable fuel online exists, the sensor's conductivity is better close by feature the fueloline mindfulness rising. Convert substitute of conductivity to compare yield of fueloline mindfulness. MQ135 fueloline sensor has unreasonable affectability to Ammonia, Sulfide and Benzene steam, furthermore tricky to smoke and distinctive hazardous gases. It is with low worth and proper for assorted projects like perilous gases/smoke identification.

Features:

1. Extensive DetectingScope
2. Fast Reaction and Excessive Sensitivity
3. Stable and Long Existence Easy ForceCircuit
4. Wireless. Length: 35mm X 22mm X 23mm (Duration X Width X Top)
5. Operating Voltage: Dc Wi-FiV
6. Signal OutputInstruction.
7. DualSignalOutput(AnalogyOutput,AndExcessive/Low DigitalOutput)
8. Four-2v Analog Output Voltage, The Higher the Concentration The Higher the Voltage.

Applications:

1. Domestic PollutantsDetector
2. Commercial Pollution Detector
3. Transportable Pollutants Detector

ESP 8266 MODULE:

The ESP8266 WI Fi Module can in like manner be a free SOC with included TCP/IP
show stack that could give any microcontroller get section to on your Wi Fi social class. The ESP8266 can either working with an application or offloading all Wi Fi arranging limits from some other application processor.

Each ESP8266 module comes pre-redone with an

AT request set wirelessrmware, that suggests, you will when in doubt append this in your Arduino gadget and gather about the most outrageous whole Wi Fi-limit as a Wi Fi defend gives (it is scarcely out of the box)

Fig 2: Wi-Fi Module

NOTE:
The ESP8266 Module isn't always able to five-3V good judgment moving and might require an outside Logic Level Converter. Please do not strength it immediately out of your 5V dev board.

Power supply:
Force supply is a reference to a wellspring of electrical force. A contraption or framework that plans electrical or different sorts of energy to a yield weight or collecting of loads is known as a force supply unit or PSU. The term is most generally applied to electricalenergy supplies, less constantly to mechanical ones, and occasionally to others.
This force supply parcel isneeded to change over AC sign to DC sign and to decrease the plentifulness of the sign.

yet the required is DC voltage (no rehash) with the plentifulness of +5V and +12V for different applications.
In this part we have Transformer, Bridge rectifier, are connected progressively and voltage controllers for +5V and +12V (7805 and 7812) using a capacitor (1000µF) in identical are connected comparably as shown in the circuit layout under.
Each voltage regulator yield is again isassociated with the capacitors of characteristics (100µF, 10µF, 1 µF, 0.1 µF) are related similarly through which the
looking at yield (+5V or +12V) are contemplated.

BUZZER:
A buzzer/beeper may want to also be mechanical, electromechanical, or piezoelectricandit gives output which is audio in nature. Makes use of-alarm tool, timers, click on or keystroke which may be an affirmation of user input. Buzzer associated with Arduino gives us an alert sign

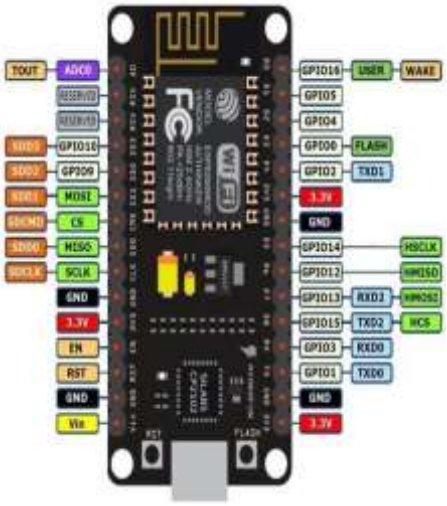


Fig-3: Buzzer

In-side the product framework gives benefits asfaras security, capacity to respond. Other than that, IOT prepared to work at whatever point with the association relationship with record all the data in Favorite stage. The customer can screen wherever and at whatever point whenever they're distant from their home. Such thing used to perceive this of smoke just as used for expectation against fire scene. Later on, it's proposed the motorized smoke caution with Favorite stage are often advertisement libbed using future development like distant sensor so as that the customer prepared to screen viably without permission to the Favorite stage. In extra, it'd be satisfactory if the customer can change the affectability of sensor and edge regard without program it.

4. RESULTS:

The programmed smoke location gadget is tried at a neighborhood in the town home to mimic genuine room climate and in this manner the hole is given four Mbps TM development of net association.A neighborhood for the length of a customary circumstance (with out existence of smoke), the smoke level might be a more modest sum than wi-five ppm which depends upon at the MQ2 sensor affectability in smooth air factor opposition. The smoke esteem starts as lower smoke presence. Along these lines, the sting stage has been settled on for this trial is 80 ppm and 100 ppm to gauge

how quickly the

MQ-2 smoke sensor can detects and provoke the signal.In extra, the charge of 80 ppm and 100 ppm can welcome on to hack, sore eyes and hard relaxing. Proposes the exploratory outcome accumulated from three consuming materials.

5. CONCLUSION

Modified smoke caution utilizing IOT permits customer see the room's smoke condition whenever they're faraway from their home through the Favorite stage by utilizing Personal Computer, Personal Computer or compact. All the data are recorded in data move through IOT medium.

At the point when the fireside is recognized, the admonition message is having the chance to be dispatched off the fireside and Rescue Department to interest for rescueaction. To this point, edge an impetus for the automated smoke.

REFERENCES:

[1] M. D. Stephenson, automated wi-fireplace-Detection

[2] structures, world wide magazine of Electronics & power,vol. 31, pp. 239-243, Mar1985.

[3] Crytrontechnologies,ESPWiFi protect-user guide Rev-2.zero,pp,1-17,April 2016.

[4] wi-fiwiwireless safety-widespread

Face Recognition Based Smart Attendance Management System

C.Thippeswamy[1]C. jahnavi[2]D. Geeta Maduri[3]P. Chandu[4]D. Jaya Bhargav[5]

Assistantprofessor[1],UGScholars[2,3,4,5]

[1,2,,3,4,5]DepartmentofECE,Srinivasa Ramanujan Institute Of Technology,Anantapuram,AndhraPradesh

Abstract— Attendance is a tool to record the regularity of a student, teacher, and employee on a day to day basis. When students improve their attendance percentage, they improve their knowledge and improve their academics results. However, the manual attendance process is very time consuming and proxy. We need a system which may deal with the time, proxy attendance and basically a system which replaces the current manual attendance management system. A lot of time is spent on attendance time sheets. Hence, an effective replacement of manual attendance is required which will reduce the manpower and it also makes the attendance process faultless.

Biometrics is certainly the most secure and good genuine form of credentials,it is very hard to imitate and proxy because biometrics are unique for everyone. Basically, what the biometric does is, it makes sure that aindividual is present at that time, that is nothing but we cannot use proxy result. It will make the attendance system flawless. Face, Iris and fingerprint are the widely used biometrics for attendance Management system. It can used for security, authentication, identification, and has got many more advantages in many applications. Some of them use frontal faces, which is again a prolonged task, but none of them commented on developing an application layer for the end users.

This project aims to design a robust face recognition based attendance system using deep learning. The purpose of this system is to build an attendance system which is based on faced recognition technique. The major steps in this project are face detection using Convolutional Neural Network (CNN), face recognition using FaceNet Model and design of android application for the end user. Face detection is done by employing facial feature extraction and mapping. This project aims to provide an attendance solution for schools, educational institutes and hospitals. The proposed method obtained a real- time accuracy of (99.63%) which is better than that of the existing model.

Keywords— Face Recognition, Face Detection, Attendance system, Convolutional Neural Network (CNN), FaceNet, android application.

I. INTRODUCTION

Face recognition is an effective system for attendance management. The good thing about biometrics is that you don't need to remember your passwords and no problem with the remembering power. Because you don't need to remember how your face looks, it's part of who you are. This system can be easily be deployed in schools, colleges and educational institutes for attendance management system.

The whole project can be divided into three major steps which include face detection, face recognition and android application. Face detection can be achieved using a deep learning method that is Convolutional Neural Network (CNN). For facial RecognitionEach face is mapped to a 128 byte array of facial features using FaceNet Model. A local database of the students and their facial features is required to detect and identify their faces. When a student comes in front of the system the camera takes a photograph and identifies the face in it followed by the generation of 128 byte facial features array, this array data is the matched with the existing students data in the local data and the name is retrieved .The attendance status of the person is then send to the cloud that is done by using the Google spreadsheets and a mail is sent to the student regarding his attendance for that session. The student can also monitor his attendance record in the android application. The enrolment of new students is also possible. Whenever a new student is enrolled his name and email address are stored in the cloud that is done by the Google spreadsheets along with his photo in the local database. An email

regarding his credentials for the application is also sent.

The proposed system is developed using OpenCV, Ananconda3 Spyder and email where we can check the attendance status in real time. For the cloud storage Google sheets are used and an android application for the end user is developed using MIT app inventor.

I. LITERATURESURVEY

Visar Shehu, A Dika [9] proposed "Using real time computer vision algorithms in automatic attendance management systems,"Information TechnologyInterfaces
(ITI), 2010 32nd International Conference on, pp. 397–402, 2010. In this paper they used Using HAAR Classifier and computer vision algorithm to implement face recognition.The system integrated with the existing system that can use the existing feature fromLearning Management System.

In [10] AalamGumber, NavneetKaur "Face Recognition Based Automated Attendance Management System using Principal Component Analysis" , International Journal of Science and Research (IJSR) , Vol 4, Issue 6, June 2015. Using PCA to train and reduce dimensionality and ANN to classify input data and find the pattern. The accuracy is high due to the combination PCA with ANN. ANN use for classificaton is more accuracy than PCA with Eigenface.
N Kar, MKDebbarma,ASaha [11] stated a model as "Study of Implementing Automated Attendance System Using Face Recognition Technique," International Journal of Computer and Communication Engineering, vol. 1, no. 2, pp. 100–103, 2012 Using Eigenvector and Eigenvalue for face recognition. The system have prevented the fake attendance due to the implementation clock time in and time, which used for checking the student presence inside the class for the period ornot.

II.EXISTINGSYSTEM

Face Recognition based smart attendance systemusing Raspberry Pi

[12]This project describes the method of detecting and recognizing the face in real-time using Raspberry Pi. Raspberry Pi usage helps in minimizing the cost of the product and the usability as it can be connected to any device to take the attendance. It uses modified Haars Cascades and LBP histograms for face recognition and MYSQL to upload database. It has five modules-Face Detection, Face Preprocessing, Face Training, Face Recognition and Attendance Data base. Camera captures the Image and referred to the database, if matched then attendance is taken otherwise it marks absent.

Fig1: Existing model Block diagram

III. DRAW BACKS IN EXISTINGSYSTEM

The existing model does not provide an application layer for the end user and the system is prone to loss of data. The student does not have any real-time information regarding his attendance status and his attendance record is also not known. The algorithm that the existing model used Haars cascade which is less accurate and training the pictures takes much time and very difficult to train the cascade and it is sensitive to location of an object in an image and too much computation.

IV.PROPOSEDMETHODOLOGY

Biometric is a powerful weapon for the person authentication and security. Facial Biometric is already quite accurate in measuring unchanging and unique ratios between facial features that identify you as you. It's like a fingerprint. If we use this facial biometric for our attendance management system then it is very prone for students and faculty.
The proposed model provides real-time acknowledgement of the attendance status to the student and an email is sent regarding the same. A cloud database also gets the attendance status so that the admin can manage the data. An android application is developed for the end user whereby he can check his attendance data.

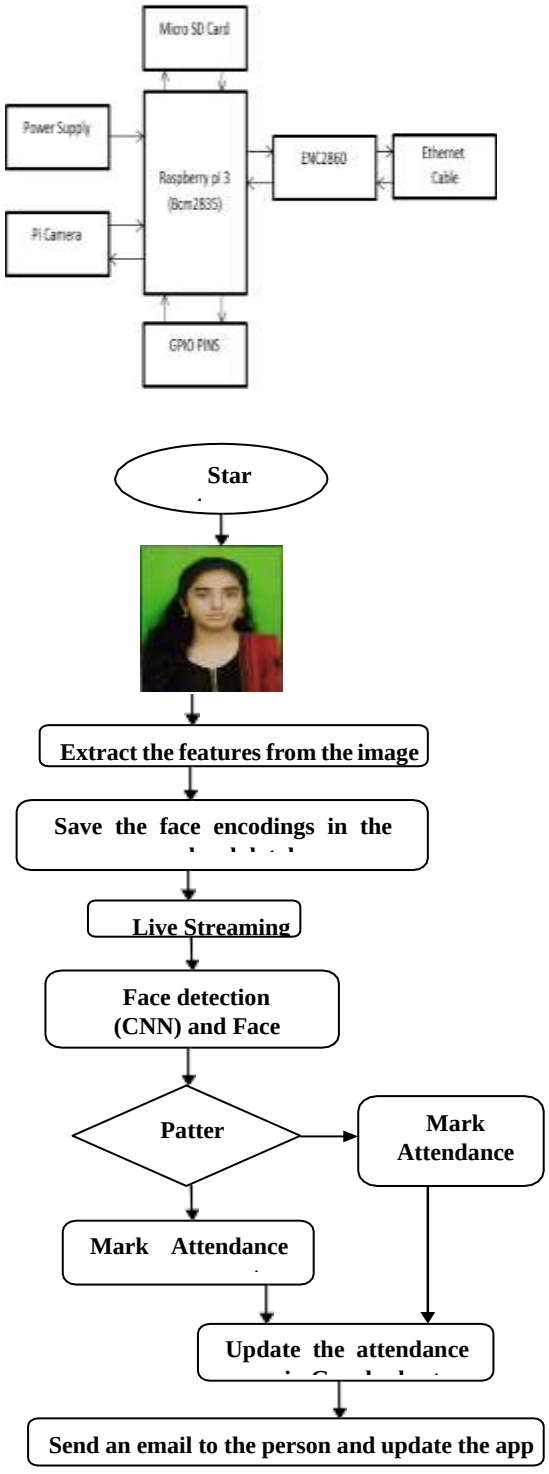


Fig2: Flow of the proposed model

Here the proposed use Anaconda3 python for creating virtual environment and for editing the algorithm through spyder editor. It uses the OpenCV for computer vision and the face detection and face recognition is done by Convolutional Neural Network (CNN) and FaceNet Group of student image is captured and also the recognized on an individual basis.The images are going to be captured via web camera and also the recognition algorithmic program to be performed. Once the recognition done faces matches with the face encoding data with the database. If match found, attendance will be marked for the respective student at the end of the session in Google Sheets and also a mail is send to the respective student regarding his attendance.

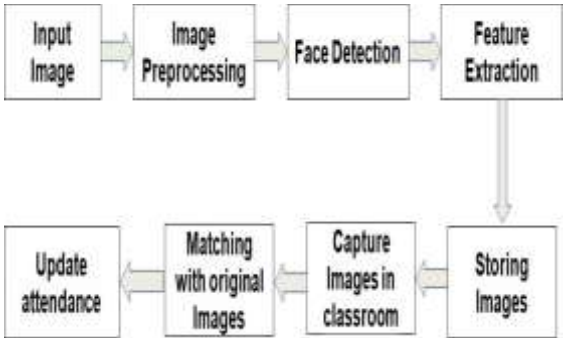


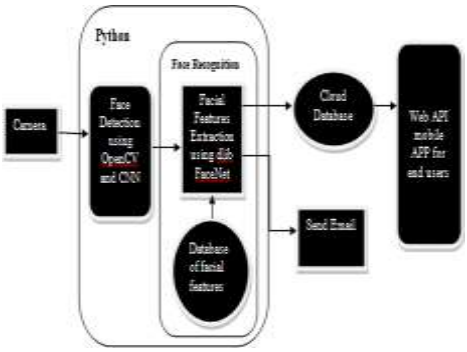
Fig3: Block diagram of proposed model
This system consists of four phases- database creation, face detection and face recognition, Real time Acknowledgement with Email and Application layer.

Flowchart:

atabase is created by the images of the students in class. Face detection and recognition is performed using Convolutional Neural Network algorithm and FaceNet respectively. Attendance will be updated and student will be provided with the MIT app for Attendance verification.

VI IMPLEMENTATION

6. a Database Creation:
The student should be enroll themselves before the attendance. This can be done via camera, the camera captures the photo of the student and detects the face of the student by Convolutional Neural Network (CNN) and facial features are extracted and face encoding of that particular student is stored in the local database. Along with his name and email and otp for the app are updated in Google sheets and email will be send regarding the appotp.



6. b Face detection and recognition:

The face recognition is done by facial feature extraction and matching. Photographs and the facial features of the faces that are to detect are pre-stored in the local database. Whenever new faces are detected a 128 byte array of their facial features is created, this data is the matched with the existing database and the name of the person is displayed. The matching process is done by calculating the Euclidian distance between the required data and theexisting data and theminimum of the Euclidian distance is taken. The minimum distance is compared with the predefined threshold if it is less that the threshold the name of the person is returned.

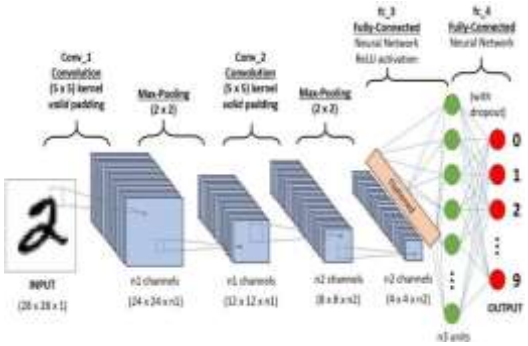
6 .c Real-time acknowledgement with email:

The returned person's attendance status is updated in the Google sheets. The email address corresponding to the student is fetched from the server and an email regarding the attendance status along with the date is sent to the user.

6. d Application layer:

An android application is developed that can show the attendance record of a particular student. The app uses a login page for the authentication of the user, once the user logs in it fetches the data from the Google sheet and displays it in a list view along with the total number of lectures attended and attendance percentage. edges, curves, nose ear, and mouth within the image.ANN attempt to learn a function by taking a combination of all of the functions at each stage in the network. Convolution is a linear operation, so combining many convolution layers will still only allow us to learn a linear function.

VII ALGORITHM



7.1 CNN is a kind of deep neural network were introduced to solve the problems of ordinary neural network like MLP. A CNN consists of one or more convolution layer, sub sampling or pooling layer followed by one or more fully connected layers as depicted in Figure.1. Convolution layer performs the convolution operation on the image pixels within the kernel or receptive field and kernel weights.The output of the convolution layer is the sum of the pixel values within the kernel multiplied by the Corresponding kernel weight. . It is used to detect the presence of the feature like This unfortunately is not adequate for most real-world tasks. To tackle this problem, non-linear function is introduced. In CNN, this is done by applying a non-linear function to each of the feature maps produced in the convolution layers.

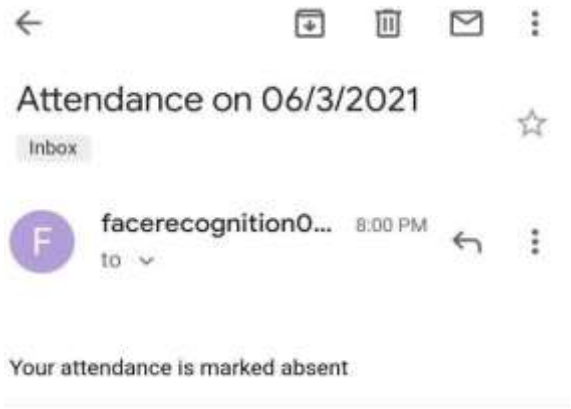
The most common non-linear function used is the Rectified Linear Unit (ReLU).

It is an element-wise operation which replaces negative values with 0.

It's one of the most widely used non-linear functions in neural networks because it has some nice properties which help to avoid problems such a gradient saturation during training.

Pooling layers are a form of down sampling which usually follow convolution layers in the neural network. Its function is to progressively reduce the spatial size of the representation to reduce the number of parameters and computation in the network. Pooling layer operates on each feature map independently. The most common approach used in pooling is max pooling. Fully connected layer is the last layer of CNN. It allows the network to learn a

function which maps the final layer of high-level



feature maps to each of the imageclassifications.
Fig4: Architecture of CNN

7.1 FaceNet:

FaceNet uses a deep convolutional network. **FaceNet**is a deep neural network used for extracting features from an image of a person's face. **FaceNet**takes a person's face and compresses it into a vector of 128 numbers. **FaceNet**is trying out many
different combinations of these features during training until it finds the ones that work the best.

Fig5: Architecture of FaceNet

Our network consists of a batch input layer and a deep CNN followed by L2 normalization, which results in the face embedding. This is followed by the triplet loss during training. The Triplet Loss minimizes the distance between an anchor and a positive, both of which have the same identity, and maximizes the distance between the anchor and a negative of a different identity.

VIII RESULTS AND DISCUSSIONS

For face recognition implementation, the following results were obtained –
Software results:

8.1. Face detection and enrolling theperson

Enrolling the person via camera in spyder editor in a virtual environment created by the Ananconda3python

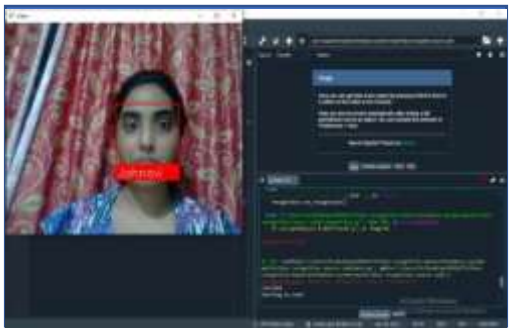


Fig6: Enrolling the image viacamera

8.2. FaceRecognition

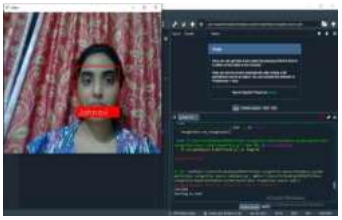


Fig7: Detected image with a bounding box around the face

On carrying out the recognition process, feature comparison takes place with respect to the features stored in the database. The face is displayed along with corresponding name of the student and used for marking the attendance.

8.3. Updating the attendance in Google sheets

After the recognition the faces that were detected are marked as present and rest will be marked as absent in the Google sheets

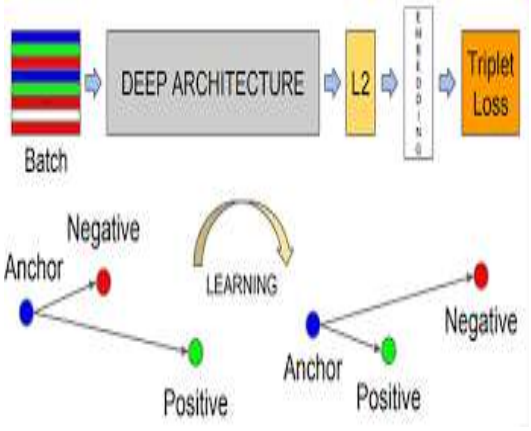


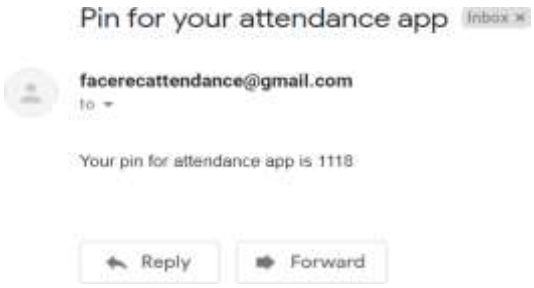
Fig8: Google sheet as cloud database

8.1. Pin for your attendanceapp

Pin for the attendance app is mailed to the respected students individually for each and every person who are enrolled. The generated pin for attendance app is helpful in the app access to the respective student. Students have to download the MIT app Inventor from Google meet and scan the QR code for the app to download.

Fig9: Mail regarding the pin for newly enrolled student

8.4. Real time acknowledgment throughmail



The students get the mail regarding their attendance attendance in that session, a mail will be notified to them in a real time acknowledgment for the verification of their attendance.

Fig10: Mail regarding the attendance status.

8.6. Results from android app:

Fig11: Login page

Fig12: Signup Page.

IX. CONCLUSION

In our study, we have introduced an approach for detecting a person is attending to class or not using Face net model. It performs really well in images and our detection results were also quite good. A robust facial recognition based attendance system is made for deployment in schools, colleges and educational institutes. In future, the recording of biometrics, such as fingerprints, iris pattern or facial image means that we will have a much stronger way of linkingidentitytotheperson.AnationalIDcardwill bearobust,secureway to establish that identities are real, not fabricated. This project eliminates the disadvantages of the exiting model with high accuracy (99.63%). With this we can take the attendance in our classrooms colleges and hospitals as well.

REFERENCES

[1] Shubhobrata Bhattacharya, Gowtham Sandeep Nainala, Prosenjit Das and AurobindaRoutray, Smart Attendance Monitoring System (SAMS):A Face Recognition based Attendance System for Classroom Environment, 2018 IEEE 18th
[2] International Conference on Advanced Learning Technologies,2161
[3] Aftab ahmed, Jiandongguo, Fayazali, Farha deeba, Awaisahmed, LBPH Based Improved Face Recognition At Low Resolution, International Conference on Artificial Intelligence and Big Data, 978-1-5386-6987-7/18/$31.00 ©2018IEEE
[4] Hemantkumar Rathod, Yudhisthir Ware, Snehal Sane, Suresh Raulo, Vishal Pakhare and Imdad A. Rizvi, Automated Attendance System using Machine Learning Approach, 2017 International Conference on Nascent Technologies in the Engineering Field (ICNTE-2017), 978-1-5090-2794- 1/17/$31.00 ©2017IEEE.
[5] Poornima S1, Sripriya N2, Vijayalakshmi B3,Vishnupriya P4, Attendance Monitoring System using Facial Recognition with Audio Output and Gender Classification, IEEE International Conference on Computer, Communication, and Signal Processing (ICCCSP-2017),978-1-5090-3716-2/17/$31.00 ©2017IEEE

DESIGN OF RELIABLE SOCS WITH BIST HARDWARE

DR N.KHADAR BASHA, BALA PRANEETHA P, GANESH E, JAYASREE K, KALYAN SAI
Electronics and Communication Engineering, Srinivasa Ramanujan Institute OfTechnology, Rotarypuram ,Anantapuramu,515701,Andhra Pradesh, India

ABSTRACT:

This paper presents the planning of dependable SoCs with BIST Hardware and programming carried out with Machine Learning Predictor. The proposed framework utilizes the BIST sort of innovation whichcan check if any issue present in the circuit. Here, in our proposed stream of the model, we convert ATPG delay test designs into LBIST examples to enact close basic ways in the field by tracking down the necessary example for the LFSR register. The gate overlap and path delay aware algorithm calculation are utilized to upgrade the arrangement of examples and these are givento the circuit to be tried and check malfunctionality of that circuit. The Speed, time, and power utilization will be decreased in this framework. We complete our proposed framework on Soc plan and yield executed itsexactness.

Keywords: BIST Hardware,LBIST,LFSR, gate overlap and path delay aware algorithm

INTRODUCTION:

A BIST is a technique which allows a machine into test. BIST has been intended to meet necessities like High dependability, low inactivity in cycle and minimal expense of testing. The reduction in Intricacy and no need of using any external source for test can be decreased by 2 different ways:1) Reduces the test cycle length 2)Reduces the Intricacy of test arrangement by diminishing the quantity of input-output flags that should be driven under test control. Test pattern Generator and output analyzer are put on similar chip to

continue the testing interaction procedure. As difficulty of circuits goes on increasing day by day, numbers of faults are producing in the designs so that it is compulsory to find out on the chip.

In the present quick world, there are heaps of new specialized progression going through at a quick speed where the circuits are been planned in such a way in which, it could play out any sort of action with a decreased measure of speed, and the size of the circuit is definitely being decreased. A little chip is playing out a lot of numerous tasks. Since these circuits arebeing intended to perform more perplexing, the development of these circuits is going on by utilizing a huge number. At the point when these circuits are being utilized a ton ordinarily, there are numerous odds for the circuit to get broken down because of different specialized reasons. So to stay away from those imperfections in the circuits we may utilize the underlying self-testing circuits. By utilizing BIST sort of circuits this issueis run-overloaded and the blemish is been recognized and is repetitive and an electivecircuit is been utilized and the specific capacity is handled. Utilizing Built-In Self Testing is that these circuits are truly productive in nature and less tedious. The simulation of this process has been finished by using Xilinx ISE tool and modelsim tool. In this tool we may simulate, synthesis, and know the time and power consumed by our design.

22. LITERATURE SURVEY:

M. Sadi, G. Contreras, D. Tran, J.Chen,

L. Winemberg, and M. Tehranipoor, proposed BIST-aided dependability on the board of SoCs using on-chip clock clearing and AI. To precisely foresee the disgrace because of maturing systems inan SoC at run-time by using the current LBIST equipment and programming carried out Machine Learning classifier.

Utilizing an imaginative strategy, we convert ATPG-created change delay pattern designs into LBIST designs, and the comparing reactions are used in fostering the indicator. An gate overlap and path delay aware algorithm example determines the calculation select the highlights for the more useful. Utilizing clock swapping, LBIST can catch the maturing impact on focused ways. The aging effect of AI is then used to enact countermeasures to cure the debasement in the field.

23. A.Vijayan, A.Koneru, S.Kiamehr, K.Chakrabarty, and M. B. Tahoori, proposed "Fine-grained aging-induced delay prediction based on run-time stress monitoring,"

Chip health observing is, hence, important to follow delay changes for every chip premise over the chip lifetime activity. In this research, we present, in light of AI techniques, a low-cost, fine-grained responsibility induced pressure checking strategy to precisely predict maturing prompted delay. To reduce the cost of observing the responsibility, we add reality inspection of specific flip-flops into the runtime checking framework. The expectation model is prepared disconnected utilizing support-vectorrelapse and executed in programming. This methodology can use proactive variation strategies to alleviate further maturing of the circuit by observing maturing patterns.

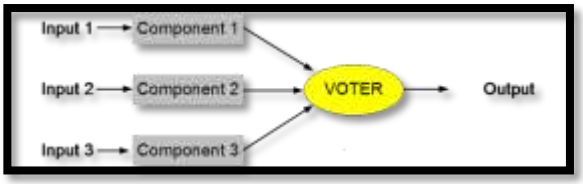
24. EXISTING SYSTEM:

TRIPLE MODULAR REDUNDANCY:

Triple Modular Redundancy whenit comes to computing it is known as Triple Mode Redundancy where 3 systems(or) Machines may accomplish the operation and the output of that task is carried out by a majority voting system to generate one output. If failure of all the 3 machines were occupied, then other 2 machines will correct the result and improvement of the fault

This TMR concept may be performed to other forms of redundancy, such as in software redundancy which commonly found in fault-tolerant systems. It is a procedure for producing the tolerance against the single equipment partof failures in Tripling of that segment called Triple Modular Redundancy (TMR).

Block diagram:



Description:

In this system, TMR 3 type of same identical logic gates is used to perform the same set of functions. If there were no failures in all circuits may get the as same output. But if there occurs a failure, the result of the entire circuit may be non-identical/disparate .Here in this TripleModular Redundancy, voter plays aprominent role, it is also called a majority logic gate where it is used to determine which one of the circuit output is correct.

There will exist some cases

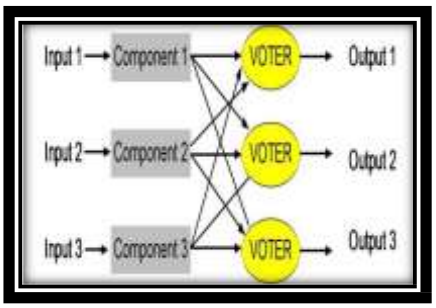
i. If none of the circuits has failures, then all the identical circuits will generate the result as 1 and the voting machine also provide the output value as 1

ii. If any one of the circuit in that system fails and produces the result as 0, while are other circuits are performing well and generates the result as 1, then voting machine decides and produce the output as 1

iii. Also, comparably for the situation when the Boolean capacity processed by 3 identical circuits has output value as 0, consequently the voter gate output isdestined to be right as long as close to one of the 3 identical logic circuit has fizzled.

For a TMR framework, with a single voter of reliability, the probability of being correct can be demonstrated as $R_{TMR}= R_V (3RM^2-2RM^3)$.

25. Triplicated TMR:



In the normal TMR, if the single votermachine failed, then the entire circuit may

get worthless. To avoid this issue of the danger of failures of the voting mechanism itself, the introduction of this Triplicated TMR takes place. The disadvantages of this TMR process is time, speed and power consumption is more. Exact detection of fault may not have occurred.

26. PROPOSED SYSTEM:

Block diagram of our system:

DESCRIPTION:

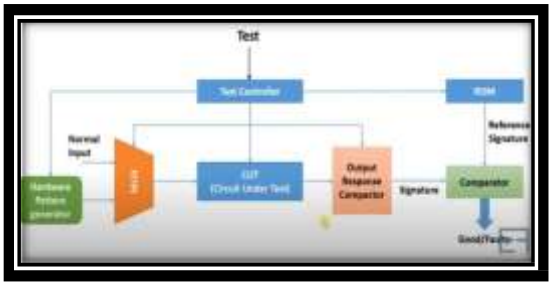
Hardware Test Pattern Generator: This module implements the test patterns whichare useful to detect the faults and propagate the effects to the results of circuit we tests. As the test pattern generator is having a limited area, so it may be a circuit. Storing of the test patterns and implementing of those patterns will be obtained by using ATPG algorithms. In this pattern generator, Gate overlap and path delay aware algorithms are used to optimize the seed patterns given to circuit under tests (CUT).In this hardware pattern generator ATPG patterns are converted into LBIST patterns

Input Mux : Multiplexer is a device which selects from many inputs to give a single output based on the selection line.In this architecture, test controller is actinglike a selector. When the test controller is enable, the input from pattern generator is selected by mux or if it is disabled, normal input is selected by the mux.

Output Response Compactor: The compactor's response is used to compress the CUT's outputs in a lossy manner. In BIST, the CUT output is compared to predicted response called Golden Signature. In the case of off-line testing, and the error is recognized if the CUT output doesn't match the expected result. Expected output results can't be predicted, just as they cannot predicted for test pattern generator and also cannot be storedspecifically in memory and when compared to CUT's responses

The CUT's output patterns to the test patterns are almost compressed into signatures that have been compared with the expected signature for the error-less circuit. As a result, pass/fail identification is frequently made up of set of bits of data containing the BIST sequence signature accompanied by a single pass/fail bit. It's important to note that the term, Compaction is used instead of compression which implies no loss of information whereas most ORA techniques indicate some loss of information, so Compaction is the moreaccurate phrase.

ROM: It will saves the golden signature patterns which are ideally stored in on-chip memory and this patterns are needed to be compare with



compressed CUT patterns.

Comparator: Comparator is a devicewhich is used to compare two results and gives an output. In this architecture, an ideal response saved in

on-chip memory is compared with compressed responses obtained from CUT.

Test Controller: The test initiates the BIST procedure to control the BIST

whenever an IC is powered up, if fault is detected, the status line rises high when the test is completed. After that the controller uses the multiplexer to interconnect standard inputs to CUT, began to prepare to use. The Hardware testpattern generator and response compactor are the most critical of the components mentioned above. The normal digital blocks are included in this.

The various stage of process can be done in this system as follows:

Stage-1: **Identification of High Usage Critical/Near-Critical Paths**

Two criteria are used to determine the paths that are most likely to become critical. Critical pathways are those thatdepreciate by 12.5% over the expected lifetime. The switching rate or usage factorhas a direct impact on hot carrier depreciation. The switching rate at the output of the nth on-path gate is defined as the path's high-usage factor. P1 is a list of all the pathways that meet these two requirements. The step is to analyze critical pathways that could become critical at any point throughout the chip's lifecycle, despite of workload activity patterns.

Stage-2: **Path identification of LBIST**

1) **Generation of ATPG patterns:** The exciting paths are usually shorter and avoid the longest paths,
i.e. the speed-limiting critical/near- critical paths. We employed the small-delay defect (SDD) transition fault detection test methodology to address this issue, which systematically targets longer pathways. All pathways with a

delay greater than d_{cutoff} are examined for the SDD pattern in our scenario.

2) **Seed extraction of LBIST:** Methods for obtaining seeds from ATPG patterns have been developed. The algorithm assumes that the SoC already has LBIST architecture for in-field testing. An initial set of ATPG patterns for the complete fault list is constructed to provide seeds for SDD TDF patterns. To find the solution that meets all of the ATPG care-bit constraints, a binary tree search algorithm is used. Each ATPGpattern in large benchmarks and sophisticated designs often has a significant number of care-bits. In these circumstances, it generates numerous sets of ATPG patterns using partial ATPG patterns. Each pattern has fewer detected flaws than the others, and each pattern has the same collection of problems. All of the seeds are then saved on the chip and can be usedat any time. The process iterates, creating new patterns for the remaining "uencoded" defects,which are then reproduced in the same manner as the originalpatterns. This method is computationally costly and could take a long time to complete.

SIMULATION AND RESULTS:

In this project Ripple carry adder is used as CUT. Xilinx and Modelsim tools ad used to simulate the process and result obtained as shown in below figures.

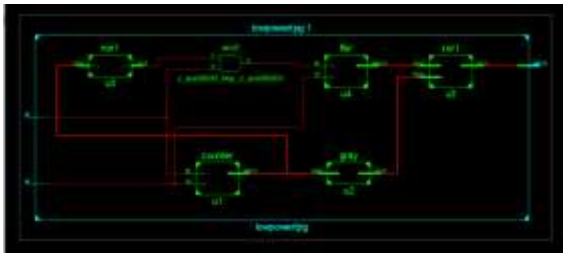
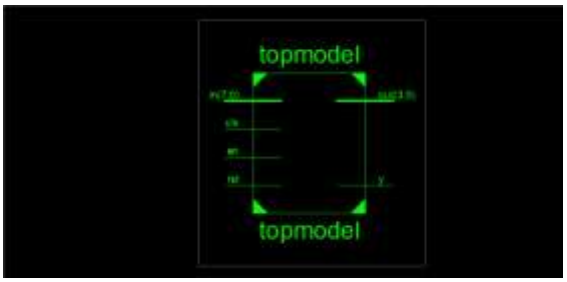
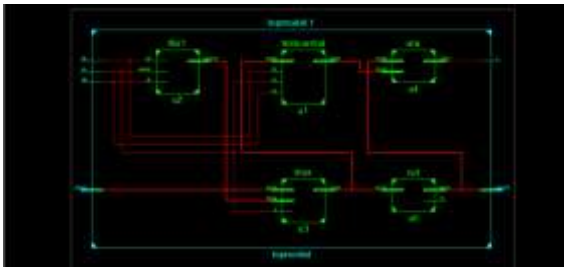


Fig: low power schematic diagram





OUTPUT:

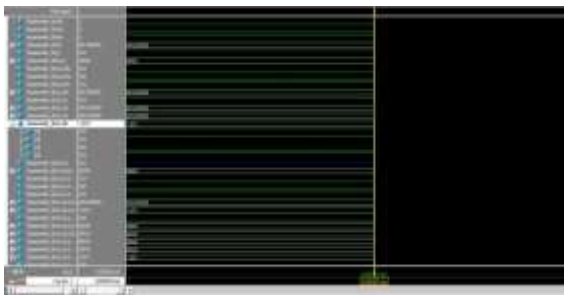


Fig. Modelsim report

For the pattern 1101, the output getting is 1→ if result is 1, then the test is failed or ifresult is 0, then test is passed

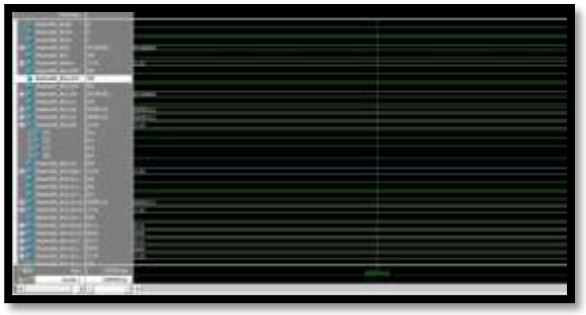


Fig. Modelsim report

For the pattern 1110, the output getting is 0→ if result is 1, then the test is failed or ifresult is 0, then test is passed.

27. CONCLUSION:

We've shown how to collect delay degradation data from high-usage critical/near-critical paths in the field using the SoC's existing LBIST hardware. The proposed approach enables ongoing infieldwork. Over the course of a chip's lifespan, timing reliability management is performed. We demonstrated that the suggested methodology enables for accurate and fine-grained infield ageing prediction utilising simulation results and analysis. Furthermore, the expected findings can be used to activate adaptive approaches to correct timing issues.

REFERENCES:

- Mano, M. Morris,. Digital Design, 2/e. Prentice-Hall of India . 1995.

- P. H. Bardell, W. H. McAnney, and J. Savir, Built-In Test for VLSI: Pseudorandom Techniques. New York : John Wiley and Sons, Inc., 1987.

- R. A. Frohwerk, “Signature Analysis: A New Digital Field Service Method,” Hewlett-Packard Journal, vol. 28, no. 9,pp. 2–8, May 1977.

- S. Z. Hassen and E. J. McCluskey, “Increased Fault Coverage Through Multiple Signatures,” in Proc. of the International Fault-Tolerant Computing Symp., June 1984,pp. 354–359.

- M. Bushnell and V.D. Agrawal, “Essentials of Electronic Testing for Electronicsl, Memory & GroupedCircuits”, Kluwer Academic Publishers, 2000

https://nptel.ac.in/content/storage2/courses/108105057/Pdf/Lesson-40.pdf

PREPROGRAMMED GATECONTROL SYSTEMBASE DONVEHICLE REGISTRATION PLATE IDENTIFICATION(VRPI) USING RASPBERRYPI 3 MODELB

.P. Deepthi Jordhana[1] T. Krupa[2] N.Bhavana[3] M.Narasimhulu[4]

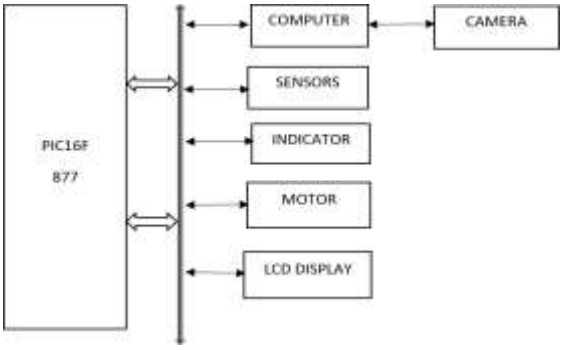
S.Javeed Basha[5] Professor[1], UG Scholars[2,3,4,5]

[1,2,3,4,5]DepartmentofECE,Srinivasa Ramanujan InstituteofTechnology,Anantapur,

AndhraPradesh

ABSTRACT - WholeworldisrunningbehindTIME.Automationis a solution to perform task in lesser time andreduceanpower. Smartcitiesaredevelopinginthiscontextofautomation.Modernization is growing as huge building and Offices for workand residence. Security and safety are a challenging take in suchlocations. This can be provided if only for authorized people andvehiclesareallowedintopremises. Weproposeanauthentication technique for allowing vehicles into work spaces/offices.Itiswellknown thatRegionalTransport office(RTO)providesauniqueregistrationnumberforvehicles anditisdisplayed on the number plates. These numbers can beused asauthentication parameters forentering thepremises.Adatabaseofauthorizedvehiclesismaintainedandonlythosemustbeallowed. In order to reduce manpower at the entrance/ exit anautomaticgateisdesignedtoopen/closeforauthenticatedvehicles. A camera is placed in such a position that it captures theimageofthevehicle'snumberplate.Digital ImageProcessingTechnique is used to extract text fromthecaptured image andauthorization is verified, based on Optical Character Recognition(OCR) technology is used to recognizethe text within a digitalimage.Ifthe vehicle is authorized,the Raspberry Picontroller will send instructions to the motor attached to the entrance gate to open,else itremains closed.The same information is sentand saved to the control room as email. Digital Image Processing(DIP),EmbeddedSystem(ES)andInternetof Things(IoT)technologiesareusedforimplementingthisapplicationofpreprogrammed gatewayControl System stand on Vanity-PlateacceptancebyutilizingRaspberryPi3modelB.

Keywords: Automatic gate control system, licenseplate,OpticalCharacterRecognition(OCR),RaspberryPi,Python,Database,Email.



INTRODUCTION

grammedNumberPlateRecognition (PNPR) is accomplished through camcorders catching picturesthataredissectedutilizingOpticalCharacterRecognition(OCR)algorithm,whichinspectseachsocialeventofpixelsinside the photos and measures whether it might be a letter andreplacesthepixelswiththeAmericanStandardCodeforInformation Interchange (ASCII) code for each character. This algorithm is the basis innovation utilized in NPR and gives the capacity to cache and categorized information. The camera should be an exceptional kind and arranged in certain assigned boundaries.Asan automobile moves toward the polarised, the product takes a progression of 'previews' and reserves them in a record. At this point when the license plate is of adequate length for this algorithm, the casing is examined and the enlistment digit is changed over to uni-code and held in a rundown. This proceeds for a progression of pictures as indicated by the speed and location of the vehicle guaranteeing that the ideal perspective on the tag is accomplished. ANPR get is dependent upon the right set-up of camera, point of convergence, lighting, perspective,and plan.

Fig 1 ANPR Methodology

PREVIOUS WORK

Almost everything in the modern world is going automatic; we have built this project to increase

theconvenience and security at the entrance gate. Vehicle license plate recognition is an image processingtechnology used to identify vehicles by their license plates. This technology can be used in various securityand traffic applications, such as finding stolen cars, controlling access to car parks and gathering traffic flowstatistics. The purpose of this paper is to develop an automatic gate control application which recognizeslicense plates from cars at entrance gate and take an action to let cars enter or not. The system, based on PICmicrocontroller and regular PC with video camera, catches video frames which include a visible car licenseplateand processes them.

This is the main part of the project, which we have used MATLAB software to implemented our algorithm.This Recognition of any License Plate Recognition system is the effectiveness of its algorithms. As a whole,aseriesofsixprimaryalgorithmsarenecessaryforaLicensePlateRecognitionsystemtobesuccessfulwhichare:

1. LicensePlateLocalization
2. LicensePlateSizingandOrientation
3. Normalization
4. CharactersSegmentation
5.Opticalcharacterrecognition(OCR)

6.Syntactical/Geometricalanalysis.

Fig 2 Block diagram

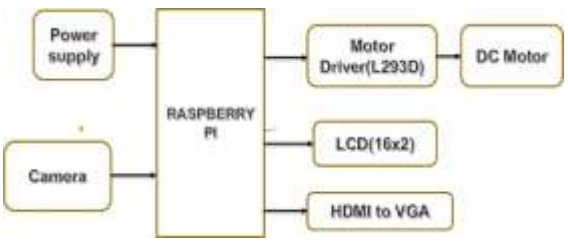
I. PROPOSED METHODOLOGY

Inthisventure,weproposearobotizedtagacknowledgmentframework.Theventure targetsplanning aframework that naturally catches the picture of the registrationnumberofaautomobileandthesesubtletieswerecheckedutilizingBroadcomBCM2837 64-bitARMv7QuadCoreProcessor for verification. The framework likewise alarms thespecialistsifanyunapprovedwasidentifieddata sentViaEmail. Right when the supported vehicle was recognized thenthestructureworkstheentrywayusing directcurrentmotor.

Fig 3 Block diagram

Description- In this framework, we use the power supply of 5vto work the Raspberry Pi. In this number, plate acknowledgmentshould be possible by utilizing the camera. Contribution from thecameraisgiventotheOCR calculationtoperceivethecharactersina number plate. The character from the number plate is put away inthe Raspberry pi and afterward, it is contrasted and informationbase. At the point when it is coordinated naturally the Raspberry Pisends the guidelines to the engine driver then the engine driverdrives the DC engine to open/close the door. Here the open/close ofthedoorisjustaccomplishedforapprovedvehicles .

Working-In this proposed framework we are providing 5V offorce supply to the raspberry pi 3 model B chip size based minicomputer. Here the polaroid is utilized to catches a picture of thenumber on the number plate of the vehicle, the separated data willship off theprocessor.Theprocessorcontrasts thenumber anddata in the data set, if the number has a place with authorized,Itwill open or close the door with the assistance of aDC



enginedrivenbytheenginedriver.Ontheoffchancet hatthenumberhas a place with approved/unapproved a similardata sent and save tothecontrolroomthroughanEmail.

Step-1: These are the associations and game plan of gadgets of ourtask named as "Programmed door control framework dependent onvehicle number plate acknowledgment by utilizing Raspberry Pi 3Model B".

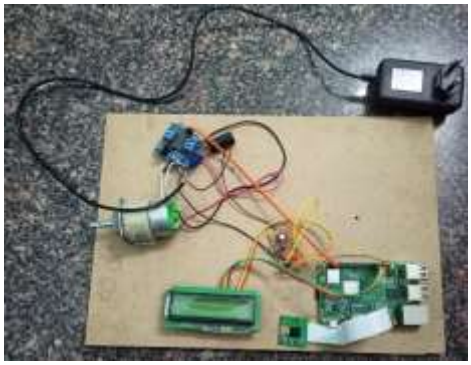


Fig 4 Hardware Arrangements

Step-2: HereweareutilizingtheVNCViewerterminalf ortheinterfaceofourequipmentandprogrammin galongsidetheOSRaspbian.

Fig 5 VNCViewerterminal

Step-3: After running our program which was written in the Pythonprogramming language. The beneath Figure shows the subtleties ofRegistration,Validation, Displaydetail.
Ifweenter1,weneedto enlistthenumberplate,andcompletedataisput awayinthedatabase(SQL).
If weenter 2,tag approvalwill befinishedby ourprogramand thepresentation ofthedataasdisplayedintheunderneathfigure.

Ontheoffchancethatweenter3,wecangettheshow casesubtletiesofvehiclenumberplate.

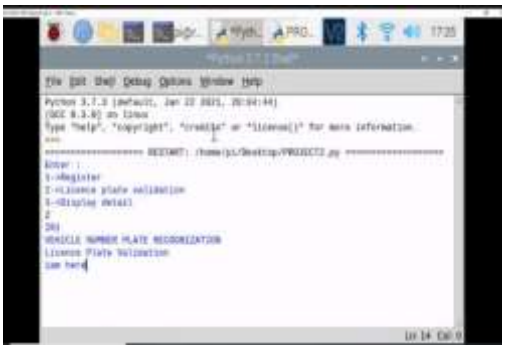


Fig6Licenseplatevalidation

Step-4: The contribution to the model is a picture taken by theRaspberryPicameraappendedtotheCSIportofRas pberryPiwhichisput at theentranceoftheentryway.

Fig7Cameracapture fromvehicle numberplate

Step-5: Fromtheinputpicture,thenumberplatewasseparate dasdisplayed in the underneath figure which is set

apart as red inshading.

Fig8.Extractingnumberfrom capturedimage

Step-6: The separated RGB design picture is changed over into thegrayscalepictureasaBlackandWhitepicture.

Fig.9.Gray-levelimage

28.

II.

29.

30.

31.

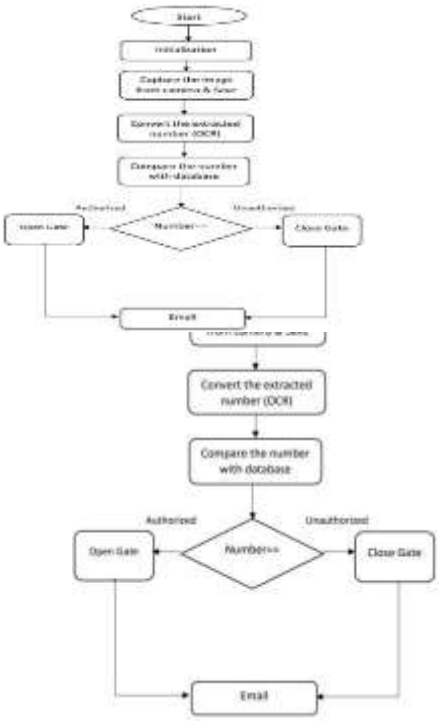


Fig10.Flowchart

III. Result

If the vehicle is approved, the Raspberry pi conveys themessage to theMotordriverto drive the engineto open the door.Assuming the vehicle is unapproved, theRaspberry pi conveys themessage to the engine driver to not open the entryway.The dataaboutapprovedissentandsavedtothecontrol roomthroughemail.

Fig11.Displaydetails

32.

33. If the vehicle is endorsed, the Raspberry pi 3 model B passes on themessageto theMotordriverto drivetheDCMotortoopentheentrywayandshowedinLCDas"AUTHORIZED".

34.

Fig12.VehicleAuthorized

Fig13.Authenticatedvehicledetailsvia,Email

VI Conclusion

This project explains quick calculations for vehicle number plate recognition and confirmation. Rather than MATLAB, we utilized raspberry pi that gives us more exactness and accurate programming time. we used vehicle registration plates for the process and executed the application in different ways.

Next, we did the process on 5 number plates based on

application, and the other 3 registration plates performed on motion-based application. we blurred the number plates and performed it on the remaining 2 number plates. The accuracy of the first 5 number plates is 98%, the exactness of the 3 plates is 50% which is performed on motion-based application. Lastly, the precise of 2 registration plates that are blurred is 30%.

This blend of programming as picture handling apparatus, OCR, Python, open cv, and equipment goal camera, observing presentation, dc engine, Email gives us more mechanization in field of electronic and advancing making India dream who makes Digital India.

We can expand our venture by carrying out a sweep card comprising of information like a unique mark with an enlisted vehicle number, Wecan likewise execute face acknowledgement and exceptional names made distinctly for approved to keep away from control (counterfeit acknowledgment passage)

VIII REFERENCES

[1]B.Hongliang andL.Changing, “A hybrid licenseplateextractionmethodbasedonedgestatisticsa ndmorphology,”inProc.ICPR,pp.831-834,2004

[2]D.Zheng,Y.Zhao,andJ.Wang,“Anefficientmetho d of license plate location,” Pattern Recognition. Lett.,vol.26,no.15,pp.2431-2438,Nov.2005

[3]H.J Lee, S. Y. Chen, and S.Z. Wang, “Extraction and recognition of license plates of motorcycles and vehicles on highways,” in Proc. ICPR, pp. 356-359,2004.

[4]B. Hongliang and L. Changing, “A hybrid license plate extraction method based on edge statistics and morphology,” in Proc. ICPR, pp. 831-834, 2004

[5]D. Zheng, Y. Zhao, and J. Wang, “An efficient method of license plate location,” Pattern Recognition. Lett., vol. 26, no.15, pp. 2431-2438, Nov. 2005.

[6]H.J. Lee, S.Y. Chen, and S.Z. Wang, “Extraction and recognition of license plates of motorcycles and vehicles on highways,” in Proc. ICPR, pp. 356-359, 2004

Group Data Sharing in Cloud environment using EnhancedThreshold Multi-Keyword Search scheme

.Dr.Y.Pavan Kumar Reddy[1] Sd.Shaziya [2] M.Divya Sree [3] P. B.Reshma [4] M.Sandhya

Professor[1] UG Scholar, [2, 3,4]

[1, 2, 3, 4,] Department of CSE, Geethanjali Institute of Science and Technology, Nellor, A.P

Abstract - Searchable Encryption (SE) is a popular cryptographic primitive for building ciphertexts retrieval systems with far-reaching applications. However, existing SE schemes generally do notsupport threshold access control (i.e., data usersmust collaboratively issue search and decryptionoperations over encrypted cloud data) in a group-oriented cloud data sharing setting, whichis increasingly receivingmuchattention in the research community. Then, we extend this basicTMS to realize threshold result verification andthreshold traceability (referred to as enhancedTMS). Furthermore, the enhanced TMS is extendedto support public result verification and dynamic operations with the public verifier and improvedhashtables,respectively. Our formal security analysis proves that both basic TMS and enhancedTMS are semi-adaptively secure and can resist Chosen Keyword Attack (CKA). Our theoretical evaluation and empirical experiments demonstrate the potential utility of both schemes.

keywords—Searchable encryption, threshold access control, threshold multi-keyword search, threshold decryption, short record ciphertext size.

1. I.INTRODUCTION

Cloud computing is widely used by individuals, organizations and governments, as it allows users to share data (i.e., documents, images, etc.) with specified/intended recipients in a group setting Although cloud-related security and privacy are two topics that have been extensively studied in the literature, there remain challenges that have yet to beully addressed. For example, to guard against some cloud providers (and their employees) from accessing the data stored in these cloud servers, we can outsource highly sensitive data in the encrypted form only. However, in practice, this limits the users' search capabilities over such encrypted Hence, there have been interest in designing partial but practical Searchable Encryption (SE) schemes Such schemes donot degrade data security and usability, and can be potentially used in various settings such as tasks recommendation in crowd sourcing healthcare cloudservices and group data sharing .In addition toensuring strong security guarantees a practical SE should also achieve features such as expressive search and cost-effective storage. However, one of the main limitations of the conventional SE solutions is that these schemes do not place any restriction on access control in group-oriented applications (i.e., social network, wireless body area network, etc.). In other words, there is a risk of unauthorized access, thereby compromising data privacy. There have also been attempts to use Ciphertext Policy Attribute-Based Keyword Search (CP-ABKS) to facilitate keyword-based ciphertext retrieval while providing fine-grainedaccess control by integrating (CP-ABE) with SE. However, the associated encryption and decryptionoverhead is relatively high[1]. As encryption and decryption processes are often executed on computationally weak devices.

In other words, security, expressive query, access control, and efficiency are four main features typically expected in any practical SE scheme. Although there are many published SE schemes, designing practical SE schemes that also facilitate threshold access is an understudied area. In group-oriented data sharing applications (i.e., electronic auction, electronic voting, etc.), we may not fully trust a single individual. Instead, we may trust a group of individuals to access our sensitive information. One classic

example is the electronic voting, where a pool of individuals are trusted to open the final result but not allowed to leak ballots to any individual. Moreover, it is required that these data can still be accessible if some individuals in the authorized group are compromised or offline.

To implement threshold access in SE, we can utilize Threshold Public-Key Encryption (TPKE) mechanism ,to enable at least a threshold number of authorized data users in a group to cooperatively generate the valid trapdoor and decrypt search results. Examples of following this approach include those described in. However, this approach generally results in long trapdoor size when supporting multi-keyword search, and is not capable of providing result verification in the semi-honest-but-curious cloud computing environment or threshold traceability in the event of a dispute. For example, the compromised or attacked cloud server, may forge or tamper results due to various incentives. Schemes such as those presented in attempted to prevent the semi-honest-but-curious cloud server from returning incorrect search results, butthese solutions have high false-positive rates due to the use of Bloom filter. Besides, the individual traceability in prior group signature solutions allows each group member to reveal the real signer's identity, but may incur excessive abuse if each group member is given this capability in some applications.

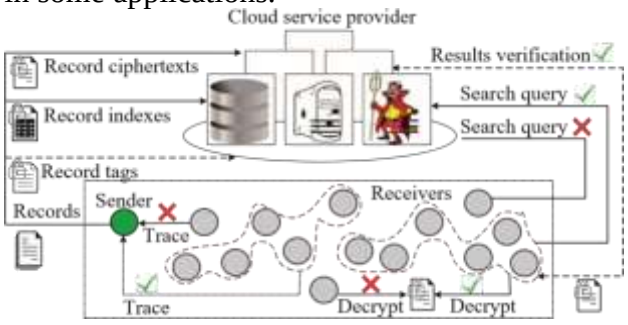


Fig. 1: Features of basic (or enhanced) TMS.

In this paper, we first devise the basic Threshold Multikeyword Search (TMS) scheme in the group-oriented data sharing framework, by using the broadcast encryption . Then, we improve the basic TMS scheme to form the enhanced TMS, supporting

contributions in this paper is as follows:

Threshold multi-keyword search[2]. Different from previous SE schemes supporting multi- keyword search, our proposed schemes consider the group sharing scenario rather than thegeneral setting in which each authorized data user is allowed to access encrypted data. Given an authorized group, our basic or enhanced TMS scheme allows each group member to generate a trapdoor share based on a list of keywords by using the respective secret key. It also enables at least a threshold number of group members to form the final trapdoor by using the Lagrange interpolation technique, which guarantees thatthe ciphertexts are accessible even if some group members are compromised or offline. In comparison to previous SE schemes, the trapdoor size in basic or enhanced TMS does notgrow with the number of queried keywords. Thus, both proposed schemes can be deployed on resource-limited devices.

- *Short record ciphertext size and low threshold decryption overhead*. Compared with previous threshold public encryption schemes, our basic and enhanced TMS schemes do not lead to long record ciphertext size[3] that is proportional to the group size. In other words, the ciphertext size of our basic or enhanced TMS is not affected by the group size. Besides, previous schemes allow each authorized data user to gain the decryption key, while our basic or enhanced TMS requires thatat least a threshold number of group members togenerate their decryption shares and then integrate them to recover each record decryption key cooperatively. Furthermore, previous schemes deliver the complete decryption task to data users, which incurs high computation overhead on resource-limited data users. Our enhanced TMS scheme can significantly reduce the decryption overhead by using an outsourced decryption mechanism.
- *Threshold result verification*. Unlike the honest-but curious cloud server assumption in the

conventional SE schemes, we consider a semi-honest-but-curious cloud server that honestly executes the requested search operations most of time but may return partial false search resultsthreshold result verification and threshold traceability due to financial incentives (e.g., saving storage space and computation resources) in our enhanced TMS scheme. In addition, previous SE schemes just allow a third-party or a single user to check the correctness of search results.In the group sharing scenario, one group member's verification result cannot convince other group members. Thus, our enhanced TMSscheme allows a threshold number of receivers to guarantee the reliability of search results by attaching a homomorphic verifiable tag to each record.

. *Threshold traceability*. Unlike the conventional group signature schemes, our enhanced TMSscheme does not rely on the group manager and ensures threshold traceability rather than individual traceability. Previous individual traceability mechanisms allow any group member to trace the signer's identity, which willcause the excessive abuse. To solve this problem, our enhanced TMS achieves threshold traceability. Specifically, in our enhanced TMS scheme, each group member can sign the recordon behalf of the specified group by generating its corresponding signature as well as some auxiliary information, and this authorized groupwith at least a threshold d data

Threshold Public-Key Encryption (TPKE). In contrast to conventional public-key encryption, TPKE schemes [22], [23] enable at least a threshold number of expected members to cooperatively decrypt the ciphertexts, and guarantee data accessibility even if some members are not online. Note that this cryptographic primitive includes threshold broadcast encryption [35], [50] and threshold group signature [27], [51]. To achieve adaptive security and shorten ciphertext size in number of group members can jointly reveal the signer's identity in potential disputes.

II. RELATED WORK

Cloud-based group data sharing [36], [37] has gained increased popularity, particularly in collaborative andincluding group-oriented scenarios.

Apart from supporting expressive search (i.e., range query, conjunctive query, subset query, etc.) and providing strong security, ASE schemes should also permit the sender to selectively share his/her data at a fine-grained (rather than coarsegrained) level. As the single keyword search [4] will yield many non-relevant results and waste bandwidth resources, the capability ofsupporting multi-keyword search [43] or Boolean search [44] is crucial for expressive queries. In addition,in practice, a sender may require fine-grained search permissions among the intended group members at the granularity of each record. Thus, Zheng *et al.* [30] integrated CP-ABE with SE and coined the notion of CP-ABKS, in order to achieve finegrained keyword search. Although Xu *et al.* [45] presented a secure fine- grained group data sharing scheme by combining both identity-based encryption and ABE techniques, in orderto efficiently update ciphertexts without any delegated key, such an approach cannot facilitate keyword-based search over encrypted clou

conventional TPKE schemes, Qin *et al.* [35] proposed a secure TPKS with constant ciphertext length, based on adaptive broadcast encryption [34]. However, this approach has a long secret key size, which is proportional to the group size, and is notand secure data sharing among group-oriented members remains a research challenge. Two veryrelated techniques are illustrated as follows:

Searchable Encryption (SE). SE schemes, such as(SSE) and Asymmetric SE (ASE) schemes. SSE schemes are not practical for group data sharing deployments as the sender (or data owner) needs to distribute the secret keys to intended receivers (or data users) via some security channels, which results in considerable communication and key management

and allow any group member to perform keyword-based search queries using the relevant secret key, such schemes can be efficiently implemented in a multi-user setting,requiring the group manager, only supporting individual traceability, etc.) in conventional group encryption schemes [51], Zheng *et al.* [27] presenteda *democratic* group signature scheme, which provides threshold traceability and does not involve any trusted group manager.

III. PROPOSED WORK

In this project, we first devise the basic Threshold Multikeyword Search (TMS) scheme in the group- oriented data sharing framework, by using the broadcast encryption.
Then, we improve the basic TMS scheme to form the

traceability. Particularly, the enhanced TMS scheme can be further extended to provide public result verification and dynamic operations, by employing state-of-the-art techniques (rather than reinventing the
enhanced TMS, supporting threshold result verification wheel). Both basic TMS and enhanced TMS schemes and threshold traceability using democratic group signature.

II. RESULT

Fig 2: Threshold Multi-keyword Search Home page

This is the home page here there are four phases like Cloud service provider and Trusted authority and Sender along with Receiver.

Fig 3 : Download File

In Receiver we have an option decrypt and downloadby clicking that the file will be downloaded.

III. CONCLUSION

Motivated by the observation that there does not yet exist any scheme that provides flexible access controlin group oriented data sharing setting, we design two threshold multi keywords search schemes (namely, a basic TMS scheme and the enhanced TMS scheme) which achieve versatile features such as threshold decryption, threshold result verification and threshold
are then shown to achieve semi-adaptive security and resist CKA. Besides, the enhanced TMS scheme is shown to guarantee record tag unforgeability

I . REFERENCES

[1] B. Cui, Z. Liu, and L. Wang, "Key-aggregate searchable encryption (kase) for group data sharing via cloud storage," *IEEE Transactions on computers*, vol. 65, no. 8, pp. 2374–2385, 2016.

[2] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, "Attributebased keyword search over hierarchical data in cloud computing," *IEEE Transactions on Services Computing*, pp. 1–14, 2017.

[3] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symposium on Security and Privacy (S&P'00)*. IEEE, 2000, pp. 44–55.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. International conference on the theory and applications of cryptographic techniques (EUROCRYPT' 04)*. Springer, 2004, pp. 506–522.

[5] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "Dual-server publickey encryption with keyword search for secure cloud storage," *IEEE transactions on information forensics and security*, vol. 11, no. 4, pp. 789–798, 2016.

[6] . Zhang, Y. Tang, H. Wang, C. Xu, Y. Miao, and H. Cheng, "Latticebased proxy-oriented identity-based encryption with keyword search forcloud storage," *Information Sciences*, vol. PP, pp. 1–15, 2019.

[7] R. Chen, Y. Mu, G. Yang, F. Guo, X. Huang, X. Wang, and Y. Wang, "Server-aided public key encryption with keyword search," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2833– 2842, 2016.

[8] J. Shu, K. Yang, X. Jia, X. Liu, C. Wang, and R. Deng, "Proxy-free privacy-preserving task matching with efficient revocation in crowdsourcing,"

IEEE Transactions on Dependable and Secure Computing, pp. 1–14, 2018.

[9] R. Zhang, R. Xue, and L. Liu, "Searchable encryption for healthcare clouds: a survey," *IEEE Transactions on Services Computing*, vol. 11, no. 6, pp. 978–996, 2018.

[10] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block designbased key agreement for group data sharing in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, pp. 1–15, 2017.

[11] R. Chen, Y. Mu, G. Yang, and F. Guo, "Bl-mle: block-level messagelocked encryption for secure large file deduplication," *IEEE Transactions*

Ciphertext-Policy Attribute-Based Data Sharing and Keyword Searching Scheme For Encrypted Cloud Data

Dr. M. Mathan Kumar[1] V. Akhila[2] K. Nandini[3] T. Sindhu[4] T. Keerthi[5]
Associate Professor[1], UG Scholar[2, 3, 4, 5]
[1, 2,3,4,5]Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh

ABSTRACT

The emergence of cloud infrastructure has significantly reduced the costs of hardware and software resources in computing infrastructure. To ensure security, the data is usually encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to conduct a quick search and return the result without losing data confidentiality. To overcome these problems, we propose a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The proposed solution not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which contrasts with the existing solutions that only support either one of two features. Additionally, the keyword in our scheme can be updated during the sharing phase without interacting with the PKG. In this project, we describe the notion of CPAB-KSDS as well as its security model. Besides, we propose a concrete scheme and prove that it is against chosen ciphertext attack and chosen keyword attack secure in the random oracle model. Finally, the proposed construction is demonstrated practical and efficient in the performance and property comparison. Unfortunately, traditional attribute- based encryption just ensures the confidentiality of data. Hence, it does not support searching and sharing.

An alternative method is to delegate a third party to do the search, re-encrypt and keyword update work instead of Alice. Alice can store her private key in the third party's storage, and thus the third party can do the heavy job on behalf of Alice. In such an approach, however, we need to fully trust the third party since it can access to Alice's private key. If the third party is compromised, all the user data including sensitive privacy will be leaked as well. It would be a severe disaster to the users.

Cloud Data Sharing, Searchable Attribute-based Encryption, Attribute-based Proxy Re-encryption,

party's storage, and thus the third party can do the heavy job on behalf of Alice. In such an approach, however, we need to fully trust the third party since it can access to Alice's private key. If the third party is compromised, all the user data including sensitive privacy will be leaked as well. It would be a severe disaster to the users.

Unfortunately, traditional attribute- based encryption just ensures the confidentiality of data. Hence, it does not support searching and sharing.

An alternative method is to delegate a third party to do the search, re-encrypt and keyword update work instead of Alice. Alice can store her private key in the third party's storage, and thus the third party can do the heavy job on behalf of Alice. In such an approach, however, we need to fully trust the third party since it can access to Alice's private key. If the third party is compromised, all the user data including sensitive privacy will be leaked as well. It would be a severe disaster to the users.

2.RELATED WORK

INTRODUCTION

CLOUD computing has been the remedy to the problem of personal data management and maintenance due to the growth of personal electronic devices. It is because users can outsource their data to the cloud with ease and low cost. The emergence of cloud computing has also influenced and dominated Information Technology industries. It is unavoidable that cloud computing also suffers from security and privacy challenges.

Encryption is the basic method for enabling data confidentiality and attribute-based encryption is a prominent representative due to its expressiveness in user's identity and data [1]– [4]. After the attribute-based encrypted data is uploaded in the cloud, authorized users face two basic operations: datasearching and data sharing.

In an ABE, the users' identities are described by a list of attributes [1]. After ABE's pioneering work [1], several scholars extended the notion of ABE. For example, key-policy attribute-based encryption (KP-ABE) [2], where the private key of a user is related to an access policy and the ciphertext corresponds to an attribute set. In contrast, there is another example called ciphertext-policy attribute-based encryption (CP-ABE) [3], where the private key is generated with an attribute set and the ciphertext is related to an access policy. In both KP-ABE and CP-ABE, the ciphertext length is linear with the size of the access policy. To reduce the ciphertext length, Emura et al. [8] proposed aciphertext-policy attribute-based encryption scheme with constant ciphertext length. Although it supports the AND-gates on multi attributes, it doesn't support the monotonic express on attributes. After that, a number of constructions have come out to enhance the efficiency, security and In our scheme, ciphertexts are encrypted with an access policy and a keyword, and the private key is connected with an attribute set S. U is the attribute universe whose size is polynomial of λ. KW ∈ {0, 1}* denotes a keyword. The following describes our proposed CPAB-KSDS scheme.

1) Setup (λ, U): Chooses a bilinear map tuple (p, g, G, G_T , e), and randomly select α, β, a, b, c ∈ Z^*_p , f, g˜ ∈ G, compute $f_1 = g^c$, $f_2 = g^b$, $Q = g^\beta$. For ∀i, ≤ i ≤ |U|, choose $h_1, \cdots, h_{|U|} \in G$. Choose collision-resistant hash functions: $H_1 : \{0, 1\}^* \rightarrow G$, $H_2 : G_T \rightarrow \{0, 1\}^*$, $H3 : \{0, 1\}^* \rightarrow Z^*_p$, $H4 : \{0, 1\}^* \times GT \rightarrow Z^*_p$.

expressiveness [4], [9], [10]. To illustrate the ABE's application, Li et al. [11] adopted the notion of attribute-based encryption in the PHR system to achieve finegrained access control on personal health records. A ciphertext policy attribute-based encryption with hidden policy [12] was proposed to hide the access policy which may leak the user's privacy in the PHR system. The concept of outsourcing decryption attribute-based encryption was introduced to enable a computation-constrained mobile device to outsource most of the decryption work to a service provider [13]. However, there is no guarantee that the service provider could return the correct partial decryption ciphertext. To overcome this issue, Lai [14] and Li [15] proposed attribute-based encryption with verifiable outsourced decryption schemes respectively.

3.**Proposed System**

Choose a CCA-secure symmetric key encryption SY =(S.Enc, S.Dec). Output msk = (g^α, a, b) and mpk = ($e(g, g)^\alpha$, g^a , g˜, f, f_1, f_2, Q, H_1, H_2, H_3, H_4, $h_1, \cdots, h_{|U|}$, SY).

2) Keygen (msk, S): Randomly choose t, r ∈ Z^*_p and compute the secret key sk_S as

$K = g^\alpha f^t$, $L = g^t$

$V = g^{(ac-r)/b}$, $Y = g^r$, $Z = g^{\sim r}$,∀x ∈ S, {$K_x = h^t_x$, $Y_x = H_1(x)^r$ }.

Note that, V can be computed as $V = f_1^{a/b} / g^{r/b}$. The secret key sk_S implicitly contains S.

4.RESULTS

The implementation involves various steps. They are:

- Cloud Server
- Data Owner
- Delegate
- Delegator

DATA OWNER

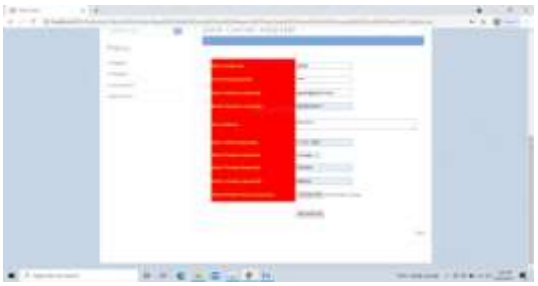


Fig: Data Owner Registration Page

Description: The Data owner will initially register the cloud

DATA OWNER

Fig: Add Patient Details

Description: Data owner will add the patient details in the cloud

DATA OWNER

Fig: Entering Patient Details

Description: Here data owner will enter the patient details and upload in encrypted format.

DELEGATOR

Fig: Delegator Registration Form

Description: Delegator will enter the details for registering their data in to the cloud.

CLOUD SERVER

Fig:View and Authorize Delegator

Description: here cloud server will be giving the permission to the delegator who are waiting for permission.

DELEGATOR

Fig: Search Patient Details

Description: here delegator will search the patient details by giving the patient name or keyword.

CLOUD SERVER

Fig: View Patient Details in Encrypted Form

Description: Here we will see the patient details in the encrypted form.

CLOUD SERVER

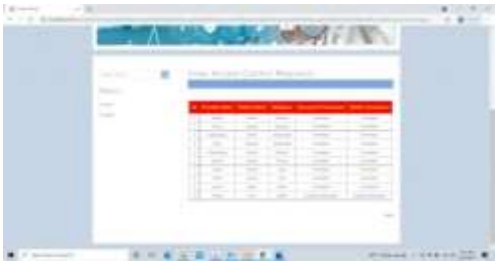


Fig: View Access Control Request

Description: cloud server will give the both document and details permission to the delegator.

DELEGATOR

Fig: View Patient Details in Decrypted Form

Description: Here we will see the patient details in decrypted form.

5.CONCLUSION

In this work, a new notion of ciphertext-policy attribute-based mechanism (CPAB-KSDS) is introduced to support keyword searching and data sharing. A concrete CPAB-KSDS scheme has been constructed in this project and we prove its CCA security in the random oracle model. The proposed scheme is demonstrated efficient and practical in the performance and property comparison. This project provides an affirmative answer to the open challenging problem pointed out in the prior work [36], which is to design an attribute-based encryption with keyword searching and data sharing without the PKG during the sharing phase. Furthermore, our work motivates interesting open problems as well including designing CPAB-KSDS scheme without random oracles or proposing a new scheme to support more expressive keyword search.

6.REFERENCES

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Annual International Conference on the Theory and Applications of Crypto graphic Techniques, pp. 457–473, Springer, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98, Acm, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in Security and Privacy, 2007. SP’07. IEEE Symposium on, pp. 321–334, IEEE, 2007.

[4] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in International Workshop on Public Key Cryptography, pp. 53–70, Springer, 2011.

[5] H. Qian, J. Li, Y. Zhang, and J. Han, “Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation,” International Journal of Information Security, vol. 14, no. 6, pp. 487– 497, 2015.

[6] J. Liu, X. Huang, and J. K. Liu, “Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption,” Future Generation Computer Systems, vol. 52, pp. 67–76, 2015.

[7] L. Fang, W. Susilo, C. Ge, and J. Wang, "Interactive conditional proxy re-encryption with fine grain policy," Journal of Systems and Software, vol. 84, no. 12, pp. 2293–2302, 2011.

[8] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in International Conference on Information Security Practice and Experience, pp. 13–23, Springer, 2009.

ANALYSING DATA FOR OPTIMIZED PREDICTION IN HEALTH CARE USING MACHINE LEARNING ALGORITHMS

K. Chiranjeevi[1] Ch. Jyothsna[2] T. Vennela[3] T. Swapna[4] G. Anusha[5] Assistant professor[1], UG Scholars[2,3,4,5]

[1, 2, 3, 4,5] Department of CSE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh

ABSTRACT - Data in the health care sector is growing beyond dealing capacity of the health care organizations and is expected to increase significantly in the coming years. This data is effectively used for analysis and prediction. A better approach to health care is to prevent a disease with early intervention rather than taking a treatment after it is recognized. The main aim of this project is to make a comparative study of machine learning algorithms such as Support Vector Machine, Extra Tree Classification and K – Nearest Neighbor Classification in predicting heart disease.In this project we are using real time heart disease dataset collected from kaggle website and the data set is preprocessed as per the requirements to perform comparative study of specified machine learning algorithms. Confusion matrix, F1-score and accuracy have been considered as metrics for evaluating the performance of algorithms in the context of predicting heart disease.

Keywords: Prediction, Machine Learning

I. INTRODUCTION

Machine Learning (ML) is defined as Field of study that gives computers the capability to learn without being explicitly programmed. In simple way, ML can be explained as automating and improving the learning process of computers based on their experiences without being actually programmed i.e.
without any human assistance. The

process starts by providing good quality data and then training our machines
(computers) by building machine learning models using the data and different algorithms. The choice of algorithms depends on what type of data do we have and what kind of tasks we are trying to automate. Finally these models which are built are used for making predictions.

In today's chaotic world we all have very busy life, tough schedule and competitive activities for growing up and to achieve success in our life but we are neglecting our health issues because of this, we encounter many diseases that are threat to our lives. Many diseases if they will not be treated properly they cause death. Heart disease is one of the chronic illnesses that produce different signals from early stage but we fail to recognize these signals which lead to long term illness or loss of life. According to the report of WHO world health organization's statistics 24% death in world that are not communicable happens because of heart illness. One-third of death worldwide due to heart disease. A heart problem can occur in any age of life young, middle or old, environment where we live, it can also cause because of genetic and in heart disease gender plays an important role. Some reasons of heart disease are not doing exercise or laziness, alcohol, smoking, tension, stress and consumption that exceed the body needs.

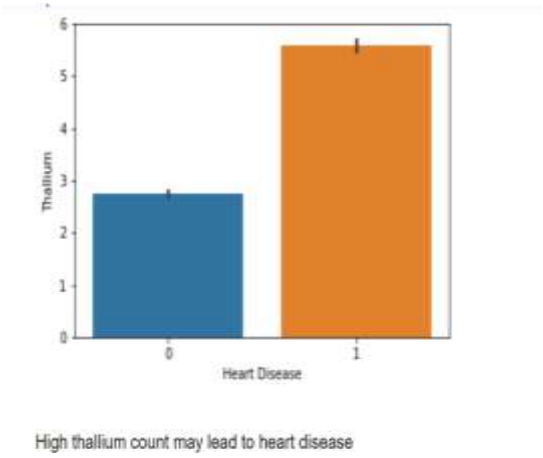
To contribute to this human crisis our study aims to do the comparative study of machine learning algorithms such as

Support Vector Machine (SVM), K- Nearest Neighbor Classification (KNN) and Extra Tree Classification algorithm and builds the best model for heart disease prediction. These models are trained using real time Heart Disease dataset collected from kaggle website. The dataset has been divided in to training data and testing data and preprocessed as per the requirements of algorithms. Finally these models are evaluated using evaluation metrics like Confusion Matrix, F1_score and Accuracy score.

II. PREVIOUS WORK

Many research papers have been published on predicting heart disease using a machine learning algorithm. Research with improvedaccuracy of heart disease prediction has been reported by using train test split validation followed by logistic regression was used

for prediction which showed the better results on UCI dataset set [1]. In [2] author has focused on ensemble classification techniques. In this case, multiple classifiers



are used followed by score level ensemble for improvement of prediction accuracy. A Hoeffding tree algorithm with a K-fold cross-validation method is used on UCI dataset and reported a high accuracy [4]. In [3] author has proposed to find a significant feature of clinical heart disease dataset by using hybrid machining algorithm.

III. PROPOSED METHODOLOGY

This Paper is based on comparative study of supervised machine learning algorithms such as Support Vector Machine (SVM), K – Nearest Neighbor Classification (KNN), Extra Tree Classification in the context of heart disease prediction.

A. DATASET

We collected this dataset from kaggle website. Dataset has 1763-tuple including 14 different attributes. The attributes include age, sex, chest pain type, BP,Cholesterol, FBS over 120, EKG results, Max HR, Exercise angina, ST depression, slope of ST, Number of vessels fluro, Thallium and Heart disease.

Data analyzation has been done through visualization. Some of the insights has been drawn from the dataset. Some of them are shown below.

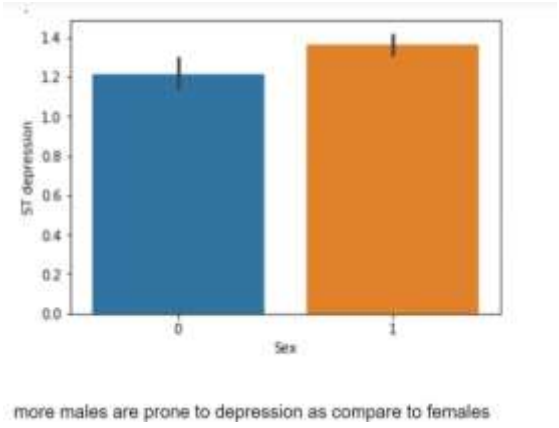


Fig 3: Sex Vs Depression

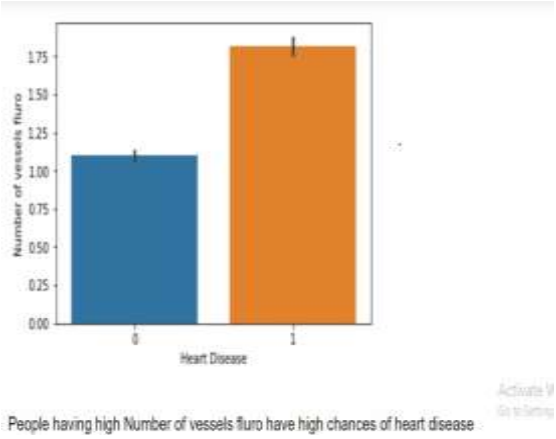


Fig 4: Heart Disease Vs Number of vessels fluro

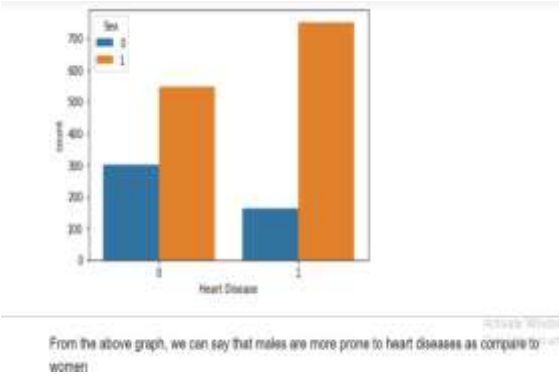


Fig 5: Heart Disease Vs Thallium

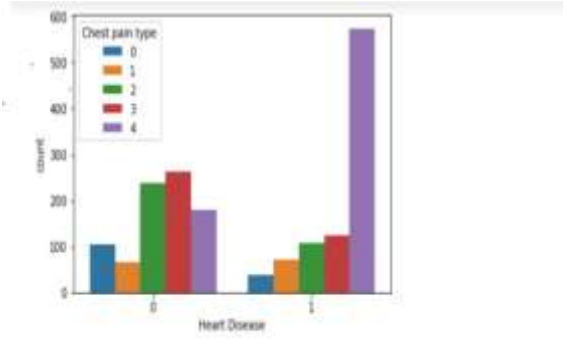
B. LIBRARIES AND TOOLS

For applying this model, we have used python language and its libraries. For python, we have used a Jupyter (Anaconda) tool. Libraries used in the model are NumPy, pandas, sklearn, SVC,

KNeighborsClassifier, Extra tree classifier and Seaborn is used for plotting graphs.

C. PREPROCESSING

Data Preprocessing is an important in machine Learning. Without preprocessing it will give the biased or impure result. The preprocessing techniques used are replacing zeroes with their mean values and feature scaling.MACHINE LEARNING MODELS



It seems that people who suffered from pain type 4 have more chances of heart disease

1. SUPPORT VECTOR MACHINE

Support Vector Machine is supervised machine Learning algorithm. The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data in the correct category in the future. This best decision boundary is called a hyperplane. The data points that are the closest to the hyperplane and which affect the position of the hyperplane are termed as Support Vector. As these vectors support the hyperplane, hence called a Support vector.

2. K – NEAREST NEIGHBOR CLASSIFICATION

The K-Nearest Neighbor is a simple, supervised machine learning algorithm that can be used for both classification and regression problems. K-NN algorithm assumes the similarity between the new case/data and available cases/data and put the new case into the category that is most similar to the available categories. This similarity is identified by measuring the Euclidean distance between new data point and the K – Nearest data points.

3. EXTRA TREE CLASSIFICATION

Extra Trees is an supervised ensemble machine learning algorithm. It is an ensemble of decision trees and is pertained to other ensembles of decision trees algorithms such as bootstrap aggregation (bagging) and random forest. The Extra Trees algorithm works by creating a large number of unpruned decision trees from the training data. Predictions are made by majority voting from decision trees.

D. EVALUATION METRICS

The models are evaluated by using metrics such as confusion matrix, F1-score and Accuracy score.

1. Confusion Matrix: A Confusion matrix is an N x N matrix used for evaluating the performance of a classification model, where N is the number of target classes. The matrix compares the actual target values with those values predicted by the machine learning model. This gives us a comprehensive view of how well our classification model is performing and what kinds of errors it is making.

2. F1-Score: The F-score is a way of combining the precision and recall of the model, and it is defined as the harmonic mean of the model's precision and recall.

$$\text{F1 Score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}}$$

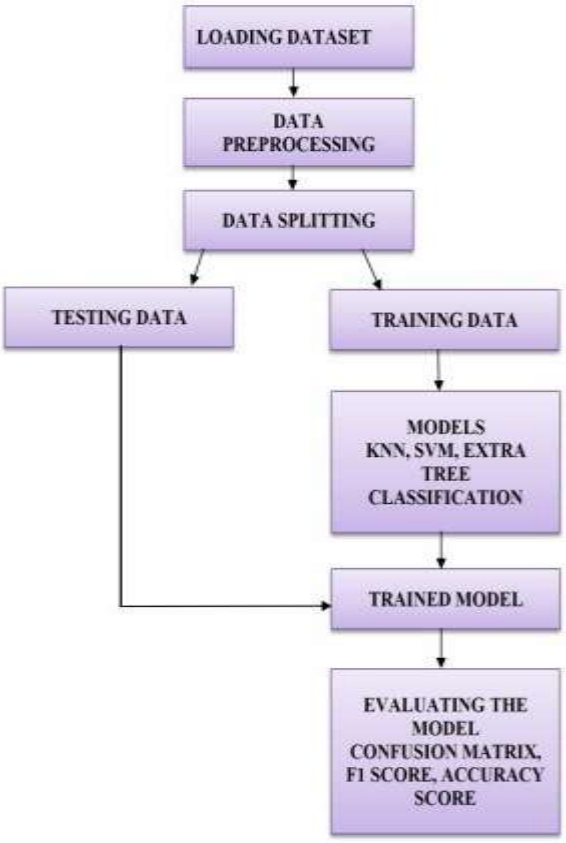
$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

$$\text{Recall} = \frac{True\ Positive}{True\ Positive + False\ Negative}$$

3. Accuracy Score: Accuracy is one metric for evaluating classification models. Accuracy is the fraction of correct predictions to total predictions.. Formally, accuracy has the following definition:

$$Accuracy = \frac{Correct\ Predictions}{All\ Predictions} = \frac{TP + TN}{TP + TN + FP + FN}$$

WORKFLOW



In this project we are using real time heart disease dataset collected from kaggle website and the data set is preprocessed as per the requirements to perform comparative study of the specified machine learning algorithms. After preprocessing, the data is divided in to testing and training sets. With this training data the models such as SVM, KNN and Extra Tree Classification gets trained for making predictions. Now these trained models are tested by providing testing data. Finally the performances of these models are evaluated by using evaluation metrics like confusion matrix, f1-score and accuracy score.

V. RESULTS

The results of comparative study of Support Vector Machine, K-Nearest Neighbor and Extra Tree Classification algorithm are shown below in table1. The K-Nearest Neighbor Classification

algorithm achieved highest accuracy of 90.47%.

EVALUATION METRICS	SUPPORT VECTOR MACHINE	EXTRA TREE CLASSIFICATION	K-NEAREST NEIGHBOR CLASSIFICATION
CONFUSION MATRIX	0 1 0 196 12 1 41 192	0 1 0 183 25 1 26 207	0 1 0 197 11 1 31 202
F1 SCORE	87.87	89.03	90.58
ACCURACY SCORE	87.98	88.43	90.47

VI. CONCLUSION ANDFUTURE SCOPE

Machine learning algorithms are vastly used in the prediction of diseases. The results obtained from the comparative study of supervised machine learning models like K – Nearest Neighbor Classification, Support Vector Machine and Extra Tree Classification show that K- Nearest Neighbor is the best model for predicting heart disease. The performance of K – Nearest Neighbor Classification model should be compared with the advanced models of machine learning in future so that the best model can be build for heart disease prediction.

VII. REFERENCES

[1] R. Kannan and V. Vasanthi, "Machine learning algorithms with ROC curve for predicting and diagnosing the heart disease," in Soft Computing and Medical Bioinformatics. Springer Singapore, jun 2018, pp. 63–72.

[2] C. B. C. Latha and S. C. Jeeva, "Improving the accuracy of prediction of heart disease risk based on ensemble classification techniques," Informatics in Medicine Unlocked, vol. 16, p. 100203, 2019.

[3] S. Mohan, C. Thirumalai, and G. Srivastava, "Effective heart disease prediction using hybrid machine learning techniques," IEEE Access, vol. 7, pp. 81542–81554, 2019.

[4] S. Thaiparnit, S. Kritsanasung, and N. Chumuang, "A classification for patients with heart disease based on hoeffding tree," in 2019 16th International Joint Conference on Computer Science and Software Engineering (JCSSE). IEEE, jul 2019

[5] T. K. Ho, "Random decision forests," in Proceedings of 3rd international conference on document analysis and recognition, vol. 1. IEEE, 1995, pp. 278– 282.

PREDICITING STOCK MARKET TRENDS USING MACHINE LEARNING ALGORITHMS

Mr. K. Chiranjeevi[1], G. Ashok[2], W. Sivatharun[3], K. Avinash[4],SK. Kalam[5],D. Leela Krishna reddy[6]
[1,2,3,4,5,6] **Department of CSE,Geethanjali Institute of Science and Technology,Nellore, Andhra Pradesh.**

Abstract - The nature of stock market movement has always been ambiguous for investors because of various influential factors. This study aims to significantly reduce the risk of trend prediction with machine learning algorithms. Four stock market groups, namely diversified financials, petroleum, non-metallic minerals and basic metals from Tehran stock exchange, are chosen for experimental evaluations. In this model we use Support Vector Machine(SVM). We consider [+1,-1] as Uptrends and Downtrends and it acts as the input as well as output for SVM model.

Keywords –Machine learning, Prediction, Stock market, Regression

1.INTRODUCTION

Machine learning is the study of computer algorithms that improve automatically through experience. Machine learning algorithms build a mathematical model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed. Machine learning algorithms are used in a wide variety of applications, such as email filtering and computer vision, where it is difficult or infeasible to develop conventional algorithms to perform the needed tasks.

It is closely related to computational statistics which focuses making predictions using computers. Data mining is a related field of study focusing on exploratory data analysis through unsupervised learning. Machine learning is also referred to as predictive analysis.

Stock markets are generally predicted by financial experts in the past time but now data scientists have started solvingprediction problems with the progress of learning techniques. Stock market prediction is full of challenges and data scientists usually confront some problems when then try to develop a predictive model. Stocks are issued by the companies to raise their capital in order to grow up the business or to undertake new projects. There are some distinctions between buying the shares directly or from any another shareholder. By using machine learning we can determine the future risk of predicting stocks.

II. RELATED WORK

1. A local and global event sentiment based efficient stock exchange forecasting using deep learning:

Stock exchange forecasting is an important aspect of business investment plans. The customers prefer to invest in stocks rather than traditional investments due to high profitability. The stock markets are often volatile and change abruptly due to the economic conditions, political situation and major events for the country. In this study, we consider four countries- US, Hong Kong, Turkey, and Pakistan from developed, emerging and underdeveloped economies' list. We have explored the effect of different major events occurred during 2012–2016 on stock markets. We use the Twitter dataset to calculate the sentiment analysis for each of these events. The
dataset consists of 11.42 million tweets that were used to determine the event sentiment. The performance of the system is evaluated using the Root Mean Square Error (RMSE) and Mean Absolute Error (MAE). The results show that performance improves by using the sentiment for these events.

2. A machine learning approach to automated trading:
Stock market prediction regards the forecasting of the price of any given stock with in a desired time-frame and has been a heavily researched topic over past years due to the difficulty of predicting time-series that are considered to be random walks. Whilstere are those that use traditional Technical Analysis methods such as the calculation and consideration of trends, more recently the problem has attracted the attention of Machine Learning and ArtificialIntelligence approaches. This project explores and compares the current Machine Learning approaches involved in predicting the direction and prices of selected stocks for a given time range, considering short, medium and long-term investments. Using these models alongside Natural Language Processing of financial news to predict sudden, extreme fluctuations and Portfolio Optimisation to balance risk and expected return prior to trading, an automated trading agent is designed, implemented and evaluated against the index performance that the stocks are traded upon (NASDAQ100).

3. Evaluation of the effect of investor psychology on an artificial stock market through its degree of efficiency:
The main objective of this article is to develop a Cellular Automation Model in
which more than one type of stockbroker interact, and where the use and exchange of information between investors describethe complexity measured through the estimation of the Hurst exponent. This exponent represents an efficient or random market when it has a value equal to 0.5. Thanks to the various proposals, it can be determined in this investigation that a rational component must exist in the simulator in order to generate an efficient behavior.

4. Forecasting stock market movement direction with support vector machine :
Support vector machine (SVM) is a very specific type of learning algorithms characterized by the capacity control of the decision function, the use of the kernel functions and the sparsity of the solution. To evaluate the forecasting ability of SVM, we compare its performance with those of Linear Discriminant Analysis, Quadratic Discriminant Analysis and Elman Back propagation Neural Networks. The experiment results show that SVM outperforms the other classification methods. Further, we propose a combining model by integrating SVM with the other classification methods. The combining model performs best among all the forecasting methods.

III. PROPOSED WORK

KNN:

The K-nearest neighbors' algorithm is a non-parametric classification method which is used to solve both regression and classification problems. Two properties usually are suggested for KNN, lazy learning and non-parametric algorithm, because there is not any assumption for underlying data distribution by KNN.

Logistic Regression:

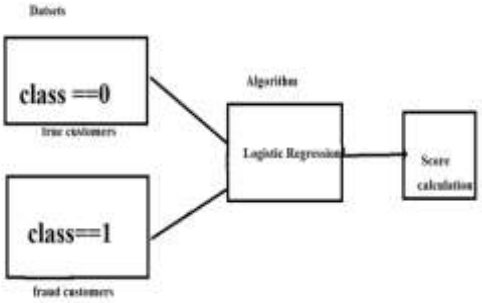
Logistic regression is a mathematical model used in statistics to estimate the probability of an event occurring based on previous dataLogistic regression is used to assign observations to a separated set of classes as a classifier. The algorithm transforms its output to return a probability value with the logistic sigmoid function, and predicts the target by the concept of probability

SVM:Support vector machine is a linear model for classification and regression problems. SVM is a supervised machine learning model that uses classification algorithms for two group classification problems.

IV. METHODOLOGY:

- ✓ **Logistic regression:**

Logistic regression is the appropriate regression analysis to conduct when the dependent variable is dichotomous (binary).
Like all regression analyses, the logistic regression is a predictive analysis. Logistic regression is used to describe data and to explain the relationship between one dependent binary variable and one or more nominal, ordinal, interval or ratio-level independent variables.
By using sigmoid function it calculates the probability and it compares that probability to the threshold probability and predicts the class of the observation



SVC:

Support Vector Machines (SVMs) are a set of supervised learning approaches that can be employed for classification and regression problems. The classifier version is named SVC. The method's purpose is finding a decision boundary between two classes with vectors. The boundary must be far from any point in the dataset, and support vectors are the sign of observation coordinates with a gap named margin. SVM is a boundary that best separates two classes with employing a line or hyperplane. The decision boundary is defined in Equation 1 where SVMs can map input vectors xi ϵ Rd into a high dimensional feature space Φ(xi) ϵ H, and Φ(.) is mapped by a kernel function K(xi, xj).

KNN:

Two properties usually are suggested for KNN, lazy learning and non-parametric algorithm, because there is not any assumption for underlying data distribution by KNN. The method follows some steps to find targets: Dividing dataset into training and test data, selecting the value of K, determining which distance function should be used, choosing a sample from test data (as a new sample) and computing the distance to its n training samples, sorting distances gained and taking k-nearest data samples, and finally, assigning the test class to the sample on the majority vote of its k neighbors.

V. CONCLUSION:

The purpose of this study was the prediction task of stock market movement by machine learning algorithms. Four stock market groups, namely diversified financials, petroleum, non-metallic minerals and basic metals, from Tehran stock exchange were chosen, and the dataset was based on ten years of historical records with ten technical features. SVM machine learning model is used for prediction.

.VI. REFERENCES:

[1] Murphy, John J. Technical analysis of the financial markets: A comprehensive guide to trading methods and applications. Penguin,1999.

[2] Turner, Toni. A Beginner's Guide To Day Trading Online 2nd Edition. Simon and Schuster,2007.

[3] Maqsood, Haider, et al. "A local and global event sentiment based efficient stock

exchange forecasting using deep learning." International Journal of InformationManagement 50 (2020): 432-451.

[4] Long, Wen, Zhichen Lu, and Lingxiao Cui. "Deep learning-based featureengineering for

stock price movement prediction." Knowledge-Based Systems 164

(2019): 163-173.

[5] Duarte, Juan Benjamin Duarte, Leonardo Hernán Talero Sarmiento, and Katherine Julieth Sierra Juárez. "Evaluation of the effect of investor psychology on an artificial stock market through its degree of efficiency." Contaduría y Administración 62.4 (2017): 1361-1376.

[6] Lu, Ning. "A machine learning approach to automated trading." Boston, MA: Boston College Computer Science Senior Thesis (2016).

[7] Hassan, Md Rafiul, Baikunth Nath, and Michael Kirley. "A fusion model of HMM,ANN and GA for stockmarket forecasting." Expert systems with Applications 33.1 (2007): 171-180.

[8] Huang, Wei, Yoshiteru Nakamori, and Shou-Yang Wang. "Forecasting stock market movement direction with support vector machine." Computers & operations research 32.10 (2005): 2513-2522.gg

[9] Sun, Jie, and Hui Li. "Financial distress prediction using support vector machines: Ensemble vs. individual." Applied Soft Computing 12.8 (2012): 2254-2265.

[10] Ou, Phichhang, and Hengshan Wang. "Prediction of stock market index movement by ten data mining techniques." Modern Applied Science 3.12 (2009): 28-42.

[11] Liu, Fajiang, and Jun

Wang. "Fluctuation prediction of stock market index by Legendre neural network with random time strength function." Neurocomputing 83 (2012): 12-21.

[12] Tsai, Chih-Fong, et al. "Predicting stock returns by classifier ensembles." Applied Soft Computing 11.2 (2011): 2452-2459.

[13] AraúJo, Ricardo De A., and Tiago AE Ferreira. "A morphological-rank-linear evolutionary method for stock market prediction." Information Sciences 237(2013): 3-17.

[14] Ballings, Michel, et al. "Evaluating multiple classifiers for stock price direction prediction." Expert Systems with Applications 42.20 (2015): 7046-7056.

[15] Basak, Suryoday, et al. "Predicting the direction of stock market prices using tree-based classifiers." The North American Journal of Economics and Finance 47 (2019): 552-567.

[16] Weng, Bin, et al. "Macroeconomic indicators alone can predict the monthly closing price of major US indices: Insights from artificial intelligence, time-series analysisand hybrid models." Applied Soft Computing 71 (2018): 685-697.

[17] Long, Jiawei, et al. "An integrated framework of deep learning and knowledge graph for prediction of stock price trend: An application in Chinese stock exchange market." Applied Soft Computing (2020): 106205.

[18] Rekha, G., et al. "Prediction of Stock Market Using Neural Network Strategies." Journal of Computational and Theoretical Nanoscience 16.5-6 (2019): 2333-2336.

[19] Pang, Xiongwen, et al. "An innovative neural network approach for stock market prediction." The Journal of Supercomputing (2018): 1-21.

[20] Kelotra, A. and P. Pandey, Stock Market Prediction Using Optimized Deep-ConvLSTM Model. Big Data, 2020. 8(1): p. 5-24.

[21] Baek, Yujin, and Ha Young Kim. "ModAugNet: A new forecasting framework for stock market index value with an overfitting prevention LSTM module and a prediction LSTM module." Expert Systems with Applications 113 (2018): 457-480.

[22] Chung, H. and K.-s. Shin, Genetic algorithm-optimized long short-term memory network for stock market prediction. Sustainability, 2018. 10(10): p. 3765.

[23] Kara, Yakup, Melek Acar Boyacioglu, and Ömer Kaan Baykan. "Predicting direction of stock price index movement using artificial neural network.