PROCEEDINGS of the

FIFTH
NATIONAL CONFERENCE
ON

RECENT TRENDS IN ADVANCED COMPUTING TECHNOLOGIES

EDITORS:
Dr S.V. Annlin Jeba
Prof. Minu Lalitha Madhavu
Prof. Gopu Darsan

Fifth Annual Conference series

RTACT`21

Organised by
Department of
Computer Science & Engineering
Sree Buddha College of Engineering
Pattoor, Alappuzha- 690529

PROCEEDINGS OF THE

FIFTH NATIONAL CONFERENCE ON

RECENT TRENDS IN ADVANCED COMPUTING TECHNOLOGIES

RTACT'21

Editors

Dr. S. V.Annlin Jeba

Prof. Minu Lalitha Madhavu

Prof. Gopu Darsan

Organized by

Department of Computer Science and Engineering

Sree Buddha College of Engineering

Pattoor P.O., Alappuzha - 690529, Kerala, India

Title: Proceedings of the Fifth National Conference on Recent Trends in Advanced Computing Technologies

Author's Name: Prof. Minu Lalitha Madhavu

Published By: Self Published

Publisher's Address: Sree Buddha College of Engineering, Pattoor P.O, Pandalam, Alappuzha, kerala, 690529

Printer's Details: Sree Buddha College of Engineering, Pattoor P.O, Pandalam, Alappuzha, kerala, 690529

Edition Details: I

ISBN: 978-93-5473-994-1 (e-book reader)

Cover Design: Prof. Gopu Darsan

Prof. K. Sasikumar
Chairman
Sree Buddha Group of Institutions
Tel: 94473 33269
Email:profsasikumark@gmail.com

MESSAGE

The 5th Annual Conference Series of Sree Buddha College of Engineering , Pattoor was conducted as an online event on 10th and 11th June 2021. Under the SBCE Conference Series, Department of Computer Science and Engineering hosted an Online National Conference on “Recent Trends in Advanced Computing Technologies- RTACT 2021” with subthemes relevant to recent advancements in the varied areas of computer science and engineering.

I am glad to note that the technical papers which were presented in the RTACT 2021 conferences by the academicians, researchers and students doing their research work in various areas of computer science and engineering are now published as an e-book with ISBN No 978-93-5473-994-1. I appreciate the organizers for their effort and hope that the papers in this volume would be useful as reference material for the interested researchers and students.

Prof. K. Sasikumar

Dr. K. Krishna Kumar
Principal
Sree Buddha College of Engineering
Pattoor P.O., Alappuzha, Kerala.
Tel: 91 79076 97944
Email: Kkk@cet.ac.in

FOREWORD

Sree Buddha College of Engineering (SBCE), Pattoor has been organizing Annual Conference Series from the year 2017 to provide a common forum for the academicians, researchers, industrial experts and students from the fields of Engineering and Technology to present their research outcomes, discuss recent advancements in respective fields and to explore future research avenues. The fifth Annual Conference Series was conducted as an online event on 10th and 11th June 2021. The Conference Series was inaugurated on 10th June in online mode. Dr. Amares Singh, Professor, SEGI University, Malaysia was the Chief Guest and Keynote Speaker of the function. A total of about 200 technical papers selected based on the review of received papers were presented in the six conferences by the authors which included industrialists, researchers, academicians and students from various engineering colleges in India.

Department of Computer Science and Engineering hosted an Online National Conference on “Recent Trends in Advanced Computing Technologies- RTACT 2021” with subthemes relevant to recent advancements in the various areas of computer science and engineering. The online conference RTACT’21 covered two days and included streams of up to three parallel sessions. The program was further enriched by the keynote presentation offered by Dr. Ragesh N.K, Practice Head, Cyber Security, Tata Elxsi , Technopark which addressed topics in Recent Advancements in the area of Computer Science.

I am happy that the technical papers which were presented in the RTACT 2021 conference are now published as an e-book with ISBN No 978-93-5473-994-1. I appreciate the valuable effort of the organizing team and earnestly hope that the proceedings will be useful for researchers, teachers, students and all those interested in the topics. I am glad to present this volume to the scientific community.

Dr.K.Krishakumar

Department of Computer Science and Engineering
Sree Buddha College of Engineering
Pattoor P.O., Alappuzha - 690529, Kerala, India

ACKNOWLEDGEMENT

The 5th Annual Conference on “Recent Trends in Advanced Computing Technologies (RTACT 2021) was successfully conducted as online event by Department of Computer Science and Engineering, Sree Buddha College of Engineering (SBCE), Pattoor,Alappuzha on 10th and 11th June 2021. The RTACT 2021 Organising Committee is grateful to the Hon'ble Chairman of the Sree Buddha Group of Institutions Prof. K. Sasikumar, and Dr. K. B.Manoj (Secretary) and Sri. K. K. Sivadasan (Treasurer) of the Sree Buddha Educational Society for their kind encouragement and support for conducting the conference. We thankfully acknowledge the guidance and support of Dr. K. Krishnakumar, Principal, Sree Buddha College of Engineering . We are thankful to our Key Speaker Dr. Ragesh N.K, Practice Head, Cyber Security , Tata Elxsi , Technopark for offering a presentation that addressed topics in Recent Advancements in the area of Computer Science. Delegates from various engineering colleges within and outside the state of Kerala, actively participated in the online conference. We thankfully acknowledge the contributions made by each member of Department of Computer Science and Engineering, SBCE for the success of the RTACT 2021 conference.

Dr. S.V. Annlin Jeba, Ms. Minu Lalitha Madhavu,Mr. Gopu Darsan

(Editors, RTACT’21)

CONTENTS

REPORT OF THE CONFERENCE

ONLINE NATIONAL CONFERENCE ON “RECENT TRENDS IN ADVANCED COMPUTING TECHNOLOGIES”- RTACT’21

The 5th Annual Conference Series of Sree Buddha College of Engineering, Pattoor was conducted as an online event on 10th and 11th June 2021. Aim of the conference series was to bring together innovative academicians, researchers and industrial experts in the field of Engineering and Technology in a common forum to present research findings, discuss the recent advancements and to explore the future directions in the emerging areas. Under the SBCE Conference Series, Department of Computer Science and Engineering hosted an Online National Conference on “Recent Trends in Advanced Computing Technologies- RTACT 2021” with subthemes relevant to recent advancements in the varied areas of computer science and engineering.

RTACT’21 THEME

RTACT’ 21 was the fifth annual Conference Series organized by the Department of Computer Science and Engineering of Sree Buddha College of Engineering. Aim of the conference was to bring young researchers in the field of Computer Science and Engineering to present their research findings and discuss the recent advancements in various areas of Computer Scince and Engineering such as Artificial Intelligence and Machine Learning,Data Mining and Big Data Analytics,Computer Vision and Digital Image Processing, Neural Networks and Deep Learning, Advanced Wireless Technologies and to explore the future directions in the emerging areas.

COMMITTEE OF RTACT’21

National Advisory Committee

Dr.R Rajesh
Central University of Kerala, Kasragode

Dr.M. Abdul Rahiman
Director, LBS-TVM
Dr Govinda K, Associate Professor, VIT Velloor
Dr. Ragesh N K, Senior Specialist, Tata Elxsi, Trivandrum
Dr J Satheesh Kumar, Bharathiyar University,
Coimbatore

Organizing Chair

Dr.S.V.AnnlinJeba, HoD, CSE

Organizing Secretary

Prof. Minu Lalitha Madhav,
Asst.Prof, CSE

Coordinators

Prof. GopuDarsan
Asst.Prof, CSE

Last date for abstract submission was 5th June 2021 and we had selected 35 papers for evaluation. The papers were presented on 10th and 11th June 2021.The online presentation was conducted through Google Meet. The online conference RTACT’21 covered two days and included streams of up to three parallel sessions. The program was further enriched by the keynote presentation offered by Dr. Ragesh N.K, Practice Head, Cyber Security , Tata Elxsi , Technopark which addressed topics in Recent Advancements in the area of Computer Science.

Three panels were formed for the evaluation. Panel I was chaired by Dr. Anil A.R , Associate Professor, Department of Computer Science and Engineering, SBCE Pattor with Prof. Lakshmi .S as Panel Member and Prof. Minu Lalitha Madhavu as Moderator. Panel II was Chaired by Prof. Supriyal L.P , Asst. Professor, Department of Computer Science And Engineering, SBCE,Pattoor with Prof. Dhanya Sreedharan as Panel member and Prof. Gopu Darsan as Moderator. Panel III was Chaired by Dr S V Annlin Jeba , Assoc. Professor and HOD, Department of Computer Science And Engineering, SBCE,Pattoor with Prof. Reeba.R as Panel member and Prof. Soumya Murali as Moderator.

The Paper entitled “Smart Farming Monitoring System” by Abdhul Azeez P.S,Amala Augustine,Ivy Rose Seban,Alphonse Treessa Jacob , Students of Amal Jyothi College of Engineering, Kanjirappally, Kottayam secured Best Paper Award under stream I.

The paper entitled ” Detection of Cyberbullying using Deep Learning” authored by Jobiya C Johnson, Merin Mathew, Anoop s nair,Vignesh SN , Prof. Lakshmi S , Students of Sree Buddha College of Engineering , Pattoor secured the Best Paper Award under stream II.

The paper entitled ” BOBtheBOT: An Intelligent Chatbot to Detect Mental Illness by Recognizing Emotion Through Text” authored by Vishnu B Dev, Ashwin, Vidya Prasannan, Megha P S, Prof. Lakshmi S , Students of Sree Buddha College of Engineering , Pattoor secured the Best Paper Award under stream III.

A valedictory function was conducted online on 11th June 2021 at 3.00 pm with all participants, and faculties. Dr S.V Annlin Jeba delivered the valedictory note .All Panel Chairs delivered felicitations and Ms. Minu Lalitha Madhavu, Organizing Secretary, announced the Best Paper Awards. Ms Lakshmi S, Asst Prof, Department of CSE was the host of the function and we had successfully competed RTACT fifth series.

SREE BUDDHA COLLEGE OF ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
Presents

Online National Conference on
Recent Trends in Advanced Computing Technologies
RTACT’21
10 & 11 JUNE 2021
Submit your papers before 20/05/2021

certificates and proceeding with ISBN for all participants

Registration Fee: 300/-

Google Meet
online platform

9595033964 9809557304 csesbce2002@gmail.com

SREE BUDDHA COLLEGE OF ENGINEERING
Pattoor P.O., Alappuzha -690529 www.sbce.ac.in
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
RTACT’21
Online National Conference on
Recent Trends in Advanced Computing Technologies

June 10 ,11
2021

Key Speaker

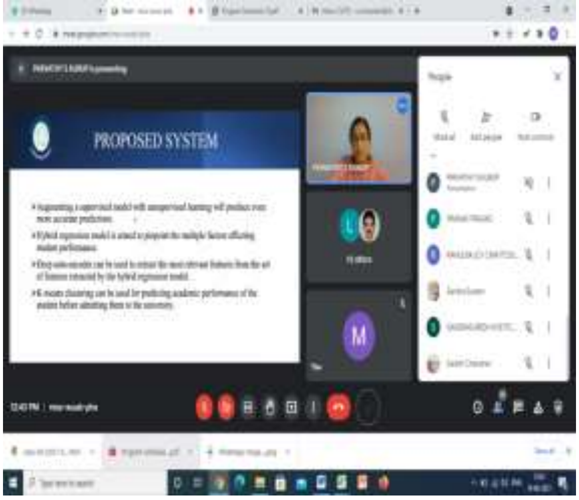
Dr. Ragesh N.K.
Practice Head
Cybersecurity
Automotive Business Unit
Tata Elxsi, Trivandrum

Google Meet
online platform

9595033964 9809557304 csesbce2002@gmail.com

AGENDA

- INTRODUCTION
- MY EXPERIENCE IN TATA ELXSI
- WHAT ARE THE OPPORTUNITIES IN INDUSTRY?
- WHAT INDUSTRY IS LOOKING FOR?
- HOW TO PREPARE?
- CHOSING THE RIGHT JOB
- BEING A CHAMPION



PROPOSED SYSTEM

Screenshot of online event

RTACT'21
FIFTH NATIONAL CONFERENCE ON
RECENT TRENDS IN ADVANCED COMPUTING TECHNOLOGIES
Highlights
June 10,11 2021
90 Authors
35 Papers
3 Panels
SREE BUDDHA COLLEGE OF ENGINEERING,ALAPPUZHA
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Expert Panel evaluating the technical papers

PAPERS PRESENTED IN THE CONFERENCE

A Novel Self-Adaptive Energy Efficient BAT Algorithm for Optimal Feature Selection

Geethu M Suresh, *Asst.Professor, Carmel College of Engineering and Technology, Kerala, India.*
Prof.Minu Lalitha Madhav, *Asst.Professor, Dept. of Computer Science, Sree Buddha College of Engineering, Kerala, India*

***Abstract*— The population-based algorithms especially swarm intelligence, may be concluded as some kind of general problem solvers, because they are applicable for all classes of optimization problems. Swarm Intelligence Based BAT algorithms are energy less processes and suffers from lack of self adaptiviness and parallel processing capabilities. The focus on issues like energy overhead in terms of computation time to find relevant features, is the critical issue addressed in this innovated implementation. So a self-adaptive parallel processing strategy with energy efficiency is proposed which optimizes the existing BAT algorithm. To handle complex batch process loops within BAT algorithms, a fitness based task parallelism is implemented to get the most benefit in terms of scalability and energy efficiency. The Task Parallelism is modeled here by accessing the number of threads to be created based on the number of swarms to be created. An algorithm for creating the tasks and assigning those to processor threads are used. The termination and executions are based on a fitness evaluation criteria, with which the necessary feature will be traced out.**

***Index Terms*—Self-Adaptive, Feature Selection, Energy Efficient, Optimization, BAT Algorithm.**

I. Introduction

The standard bat algorithm, developed by Xin-SheYang in 2010, was based on the echolocation or bio-sonar characteristics of micro bats (Yang, 2010). Before we outline the details of the algorithm, let us briefly introduce the echolocation.3.1 Echolocation of Micro bats There are about 1000 different species of bats (Colin,2000). Their sizes can vary widely, ranging from the tiny bumble bee bats of about 1.5 to 2 grams to the giant bats with a wingspan of about 2 m and may weigh up to about 1 kg. Most bats uses echolocation to a certain degree; among all the species, micro bats use echolocation extensively, while mega bats do not. Micro bats typically use a type of sonar, called, echolocation, to detect prey, avoid obstacles, and locate their roosting crevices in the dark. They can emit a very loud sound pulse and listen for the echo that bounces back from the surrounding objects (Richardson, 2008).Their pulses vary in properties and can be correlated with their hunting strategies, depending on the species. Most bats use short, frequency-modulated signals to sweep through about an octave, and each pulse lasts a few thousandths of a second (up to about 8 to 10 ms) in the frequency range of 25 kHz to 150 kHz. Typically, micro bats can emit about 10 to 20 such sound bursts every second, and the rate of pulse emission can besped up to about 200 pulses per second when homing on their prey. Since the speed of sound in air is about = 340 m/s, the wavelength λ of the ultrasonic sound bursts with a constant frequency f is given by λ = v/which is in the range of 2mm to 14mm for the typical frequency range from 25kHz to 150 kHz. Interestingly, these wavelengths are in the same order of their prey sizes. Though in reality micro bats can also use time delay between their ears and loudness variations to sense three-dimensional surroundings, we are mainly interested in some features of echolocation so that we can some link them with the objective function of an optimization problem, which makes it possible to formulate a smart, bat algorithm.

II. Literature Review

The standard bat algorithm has many advantages, and one of the key advantages is that it can provide very quick convergence at a very initial stage by switching from exploration to exploitation. This makes it an efficient algorithm for applications such as classifications and others when a quick solution is needed. However, if we allow the algorithm to switch to exploitation stage too quickly by varying A and r too quickly, it may lead to stagnation after some initial stage. In order to improve the performance, many methods and strategies have been attempted to increase the diversity of the solution and thus to enhance the performance, which produced a few good and efficient variants of bat algorithm. From a quick literature survey, we found the following bat algorithm variants:

i. Fuzzy Logic Bat Algorithm (FLBA): Khan et al.(2011) presented a variant by introducing fuzzy logic into the bat algorithm, they called their variant fuzzy bat algorithm.•
ii. Multi objective bat algorithm (MOBA): Yang(2011a) extended BA to deal with multi objective optimization, which has demonstrated its effectiveness for solving a few design benchmarks in engineering.
iii. K-Means Bat Algorithm (KMBA): Komarasamy and Wahi (2012) presented a combination of K-means and bat algorithm (KMBA) for efficient clustering.
iv. Chaotic Bat Algorithm (CBA): Lin et al. (2012)presented a chaotic bat algorithm using L´evy flights and chaotic maps to carry out parameter estimation in dynamic biological systems.

v. Binary bat algorithm (BBA): Nakamura et al.(2012) developed a discrete version of bat algorithm to solve classifications and feature selection problems.

vi. Differential Operator and L´evy flights Bat Algorithm (DLBA): Xie et al. (2013) presented a variant of bat algorithm using differential operator and L´evy flights to solve function optimization problems.

vii. Improved bat algorithm (IBA): Jamil et al.(2013) extended the bat algorithm with a good combination of L´evy flights and subtle variations of loudness and pulse emission rates. They tested the IBA versus over 70 different test functions and proved to be very efficient

III. Self-Adaptive Energy Efficient Bat Algorithm for Feature Selection.

BAT Algorithm is based on the echolocation property of bats with reference to the property of loudness and emission. Each bat moves with a velocity Vi position (solution) xi with a frequency [fmin, fmax] or wavelength [λmin, λmax] and loudness Ai, pulse rate ri .The range of loudness varies between finite (positive) A0 to a minimum positive finite value Amin. As it searches and finds its prey. Once prey is found it changes frequency, loudness and pulse emission rate where ri∈ [0, 1]. Search is intensified by a local random walk. Selection of the best bat continues until predefined stopping conditions are met. The parameters used in the BAT Algorithm are Frequency, Velocity, Bat Position, Loudness, Pulse Emission and Fitness Function.

The self-adaptive energy efficient BAT algorithm (EEBAT) consists of the following steps. i. Initialization. ii. Parallel Processing. iii. Evaluation of the Optimal Solution. iv. Replacement. In the first step of EE-BAT the various control parameters like frequency, velocity and loudness are initialized.. Also the best solution is initialized to null. The swarm division process is an iterative process. It begins by dividing the entire swarms into smaller groups by dividing into smaller subgroups using K- means Clustering algorithm. Those individuals having similar fitness will be in the same subgroup. The local search for the best individual will be performed in two stages. In the first stage each members of the group will learn only from their local minima. The position will be updated by changing the velocities. And this process is generally based on the previous knowledge and the current local minima.

In the second stage the local minima with higher fitness values will be selected and these will be moving towards the global optima. This process however continues by learning from the higher level and achieves better positions. After each iteration the bats will achieve a better position.

The iterative steps of the swarm division process is performed using Task Parallel Library. It is a library in .Net to implement task parallelism and enable concurrency. The task is heart of the library. A task can be defined as a process in execution or a process that is ready to run. Implementing tasks using TPL improves the efficiency of the code to a great extent. The library optimizes the number of threads required to process the parallel threads and evaluates the number of available process and schedules them efficiently. There is a thread pool in the library which enables a queuing mechanism for allocating the tasks among the available thread pool. When a process creates a new task this task will be attached to a global queue and when a thread becomes available it will be deleted from the queue and it will be processed by the available thread.

In the task Parallel model, the relationships between tasks are used to implement the adjacentness with in or to reduce computation costs. This Task parallel model is typically employed to solve the issues associated with the amount of data and iterations used in conventional feature selection models. Here tasks are created based on the swarm iterations to help optimize the cost of data movement among tasks. The task processing is shared with commonly addressable space. The fitness value and computational parameters are shared in this work space. The mechanisms for releasing the address space after thread terminations are also implemented. Global cache registers are released every time the whole thread is released. The volume and frequency of interactions are automatically being monitored in the Task Parallel Library included. The Scheduling of Tasks upon Processors is based on the is based on the Task Switching Routines In task parallelism, each task will be running in on 1 or P processors, the machine switching between task and data parallelism as needed. For balanced Bat implementation, the task parallelism down to some level in the bat sequence is selected. This switch will occur no later than level logd P, since at this level there will be a frontier of P identical tasks, one for each processor to work at unit efficiency. A segment of a task can be divided into a number n of parallel sections with a duration tp, then execution time will be determined by the longest stretch system costs plus time for the organization of parallelism. Acceleration coefficient (speed) at the parallel execution of this task is:

$$Acc = \frac{1}{\left((S + \frac{(1-S)}{n} \right)}.$$

Where: S is the percentage of the work that cannot be parallelized; n is number of processors.

Typical interaction-reducing techniques applicable to this model include reducing the volume and frequency of interaction by promoting locality while mapping the tasks based on the interaction pattern of tasks, and using asynchronous interaction methods to overlap the interaction with computation. The Parallel.Do method is a method defined in TPL that takes two or more delegates as arguments and potentially executes them in parallel. The two stages defined in the swarm division process can be executed as two delegates and execute them in parallel. When the function is invoked more parallel tasks will be generated as the number of subgroups in swarm division increases. TPL will check for the available number of threads and the library will execute the tasks parallel based on the available number of free threads.

IV. Evaluation Results

For the experiment five datasets were considered, WQ, NSL KDD, Vote, Heart, and Mushroom. The Water Quality dataset (Dzeroski et al. 2000) has 14 target attributes that refer to the relative representation of plant and animal species in Slovenian rivers and 16 input attributes that refer to physical and chemical water quality parameters. NSL KDD contains 43 features per record, with 41 of the features referring to the traffic input itself and the last two are labels (whether it is a normal or attack) and Score (the severity of the traffic input itself). Vote dataset represents votes for each of the U.S. House of Representative's congressmen with the class label democrat and republican.

Heart is a binary class data that contains 76 attributes although all the published experiments reference to using only 14 of the original attributes. This data has been used to predict heart diseases, whereby the class label of zero and one refers to the absence or existence of heart disease in the patient. Mushroom dataset includes descriptions of hypothetical samples corresponding to 23 species of gilled mushrooms in the Agaricus and Lepiota Family. Each species is identified as definitely edible, definitely poisonous, or of unknown edibility and not recommended.

Dataset	Number of Features	Number of Selected Features in SBAT	Number of Selected Features in EEBAT
WQ	38	13	5
NSL KDD	42	19	7
VOTE	16	5	3
HEART	13	6	4
MUSHROOM	22	11	5

Table 1. Number of Features Selected from Different Datasets

It is evident from the result of this evaluation that our proposed algorithm performs more efficiently than the SBAT [13] when the data size increases. That is when the number of swarms increases the performance of the SBAT[13] degrades. This is rectified by our approach. Our algorithm performs efficiently as the number of instances increases. The evaluation results are also plotted graphically in Fig 1.

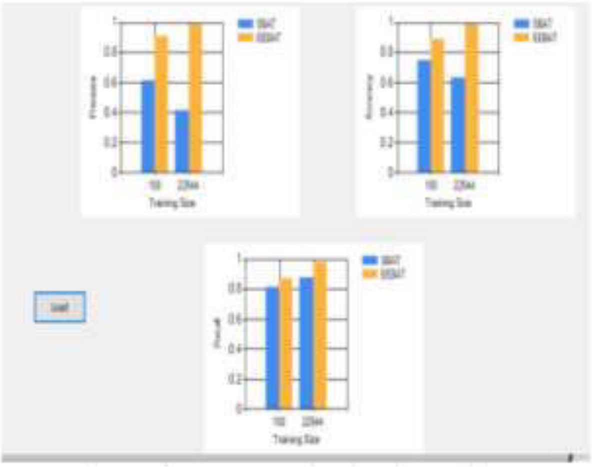


Fig 1. Accuracy of EEBAT over SBAT

The results show that our proposed approach EEBAT shows more accuracy, precision and recall than the SBAT [13]. The evaluation of the fitness function reveals that unlike other approaches our proposed algorithm converges faster than at approximately 40 iterations with a gentle slope. It obtains a higher fitness value after convergence and remains constant. It also proves that the improvement of SBAT prevent the individuals from getting trapped into local minima and search for a better solution. The proposed approach lowers the time complexity.

CONCLUSION

The goal of the work was to propose an optimal swarm based BAT algorithm which selects the relevant features in a smaller interval of time. Our aim was successful with the development of our novel self-adaptive energy efficient BAT algorithm. Our technique was examined and compared with the existing swarm based BAT algorithm. The result proved that the proposed technique has better accuracy, precision and also less time overhead than swarm based BAT.

ACKNOWLEDGMENT

This work is the outcome of guidance provided by dedicated and experienced personal of SBCE Pattoor. With profound sense of indebtedness, we use this opportunity to express our sincere thanks to our beloved Principal for providing all sort of support and necessary facilities and for the inspiration to complete our work .We express our sincere gratitude Head of the Department of Computer Science and Engineering for the inspiration and permission to carry out our work. Last but not the least ; we extend our sincere thanks to all the members of our computer science department for their help and support .And also would like to extend our deep sense of gratitude to all those who have assisted us in the successful completion of this work.

REFERENCES

[1] Bora, T. C., Coelho, L. S., Lebensztajn, L., (2012). Bat-inspired optimization approach for the brushless DC wheel motor problem, IEEE Trans. Magnetics, Vol. 48, No. 2,947-950 (2012).Colin, T., (2000). The Varienty of Life. Oxford UniversityPress, Oxford.

[2] Cui, Z. H., and Cai, X. J. (2009). Integral particle swarm optimisation with dispersed accelerator information, Fundam. Inform., Vol. 95, No. 3, 427–447.

[3] Damodaram, R., Valarmathi, M. L., (2012). Phishing website detection and optimization using modified bat algorithm, Int. J. Engineering Research and Applications, Vol. 2, No.1, pp. 870–876.

[4] Du, Z. Y., Liu B., (2012). Image matching using a bat algorithm with mutation, Applied Mechanics and Materials, Vol. 203, No. 1, pp. 88–93.

[5] Faritha Banu, A., Chandrasekar, C., (2012). An optimized appraoch of modified bat algorithm to record deduplication, Int. Journal of Computer Applications, Vol.62, No. 1, pp. 10–15.

[6] Fister Jr., I., Fister, D., and Yang, X. S., (2013). A hybrid bat algorithm, Elekrotehniˇski Vestnik (English Edition), (2013)submitted).

[7] Fister, I., Fister Jr., I., Yang, X. S., and Brest, J., (2013).On the representation of individual s using quaternions in swarm intelligence and evolutionary computation, IEEE Trans. Evol. Computation, (2013, submitted).

[8] Gandomi, A. H., Yang, X. S., Talatahari, S., and Deb, S., (2012). Coupled eagle strategy and differential evolution for unconstrained and constrained global optimization Computers & Mathematics with Applications, vol. 63, no.1, pp. 191–200.

[9] Gandomi, A. H., Yun, G. J., Yang, X. S., Talatahari,S., (2013a). Chao-enhanced accelerated particle swarm optimization,

Communications in Nonlinear Science and Numerical Simulation, Vol. 18, No. 2, pp. 327–340.

[10] Gandomi, A. H., Yang, X. S., Alavi, A. H.,Talatahari, S. (2013b). Bat algorithm for constrained optimization tasks, Neural Computing and Applications,http://link.springer.com/article/10.1007

[11] Huang, G. Q., Zhao, W. J., and Lu, Q. Q., (2013). Bat algorithm with global convergence for solving large-scale optimization problem, Application Research of Computers,vol. 30, no. 3, 1-10 (in Chinese).

[12] Jamil, M., Zepernic, H.-J., and Yang, X. S., (2013).Improved bat algorithm for global optimization, Applied Soft Computing, (2013, submitted).Khan, K., Nikov, A., Sahai A., (2011). A fuzzy bat clustering method for ergonomic screening of office workplaces, S3T 2011, Advances in Intelligent and Soft Computing, 2011, Volume 101/2011, No. 1, pp. 59–66.

[13] Jiaqi Li , Zhifeng Zhao , Rongpeng Li , and Honggang Zhang “AI-Based Two-Stage Intrusion Detection for Software Defined IoT Networks” in IEEE Internet Of Things Journal, Vol. 6, No. 2, April 2019

Predicting Student Performance Using Hybrid Regression and Clustering: A Deep Learning Approach

Ms. Dhanya Sreedharan
Assistant Professor
Department of computer Science and Engineering
Sree Buddha College of Engineering
Pattoor

Parvathy S Kurup
Department of Computer Science and Engineering
Sree Buddha College of Engineering
Pattoor

Abstract—**Educational institutions face several challenges while selecting the appropriate candidates during their admission process. Each university should strive for a valid and reliable admission criterion that select the most relevant candidates who likely to perform well academically. Several key factors affect student academic performance. This study focuses on finding out the most relevant attributes and features that affect the performance of students and thereby helping universities in admission decision making. The proposed model consists of two different modules a Hybrid regression module and a Deep learning module. The hybrid regression module is used to extract the hidden patterns and relevant features from a huge educational database. Lasso Linear Regression, Collaborative Filtering, and Fuzzy Set Rules constitute the Hybrid regression module. The Deep Learning model predicts the future academic performance of the students and it consists of Deep Auto Encoder and K-means Clustering. The Deep Auto Encoder is used here for dimensionality reduction and key feature selection from a huge dataset. K-means algorithm is used for predicting the future academic performance of the students and to predict at-risk students before admitting them to the university. A semi supervised learning approach is used here which utilizes the features of both supervised and unsupervised learning methods. This study also focuses on finding out the socio-economic and personal factors that affect student performance such as their family background, student social information and student demographic details.**

Keywords—Educational Data Mining, Machine Learning, Deep Learning, Student Performance Prediction.

I. Introduction

Education is the bedrock of national integration and development. So, quality education and skillful students are the prime factors that influence national growth. Through the years so many studies were conducted to improve the quality of education delivered by higher educational institutions. The admission mechanism is one of the complicated tasks faced by the universities. The main challenge faced by them is to find out whether the student is skilled for taking the particular course or not. Many universities in the world are using conventional statistical methods for predicting students' future performance. So, they face several challenges when analyzing their huge educational databases. Here comes the role of Educational Data Mining (EDM) which is the most popular technique used to extract hidden patterns and relevant information from a huge educational database. These extracted features can be then used for prediction. Educational Data Mining is the knowledge discovery in educational databases to solve educational problems. Predictive Analytics mainly deals with predicting student performance utilizing attributes and prediction methods.

This study is based on deep learning techniques and uses student academic details along with their family background, demographics, and social network interactions. It includes the use of the technology interaction process, class characteristics, and student characteristics. It also focuses on combining Learning Analytics (LA) and Predictive Analysis (PA). The objectives of this study are

- To find out the benefits of the semi-supervised learning technique over the conventional supervised learning method.
- To find out the impact of clustering over-classification in predictive analysis
- To pinpoint the multiple influential factors impacting student performance
- To check the efficiency of the hybrid regression model in predicting accurate results
- To prove the efficiency of deep autoencoder in feature selection and dimensionality reduction from educational data sets.
- To find out the at-risk students very early and to build a strategic plan to improve their academic performance

A hybrid regression model is used in this study to overcome the limitations of single baseline models used in most of the studies conducted in this field. It consists of three dynamically weighted techniques such as collaborative filtering, lasso linear regression, and fuzzy set rules for finding out the most influential factors from the dataset. The prediction model consists of k-means clustering along with deep autoencoders. Deep auto encoders are used here for dimensionality reduction and to filter out the redundant features.it compresses data and then recreates a new representation of the original data's input. K-means clustering predicts the future student performance by assigning data points to k-groups.

The underused metrics such as non-academic attributes is one of the focus of this study. The performance evaluation of the hybrid regression model can be done using Root Mean Square Error (RMSE). Deep autoencoders can be evaluated by means of precision and accuracy and k-means through the number of iterations and sum squared errors.

The rest of this paper is organized as follows section 2 we introduce some topics related to our model. The proposed architecture and detailed description of the mode is given in section 3. Section 4 outlines our conclusion.

II. RELATED WORKS AND RESEARCH GAPS

.

The quality and reputation of all higher educational institutions directly depends up on their student's performance. Educational data mining is currently the most commonly used technique by researchers to evaluate and predict student performance due to its significance in decision making[1]. For predicting student performance, the main factors to be considered are attributes and prediction methods. Several studies find out the relationship between the admission criteria scores and the graduation grades[2]. Pre-admission scores alone are insufficient for predicting graduation result of the student but may serve as a useful guide.one of the study showed that ethnic background of the student is statically insignificant in predicting their performance. The term time employment and family size had an adverse impact on academic performance[3]. Personal background played the most vital role in student performance prediction. A study focused on learning analytics used a combination of an online learning environment and an online practice environment with classroom teaching calculate performance prediction based on learning grades in quizzes and home works[4][1]. Focusing on course specific data improves the accuracy of grade prediction [grade prediction]. Prior courses can provide students with knowledge for future courses, so that grades of the prior courses can be used to predict grades in future course[5].

Another study states that the student performance is the reflection of the level of educational institutions. The total CGPA score alone can't be considered as a parameter to assess student growth and gender doesn't reflect student performance[6]. The socio demographic information, socio economic status, high school background, enrolment average grade, high school final grade etc are considered for prediction in a study. A segmentation framework is proposed to classify the at-risk students[7]. There are many factors that could affect student performance, one of the researches has shown that historical grades, student activities on learning platforms, student demographics information and student profile significantly affects the student performance.

All these studies enforce that student performance prediction using educational data mining helps to decrease the failure rate by predicting at-risk students and by reducing the dropout tendencies. There are several critical factors that affect the student's academic performance one is the CGPA of previous course[1] and several socio-economic factors as well as personal factors of the student. Throughout the literature either students' pre-admission record or personal attributes are used for prediction, but the combination of both are not used.

The prediction models developed in most of the literatures are based traditional regression and classification techniques. Most of them are based on supervised learning technique. The most common statistical and machine learning algorithms used in prediction are Linear regression, Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), Multiple Linear Regression (MLR), Multi-Layer Perceptron (MLP)- Artificial Neural Network (ANN), Support Vector Machine (SVM), Decision trees, Naïve Bayes etc. ANN outperformed all other classification techniques in most of the studies[1][8] . PCA along with MLR proved to improve the predictive accuracy of the model[4].

For predicting continuous values or features combining two or more regression techniques can improve the prediction accuracy. The hybrid regression model used in the study[9]showed considerable improvement compared to single baseline models and demonstrated the practicality of the proposed approach in pinpointing multiple factors impacting student performance. Deep learning approaches have found unprecedented success in a myriad of applications involving regular structured data such as images(grids) and text(sequences)[5].

To the best of our knowledge this is the first study which uses semi supervised learning method based on deep learning, clustering and uses student academic details along with their personal attributes for university's admission management system. A few studies used deep learning strategies for student performance prediction[5][10][11]. It used Recurrent Neural Network and Multi-Layer Perceptron for grade prediction under a course specific framework. Most of the studies used small dataset for prediction[8][12][3][13]. Deep autoencoders are used in literatures in the field of image processing and computer vision[11].

III. PROPOSED ARCHITECTURE AND DESCRIPTION

The proposed model is based on predicting student performance using hybrid regression and k-means clustering using deep auto encoders. It is a semi supervised learning approach and occurs when only part of the given input data has been labelled. Unsupervised and semi-supervised learning are the more appealing alternatives of supervised learning as it can be time consuming and costly to rely on domain expertise to label data appropriately for supervised learning. Semi-supervised learning is an approach to machine learning that uses a combination of a small amount of labelled data with a large amount of unlabeled data during training. Semi-supervised learning has the properties of both unsupervised learning (with unlabeled data) and supervised learning (with labelled data). It occurs when part of the given input data has been labelled. It is a special instance of weak supervision. Learning accuracy can be considerably improved by joining large amount of unlabeled data with a small labelled dataset. The acquisition of labelled data for a learning problem often requires a skilled human agent or a physical experiment. Supervised learning is time consuming and quite expensive to train datasets. The appealing alternatives are unsupervised and semi supervised learning methods.

This study can be mainly divided into three parts. The first part of the study is aimed to find out the efficiency of a hybrid regression model in improving the predictive accuracy of the model. The main objective of the hybrid regression model is to pinpoint the multiple factors impacting student performance. The second part is the deep autoencoder which is used for dimensionality reduction and to recreate a new representation of the original data's input. The third part is a k-means clustering model to cluster dataset into groups based on similarity and dissimilarity.

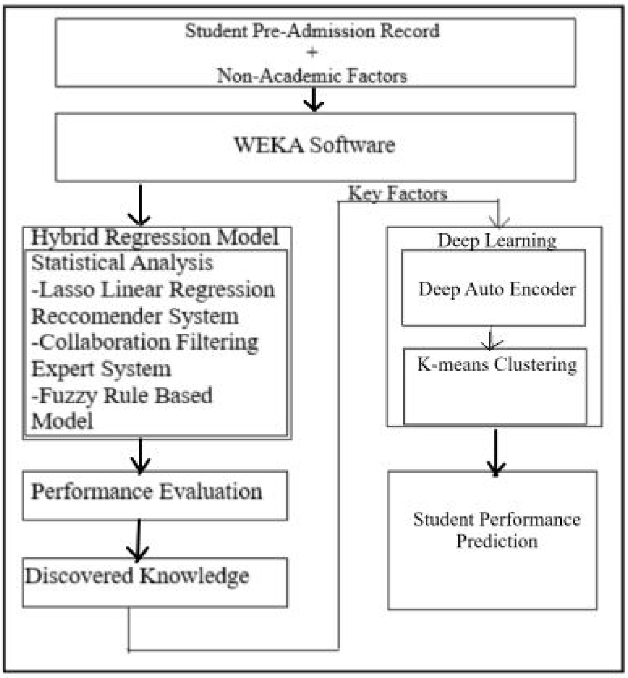


Fig .1. Proposed system architecture

A. HYBRID REGRESSION MODEL

It is a supervised learning model which uses a training set to teach models to yield the desired output. The training dataset consist of inputs and the desired outputs, which allows the model to learn overtime. The hybrid regression model consists of three learning models namely Lasso Linear Regression, collaborative filtering and fuzzy rule-based model.

a)Lasso Linear Regression

It is a statistical method which is an optimized type of linear regression also called regularized linear regression. It uses a regularization parameter that can be multiplied by the summation of absolute value of weights and get added to the loss function. It is used in data analysis to perform both variable selection and regularization to improve the prediction accuracy and interpretability of the model. It can enhance the overall accuracy of the regression model in two ways.

i. It uses a feature selection latently, which removes irrelevant features.
ii. It estimates sparse coefficient by adding a loss function as a regularizer.

In this study lasso linear regression is used to avoid irrelevant features as well as data outlier subsets because a greater number of features are used for predicting student performance.

b)Collaborative Filtering

Collaborative Filtering predicts student performance by discovering the hidden patterns in the historical student-course relations in a neighborhood-based approach. It is a paramount approach used for recommender systems based principally on the overall past relationships between students and their studied courses. Matrix factorization is used along with collaborative filtering for scalability, performance and accurate predictions. Non-negative matrix factorization technique can be used for regression prediction.

c)Fuzzy Rule Based model

It is an expert system with more rules and fuzzy membership operations that is beyond the classical Boolean logic. It consists of two main components

i. A knowledge base represented as if…then rules
ii. An inference methodology for reasoning

Fuzzy model focuses on predicting student grades by analysing their past studied courses individually. In this study we use fuzzy rule-based model for predicting the highest overall grade obtained by the student based on course difficulty level by training model with course difficulty level.

The second part of the study consists of a deep autoencoder which is used to extract the most relevant features from the set of features extracted from the hybrid regression model.

B. DEEP AUTO-ENCODER

It is an unsupervised learning method uses back propagation to learn patterns from the given data set. In this study deep autoencoder is used for dimensionality reduction that is to compress data and then recreate a new representation of the original data's input. Deep learning approaches have made unprecedented success in a myriad of applications involving regular structured data such as images and texts. The essence of deep auto encoder is its ability to learn and it is recognized by many researchers. There are numerous layers associated with deep autoencoders they are input layer output layer and the hidden layer. Hidden layer specifically acts as a bottleneck to compress the input layer prior to reconstructing with the output layer, there are two stages

i. Stage from the input to the hidden layer: Encoding
ii. Stage from the hidden layer to the output: Decoding

This kind of processing can effectively reduce the number of parameters in the encoding and decoding stages in the network.
The third part of the study consists of a prediction model which is used for predicting student performance and to thereby identifying the at-risk students. K-means clustering is used here for student performance prediction.

C. K-MEANS CLUSTERING

Clustering is a useful tool in data science and machine learning. It is a method for finding a cluster structure in dataset that is characterized by the greatest similarity within the same cluster and the greatest dissimilarity between different clusters. The k-means is a well-known clustering algorithm in which data points are assigned into k-groups where ‘k’ represents the number of clusters based on the distance from each group’s centroid. Here k-means is used for clustering students based on their performance prediction to reduce the dropout tendencies and failure rate.

IV. CONCLUSION

The aim of this study is to help universities in their admission decision making by predicting students’ future academic performance before admitting them to the universities. A prediction model is proposed using a hybrid regression model along with deep autoencoders and k-means clustering based on a deep learning approach. Based on the literature survey we hope that our proposed model will be successful when implemented.

REFERENCES

[1] H. A. Mengash, “Using data mining techniques to predict student performance to support decision making in university admission systems,” *IEEE Access*, vol. 8, pp. 55462–55470, 2020, doi: 10.1109/ACCESS.2020.2981905.

[2] A. I. Adekitan and O. Salau, “Toward an improved learning process: the relevance of ethnicity to data mining prediction of students’ performance,” *SN Appl. Sci.*, vol. 2, no. 1, pp. 1–15, 2020, doi: 10.1007/s42452-019-1752-1.

[3] S. Sothan, “The determinants of academic performance: evidence from a Cambodian University,” *Stud. High. Educ.*, vol. 44, no. 11, pp. 2096–2111, 2019, doi: 10.1080/03075079.2018.1496408.

[4] S. J. H. Yang, O. H. T. Lu, A. Y. Q. Huang, J. C. H. Huang, H. Ogata, and A. J. Q. Lin, “Predicting students’ academic performance using multiple linear regression and principal component analysis,” *J. Inf. Process.*, vol. 26, pp. 170–176, 2018, doi: 10.2197/ipsjjip.26.170.

[5] Q. Hu and H. Rangwala, “Reliable Deep Grade Prediction with Uncertainty Estimation,” *arXiv*, pp. 76–85, 2019.

[6] Y. Yao, Z. Zhang, H. Cui, T. Ren, and J. Xiao, “The Influence of Student Abilities and High School on Student Growth: A Case Study of Chinese National College Entrance Exam,” *IEEE Access*, vol. 7, pp. 148254–148264, 2019, doi: 10.1109/ACCESS.2019.2946503.

[7] V. L. Miguéis, A. Freitas, P. J. V. Garcia, and A. Silva, “Early segmentation of students according to their academic performance: A predictive modelling approach,” *Decis. Support Syst.*, vol. 115, pp. 36–51, 2018, doi: 10.1016/j.dss.2018.09.001.

[8] L. M. Abu Zohair, “Prediction of Student’s performance by modelling small dataset size,” *Int. J. Educ. Technol. High. Educ.*, vol. 16, no. 1, 2019, doi: 10.1186/s41239-019-0160-3.

[9] A. Alshanqiti and A. Namoun, “Predicting Student Performance and Its Influential Factors Using Hybrid Regression and Multi-Label Classification,” *IEEE Access*, vol. 8, pp. 203827–203844, 2020, doi: 10.1109/access.2020.3036572.

[10] A. Hernández-Blanco, B. Herrera-Flores, D. Tomás, and B. Navarro-Colorado, “A Systematic Review of Deep Learning Approaches to Educational Data Mining,” *Complexity*, vol. 2019, 2019, doi: 10.1155/2019/1306039.

[11] W. Yan, D. Wang, M. Cao, and J. Liu, “Deep auto encoder model with convolutional text networks for video recommendation,” *IEEE Access*, vol. 7, pp. 40333–40346, 2019, doi: 10.1109/ACCESS.2019.2905534.

[12] R. C. Deo, Z. M. Yaseen, N. Al-Ansari, T. Nguyen-Huy, T. A. M. P. Langlands, and L. Galligan, “Modern Artificial Intelligence Model Development for Undergraduate Student Performance Prediction: An Investigation on Engineering Mathematics Courses,” *IEEE Access*, vol. 8, pp. 136697–136724, 2020, doi: 10.1109/ACCESS.2020.3010938.

[13] A. Polyzou and G. Karypis, “Grade prediction with models specific to students and courses,” *Int. J. Data Sci. Anal.*, vol. 2, no. 3–4, pp. 159–171, 2016, doi: 10.1007/s41060-016-0024-z.

“Parking Wallet”- *A smart parking booking system*

Sandra Suresh
dept. of CSE
Carmel College of Engineering and Technology
Alappuzha,Kerala,India
sandrasuresh1399@gmail.com

Sarath chandra prasad R
dept. of CSE
Carmel College of Engineering and Technology
Alappuzha,Kerala,India
sarathchandravilasam@gmail.com

Rahul Raj C V
dept. of CSE
Carmel College of Engineering and Technology
Alappuzha,Kerala,India
rahulrajcv55@gmail.com

Geethu M Suresh
Assistant Professor
dept. of CSE
Carmel College of Engineering and Technology
Alappuzha,Kerala,India
geethum@carmelcet.in

0000-0001-6991-284X

***Abstract*—In the modern society, there is an ever-increasing number of vehicles. This is leading to problems such as large urban parking lots becoming inefficient, increasing difficulty to find open spaces in busy parking lots, as well as the increasing need to devote larger areas of land for additional parking spaces.For resolving these issues we propose a parking management application : *“Parking Wallet”*.It is a android based application with multiple user services are provided regarding parking.**

I. *Introduction*

Today car parking is a major issue in cities due to rising in the number of personal vehicles over the years and it is expected to rise even more in the next coming years. This project develops an online system to manage parking and provide the facility to take an online reservation in the parking centers. The purpose of this project is to track and manage the occupancy of car parking in the parking centers. • The conventional parking system requires the driver to queue at the boom gate while waiting for the ticket which will be available when there is an empty parking space. • The driver also needs to search the parking lot by themselves. This will bring difficulties in searching the available parking lot which leads to time and fuel wasting especially while idling or driving around parking lots that lead to more carbon dioxide (CO2) emission being produced. • Now we are going to introduce an online system for the parking centers.It helps us to improve the customer satisfaction as well as a great deal of traffic congestion in cities generally is caused by drivers looking for parking spots.

II. *Literature Review*

Considering the growing requirement of a smart parking system, different parking systems have been presented in the past. Several researchers have designed and enhanced smart parking systems to make them efficient and reliable so that people can easily locate an ideal parking lot according to their requirements. Various approaches and techniques have been deployed in the past years with different outcomes. Propositioned an intelligent parking system that lets users reserve parking for cars and directs them to the free parking for cars simultaneously. The given solution not only assists in a significant reduction in traffic arising due to parking space search but also improves the occupancy by easily managing the space for parking, an expensive resource in large cities

Alkharabsheh [1] has introduced an intelligent cooperative parking system based on multi-agents. The given solution chiefly consisted of a multi-agent approach combined with hardware elements like IR sensor nodes to detect the parking slot status and accordingly transmit the information to Arduino. A device called gateway can be used to gather the status from the sensors wirelessly. The system of agents will be used to assess the information collected, and then send the drivers the relevant results in real time through the Internet. This solution can be used to solve many issues like the cost of petrol, car accidents, and traffic management. The outcomes demonstrate the practicality of the proposed solution, which also achieved excellent results.

Mendiratta et al. [2] put forward a mechanism for the detection of car parking space with the help of an ultrasonic sensor, combined with the concept of the Internet of Things. It was achieved by transmitting the parking slot status to the Internet. This technique sends the data from the ultrasonic sensor via Wi-Fi in which the IoT platform is also involved. The problem in that system was that the ultrasonic sensor was getting rust on its surface. That led the system to misbehave.

Caballero-Gil et al. [3] also used IoT for smart parking guidance systems. Their solution includes a central system to estimate available indoor parking areas, and an inexpensive smartphone application to get data of predicted and actual parking occupancy. This scheme utilizes data from each of the two sources directionally in order that the central forecast system is provided with data acquired from the distributed system which is based on smartphones, and the other way around. The mobile application employs various wireless technologies to supply the estimation system with real-time parking data and obtain useful suggestions from the system regarding the parking space.

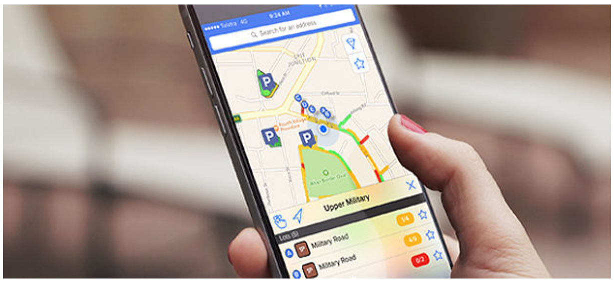
III. *Methodology*

Basically this system is a combination of smart parking, smart reservation and management system with the android application. Idea behind Slot Allocation: In this method latitude and longitude are used for smart parking and the functions are as follows:

1.Initially, the Latitude and Longitude of the center of the slot will be stored in the database.

2.For User side, slot selection is made from the mobile application.

3.The user will have to reach the parking lot in 30 minutes. After reaching in the parking, the user will go to his booked slot and press a button.



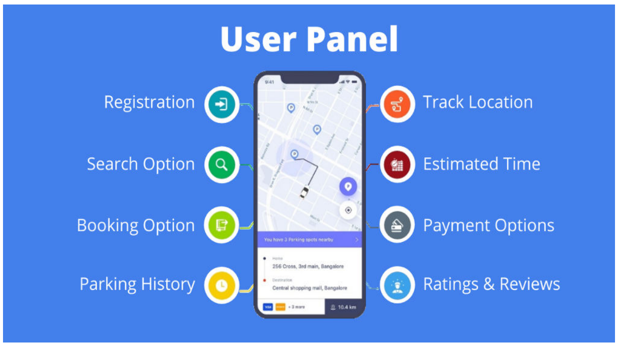
4. After pressing the button, two things will be found.

1 user's current Latitude and Longitude Points .

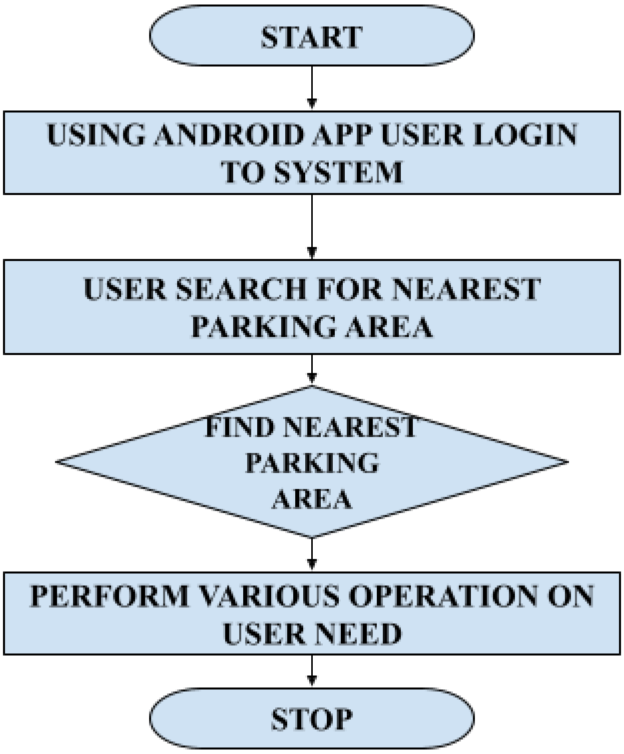
2 with the help of point of slot, the fictional circle with a radius of 2 meters will get.

5.If the current point is within this circle then the user's slot will be confirmed and it will get a confirmation message. And if it is not in the points of the circle then it will be given an error message. Note that if the user will not reach within 30 minutes then his booked slot will be canceled.

6.Also the application includes a payment platform for user.



This system is used for finding a location near by the user. The user can login the application and create an id.then the user can view various slots. select nearby or specific area of their choice to view whether space is available or not.If the booking space is available, then user can book it for specific time slot.The booked space will be marked and will not be available for anyone else for the specified time.This system provides an additional feature of cancelling the bookings.user can cancel their reserved space anytime. For finding the distance we use the dijkstra algorithm. And we provided an online map to track the location.


START
USING ANDROID APP USER LOGIN TO SYSTEM
USER SEARCH FOR NEAREST PARKING AREA
FIND NEAREST PARKING AREA
PERFORM VARIOUS OPERATION ON USER NEED
STOP

.Dijkstra algorithm

Dijkstra's algorithm is an algorithm for finding the shortest paths between nodes in a graph, which may represent, for example, road networks. It was conceived by computer scientist Edsger W. Dijkstra in 1956 and published three years later [7]. The algorithm exists in many variants; Dijkstra's original variant found the shortest path between two nodes, but a more common variant fixes a single node as the source node and finds shortest paths from the source to all other nodes in the graph, producing a shortest-path tree. The Dijkstra algorithm has been implemented in the parking system. The way that has been used to determine the distance via a pathway. The algorithm used the minimum value between two points. The algorithm finds the shortest path between that node and every other [8]. It can also be used for finding the shortest paths from a single node to a single destination node by stopping the algorithm once the shortest path to the destination node has been determined. Let the node at which we are starting be called the initial node. Let the distance of node Y be the distance from the initial node to Y. Dijkstra's algorithm will assign some initial distance values and will try to improve them step by step.Mark all nodes unvisited. Create a set of all the unvisited nodes called the unvisited set.

1. Assign to every node a tentative distance value: set it to zero for our initial node and to infinity for all other nodes. Set the initial node as current.

2. For the current node, consider all of its unvisited neighbours and calculate their tentative distances through the current node. Compare the newly calculated tentative distance to the current assigned value and assign the smaller

one. For example, if the current node A is marked with a distance of 6, and the edge connecting it with a neighbour B has length 2, then the distance to B through A will be 6 + 2 = 8. If B was previously marked with a distance greater than 8 then change it to 8. Otherwise, the current value will be kept.

3. When we are done considering all of the unvisited neighbours of the current node, mark the current node as visited and remove it from the unvisited set. A visited node will never be checked again.

4. If the destination node has been marked visited (when planning a route between two specific nodes) or if the smallest tentative distance among the nodes in the unvisited set is infinity (when planning a complete traversal; occurs when there is no connection between the initial node and remaining unvisited nodes), then stop. The algorithm has finished.

5. Otherwise, select the unvisited node that is marked with the smallest tentative distance, set it as the new "current node", and go back to step 3.

When planning a route, it is actually not necessary to wait until the destination node is "visited" as above: the algorithm can stop once the destination node has the smallest tentative distance among all "unvisited" nodes (and thus could be selected as the next "current").

IV . *CONCLUSION*

The smart parking online booking system has been successfully designed. Based on this system, it is proved that the system has provided convenience parking system to the user. since the priority is to find and provide the nearest parking lot to the entrance for the user. The driver doesn’t need to waste their time searching the vacant parking and he also can obtain the nearest parking to the entrance with the help of the system. Besides that, the smart indoor parking system has provided the nearest parking lot to entrance according to the Dijkstra Algorithm. Dijkstra Algorithm is the calculation method for determining the shortest distance. By applying Dijkstra Algorithm, all the parking lot in the parking system can be utilized efficiently

ACKNOWLEDGMENT

This work is the outcome of guidance provided by dedicated and experienced personnel of Carmel College of Engineering and Technology,Alappuzha. With profound sense of indebtedness, we use this opportunity to express our sincere thanks to our beloved Principal Dr. Paul K Mathew for providing all sort of support and necessary facilities and for the inspiration to complete our work .We express our sincere gratitude to Prof. Anoop R S Head of the Department of Computer Science and Engineering for the inspiration and permission to carry out our work. We wish to extend our thanks to our project guide Ms. Geethu M Suresh, Assistant Professor, Computer Science and Engineering for her valuable guidance and support rendered throughout our project. Last but not the least ; we extend our sincere thanks to all the members of our computer science department for their help and support. And also would like to extend our deep sense of gratitude to all those who have assisted us in the successful completion of this work.

REFERENCES

[1] R. Sehdehi, T. Henderson, M. Nadeem, A novel inductively powered intelligent parking solution, International Conferenceon Industrial Electronics for Sustainable Energy Systems(IESES), pp391-396, Waikato, New Zealand, 31 Jan-2 Feb 2018

[2] A.R.A. Alkharabsheh, An intelligent cooperative multi-agents-based parking system: design and implementation. Journal of Theoretical & Applied Information Technology, Vol. 96(No.10): 2804-2815, May 2018.

[3] S. Mendiratta, D. Dey, and D. R. Sona, Automatic car parking system with visual indicator along with IoT. 2017 International conference on Microelectronic Devices, Circuits, and Systems (ICMDCS), pp. 1-3, TamilNadu, India, August 2017.

SURVEY ON RELIABILITY TECHNIQUES IN NETWORK ON CHIP

Smt .Vaishnavi S[1] & Smt. Mala J B[2]
[1]Student, [2]Assistant Professor
Dept. of Information Technology
Government Engineering College Barton hill, Trivandrum
vaishnavilekshmi2014@gmail.com,malajb83@gmail.com

ABSTRACT: In recent years, NOC is developing rapidly with its advantages of higher operating frequencies, less wire routing congestion. Although the development of the operations of NOC is rapid, more and more accidents also occur. So the reliability of NOC becomes the important factor that hinders its development. Many techniques were developed to improve the reliability of NoCs. Several solutions are dedicated to enhancing reliability, which in turn will increase the energy efficiency of the system. This paper discusses such solution methods and compares them through the table.

Keywords: Dynamic reliability; Network-on-chip; thread migration; DVFS; LSTM; REST; Kalman Filtering

I.INTRODUCTION

In recent days the continuous increase in computational demands has made chip multiprocessors (CMPs) the workhorse of most computing systems. Crosstalk and aging are the common problems that occur in NOC. The most aging mechanisms are time-dependent dielectric breakdown (TDDB) and negative bias temperature instability (NBTI). These two mechanisms will affect the performance of the chip. The common factor that impacts TDDB and NBTI is temperature [1]. Due to these reasons, the reliability of CMP became an important factor. Bayes classifiers [2], autoregressive moving average (ARMA) [3] are used for real-time predictions in the case of thermal management.

In previous technologies, the reliability estimation is predicted using static and dynamic methods. In static estimation the problem is predicted at the design time, Dynamic estimation will predict the problem at the runtime. Dynamic methods are the commonly used approach for finding the Reliability of NOC. Dynamic reliability management (DRM) scheme is used to address time-dependent dielectric break down and negative-bias temperature instability aging mechanisms in network-on-chip (NoC) based CMPs [4]. Dynamic Voltage/frequency scaling (DVFS) based technique is used to estimate the dynamic reliability of NOC. DVFS is the primary technique to change the CMP operation to increase the lifetime reliability of the overall system [5]. Thread migration is another method that helps to predict the dynamic reliability of CMP. A dynamic reliability management (DRM) algorithm uses a hybrid of DVFS and thread migration. It uses NN based MTTF estimator for evaluating the reliability of CMP [6]

This system, which uses an LSTM predictor for evaluating the reliability of CMP. The proposed system contains a DRM controller and an LSTM predictor for increasing the lifetime reliability of the overall system and thereby increasing the energy efficiency of the system.

This paper is organized as follows. Section 2 includes a literature survey on predicting dynamic reliability methods on the network-on-chip. Section 3 describes an analysis of the methods. And section 4 includes the conclusion.

II.RELATED WORK

In this section, we discuss previous literature on reliability and energy management in processors. A joint temperature and energy management solution for heterogeneous multicore processors is proposed in [7]. It uses both DVFS and temperature- and performance aware task assignment strategy that maximizes the energy savings while maintaining the temperature at safe levels. A control-theoretic approach is introduced in [8] that use data from aging sensors to compute the wear-out degradation and to maximize the lifetime of homogeneous multicore systems. For achieving additional energy savings some latest work also took a sophisticated approach and applied DVFS to both CPU and the DRAM. They reported for a server platform with an Intel i5-4590 quad-core processor and 8 GB of main memory as much as 22% energy savings with a low-performance loss. For predicting workload in the next control period for which voltage-frequency pairs must be selected, a Kalman filtering-based approach [9] is employed. The study in [10] employed a combination of recursive least squares (RLS) and Kalman filters (KF) to estimate processor package temperature and to construct a dynamic energy management controller to predict the optimal voltage/frequency setting to achieve maximum energy efficiency under temperature constraints. the study in [11] proposed DVFS and temperature and performance-aware task assignment strategies for heterogeneous processors that maximize energy savings, while maintaining the temperature at safe levels.

III. RELIABILITY ANALYSING METHODS

1. Dynamic reliability management using NN estimator

The NN-based estimation uses a dynamic reliability management algorithm [6]. This algorithm contains an NN estimator and a DRM controller. This dynamic reliability management algorithm works periodically according to a pre-defined control period. It uses the input temperatures as well as the user set desired reliability target to generate output control commands. That control commands dictate how to perform thread migration among tiles and DVFS of individual tiles is done during the next control period. The lifetime reliability converges toward the desired target by using these commands. This reliability management algorithm is implemented in software and has two main components. The first component is implemented with a neural network (NN) model and estimates the current lifetime reliability. This NN predictor is used to produce an estimate of the meantime to failure (MTTF) of the entire CMP for measuring the lifetime reliability. We use an NN model-based predictor for efficiency reasons and because NN models have been shown to provide high-quality prediction and classification results.

The second component shown in Fig. 1 is the DRM controller. Its role is to compare the currently estimated or projected MTTF to the desired target and then decide for each tile whether the clock frequency must be throttled, increased, or left unchanged or whether threads should be migrated from hot to colder tiles.

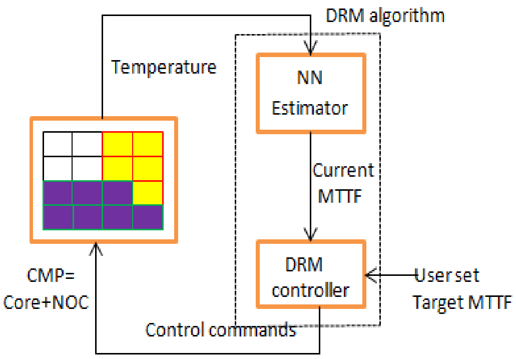


Fig1. Block diagram of the DRM algorithm, which includes the NN estimator and DRM controller The CMP is composed of several tiles. A tile is (core + NoC router).

The input into the DRM algorithm includes temperatures of all the major modules of the tiles formed by cores and NoC routers of the assumed regular mesh NoC as well as individual tile supply voltages. The neural network estimator uses temperature and tile supply voltage as input to estimate lifetime reliabilities (as MTTF) of each tile containing a core and a router as well as of the overall CMP. After the comparison between the currently estimated MTTF with the desired target MTTF, the algorithm uses either the thread migration technique or the DVFS technique, based on the current number of cold tiles.

2. Dynamic reliability management using Kalman filtering

The Kalman filtering method uses a set of recursive equations. For minimizing the variance of the estimation error [12] it employs a feedback control mechanism. Using the notation from [28], the process can be described by the following state and output equations by using the notations from

Xn = Axn−1 + Bun−1 + wn−1 (1)

Here A, B, and H are matrices. A is the state transition model applied to the previous state xn−1. It relates the states at time steps n − 1 and n, in the absence of process noise or control input. The optional control input u to the state x is related by B, and the matrix H relates the state x to the measurement or observation z. The random variable wn−1 models the process noise assumed to be a white Gaussian noise with zero mean and covariance Q, w ∼ N(0, Q).

Zn = Hxn + vn (2)

In equation (1) vn is the measurement noise also assumed to have a Gaussian distribution with zero mean and covariance R, that is independent of Q, v ∼ N (0, R). Kalman filter is constructed in two phases. The first phase is called the predict phase (or time update phase), and here the state x is predicted a priori as xˆ − n. The second phase is called the update phase (or measurement update phase). This is where the predicted xˆ − n is updated a posteriori as xˆn.

$$p_n^- = \mathrm{E}\,[e_n^-\ e_n^{-T}\ ] \qquad (3)$$

$$p_n = \mathrm{E}\,[e_n e_n^T] \qquad (4)$$

Where P− n and Pn represent the estimated error covariance for a priori and a posteriori errors, respectively, at time n.

$$x_n^- = \mathrm{A}x_{n-1} + \mathrm{B}u_{n-1} \qquad (5)$$

$$p_n^- = \mathrm{A}p_{n-1}A^T + \mathrm{Q} \qquad (6)$$

In the predict phase, the filter first projects the state ahead from the previous state x_{n-1} and certain input matrix Bu_{n-1}. The error covariance ahead with process noise covariance Q is projected by the filter.

$$k_n = p_n^-\ H^T\ (\mathrm{H}p_n^-\ H^T + \mathrm{R}) - 1 \qquad (7)$$

$$x_n = x_n^- + k_n(z_n - \mathrm{H}x_n^-\ ) \qquad (8)$$

$$p_n = (1 - k_n \mathrm{H}) p_n^- \qquad (9)$$

With the measurement of the actual state value at time n, the update phase starts right after the predict phase. The three equations utilized in this phase are indicating in equations (7), (8), and (9). The Kalman gain,k_n, is first computed by using the a priori estimate error covariance p_n^- and measurement noise covariance R.

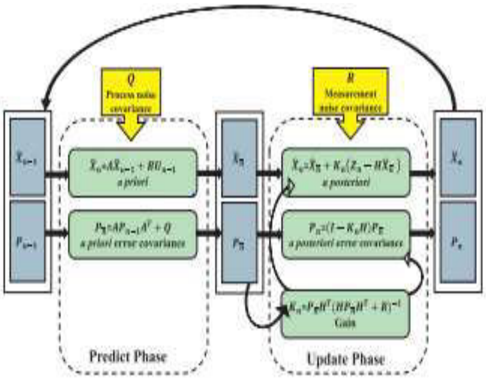

Q
Process noise covariance
R
Measurement noise covariance
a priori
a priori error covariance
a posteriori
a posteriori error covariance
Gain
Predict Phase
Update Phase

fig2. Kalman filter predicts phase and update phase procedure.

Kalman filter had been proven to be one of the best techniques in terms of complexity of implementation in software only, efficiency, and effectiveness in making accurate predictions over a short horizon. . Fig. 2 shows how the Kalman filter works.

3. Dynamic reliability management using LSTM

The LSTM is long short term memory network LSTM is an RNN (recurrent neural network) that uses special units rather than the standard units. LSTM units include memory cells that can store information for long periods in addition to special units called gates that control the flow of information. These gates are used to determine what to store as well as when to allow reads, writes, and erasures of information into/from cells.

Classic RNN can keep track of long-term dependencies in the input sequences. The problem with vanilla RNNs is computational when training a vanilla RNN using back-propagation, the gradients which are back-propagated can "vanish “or "explode", Which uses finite-precision numbers, because of the computations involved in the process. LSTM units allow gradients to flow unchanged, so RNNs using LSTM units partially solve the vanishing gradient problem

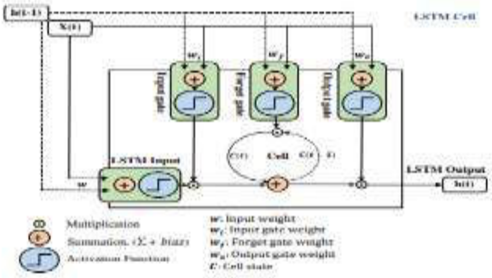


Fig.3 diagram of LSTM network

Fig. 3 shows the simplified diagram of LSTM networks. From the above diagram, it can be observed that the LSTM cell is more complex. It is due to the input, forget and output gates. These gates decide whether to let new inputs in, erase the present cell state, and let the state impact the output at a given time step. Weighted signals connected to an activation function, these weighted signals help to activate these gates. During the learning process, these weighted signals are adjusted. Through the iterative process of making guesses, backpropagation of errors, and adjustment of weights via the gradient descent technique, the cells learn when to allow data to enter, leave, or be deleted. LSTM model can capture history in time series.

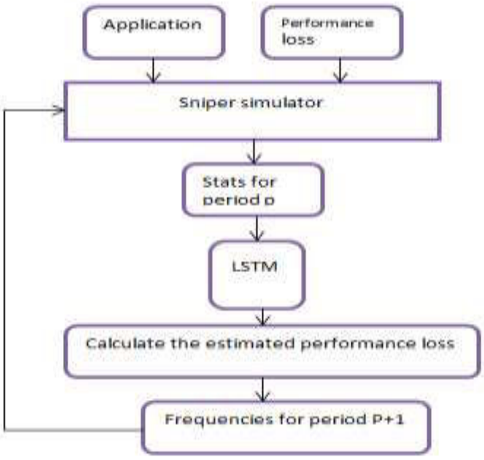

Application
Performance loss
Sniper simulator
Stats for period p
LSTM
Calculate the estimated performance loss
Frequencies for period P+1

Fig4. Block diagram of LSTM framework

The LSTM framework is implemented as a control loop inside a Sniper simulation framework [13]. It is constructed with just one hidden layer of 4 LSTM blocks or neurons and the sigmoid activation function is used for each block. The LSTM model is first trained for using the predictor. The input features for a moving window of w = 20 for the prediction to take into consideration the past 20 data sequences is training data which include CPI and instruction count. The collection process is done during separate runs of the custom Sniper simulation framework and without any DEM algorithm. The model is trained with 20,000 samples collected at intervals of 1 ms during simulations of only a small number of benchmarks on architectures with 16 and 64 cores. The training samples are collected from all individual cores in these architectures. Sniper system simulator that is integrated with the McPAT power calculator. The machine learning library Keras is integrated with our simulation framework and Employed to build and train the LSTM predictor. We conduct simulations using sixteen Parsec and Splash2x benchmarks [14].

4. Dynamic reliability management using REST tool

Dynamic lifetime reliability can be obtained by using the REST tool. It is based on a Monte Carlo algorithm. The system treats the CMP in a unified manner as a combination of communication and computation units. In NOC, the power consumption can be as much as 25–40% of the overall chip power consumption. The neighboring processing elements (PE) or cores affected by the power dissipation and introduce errors in their temperature estimations. When the PE of a tile is inactive, while its router is highly active due to the traffic between another source–destination communication pairs then the power dissipation problem is raised. The main steps of the reliability evaluation methodology and is shown in Fig. 5

REST tool utilizes the GEM5 full-system simulator [15], which is a combination of the M5 full-system simulator [16] and GEMS [17]. The power estimator McPAT [18] will take input as performance data from each core. Power consumptions of each sub-block of each core are treated as the output of the McPAT power estimator. Processors power consumptions provided by McPAT and the power consumption of individual routers of the NOC (provided by GEM5) is fed then to HotSpot [19]. The hotSpot is an accurate and fast thermal model based on an equivalent circuit of thermal resistances and capacitances that correspond to microarchitecture blocks. The output of the HotSpot simulation is a list of average temperatures for all NoC routers and each subblock of all cores of the CMP. The Monte Carlo simulation engine utilizes the temperatures with the system-level architecture floor plan to estimate the time to failure of the whole system.

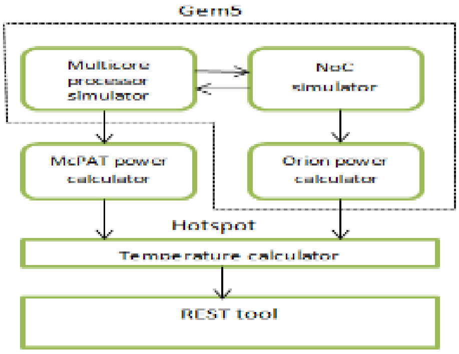


Fig.5.Block diagram of REST tool framework

The Monte-Carlo algorithm is used to implement the REST tool for finding the reliability of the system. The Floor plan of the CMP and power consumption of all sub-blocks is the input to the Hotspot temperature calculator. The output of Hotspot is a list with temperatures for all routers and sub-blocks of each processor core. This temperature depends on the individual utilization of all cores and routers.

IV.ANALYSIS

Four reliability prediction methods are discussed in the previous section. Some evaluation parameters are used to evaluate the reliability prediction methods. Those are:

- Node Availability: Occupation rate of healthy nodes as node availability. Healthy nodes are the nodes that are participating in the routing process.
- Frequency: The rate at which something occurs over a particular period or in a given sample
- Link bandwidth: the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another
- Transition latency: Latency is defined by the total cycles of a packet to reach the destination node from the source node. It defines a length of time to delay the start of a transition.
- Network Size: Network size refers to the total size of the system which is proportional to the number of nodes in NoC.

Table 1: Evaluation parameters of each reliability prediction method.

Reliability prediction methods	Node availability (nm)	Frequency (GHz)	Link bandwidth (bits)	Transition latency (ns)	VDDs (v)	Network size
NN estimator	65	2	32	Not considered	1.1-0.95	8x8
Kalman filtering	45	2	64	2000	1.2	8x8
LSTM	45	2 to 1	64	2000	1 to 1.2	16x16
REST	65	2 to 1.5	32	Not considered	1.1	4x4

Based on these parameters, compare the reliability prediction methods shown in table 1. In the NN estimator method, an 8x8 mesh was used for the implementation. The VDDs value rages from 0.95v to 1.1v.NN estimation method have 32 bits link bandwidth and 2GHz frequencies. Node availability of NN-based estimation is up to 65nm. In Kalman filtering-based reliability prediction method uses 8x8 meshes for implementation. This is used to predict the instruction count and average CPI in the next control period for each core. Its VDDs value is up to 1.2v. This method introduces transition latency up to 2000ns. Kalman filtering needs a link bandwidth up to 64 bits and a frequency of 2 GHz.It needs technology parameters up to 45 nm.

LSTM based reliability prediction method uses 16x16 mesh for implementation. The VDDs value rages from 1v to 1.2v. This method introduces transition latency up to 2000ns same as Kalman filtering. It has a link bandwidth same as like Kalman filtering method.LSTM needs frequency ranges from 1GHz to 2GHz and its technology parameter same as Kalman filtering.REST tool needs 4x4 mesh for implementation. The VDDs value for REST is 1.1v. This method does not consider the transition latency. It has a link bandwidth same as like NN estimator method. REST need frequency ranges from 1.5GHz to 2GHz and its technology parameter same as like NN estimation method.

V.CONCLUSION

This paper introduces the different reliability prediction methods on mesh topology. Those are NN-based estimator, Kalman filtering, LSTM, REST tool. Each has its unique features. The NN estimator and REST tool combine thread migration and DVFS techniques to change the CMP operation such that the MTTF of the overall system is increased to the desired target with minimal performance degradation. LSTM model can be used to construct an effective DRM algorithm that provides a good mechanism to trade off performance versus energy consumption; it is only slightly better than the Kalman filtering approach for prediction.

VI.REFERENCES

[1] Failure Mechanisms and Models for Semiconductor Devices, JEDEC Publication JEP122E, 2009

[2]Ahmed Ammari, Deriving a near-optimal power management policy using model-free reinforcement learning and Bayesian classification, DAC '11: Proceedings of the 48th Design Automation Conference, 2011.

[3] T.S. Rosin, Utilizing predictors for efficient thermal management in multiprocessor SoCs, IEEE Trans. CAD Integr. Circuits Syst. (TCAD) (2009).

[4] Alexandre Yasuo, unified reliability estimation and management of NoC based chip multiprocessors, Microprocessors & Microsystems, February 2014

[5]Milad Gorbani Moghaddam, “Investigation of DVFS based dynamic reliability management for chip multiprocessor, 2015

[6] Cristinel Ababei, Senior Member, IEEE, “Dynamic lifetime reliability management for chip multiprocessors,” IEEE Trans. on Multiscale Computing Systems, 2018.

[7] S. Sharifi, Hybrid dynamic energy and thermal management in heterogeneous embedded multiprocessor socs, in ACM/IEEE Asia and South Pacific Design Automation Conference (ASP-DAC), 2010.

[8] P. Mercati, L. Benini, Workload and user experience-aware dynamic reliability

management in multicore processors, ACM/IEEE Int. Design Automation Conference (DAC), 2013

[9]Milad Ghorbani Moghaddam, Dynamic energy management for chip multi-processors under performance constraints, / Microprocessors and Microsystems 54 (2017) 1–13

[10] V. Hanumaiah, STEAM: a smart temperature and energy-aware multicore controller, ACM Trans. Embedded Comput. Syst. (TECS) 15 (13) (2014).

[11] Ayşe Kivilcim Cookson, "Hybrid dynamic energy & thermal management in heterogeneous embedded multiprocessor SoCs," ASP-DAC '10: Proceedings of the 2010 Asia and South Pacific Design Automation Conference, 2010.

[12] G.Bishop, An introduction to the Kalman filter, University of North Carolina, Chapel hill, NC, 1995

[13]T.Herman, exploring the level of abstraction for scalable and accurate parallel multi-core simulation" SC '11: Proceedings of 2011 International Conference for High-Performance Computing, Networking, Storage and Analysis

[14]PARSEC and Splash2 benchmarks, 2017. [Online]. Available: HTTP:// parsec.cs.princeton.edu

[15] Beckmann, G. Black, D.A. Wood, The gem5 simulator, ACM SIGARCH Comput. Architect. News Arch. (2011).

[16] N.L. Blinker," The M5 simulator: modeling networked systems", IEEE Micro 26 (4) (2006) 52–60.

[17] M.M.K. Matin, General execution-driven multiprocessor simulator (GEMS) toolset, Computer. Architect. News (CAN) (2005).

[18] Norman P. Jouppi, McPAT: an integrated power, area, timing modeling framework for multicore and many core architectures, 2009 42nd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)

[19] Ghosh, S. Velusamy, K. Sankaranarayanan, K. Skadron, HotSpot: a compact thermal modeling method for CMOS VLSI Systems, IEEE Trans. (2006).

Smart Farming Monitoring System

Alphonse Treesa Jacob
Computer Science and Engineering
Amal Jyothi college of Engineering
Email: alphonsetreessajacob2021@cs.ajce.in

Amala Augustine
Computer Science and Engineering
Amal Jyothi college of Engineering
Email: amalaaugustine2021@cs.ajce.in

Ivy Rose Seban
Computer Science and Engineering
Amal Jyothi college of Engineering
Email: ivyroseseban2021@cs.ajce.in

Abdhul Azeez
Computer Science and Engineering
Amal Jyothi college of Engineering
Email: abdhulazeezps2021@cs.ajce.in

***Abstract*: In India, there are many people who are interested in growing, caring and monitoring the plants. This might be out of their interest in plants or to sell the fruits and flowers of the plants or to reduce the effect of global warming. India's 58 percent population is dependent on agriculture as their primary income is based on agriculture and they have to monitor the plants and irrigate them properly. The irrigation of the plants should be done properly because if there is excess water or less water in the plant, the plant may be spoiled. So, we should irrigate the plant properly and give only sufficient amount of water that the plant needs. Smart Farming is an emerging concept that refers to managing farms using modern Information and communication technologies to increase the quantity and quality of products while optimizing the human labor required. Sensors, soil, water, light, humidity, temperature management. Aquaponics and hydroponics are two examples of such farming system. Aquaponics is a combination of aquaculture, which is growing fish and other aquatic animals, and hydroponics is a type of horticulture and a subset of hydroculture, which is a method of growing plants,usually crops, without soil, by using mineral nutrient solutions in an aqueous solvent.**

Keywords: Energy Efficient Lamp, Power Quality, Total Harmonic Distortion (THD), Electrical Parameters, Photometric Parameters.

I. INTRODUCTION

Agriculture is the most important sector in the Indian economy. Almost 18 percent of the gross domestic product of India is contributed by Indian agriculture. Most of the Indians are directly or indirectly related to agriculture in one or other way. Hydroponic System is a system of growing crops without soil, often called soilless farming. In the hydroponic system, the plant roots grow in a liquid nutrient solution. The liquid nutrient solution is a mixture of essential plant nutrients in the water. Plant roots get in direct contact with the water soluble nutrient content and this helps in faster absorption and growth. The idea of hydroponic farming is believed to serve two purposes, one is it can be practiced by people to grow fresh fruits and vegetables where the soil condition is not suitable for conventional farming,second it is a solution for satisfying sustainable food requirements in urban areas where the land for conventional farming is not easily available due to other commercial business ventures.

Aquaponics refers to a food production system that couples aquaculture with hydroponics in a symbiotic environment whereby the nutrient rich aquaculture water is fed to hydroponic grown plant, involving nitrifying bacteria for converting ammonia into nitrates. Aquaponics and hydroponics are two examples of such farming system. Aquaponics is a combination of aquaculture, which is growing fish and other aquatic animals and hydroponics is a type of horticulture and a subset of hydroculture, which is a method of growing plants,usually crops, without soil, by using mineral nutrient solutions in an aqueous solvent. Hydroponic systems focus solely on plant growth, while aquaponic systems attempt to achieve a healthy life balance between both plants and fish. Aquaponics takes the more natural path, while many hydroponic systems rely on simplicity. Nutrients added to the water are fed to the plants in a variety of ways.

Hydroponic systems are essentially hands-off when it comes to feeding the plant. Everything is usually done automatically, aside from the addition of the nutrient solution. The waste contained in the aquarium water is pumped up to a growing tray that houses the plants and contains the growing medium. Plants rely on the waste for its nutrients, and the clean, relativelywaste-free water goes back into the aquarium for the fish. Hydroponics is also better if you only want to grow a few plants, as a simple system consisting of a few parts — such as an air pump, air stone and container — is all that's needed. But as we grow more plants, hydroponic systems are more work and more of an investment. They require a nutrient solution that must be flushed occasionally to prevent the buildup of salts and chemicals.

II. OVERVIEW

Along with the socio-economic development, more high living standards have been pursued by human beings. However, more time has been spent engaging in work and they have no extra time to look after their playthings (e.g., fishes, flowers). The primary objective is to design a smart monitoring and control device for aquaponics, which is an eco-friendly system for ornamental fish and hydroponic plants. The significance and specific functions of the system was firstly described in details, and then the architecture, hardware components and software design were also introduced. The system consists of three parts: data acquisition, mobile transfer and intelligently interactive application.Specifically, the data that acquired by webcam and some smart sensors are analyzed and processed for man-machine interaction. Meanwhile, users can also use the mobile terminal to monitor and control the smart aquaponics remotely. The design of the system can promote the rapid development of smart aquaponics.

III. OBJECTVE

Along with the rapid development of sensor technology, Internet technology, communication technology and computer technology, smart life style will become a popular trend for our future life . To solve the current shortcoming, this study designs a smart monitor and control system based on IoT, which can make it easy to implement the connection of monitoring field and remote monitoring center. The system can monitor the environment of aquaponics device through some sensors in a real-time and stable way, and then accurately and automatically transmit the data of temperature, humidity, light intensitY and water level in real time. Users can view the data and photos remotely from either mobile client or web . They can decide whether to open air pump, water pump, lights, and feeder or not based on the obtained information.

IV. EXPECTED OUTCOME

Modern people have been always engaged in work and they have no more extra time to look after ornamental fish and hydroponic plants. On the one hand, ornamental fish conserves flings stuff and it is also tedious to replenish oxygen, maintain temperature and smears distinctly illumination. On the other hand, plants need watering and fertilization frequently. The whole process is so complex and time-consuming. Based on the above shortcomings, the automatic control system is proposed . Unfortunately, current automatic control system is not stable that some unexpected errors always occur, especially it is difficult to realize remote monitoring and control. Consequently, it isvery necessary to design a smart monitor and control system, especially for people who travel frequently.Some sensor nodes are used to form the sensor data acquisition module, which are deployed near to the aquaponics system to collect real-time environmental information, such as temperature, humidity, light intensity, water level and photos. After an initial processing, the data is transmitted to database.

V. LITERATURE SURVEY

Monitoring Water Quality in Aquaponics Systems: Water chemistry requirements are especially difficult to balance.constantly monitoring the aquaponics system with the right equipment, including pH sensors, dissolved oxygen sensors, and conductivity sensors is used. If and when the system appears to become unbalanced, the quicker the adjustments make, the lower the risks will be.The programmable microcontroller collects the input signal converted into values of level of water via the sensors. As the microcontroller starts gaining signals, an output is created that forces the relay for running the water pumping motor. The values of moisture contentin the soil and the water level can be seen in an LCD monitor connected to it. First, a proper water source must be identified. After all, a painting can only be as good as its canvas. As such, even a basic aquaponics setup must be supplied with good water. However, even the best source water will not ensure a proper balance between the hydroponic needs of the plants and the needs of aquaponic fish farming. Good aquaponics system plans will include frequent testing. When first building and implementing your aquaponic system, daily testing should be conducted. Dissolved oxygen, pH levels, conductivity or total dissolved solids, ammonium ion (NH4+), and nitrate ion (NO3-) must all be closely monitored.

Wick System: The wick system is notable for not using aerators, pumps, or electricity. In fact, it’s the only hydroponic system that doesn’t require the use of electricity. With the majority of wick systems, the plants are placed directly within an absorbent substance like perlite or vermiculite. Nylon wicks are positioned around the plants before being sent straight down into the nutrient solution. While this system is fantastic for smaller plants, you’ll want to avoid growing plants like peppers and tomatoes. These plants are considered to be heavy-feeding plants, which means that they require more nutrients than the wick system will be able to provide. Another negative aspect of this growing system is that water and nutrients aren’t absorbed evenly, which could lead to the buildup of toxic mineral salts. When you use this system, make sure that you flush any extra nutrients with fresh water every 1-2 weeks.

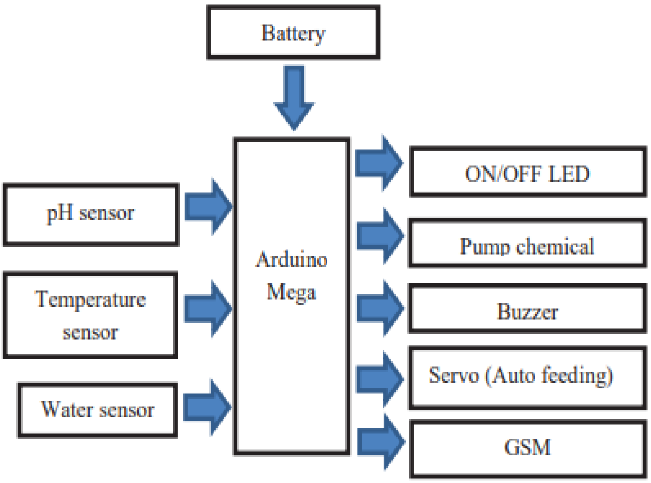
Ebb and Flow: With this type of system, the plants are positioned in a spacious grow bed that's packed with a grow medium like Rockwool or perlite. Once the plants are carefully planted, the grow bed will be flooded with a nutrient-rich solution until the water reaches a couple inches below the top layer of the grow medium, which ensures that the solution doesn't overflow. The water pump that floods the grow bed is outfitted with a timer that will switch the pump off after a certain amount of time. When this occurs, the water will be drained from the grow bed and sent back into the pump. The ebb and flow system has been found to be effective at growing nearly all types of plants, which includes certain root vegetables like carrots and radishes. However, it's recommended that you don't use particularly large plants with this system. Because of how much space these plants will require, you may not be able to fit enough of the grow medium and nutrient solution into the grow bed with larger plants. The main issue with the ebb and flow system is that the pump controller can malfunction, which halts operation until the pump is fixed or replaced.

Drip Systems: A drip system is an easy-to-use hydroponic system that can be quickly altered for different types of plants, which makes this a great system for any grower who plans to make regular changes. The nutrient solution that's used with a drip system is pumped into a tube that sends the solution straight to the plant base. At the end of each tube is a drip emitter that controls how much solution is placed into the plant. You can adjust the flow to meet the needs of each individual plant. These systems can be as small or large as you want them to be. They can also be circulating or non-circulating systems. A circulating system will drip almost constantly. Any extra nutrients will be sent back into the tank that holds the nutrient solution. Since you can readily alter the size and flow rate of this hydroponic system, it can be used to grow practically any plant. If you decide to use a circulating system, the main problem that you'll run into is that you'll need to consistently maintain the fluctuating nutrient and pH levels that occur when the solution is recirculated.

N.F.T. (Nutrient Film Technology): The N.F.T. system has a simple design but is widely used because of how well it scales to a variety of different applications. When you use this systems, the nutrient solution is placed into a large reservoir. From here, the solution is pumped into sloped channels that allow the excess nutrients to flow back into the reservoir. When the nutrient solution is sent into the channel, it flows down the slope and over the roots of each plant to provide the right amount of nutrients. It's highly recommended that you use net pots with this type of hydroponic system. In most cases, the N.F.T. system won't make use of a grow medium. Since the channels that are used with this system are relatively small, it's recommendedthat you pair it with plants that have smaller roots. Even though this system can't readily accommodate larger plants, it does scale well, which means that you can alter it to allow for the growth of a large number of plants at the same time. Since it scales well, thissystem is commonly used by commercial growers alongside home growers.

VI. PROPOSED SYSTEM

The system proposed is a form of integrated agriculture that combines two major techniques, aquaculture and hydroponics. In one continuously recirculating unit, culture water exits the fish tank containing the metabolic wastes of fish. The water first passes through a mechanical filter that captures solid wastes, and then passes through a biofilter that oxidizes ammonia to nitrate. The water then travels through plant grow beds where plants uptake the nutrients, and finally the water returns, purified, to the fish tank.The biofilter provides a habitat for bacteria to convert fish waste into accessible nutrients for plants. These nutrients, which are dissolved in the water, are then absorbed by the plants. This process of nutrient removal cleans the water, preventing the water from becoming toxic with harmful forms of nitrogen (ammonia and nitrite), and allows the fish, plants, and bacteria to thrive symbiotically. Thus, all the organisms work together to create a healthy growing environment for one another, provided that the system is properly balanced.There are 5 sensors available in the platform to measure the key parameters in the fish tank such as temperature, pH or Conductivity and then some others to control the correct state of the fish tank (level and leakages). In addition, there are 4 different actuators to automate tasks such as heating or cooling the water, feeding the fish, activating the pumps for water change or medicines administration, and controlling the intensity of the light to simulate the day/night cycles. A complete Open Source API is included to easily control the board through Arduino. And we have also designed a web application that allows to store in a data base the information gathered and visualize it from a browser and from iPhone / Androiddevices.



VII. PROPOSED ARCHITECTURE

The figure below shows a block diagram of the smart farming system using Arduino microcontroller. The developed program is stored in the microcontroller Arduino Mega board and ready to be executed when needed. The pH sensor circuit, temperature sensor, water sensor, servo, LCD, GSM and peristaltic pump are connected to the Arduino board. The program and hardware parts of the aquaponics system are combined together to perform the functionality.

The program is started by executing the servo to rotate and feeding the fish by dropping the fish palette to the fish tank. to maintain the pH value. Meanwhile, the water sensor is used to detect the water flow into the fish tank through the siphon outlet. If the water flow through a siphon outlet is stopped, the buzzer will be triggered. Therefore, no water is pumped from fish tank to grow bed. When the pH,temperature and water sensor are out of the ranges, a message will be sent to a mobile phone through GSM modem for notification. The servo is used to auto feed fish every 12 hours. The function of pH sensor is to detect the pH value of the water. The pH sensor functionality is constructed by connecting the analog input port of the Arduino board with the sensor circuit board. The pH sensor circuit consists of three wires which are ground, +5 V and analog output. In addition to that, the temperature sensor functionality is also constructed in a similar way. The sensor consists of three wires which are indicated +5 V (red), ground (black) and data (yellow). The wires are connected to the Arduino board using a 4.7 k resistor to form a pull up resistor. Pull up resistor is employed to make sure that the signal will be a valid logic if the peripheral is disconnected or high impedance is introduced. Similarly, the water sensor consists of three wires is connected to 5 V, ground and digital pin 7 of the Arduino board. Additionally, the water sensor is also connected to a buzzer using a transistor. The servo is used in this system to auto feeding fish in the tank.

This servo consists of three wires which are yellow, red and black wire. Red wire is connected to 5V, black wire is connected to ground and yellow is connected to digital pin 12 of the Arduino board. The pH sensor, temperature sensor, water sensor circuit and servo connection is shown in Fig. 3.2.

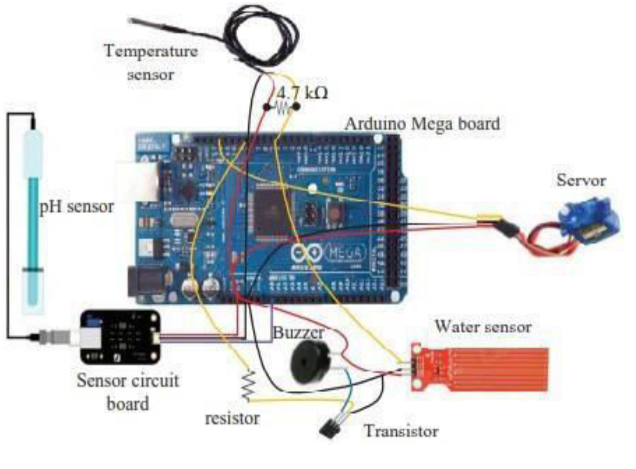


Figure 3.2: pH sensor, temperature sensor, water sensor circuit and servo connection

A peristaltic pump is used in this system to pump the chemical solution into the fish tank in order to balance back the pH value of water. This pump is connected in parallel with an lN4001 diode to protect the Arduino board from reverse electromagnetic force produced by the pump motor. The negative terminal of the diode is connected to a transistor collector for use as current amplification since the Arduino board cannot supply enough current to drive the peristaltic pump. The positive terminal of the pump is connected to a supply voltage.

Meanwhile, the base of the transistor is connected to digital pin 9 of the Arduino board and the emitter of the transistor is connected to the ground. The GSM is used in this system to send the notification if the pH and temperature values are out of ranges and also if the siphon water flow not working. GSM has three wires connection which are black and red colors. The black wire is connected to a ground and the red wire is connected from digital pin 3 to STXD of GSM and another red wire is connected from digital pin 10 to SRXD of GSM.Liquid crystal display (LCD) with 20 characters x 4 lines is used with an Arduino board to display the water parameters and feeding time cycle. This type of LCD is chosen because four's information is required to be displayed. This LCD consists of 16 pins connector and each pin has its own function.

The system uses an Arduino mega board for the analysis of the received data and control- ling the devices.

A. Hardware

The system uses an Arduino micro controller .The general structure is made of aluminum. The structure through which the water circulates consists of PVC pipes cut and glued by hand, and consists of 2 levels through which the water passes. Each level has been drilled to place pots. 3D pieces have also been designed so that the pots do not move and to support the lighting. In the lower part there is a tank in which the water of the system falls and through which different components can be added to the water. In case of having to drain the tank, we have a manual drain.

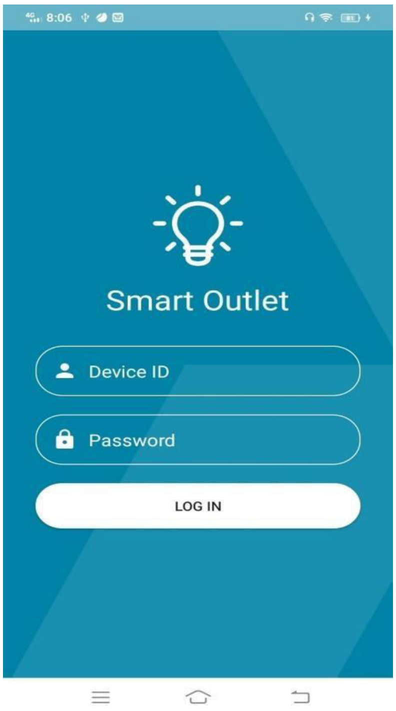
B. Software

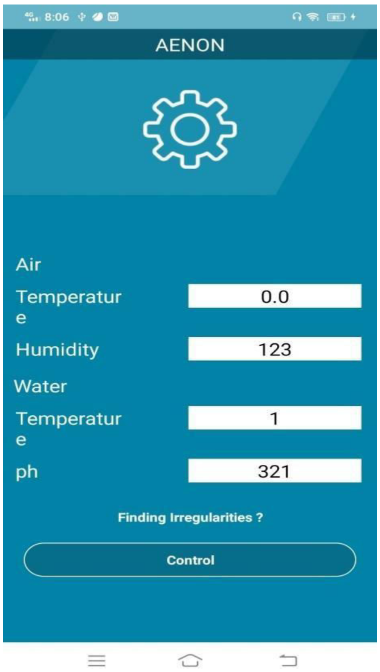
The system uses Arduinos which are programmed using the Arduino IDE. It is a modified version of the C++ programming language. An App is designed for the real time viewing of data and the control of equipment's. The device periodically sends the information to the App that allows this data to be visualized from an Android device.

Aenon offers a mobile phone application that allows accessibility to the data and to control the equipment's attached. Through the application users can monitor the readings control the motor, grow-light and feeder. Fig. 3.3 shows the data interface of the application. The system also notifies the user if values of the parameters drift out of the bounds abnormally. This can be caused by not closing the system properly, sensor failure, or a node failure. This piece of code runs on the local server which is independent of all the electronics that are responsible for the operation of the system. This means that a failure in the electronic components controlling the system will not cause these messages to be disrupted.

VIII. RESULTS

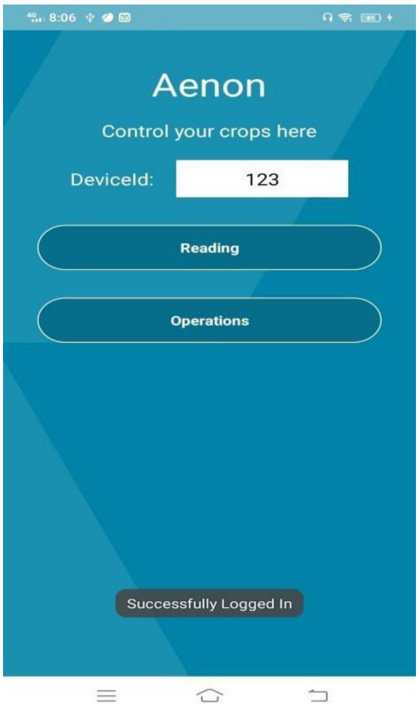
Given in the next page are the are sample screenshots of the application created to control our system.The most basic one, such as the one provided will have a login page, a page to display the readings and a page to control the device according to our needs.Further developments can be done with improvements in system design.





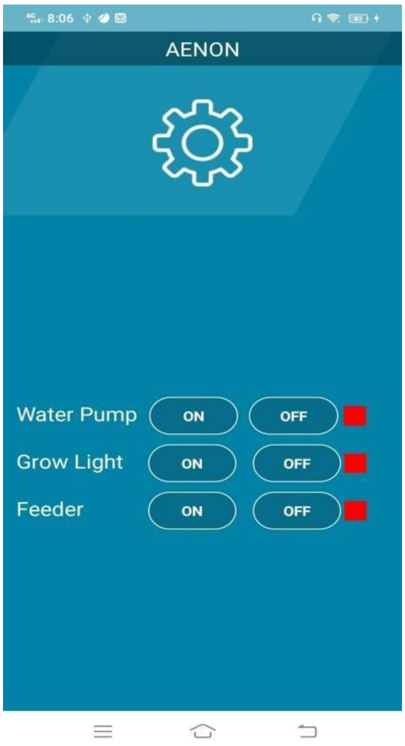
Air Temperatur e	0.0
Humidity	123
Water Temperatur e	1
ph	321

Finding Irregularities ?



DeviceId: 123

Successfully Logged In



IX. CONCLUSION

The System has high efficiency and accuracy in fetching the live data of temperature and soil moisture. This smart farming system being proposed via this report will assist farmers in increasing the agriculture yield and take efficient care of food production as the system will always provide helping hand to farmers for getting accurate live feed of environmental temperature and soil moisture. Hydroponically grown plants do not come in contact with soil borne pests and diseases thus saves costs of soil preparation, insecticides and fungicides. Since the amount of nutrients is fed directly to the plants, there is no wastage of water due to run off or evaporation. Today, hydroponics is an established branch of farming. Progress has been on large scale and results obtained in various countries in the world have proved that this technology is thoroughly practical and has very definite advantages over conventional methods of crop production. The proposed platform is composed of readily available sensors and modular components, therefore it is affordable as well as simple to set up and use. The system can hence be easily replicated and other sensors can be added if needed. The system can be used to collect the sensor data to carry out a quantitative assessment of the farm and can also be used for high-level decision making, once enough data are collected. Moreover, the proposed monitoring platform represents a starting point to make the farm truly autonomous, using the sensor data as input signals. Such a system can unlock the potential of hydroponics, making it a valid alternative to ordinary agriculture for facing future climate changing related challenges. Future work would be focused more on increasing sensors on this system to fetch more data especially with regard to pest control and by also integrating GPS module in this system to enhance full-fledged agriculture precision ready.

X. REFERENCES

[1] A review on plant without soil hydroponics., International Journal of Research in Engineering and Technology

[2] The potential of soilless culture Systems in producing Tomato and cucumber under greenhouse conditions

[3] Hydroponics: A versatile system to study nutrient allocation and plant responses to nutrient availability and exposure to toxic elements.

[4] Comparison between growing plants in hydroponics system and soil based system

A STUDY ON DEEP NEURAL NETWORK APPROACHES FOR TRAFFIC DATA FORECASTING

Arppitha Anna John
Student, Dept of CSE
Sree Buddha college of Engineering,
patoor
arppithaannaj@gmail.com

Supriya L.P
Assistant Professor, Dept of CSE
Sree Buddha college of Engineering,
patoor
supriyabinnyb@gmail.com

Abstract *- Accurate and a well time traffic flow data is important for the successful deployment of intelligent transportation systems (ITS). The traffic prediction is a very challenging problem because the traffic data is a type of spatio-temporal data which shows correlation and heterogeneity simultaneously in both space and time. Due to the high nonlinearity and the complexity of the traffic flow, the traditional methods are not able to satisfy the requirements of mid-and-long term prediction tasks and often neglect the spatial and temporal dependencies. In this project, Spatio-Temporal Graph convolution unit (STGCU), a novel deep learning framework is proposed to tackle the time series prediction problem in the traffic domain. The STGCU effectively captures the comprehensive spatio-temporal correlations and it achieves faster training, easier convergences, and fewer parameters with flexibility and scalability. Instead of applying regular convolutional and recurrent units the problem is formulated on the graphs and build the model with complete convolutional structures, which enable much faster training speed with less parameters.*

Keywords:Traffic prediction, Spatio-Temporal data, Deep learning, Spatio-Temporal Graph Convolution Unit

I. INTRODUCTION

Transportation plays an essential role in everyone's life. With the development of social economy, the number of vehicles in the road is increasing drastically. Due to this drastic increase of vehicles may cause traffic congestion. The traffic flow prediction aims at estimating the number of vehicles in a particular region and in a time interval, which is a major problem in transportation management system. Reliable and accurate real-time traffic flow prediction should support the real-time route guidance in advanced traveller information systems for saving time and money. The reliable traffic control policies in advanced traffic management systems for decreasing the traffic congestion and accidents on the road.

Traffic prediction have a major role in terms of data mining application. A vast variety of data sets differs in volume, variety and velocity that are generated. When the number of vehicles goes beyond the limit of the road, traffic occurs. Nowadays, many countries suffer from this traffic problems that affect the transportation system and cause serious difficulties. With the progress of computing facility provided by computer science technology, it is now feasible to predict the traffic more accurately. Transportation uses recent digital techniques to achieve efficient traffic flow, minimize accidents on the road and maintain the speed the on road. Traffic predictions helps in route planning, navigation and other mobility services. Traffic models are usually used to evaluate different past and real-time traffic data.

With the help of some tremendous traffic sensors like in-ground loop detectors and GPS devices we can easily get a large amount of traffic data. This provides an opportunity to understand the traffic data through data-driven approaches. Data-driven approaches is mainly divided into two subcategories that is traditional machine learning method and deep learning method. Modern technologies use data mining algorithm to find prediction in the transportation system. The machine learning and deep learning techniques can be used to predict the traffic data more accurately. Here Deep learning is employed because it automatically extracts all the necessary features from a large set of data.Convolutional neural networks are taken to explore the spatial features of traffic data. A convolutional neural network (CNN) is a type of artificial neural network which is used in image recognition and designed to process pixel data.

II. LITERATURE SURVEY

A study of existing theories and practices in traffic prediction helps to know more about it deeply. Traffic prediction is a fundamental module in Intelligent Transportation system (ITS), which helps to improve traffic management.

Authors Wenhao Huang, Guojie Song, Haikun Hong, and Kunqing Xie [1], proposed a deep architecture which consists of two parts that is, a deep belief network (DBN) at the bottom and a multitask regression layer at the top. The DBN is employed by the authors for unsupervised feature learning and can learn effective features for traffic flow prediction in an unsupervised fashion and a multitask regression layer is used in the DBN for supervised prediction. Authors Hao-Fan Yang, Tharam S. Dillon, Life Fellow, and Yi-Ping Phoebe Chen [2] presents a novel method that is stacked autoencoder Levenberg–Marquardt model and the model is designed using the Taguchi method. The evaluation results of the paper indicate that the SAE-LM model with an optimized structure is an accurate and efficient approach to traffic flow forecasting. The SAE-LM model with five hidden layers (four autoencoders) can generate the most accurate predicted results.

A deep-learning-based approach, called ST-ResNet is proposed by Junbo Zhang, Yu Zheng, Dekang Q [3]. Predicting crowd flows in a city is an important part in traffic management and public safety. It employs the residual neural network framework to model the temporal closeness, period, and trend properties of crowd traffic. The ST-ResNet learns to dynamically aggregate the output of the three residual neural networks and the model is better and more applicable to the crowd flow prediction. Paper [4] presents a novel traffic forecast model which is based on long short-term memory (LSTM) network. An accurate forecast result enables the commuters to make appropriate travel modes, travel routes, and departure time. The short-term traffic forecast is one of the essential issues in intelligent transportation system. The proposed LSTM network considers temporal–spatial correlation in traffic system and the LSTM network approach for the traffic volume forecast is robust.

Du Tran, Lubomir Bourdev, Rob Fergus, Lorenzo Torresani, Manohar Paluri [5], proposed an effective approach for spatiotemporal feature learning using deep 3D Convolution network. In this paper a systematic study is conducted to find the best temporal kernel length for 3D ConvNets. The C3D can model appearance and motion information simultaneously and the features of C3D are efficient, compact, and extremely simple to use. Paper [6] presents a novel long short-term memory neural network to predict travel speed using microwave detector data. The LSTM NN is able to learn the time series along with the time dependency and then automatically determine the optimal time lags. This feature is especially wise for traffic prediction problems. To validate the effectiveness of the proposed LSTM NN, the authors did a study by collecting the data of 1-month traffic speed data with the updating frequency of 2 min from two sites in Beijing expressway and the first 25 days' data was utilized for training, and the remaining was to test the algorithm performance.

A decentralized deep learning-based method is proposed by Mohammadhani Fouladgar, Mostafa Parchami, Ramez Elmasri and Amir Ghaderi [7], where each node accurately predicts its own block state in the real time based on the congestion state of the neighbouring stations. In order to achieve higher performance a regularized euclidean loss function is proposed to favour the high congestion samples over low congestion samples to avoid the impact of the unbalanced training dataset. A novel dataset is designed for this purpose. Paper [8] puts forward a hybrid spatio-temporal method of short-term traffic forecasting, i.e., Dynamic Space-Time Autoregressive Integrated Moving Average Model (Dynamic STARIMA). This method combines STARIMA model and Dynamic Turn Ratio Prediction model (DTRP) to enhance the forecasting performance and efficiency on urban intersections. The prediction accuracy of Dynamic STARIMA model is generally satisfying compared to other forecasting methods, which testifies the advantage and practicability of the proposed model.

Junping Zhang, Fei-Yue Wang, Kunfeng Wang, Wei-Hua Lin, Xin Xu, and Cheng Chen [9] did a survey on the development of D2ITS, discussing the functionality of its key components and some deployment issues associated with D2ITS. Future research directions for the development of D2ITS is also presented in this paper. The authors Shuiwang Ji, Wei Xu, Ming Yang and Kai Yu [10] developed a novel 3D CNN model for action recognition. This model extracts features from both the spatial and the temporal dimensions by performing 3D convolutions, thereby capturing the motion information encoded in multiple adjacent frames. The developed model generates multiple channels of information from the input frames, and the final feature representation combines information from all channels. To further boost the performance, the authors proposes the regularizing outputs with high-level features and combining the predictions of a variety of different models.

III. PROPOSED SYSTEM

Convolution neural network

Convolution neural networks have been a great achievement in visual recognition tasks. The logic for using this CNN is that the images have a sense of locality that is, the pixels which are closer to each other are more related. CNNs are able to capture this by convolution operations and the local region that comes into consideration which depends upon the kernel size.

Video motion Analysis

Video motion analysis is a technique which is used to get the information about moving objects from the video. In fig 1 it shows that an input video (which contains an information about the traffic) is passed to the video motion analysis, then the video motion analysis extract the information about the moving objects from the video and a GPS is connected to it for getting some unusual happening occurred on the road.

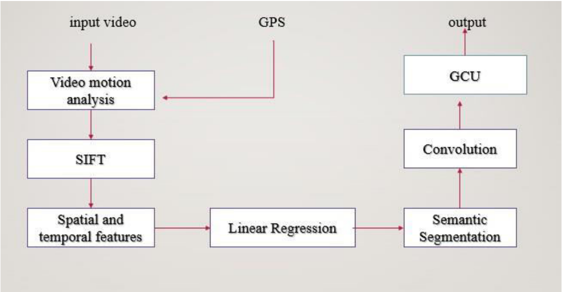


Fig 1 Proposed System.

SIFT

The scale-invariant feature transform (SIFT) is a feature detection algorithm which is used in computer vision to detect and describe the local features of an image. In fig 1 it is used to extract the spatial and temporal features from the output given by the video motion analysis.

Linear Regression

Linear Regression is a linear approach which quantifies the relationship between a scalar response and one or more explanatory variables. In fig 1 it is used to get a graphical representation. Here the dependent variable is number of vehicles, number of humans and the independent variable is spatial and temporal features.

Semantic Segmentation

Semantic segmentation is the task of assigning each pixel into a class where it belongs. A basic technique in this is that there will be an encoder followed by a decoder whose output will be an assignment at the pixel level. Here the feature vector representation of each object present in the image gets separated from other objects and brings the similar objects closer to it, this is where the encoder comes into action. It converts the color image representation to some latent space representation in which the features of the similar object are closer and the distinct objects are far away from each other. Once the features are in some latent space which separates the distinct objects and propagate the information to pixel level and this is where the decoder comes into action.

Graph Convolution Unit (GCU)

The GCU operates only on a graph like structure and there are three major steps in GCU that is Graph projection, Graph Convolution and Graph re-projection. In fig 1 GCU collects the information and converts it into a graphical format from where we get an output as a graphical representation of traffic data.

IV. Conclusion

In this paper, a novel deep learning framework ST-GCU is proposed for traffic prediction. The proposed is also used to tackle the time series prediction problem in the traffic domain. The STGCU effectively captures the comprehensive spatio-temporal correlations. Theoretically this proposed system will provide an accurate traffic prediction and it will be easy to identify the key features in it. It also achieves faster training, easier convergence and few parameters with flexibility and scalability.

References

[1] W. Huang, G. Song, H. Hong, and K. Xie, “Deep architecture for traffic flow prediction: Deep belief networks with multitask learning,” IEEE Trans. Intell. Transp. Syst., vol. 15, no. 5, pp. 2191–2201, Oct. 2014.

[2] H-F Yang, T. S. Dillon, and Y.-P. P. Chen, “Optimized structure of the traffic flow forecasting model with a deep learning approach,” IEEE Trans. Neural Netw. Learn. Syst., vol. 28, no. 10, pp. 2371–2381, Oct. 2017.

[3] J. Zhang, Y. Zheng, and D. Qi, “Deep spatio-temporal residual networks for citywide crowd flows prediction,” in Proc. 31st AAAI Conf. Artif. Intell., Feb. 2017, pp. 1655–1661

[4] Z. Zhao, W. Chen, X. Wu, P. C. Y. Chen, and J. Liu, “LSTM network: A deep learning approach for short-term traffic forecast,” IET Intell. Transp. Syst., vol. 11, no. 2, pp. 68–75, Mar. 2017.

[5] D. Tran, L. Bourdev, R. Fergus, L. Torresani, and M. Paluri, “Learning spatiotemporal features with 3D convolutional networks,” in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Dec. 2015, pp. 4489–4497.

[6] X. Ma, Z. Tao, Y. Wang, H. Yu, and Y. Wang, “Long short-term memory neural network for traffic speed prediction using remote microwave sensor data,” Transp. Res. C, Emerg. Technol., vol. 54, pp. 187–197, May 2015.

[7] M. Fouladgar, M. Parchami, R. Elmasri, and A. Ghaderi, “Scalable deep traffic flow neural networks for urban traffic congestion prediction,” in Proc. Int. Joint Conf. Neural Netw. (IJCNN), May 2017, pp. 2251–2258.

[8] X. Min, J. Hu, Q. Chen, T. Zhang, and Y. Zhang, “Short-term traffic flow forecasting of urban network based on dynamic STARIMA model,” in Proc. 12th Int. IEEE Conf. Intell. Transp. Syst., Oct. 2009, pp. 1–6.

[9] J. Zhang, F.-Y. Wang, K. Wang, W.-H. Lin, X. Xu, and C. Chen, “Datadriven intelligent transportation systems: A survey,” IEEE Trans. Intell. Transp. Syst., vol. 12, no. 4, pp. 1624–1639, Dec. 2011.

[10] S. Ji, W.Xu, M.Yang, and K.Yu, “3D convolutional neural network for human action recognition,” IEEE Trans.Pattern Anal.Mach.Intell, vol 35, no.1,pp.221-231, Jan.2013

OVERVIEW ON CAMOUFLAGED OBJECT DETECTION TECHNIQUE

DILARATH PS
Dept. of Information Technology
Govt.Engineering college Barton Hill
Thiruvananthapuram, India
dilarathps@gmail.com

DIVYA PRASAD KH
Dept.of Information Technology
*G*ovt.Engineering college Barton Hill
Thiruvananthapuram, India
divyaprasadkh@gmail.com

***Abstract*—This paper is a comprehensive study on a different technique for identifying camouflaged objects. Camouflage is a background matching process. Here objects are seamlessly embedded in their surroundings. The high intrinsic similarities between the target object and the background make COD(camouflaged object detection) far more challenging than the traditional object detection task. For identifying a camouflaged object different methods like handcrafted method, unsupervised learning, supervised learning are considered. Visual characteristics of camouflaged objects make detection and tracking tasks more difficult. Due to such complexity, less work has been done to attempt visual camouflage breaking in theliterature. Nowadays deep features are considered for COD and research is done in this area.**

***Index Terms*—Camouflaged object, Object detection, Convexity, GLCM, DWT, Deeplearning.**

I. Introduction

Object detection is a computer vision technique that allows us to identify and locate objects in an image or video. With this kind of identification and localization, object detection can be used to count objects in a scene and determine and track their precise locations, all while accurately labeling them. The term ”Camouflage ” was originally used to describe the behavior of an animal or insect trying to hide from its surroundings to hunt or avoid being hunted[1]. Camouflaged object detection (COD), which aims to identify objects that are “seamlessly” embedded in their surroundings. The high intrinsic similarities between the target object and the background make COD far more challenging than the traditional object detection task[2]. Addressing camouflaged object detection requires asignificant amount of visual perception knowledge.

Autonomously detecting/segmenting camouflaged objects is thus a difficult task where discriminative features do not play an important role. While detecting camouflaged objects is technically challenging, on the one hand, it is beneficial in various applications such as medical image segmentation, search engine, etc. This paper is a study on the various technologies used for identifying object detection.

II. CAMOUFLAGED OBJECT DETECTION TECHNIQUE

Visual features of camouflaged objects are very much similar to the background. Due to the similarity in visual features (intensity, color, texture, etc), less work has been done to attempt visual camouflage breaking in the literature[3]. Here classifying camouflage object detection method based on these visual features and deep learning basis.

A. Convexity-Based Visual Camouflage Breaking

Some animals use apathetic coloring especially to prevent their detection by gray level convexity. Based on the convexity method visual camouflage breaking did use convexity of intensity function. To detect 3D convex or concave objects under strong camouflage, an operator (“Darg”)[4] is used. The Darg operator is defined by the sum of Yarg, rotated 0°, 90°, 180°, and 270°. Yarg is the y-derivative of the polar coordinates of the gradient argument of the original image. Yarg detects the zero-crossing of the gradient argument. Thus Yarg detects convexity because the zero-crossing of the 1st derivative determines the local minimum and local maximum of the original function. Once the Darg output is obtained, then threshold the image to find the most convex points. Therefore any object of interest should be labeled by this method, whether camouflaged or not. Darg can fully utilizethe representative image gray level represented by the convexity structure of the target, set up an appropriate threshold to eliminate the influence of the background noise by the median filtering through the gray face of the target image and realize the effective detection and identification of the convexity target. Darg operator is applied directly to the intensity function. Darg is based on the 3D structure of objects and responds to smooth 3D convex or concave domains. The operator is not limited to any particular light source or reflectance function. It does not attempt to restore the 3D scene. The purpose of the operator is the detection of convex or concave objects in highly cluttered scenes, and in particular under camouflage conditions. The method does not extract the object completely and some threshold must be determined, which may change the results. Convexity-based camouflage breaking was found very robust and in many cases much more effective than an edge-based detection operator.

B. Texture Segmentation by Multiscale Aggregation of Filter Responses and Shape Elements

Texture segmentation is a difficult problem, as is apparent from camouflage pictures. A textured region can contain texture elements of various sizes, each of which can itself be textured. Meirav Galun, Eitan Sharon, and others in [6] explained discrimination of texture segment in the image by Multiscale aggregation of filter response and shape element. Texture properties are computed at multiple scales and their features are used to identify larger texture properties. Furthermore, the process identifies the shape of texture components and discriminates them by their size, aspect ratio, orientation, brightness and then uses various statistical features to distinguish among different textures. The approach can be used for the recognition and retrieval of the same texture segment. The problem with the method is how to mix the various statistical features into a single weight. To enhance this method additional statistics can be incorporated[5].

C. Multiple camouflage breaking using co-occurrence matrix and Canny Edge detector

The co-occurrence and Canny method is a simple algorithm that creates a good outline of the object, but it does not extract the object, it must have the known background and has only been tested on synthetic images and may not be effective in the real application[7]. The method can be broken into two parts. The first part determines if there is a camouflage object within the image by calculating the gray level co-occurrence matrix of the image and comparing it with the gray level co-occurrence matrix of the background. Once it is known that there is a camouflage object within the image then the second part of the process begins. The second part consists of a repeated application of the Canny edge detection operator until effective visualization of the camouflage objects is achieved. The co-occurrence matrix is used to analyze the texture present in the given image, whereas the Canny edge detector is considered to defect the edges. A combination of both co-occurrence matrix and canny edge detector enhances the separability between objects containing a different kinds of textures. Though the method provides a good result for synthetic images, it is not applied to real-life data. Also, background information needs to be known before executing data.

D. Color and Intensity based camouflaged detection

Colour and intensity play a major role in the identification of objects. The method addresses the problem when the foreground object pixel and background object pixel have the same intensity. In the color and intensity-based method[8], camouflage is divided into dark and light camouflage. Dark camouflage appears when the pixel has less intensity and disguised into a shadow. Light Camouflage appears when the foreground pixel intensity is brighter than the background pixel intensity. With the help of normalized chromaticity measures and normalized intensities from the color-intensity model, foreground detection is achieved and then applying the pixel classification technique to extract the camouflaged portion. It does not work properly with intense shadow and light. It may be enhanced by considering the cue, corner, and edges of the image.

E. Use of GLCM and Dendrogram in camouflage detection

To detect the camouflaged portion from a given image and to extract it from the background image frame uses GLCM and dendrogram method[9]. In the method, camouflage breaking or de camouflaging is carried out in an unsupervised way, the meaning of unsupervised is that we do not have any information about either the camouflaged part in the image or features of normal background. Firstly converted the input image into a grayscale image then divide an image into 16 equal blocks and calculate the GLCM value for each block of image frame then mean is computed for each block. Finally, the dendrogram is plotted for mean values of each block and the largest individual block of the dendrogram is mark now combine the adjacent blocks. The method is not feasible for an image that contains an intense shade effect. The success rate of this method to identify camouflage portion is 70%

F. Bayes classification and Gaussian mixture model for back ground observartion

Bayesian classification is based on Bayes' Theorem. Bayesian classifiers are the statistical classifiers. Bayesian classifiers can predict class membership probabilities such as the probability that a given tuple belongs to a particular class. Gaussian mixture model (GMM) was proposed for background subtraction. Guo, Yaling Dou, and others have proposed a method to divide foreground from Background in visual surveillances [10] application by using Bayes classification and Gaussian mixture model for background observation, however because of camouflage it is very difficult to choose a threshold to divide foreground from background. Generally in visual surveillance applications problem of camouflage appears when the colour properties of foreground object are similar to background image frame. So propose the method to reduce variances in background image frame by averaging video frames in sequence. In this way reduced probability of camouflage but enhancement in this work is required.

G. Color, edge and intensity based background subtraction

The background subtraction method is based on color features and edge features of an image[12][15]. The approach focused on foreground subtraction from a background in visual surveillances. Whenever the color of foreground and background are the same, a camouflage problem occurs, to solve this problem a model based on the color, edge, and intensity features was proposed. The technique detects shadow images and low contrast images to discriminate between foreground and background. The algorithm overcomes the problem of shadow effect in identifying the camouflaged image of

P. Sengottuvelan method (Performance of Decamouflaging through Exploratory Image Analysis).

Another technique to detect the camouflaged target is based on these features[11]. Here, a higher threshold value is used to detect pixel which is certainly in the foreground. The lower one is considered to detect uncertain pixels. Then, the quasi-connected component is taken into consideration to get the camouflaged target. In this case, detection accuracy is also highly dependent on the threshold. The selection of the proper threshold value itself is a problem. For slow-moving objects, the method fails to detect objects[3].

H. Weight structural similarity (WSSIM) to find camouflage texture

Camouflage texture evaluation method based on WSSIM [13] is given to access the effects of camouflage texture. The method is based on human visual model. In the method differences of background image and camouflage textures are evaluated to understand what features of camouflage texture have the greatest effect on detection. Structural features like average luminance, standard deviation, correlation, entropy of given natural image frame can be utilized to detect the camouflage texture. The camouflage texture is compared with each block of the background with same size to get the whole evaluation result. The method is helpful for evaluation and design of the camouflage texture.

I. Detection of motion camouflage by Optical Flow model

The optical flow model [15] is used to detect motion patterns of the object and the background. Based on the magnitude and location of the optical flow, motion patterns are clustered and detect the camouflaged object. After that, the Kalman filter is used to improve the detection accuracy . However theaccuracy of the model depend on the results of optical flow. For slow moving objects and objects with camera motion, the method fails to provide excellent results.

J. Object detection using top down information based on EM (Expectation Maximization) Framework

Object detection scheme that integrates the top-down information based on the expectation maximization (EM) framework, by integrating spatial, top-down, spectral features of an image for the foreground object detection based on background[16]. In the method based on state of each target, top down information is incorporated in the object model to build expectation maximization framework to construct foreground model. This foreground model can improve the detection of camouflage portion. The method is basically for the visual surveillance application but they also describe how to handle camouflage problem. Limitation of the proposed method is if component of the object shape is obscure then detection of camouflage may not be accurate.

K. Texture guided weighted voting (TGWV)

A texture-guided weighted voting (TGWV)method to detect foreground objects in camouflaged scenes. The method employed the stationary wavelet transform to decompose the image into frequency bands. Observed that small and hardly noticeable differences between foreground and background in the image domain could be effectively captured in certain wavelet frequency bands. Finally, the foreground is detected using a weighted voting scheme based on the intensity and texture of all the wavelet bands. Experimental results demonstrate that the method achieves superior performance compared to the current state-of-the-art results[17].

III. CAMOUFLAGED OBJECT DETECTION BASED ON DEEP LEARNING MODELS

Deep learning has been widely used in computer vision, machine translation, speech recognition, and other fields and achieved good results. The deep learning method is adopted to detect camouflaged object which can extract deep features automatically. In deep learning, a depth feature is learned by the network from the extensive training images. The deep feature is more generic than the hand-crafted features. It works better than hand-crafted features (color, texture, motion, and gradient)[3].

A. Bio-Inspired Camouflaged Object Segmentation

A simple and flexible end-to-end network, namely MirrorNet, for camouflaged object segmentation. Bio-inspired MirrorNet leverages both instance segmentation and mirror stream to segment camouflaged objects in images[18]. Differently from existing networks for segmentation, the network possesses two segmentation streams: the mainstream and the mirror stream corresponding with the original image and its flipped image, respectively. The output from the mirror stream is then fused into the mainstream's result for the final camouflage map to boost up the segmentation accuracy. Extensive experiments were conducted on the public CAMO dataset to demonstrate the effectiveness of the network. The method achieves 89% accuracy, outperforming the state-of-the-art.

B. Camouflaged Object Detection

A novel deep based model specifically, provided a new challenging and densely annotated COD10K dataset contains 10K images covering 78 camouflaged object categories, such as aquatic, flying, amphibians, and terrestrial, etc. All the camouflaged images are hierarchically annotated with category, bounding-box, object-level, and instance-level labels. For conducting a large-scale evaluation, developed a simple but efficient end-to-end SINet framework. Compared with existing cutting-edge baselines, SINet is competitive and generates more visually favorable results. The above contributions offer the community an opportunity to design new models for the COD task.

IV. CONCLUSION

Camouflaged objects, have a lot of similarities with the background, making them difficult to detect. It requires a lotof knowledge about visual perception to do Camouflaged Object

Detection (COD). As the color, texture, and shape of the camouflaged objects are very much similar to its surrounding, a technique based on handcrafted features are unable to extract camouflaged object well. Most of the discussed methods work well for partial camouflage images but not applicable for fully camouflage images. So supervised learning methods are used to extract more features in-depth. Deep features are considered nowadays for identifying the camouflaged object. The main problem with this deep learning approach is the availability of a large database. Researchers acknowledge that there are more areas to explore. COD help to find and protect rare species in nature, detecting apples in orchards, help in search and rescue missions, or improve search results of search engines. With more understanding of the human visual system, sure that COD will become even better in the future.

REFERENCES

[1] S. Singh, C. Dhawale, and S. Misra, “Survey of object detection methods in camouflaged image,” Journal of IERI Procedia, vol. 4, pp. 351 – 357, 2013.

[2] D.-P. Fan, G.-P. Ji, G. Sun, M.-M. Cheng, J. Shen, and L. Shao,“Camouflaged object detection,” in proceedings of the IEEE/CVFConference on Computer Vision and Pattern Recognition (CVPR), June 2020.

[3] Ajoy Mondal,Camouflaged Object Detection and Tracking: A Survey.International Journal of Image and Graphics Vol. 20, No. 4 (2020) 2050028.

[4] Ariel Tankus and Yehezkel Yeshurun Convexity based Visual Camouflage Breaking Pattern Recognition Proceedings. 15th International Conference Page(s): 454-457 vol.1 2000 IEEE.

[5] Sujit K.SinghaChitra A.DhawalebSanjayMisrac,Survey of Object Detection Methods in Camouflaged Image, IERI Procedia 4 (2013) 351 – 357 .

[6] Meirav Galun, Eitan Sharon, Ronen Basri, Achi Brandt Texture Segmentation by Multiscale Aggregation of Filter Responses and Shape Elements Proceedings of the Ninth IEEE International Conference on Computer Vision (ICCV’03) 2003 IEEE.

[7] Nagappa U. Bhajantri and P Nagabhusan Camouflage Defect Identification: A Novel Approach 9th International Conference on Information Technology (ICIT’06)0-7695-2635-7/06 2006 IEEE.

[8] I. Huerta, D. Rowe, M. Mozerov, and J. Gonzalez Improving Background Subtraction Based on a Casuistry of Color-Motion Segmentation Problems IbPRIA ‘07 Proceedings of the 3rd Iberian conference on Pattern Recognition and Image Analysis, Part II Pages 475-482 Springer-Verlag Berlin, Heidelberg 2007.

[9] P. Sengottuvelan, Amitabh Wahi and A. Shanmugan Performance of Decamouflaging Through Exploratory Image Analysis in IEEE, DOI 10.1109/ICETET 2008.

[10] Hongxing Guo, Yaling Dou, Ting Tian, Jingli Zhou, Shegsheng Yu A Robust Foreground Segmentation Method by Temporal Averaging Multiple Video Frames ICALIP 2008 IEEE.

[11] T. E. Boult, R. J. Micheals, X. Gao and M. Eckmann, Into the woods: Visual surveillance of non cooperative and camouflaged targets in complex outdoor settings,”Proc.IEEE89(10), 1382–1402 (2001).

[12] P. Siricharon, S. Aramvith, T.H. Chalidabhongse and S. Siddhichai . Robust Outdoor Human Segmentation based on Color- based Statistics Approach and Edge Combination 978-1-4244-6878-2/10 2010 IEEE.

[13] Song Liming and Geng Weidong A new camouflage Texture Evaluation Method Based on WSSIM and Nature Image Features Multimedia Technology (ICMT), International Conference Page(s): 1 – 4 Cited by 1 IEEE 2010.

[14] Pan, Y. Chen, Q. Fu, P. Zhang and X. Xu, Study on the camouflaged target detection method based on 3D convexity,”Mod. Appl. Sci.5(4), 152–156 (2011).

[15] Jianqin Yin Yanbin Han Wendi Hou Jinping Li Detection of the Mobile Object with Camouflage Color under Dynamic Background Based on Optical Flow” Advanced in control Engineering and Information Science Elsevier 2011.

[16] Zhou Liu, Kaiqi Huang and Tieniu Tan Foreground Object Detection Using Top-down Information Based on EM Framework IEEE Transactions on Image Processing 2011.

[17]. Y. Y. H. W. Hou and J. Li, Detection of the mobile object with camouflage color under dynamic background based on optical flow,”Proc. Eng.15, 2201–2205 (2011).

[18]Jinnan Yan; Trung-Nghia Le; Khanh-Duy Nguyen; Minh-Triet Tran; Thanh-Toan Do; Tam V. Nguyen,MirrorNet: Bio-Inspired Camouflaged Object Segmentation,IEEE, 08 March 2021.

SURVEY ON SIGN LANGUAGE RECOGNITION SYSTEM

Siddiqul Akbar[1] Student
siddiqulakbarn@gmail.com

Shamna HR[2] HOD
shamnahr@gmail.com

Dept.of Information Technology
Government Engineering College Barton hill Trivandrum

ABSTRACT

Sign language (SL) is the way of communication used by deaf people around the world. They face difficulty interacting with others. SL is a fully visual language with its grammar that largely differs from spoken language. Normal people find it difficult to understand the sign language and gestures made by deaf and dumb people. Innovation of new technologies such as smartphones and wearable needs to be capable of recognizing SL. This will open up the opportunity to SL users. The paper is based on a survey of the available technology that can be used to recognize SL.

1. INTRODUCTION

In day-to-day life, humans communicate with each other and interact with the computer also. Sign Language is the most natural way of exchanging information among deaf people. But deaf people are facing difficulty interacting with normal people. That's why Sign Language recognition is used to convert gestures into text or speech. The hand is the most common part of communication.

Mobile computing gives a new face to this technology. Many of the new smartphones have come with multicore chipsets and great cameras. It will help the developers to make a more efficient system for smart devices.

This paper is discussing the work done in the area of hand gesture recognition which provides an overview of this technology. This research area can be divided into two broad categories based on sign recognition.

Static sign-based recognition: The majority of research to date is conducted for the static sign. The system is mostly based on skin colour modelling techniques.

Dynamic sign-based recognition: Dynamic/ continuous sign-based sign language recognition has a lot of potentials for research. Some researchers have performed some research in the area but a lot of aspects yet to get more focused work.

2. SENSOR BASED APPROACH

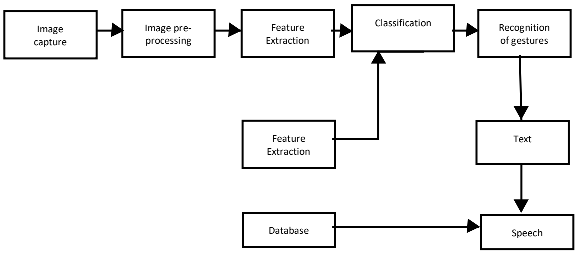
This approach collects the data of gestures performed by using different sensors. The data is then analysed and conclusions are drawn by the recognition model. In the case of hand gesture recognition, different types of sensors were used and placed on the hand, when the hand performs any gesture, the data is recorded and is then further analysed. Use of external hardware causes the natural motion of the hand. The major issue is, complex gestures are not allowed in this method. [1]

3. VISION BASED APPROACH

This approach takes an image from the camera as data of gesture. The vision-based methods mainly concentrate on the captured image of gesture and extract the main feature and recognize it. The colour bands were used at the start of the vision-based approach. The main disadvantage of this method was the standard colour should be used on the fingertips. Then the use of bare hands is preferred rather than the colour bands. [1]

4. LITERATURE SURVEY

In this paper [2] the sign and hand gestures are captured and processed with the help of mat lab and converted into speech & text form. The feature extraction of values of the images is evaluated based on 7Hu (7 moments) invariant moment technique and the classification techniques are applied using K-Nearest Neighbour (KNN) is compared with the PNN (Probabilistic Neural Network) for the accuracy rate. The performance of the proposed classifier KNN is decided based on various parameters. Parameters can be calculated by formulas, using the 7hu moment's technique for feature extraction will be done, the 7Hu moments are a vector of algebraic invariants that added regular moment. Hu moments are used in the classification [2]. The object is assigned to the class by most common among its nearest neighbour's k.



In this paper [3], hand gesture recognition can be done by wearing gloves this proposed system can work for real-time translation of Taiwanese sign language. The different hand gesture can be identified by using the 10 flex sensors and inertial sensors which is embedded into the glove, it includes three major parameters, there are

1. The posture of fingers

2. Orientation of the palm

3. Motion of the hand

The finger flexion postures can be collected from the flex sensors, the palm orientation acquired by G-sensor, also the motion trajectory acquired by the gyroscope are used as the input signals of the proposed system. The input signals will be gathered and validate or checked periodically to see if it is a valid sign language gesture or not. The orientations of palm-like up, down, right, left, etc. Will be identified by using 3D data sequence along x-axis y-axis and z-axis. Once all these processes are done the sampled signal can last longer than a predefined clock cycle, and it is regarded as a valid hand sign language gesture and will be sent to smartphones via Bluetooth for gesture identification and speech translation. The accuracy for gesture recognition in this proposed system is up to 94%.

In this paper [4] a vision-based approach is developed for performing various computer functions with the aim of human-computer interaction. The human-computer interaction aims at an easy way of interaction with the system. Image segmentation and feature extraction can done by using this technology. There are few steps are involved in this interaction method:

- Convert the binary image from the coloured images

- Find the outline of the binary image and draw this on another blank frame

- Find the centre of mass of the hand

- Find and draw the hull problem and convexity issue on a blank image

- Define and manipulate centre points which can be used in gesture control

There are few parameters to be considered:

- Point start-Point of curves where the convexity defect begins

- Point end-Point of contour where the convexity issue ends

- Point far-Point within the defect which is far from the hull problem

- Depth-Distance between the convex hulls i.e. the outermost points and the farthest points within the shape.

These points can be used as parameters for designing hand gestures for computer control.

In this paper [5], a vision-based sign language recognition system using LABVIEW for sign language is present. The goal of this project is to develop new vision-based technology for recognizing and translating continuous sign language to text. Although the deaf, who can hear and hearing signers can communicate without problems among themselves, there is a serious challenge for the deaf community trying to integrate into educational, social, and work environments.

Environmental Setup:

The image acquisition process has many concerns such as the position of the camera, lighting sensitivity, and background condition.

Result:

This sign language translator can translate alphabets (A-Z/a-z) and numbers (0-9). All the signs can be translated in real-time. This system has only been trained on a small database. This is a wearable system that provides the greatest utility for automated sign language to spoken language translators. A signer can wear this whenever communicating with a non-signer might be necessary.

In this paper [6] there are two feature descriptors used Histograms of Oriented Gradients and Scale Invariant Feature Transform. The algorithm implemented in KNN uses HOG features for an image and classifies them using the SVM technique. The algorithm implemented to recognize the gestures of Indian Sign Language is of static images in the proposed system.

Result:

Without categorizing into single and double-handed gestures:

- Accuracy using the KNN algorithm of HOG features of images is 78.84% and that for SIFT gave 80%.

- After classifying into single and double-handed gestures

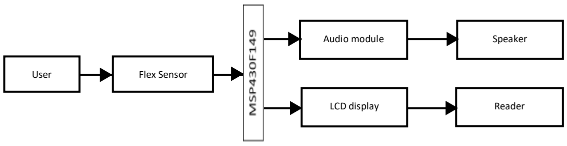
- HOG gave100% for single-handed 82.77% for double-handed

- SIFT gave 92.50% for single-handed 75.55% for double-handed

- Fusion of both gave 97.50% for single-handed and 91.11% for double handed

This paper [7] describes a new method of developing wearable sensor gloves for detecting hand gestures which use British and Indian sign language system. The outputs are produced in the text format using LCD and audio format using the APR9600 module. The hand gesture or hand signs are converted to electrical signals using a flex sensor. These electrical signals are processed to produce the proper audio and text outputs. The paper employs a method of tuning to improve the accuracy of detecting hand gestures.

A glove with a flex sensor is used to detect the signs made by the person. Gestures that are made are converted to equivalent electrical signals by the sensor. MSP430F149 pins take the signals as input. For different gestures the signals are different.



This paper [8] tells about the first data-driven automatic sign language to the speech translation system. They have combined an SL (sign-language) recognizing framework with a state-of-art phrased-based machine translation (MT) system using corpora (complete written work) of both American Sign Language and Irish sign language data. They have also explained about vision-based knowledge sources. They also inform us about the challenges that come down when a deaf and hearing person communicates. They have suggested that a data-driven output recognizer is not easily comprehensible because of different grammar and annotation formats.

Sign Language Transcription: There is a lack of a formally adopted writing system of SL. Some attempts have been take place to describe the hand form location and articulation moment. Despite this they fall short to be used in computational hence they adopt annotation. In annotation manual transcription of sign language is taken from video data. 4 methods are implemented:

1. MT for English sign language of the Netherland

2. SMT (statistical machine translation) for German sign language

3. (Chiu) Chinese and Taiwanese sign language system

4. (san-Segundo) for Spanish and Spanish sign language

Result:

The size of RWTH-Boston 104 is small to make a reliable assumption. At very least to show that SMT is capable to work as a middle step for a sign-to-speech system. For extremely small training data the resulting translation quality is sensible. Moreover, sign language produces quite a large effect known as articulation.

5. CONCLUSION

This paper deals with the different algorithms and the techniques that can be used for recognizing the sign language and the hand gesture made by different deaf and dumb people. A hand gesture recognition system is considered a way for a more intuitive and proficient human-computer interaction tool. The range of applications includes virtual prototyping, sign language analysis, and medical training. Sign language is one of the tools of communication for physically impaired, deaf, and dumb people. From the above consideration, it is clear that vision-based hand gesture recognition has made remarkable progress in the field of hand gesture recognition.

6. REFERENCES

[1] IRJTRS ISSN No.: 2454- 2024 “literature survey on hand gesture techniques for sign language recognition”.

[2] Third ICCUBEA 2017 “Moment Based Sign Language Recognition for Indian Languages” Umang Patel and Aarti G. Ambekar.

[3] Lih-Jen kau, Wan-Lin Su, Pei-Ju Yu, Sin-Jhan Wei “A Real-time Portable Sign Language Translation System” Department of Electronic Engineering, National Taipei University of Technology.

[4] Alisha Pradhan and B. B. V. L. Deepak “Obtaining Hand Gesture Parameters using Image Processing” 2015 ICSTM.

[5] Yellapu Madhuri , Anitha.G , Anburajan.M “VISION-BASED SIGN LANGUAGE TRANSLATION DEVICE” conference at SRM University

[6] Bhumika Gupta , Pushkar Shukla and Ankush Mittal “K-Nearest Correlated Neighbor Classification for Indian Sign Language Gesture Recognition using Feature Fusion” ICCCI -2016.

[7] Virtual talk for deaf, mute, blind and normal humans by Vikram Sharma, M Texas Instruments India Educators' Conference 2013.

[8] Daniel Stein, Philippe Dreuw, Hermann Ney, Sara Morrissey and Way “Hand in Hand: Automatic Sign Language to English Translation”.

Insider Prediction and Detection Using Machine learning Techniques

P. Varsha Suresh
Computer Science And Engineering
Sree Buddha College of Engineering
Pattoor, India
varsha2361995@gmail.com

Ms. Minu Lalitha Madhavu
Computer Science And Engineering
Sree Buddha College of Engineering
Pattoor, India
minulalitha@gmail.com

***Abstract*—A Cyber Attack is a sudden attempt launched by cybercriminals against multiple computers or networks. According to evolution of cyber space, insider attack is the most serious attack faced by end users, all over the world. Insider that perform attack have certain advantage over other attack since they familiar system policies and procedures. It is performed by authorized person such as current working employee, preworking employee and business organizations. Cyber security reports shows that both US federal Agency as well as different organizations faces insider threat. Compromised Users, careless Users and malicious Users are some of the ground for insider attack. User-Centric insider threat detection based on data granularity provide a new extent for insider detection since data is analysed on it's depth. but, improper selection of feature is a demerit. As a result, Data granularity with two stage confirmation method is used in the proposed system. In the first stage dual filtering using Hidden markov model and fuzzy logic is involved. In the second stage, the predicted output from first stage is again checked using profile-to-profile or template-to-template comparison.The selection of user's information as well as triple feature for generating training set is an additional advantage of the proposed approach. Two stage confirmation leads to increase in performance measure with very low false positive rate.**

***Index Terms*—Cyber Security, Machine Learning (ML), Hidden Markov Model, Fuzzy logic.**

I. Introduction

Securing information from unauthorized access is known as information Security. The practice of stopping the disclosure, disruption, modification, inspection and destruction of information without knowledge of user. Information can be anything like user's details, profile on social media, data in mobile phone or biometrics etc. Authentication and authorization are essence of information security. Authentication does the duty of confirming a person's identity while authorization does the work of providing appropriate privileges to an individual after verifying the person's identity. Cyber Security is the approach of technologies to check and to safeguard systems, networks, devices and data from cyber attacks. A cyber attack can illegally damage computers, steal data, or use a breached computer as a starting point for other attacks. Cyber Security is the state of safeguarding and recovering computer system from any type of cyber attack. Cyber attack can be divided in to insider as well as outsider attack. There are different type of cyber attack such as Phishing, Manin-the-middle attack, Denial-of-service attack etc. According to the evolution of cyber space Insider attack is the most promising attack faced by user's in today's world. A threat that originates inside the industry or government firms, and causes exploitation is known as internal Cyber threat or internal cyber attack. Insiders that perform attacks have a dominance over external attackers because they have approved system access and also may be familiar with web architecture and system guidelines. Moreover, there may be fewer safety against internal cyber attacks because many firm focal point is on protection from exterior attacks.As claimed by Clearswift Insider Threat Index (CITI) [25] annual report 74% of data security breaches in past 12 months were originated by insiders. Source of attack or behavior of attack are used to classify security attack. Source defines the place from which attack originate and behavior defines the aggressive behavior which leads to forceful access of data. Attacks are classified as insider or external attack in case of the former and in the case of the latter, they are classified as active or passive attacks. External attack originate from the outside the organization and some of the important external attack are network security attacks, physical security attacks, etc. A malicious attack caused by an individual within the organization is known as insider Insider may be a current working employee , a former employee or a business associate. Whereas, Active attack has more importance over passive attack as it tries to modify the content of the messages. In case of Passive attack, an attacker observes the messages or it's content and subsequent retransmission takes place.

According to cyber security report , 25% of all the attacks to organizations are due to insider and their number is increasing day by day. It is very much importance in the current era . According to recently published report of IBM, because of COVID- 19, 53% of employees are working from their home using personal laptops and 61% employees haven't provide tools to properly secure those devices. Which leads to loss of secure data and it is done by a known person. Actually insider threats have been an issue for companies long back, but they have gain more strength after the system gotten increasingly interconnected. The study sponsored by Ponemon Institute which was sponsored by IBM explains that insider-related incidents costs $4.3 million in year 2016. According 2018, cost for these internal cyber attacks was $8.7 million. This is the big take away and the data breach cost is trending upwards both in the US as well as globally. In 2019 also the number of attacker is increasing tremendously , which leads to increasing in lose that was faced by organization. Same time user's or each individual may effected by insider attack or an internal friend who behave as an attacker. User's personal information or credentials are traced by the attacker with out the knowledge of user. As a result, the user may also face many problems such as lose of money or their personal properties etc. Different techniques are introduced prevent insider and their harmful attack.

The objective of this paper is to understanding the harmful effect of internal cyber attack. The lose which is faced by individual or organization over years. Analysing different work to understand the move made by an insider. Understanding what are the differents methods used by business organization to prevent insider before attack takes places. To propose a new and advance techniques to detect insider and reduces the harmful effect. To bring forward a novel two stage confirmation techniques to protect from insiders.

The important contributions of this paper are outline as follows:

- We first give a brief idea of the Cyber Security, followed by providing knowledge about insider as well as outsider attack.
- we provides an information about different type of insiders which exist in the organization.
- We present a novel approach using two stage confirmation to protect from internal cyber attack.
- We mention the use of two important machine learning algorithm that is fuzzy and markov model.
- We bring the use of the concept anomaly based detection and misuse detection in the second stage of confirmation.
- We mention the advantage of data granularity and proper selection of user's information and triple features for detection of insider.
- Finally, we illustrates a theoretical analysis between the existing and the proposed insider detection models.

The remainder of the paper is Section 2 describes the Method Of study. Section 3 provides an overview of Insider Cyber Attack. Section 4 describes the related works explaining different insider detection techniques. Section 5 explains the proposed insider attack detection method. Section 6 illustrates the theoretical analysis performed between the existing and the proposed insider detection models. Section 7 concludes the paper and provides future directions.

II. Method of study

This paper propose a novel approach for insider detection using two stage confirmation. The objective is to propose a new approach which tackle the problem in the existing approach and improves the efficiency. The reviewed papers concentrate on diverse task which have been considered to study the negative effect of insider attack (Internal Cyber attack) to organization such as lose in money, reputation and secret files and data of companies. The findings of these work are very effective on learning the issues and increasing estimate to address solution. We spend most of time to explore different facts such as Taylor and francis, Elsevier, Science Direct, Springer, IEEE Explore, and other computer science journals and conference. In searching sentences and keywords we used application of cyber security in organization and government agencies. We inspect each and every article's reference list to recognize any potentially applicable research or journal title. The publication periods taken into consideration is 2010 to 2021. For exploring different we collect abstract and keywords of PDF, reports, documents and Full length paper. Furthermore, in searching different information for getting content we used journal, conferences paper, workshop papers, topics related publication, expert lectures by expert or talks and other topic related communities such as Overview of insider attack, Insider attack challenge to organization, Insider and Outsider Data Security threats. Different video and lecture class related to the harmful effect of insider, paved the way for research work. Different review and research paper on reputed journal enable us to understand the demerit of existing system and draw back of proper selection of feature. So, for this research, we collect information from two sources and take the application of machine learning to do this research with all sincerity.

III. Overview of Insider Attack

Attack that originates inside the industry or government firms, and causes exploitation is known as internal Cyber threat or internal cyber attack. Insiders have dominance over external attackers because they have permitted system access and also be familiar with the architecture of network as well as system procedures. Moreover, It has less security against insider attacks when compared with external attack.
Types of Insider Attack are:

- **Malicious insider** - A Turncloak, who maliciously and intentionally abuses credentials such as Password , to steal information for financial or personal reason.
- **Careless insider** - An innocent user who unknowingly reveal the system to outside threats. It is common type of insider threat that arises from mistakes, such as keeping a device expose. Careless insider may arises when an employee unknowingly click an insecure link, affecting the system with malware.
- **A mole** - A person who is actually an outsider but behave as an insider to gain access to a privileged network. Actually the outsider impersonate as a worker in the organization.

An insider threat is one of the most expensive types of attacks and hardest to detect. It mainly occur inside the organization by peer worker or colleague with our knowledge. An employ change in to insider due to dissatisfaction in his work. Due to avoidance of promotion or unnecessary cutting of income will change their mind. Some times, company may not provide employee proper reward or sudden termination may lead the path to an insider. This circumstance of worker is usually used by other agencies to make him insider. Most probably legible user become insider because negative effect environment in which they live.

IV. RELATED WORKS

Insider attack is a cyber attack performed by authorized person such as current working employee, pre-woring employee or business organization. Insider or Internal Cyber attack detection system proposed by several authors and their merits along with demerits on it's detection and prevention are discussed in the following sections.

A. Insider attacks at SC level by using data mining and forensic techniques

Computer systems select user IDs and passwords as the login credentials to authenticate users. Mostly,login patterns are shared by the individuals with the coworkers and request them to assist co-tasks. As a result, safety of pattern used is not up to the mark. A legitimate users of a system who perform malicious action to the system internally, are difficult to determine as intrusion detection systems and firewalls detect and destroy harmful action occurs from outside the system. Fang-Yie Leu et al. [1] propose a system, named Internal Intrusion Detection and Protection System (IIDPS), to identify insider or internal threat at system call (SC) level by mining the data as well as using forensic features.The IIDPS determine login user is a account holder by comparing with the users' personal profiles. User's usage habit is used as forensic feature for the detection purpose.The IIDPS is organized by distinct element such as System call monitor and filter, two type of server such mining and as well as detection server, grid for computation purpose, and three repositories are also used such as log files of user, profiles of user and attacker. The SC monitor and filter gather SCs submitted to the kernel and save these SCs in a format which consist of user ID, the process ID, and the SC passed by the users. User's inputs is stored in user's log file. The mining server check the log data with data mining techniques to understand the user's computer usage habits, which are then stored in the user profile. The detection server makes a comparison between users' behavior patterns with those SC-patterns gathered in the attacker profile and those in user profiles to detect harmful behaviors and attacker. When an intrusion is identified, the detection server alert the SC monitor and filter to separate the harmful user from the protected system. The purpose is to ban the user from continuously attacking the system.

Ability of identifying and preventing attack has been analyzed in this paper.This has been done by means of a experimental testbed, which consists of 12 users to verify the feasibility and accuracy of the IIDPS and the results shows that mining of information as well as historic feature are used for intrusion detection provide strong resistance against threat.

The results also demonstrate that IIDPS can effectively prevent different aforementioned attacks .Detection and mining speed of approach is high. Similarity scores in this approach helps to identify unknown user accurately. Accuracy of detection of attack in IIDPS is 94.29%, and the response time is less than 0.45 s means it can prevent protected system from insider attacks effectively and efficiently.IIDPS pay out 0.45 s to spot a user. The demerits bounded with data mining and forensic technique is that third-party shell command is not used in this approach to improve the system performance. IIDPS may detect inaccurately when user's habit suddenly changes.

B. Insider Attacks detection in Big Data Systems

Big Data is a gathering of information that is vast in volume, which is raising exponentially. It is a area with so large size and complexity that none of data management tools can process it efficiently. In such a system Information security is a major opposition for Big Data System. From a customer point of view one of the main risks in adopting big data systems is in trusting the provider who protect the information. Santosh Aditham et al. [2] propose a new system architecture in which insider or internal cyber attacks can be identified by using the replication of information on different nodes in the system. It utilize a two-step threat detection algorithm and a safe communication protocol to identify processes running in the system. Atmost two step in which construction of control instruction is the first step and second step involves their matching. The first and foremost step in the attack detection is process profiling, which is conducted independently at each and every node to identify different attacks and the second step is hash matching which is performed by replica data nodes understand about the legitimacy of attack. It is a combination of independent security modules that work simultaneously and reside on individual nodes of the system. Information transferred between the safety element in the system architecture contain meaningful knowledge about the analysis of a process. Hence, a public key cryptosystem is used for secure communication .All information transferred by node using secure communication channel is encrypted by using private key and copies of the keys are not available to anyone. The associated public key will be passed with all other duplicate nodes that a information node need to communicate. Actually the proposed security system is a combination of 3 parts that is secure communication protocol, process profiling and hash matching. The three parts are formed of different modules that need to be installed in to big data system. Secure communication protocol is used to send, receives or queue message. Process profiling is used analyze as well as encrypt data. Verification and consensus is used to decrypt, verify and notify about attack.

Different method used to increase the privacy and security of data in Big Data System.Mean while, providing a positive vibe to user who trust Big Data. Techniques used to prevent insider has been discussed in this paper. This has done by means of real-world hadoop and spark tests indicate that the system needs to consider only 20% of the code to understand a program and suffers 3.28% time overhead and the result shows that the security system can be built for any big data system due to its external workflow.

The results also demonstrate that the system detect insider attacks quickly with low overhead. It aims to provide robust security for big data systems. The limitation associated with this approach is that need to provide methods to evaluate system on security related benchmarks. Also, lack of commencing a hardware architecture of security chips that can support the system.

C. Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks

Wireless mesh networks promise to extend high-speed wireless connectivity beyond what is possible with the current WiFi-based infrastructure. However, their unique architectural features leave them particularly vulnerable to security threats. Loukas Lazos et al. [3] says that unlocked nature of the wireless channel leaves it to jamming attacks. Anti-jamming method include some type of spread spectrum (SS) communication, in which the signal is passed across a large bandwidth according to a pseudo-noise (PN) code. SS can protect the wireless communications safe to make PN codes secret. If an insider have the knowledge of the commonly shared PN codes can still make a jamming attacks. WMNs is a combination of two-tier network architecture. The first tier incorporate end users, they are also known as stations (STAs), which is merged with mesh nodes, and known as mesh access points (MAPs). The second tier or stage is made of a peer-to-peer interconnections of the MAPs. Connectivity in the second tier is supported by mid-way routers known as mesh points (MPs), which connect MAPs (MPs do not receive interrelation from end users). The interconnection of MAPs and MPs is usually static in nature , and use different frequency bands to transmit data and control information. Finally, mesh gateways (MGs) support connectivity to the wired infrastructure. Internal attacks or Insider attack, which are begin from compromised nodes, are much more knowledgeable in nature. These attacks uses ideas of secrets of networks and protocol to carefully and secretely target critical network. Internal attacks, also known as insider attacks, cannot only prevent using energetic methods that focus on network secrets, because the attacker already have an idea. If selective jamming is not effective due to anti-jamming measures, an insider can carefully drop packets. Once a packet has been accessed, the compromised node can audit the packet headers, classify the packet, and think whether to pass it or not. Such an action is often termed misbehavior. Post-reception dropping is less tensile than selective jamming because the adversary is minimal to dropping only the packets routed through it.

Ability of selective Jamming or Dropping insider attack in Wireless mesh network has been analyzed in this paper.

The results also demonstrate that to it helps to avoid the use of common secrets for protecting broadcast communications. Limitation bound with approach is that heightened tier of security comes at the expense of performance. Other one is accurate behavioral monitoring mechanisms that do not depend on continuous overhearing, and proper maintenance and dissemination of reputation metrics.

D. Geo-Social Insider Threat Resilient Access Control Frame-work (G-SIR)

The most dangerous and costly threat to institutions is denoted as Insiders. These attacks are carried out by user or person who has authorized access to the system. Preventing insider attacks is a discouraging task.Nathalie Baracaldo et al. [4] propose Framework G-SIR to deter insider threats by including current and historic geo-social knowledge as part of the entrance prevention decision process .By analyzing users' geo-social behavior, insider can be those users whose access behavior variess from the normal patterns, such anonymous character can lead to potential insider attackers who may intentionally carry out harmful activities. Such information to determine how ethical a user before granting access. The proposed system consist of AC guideline specification and enforcement strategy designed to understand users' geo-social behavior. The AC component collect present and historic geo-social interactions to predict whether an access should be granted or denied. A role may have a spatial scope that specifies particular locations where it can be activated by users assigned to it. Geo-Social constraints indicate area that users assigned to the constrained role cannot visit and user they cannot frequently meet. Vicinity constraints force a restrictions on individual that may or may not be at a particular distance from the requester at the time of an access. Mainly there are two types of vicinity constraints such as inhibiting and enabling constraints. Inhibiting constraints gives the idea that permission needs to be denied, if inhibiting users are identified in the vicinity. Enabling constraints are used to understand the importance of permission in the vicinity of the requester. Geo-social trace based constraints are constraints that a user to go after a certain geo-social path before they can be authorized to access a particular resource. Geo-social obligations are geo-social actions that users need to manage after they have been granted an permission. All monitoring and likelihood computations described take place in the Monitoring, Context and Inference Module. It specifies the context of a user, which contain information such as the current device used by the individual, type of connection used, etc. The Access Control Module is in charge of creating AC decisions.

Ability of identifying and preventing attack in G-SIR has been proposed in this paper. This has been done means of a distinct indoor simulator carried out in Java and the results indicate that this is the first and foremost effort to use geo-social information to deter insider threats by integrating it into the AC mechanism.

The results also demonstrate G-SIR is efficient, scalable and effective to detect insider by including historic and geo-social knowledge. It contain various geo-social constraints and enforcing these condition helps to minimize the risk of proximity, social engineering and probing threats. The limitation bound with this approach is that behavioral knowledge should be considered at the time AC decisions. However, designing a system that uses such information without expanding the risk exposure is a challenging task.

E. Addressing the DAO Insider Attack in RPL's Internet of Things Networks

In RPL routing protocol DAO which is a information used for control are passed by the child nodes to their corresponding parents to produce descending routes. A harmful insider node can utilize this characteristics to send fraud DAOs to its parents periodically, activate those parents to pass the fake messages to the root node. This characteristics can have a harmful side effect on the production of the network, power consumption can be increased drastically, latency, and reliability can be reduce to an extent.

RPL arrange its physical network into a shape of Directed Acyclic Graphs (DAGs), If DAG is implant at a single destination, then it is known as a Destination-Oriented DAG (DODAG). To incorporate traffic pattern to upward, DODAG should be constructed,topology centered at network root. The manufacturing of the DODAG launch with the root multicasting control messages called DODAG Information Objects (DIOs) that is passed to RPLs neighbors. Baraq Ghaleb et al. [5] demonstrate RPL node as a available stopping place from the root. An important reality of transferring a DAO message by a child node will leads to passing of many copies of DAOs that is equivalent to the number of intermediate parent nodes. An oponent can utilize this information to harm other network continuously transmitting DAOs to its parent node. In order to determine a DAO internal attack in RPL, a new approach called SecRPL is used, that prevent the count of forwarded DAOs by a parent. In fact, there are two opinion for appling this restriction. Former is to regulate the total count of transmitted DAOs regardless of the source node, the second is to prevent the count of transmitted DAO per destination. Second option is better compared to previous option and result in preventing some DAOs coming from non malicious junction or node. It may also leads to block DAOs of some nodes and no effect to some others DAO. . In addition, parent node maintain a counter with each child node in its sub-DODAG. Incase, If the number of forwarded DAOs exceeds threshold value, the parent discards any DAO message. It also make clear that no node will be blocked due to the time factor, after two consecutive DIOs, counter is reset . Mainly, when the parent node pass a DIO message, all child node counter are reset.

F. Securing Wireless Medium Access Control Against Insider Denial-of-Service Attacks

An malicious user (attacker) who default the network can start more harmful denial-of-service (DoS) attacks than a External user by passing large amount reservation requests to block the bandwidth. SecureMAC is an approach used to protect against such insider threats. It consist of four components such as channelization which is used to block large reservations, randomization method is used to counter reactive targeted jamming, coordination perform duty to to prevent control-message aware jamming and again over reserved and under-reserved spectrum should be solved and assignment of power to find out each node's contribution to the particular power. Sang-Yoon Chang et al. [6] demonstrate a general handshake-based MAC framework where it denote how to send a packet, how the transmitter shows a MAC-layer decision based on its observations and the knowledge from previous transmission rounds. Save as well as reserve the channels for data transmission. Reserved channels is used for transmission of data packets and feedback is gain from the receiver as well as the network.

In wireless MAC, an internal attacker can carry out the following actions that are more damaging than those from an external users. False reservation injection means holding the channel resources without operating them, false feedback distribution consist of announcing wrong data to twist the action on MAC control to the attacker's favor , and MAC-aware jamming where jamming is based up on to the received control messages. False reservation hide bandwidth to actual users and takes small insider resources and use network resources out of proportion to attacker effort, it is more efficient mistake than jamming. The goal of channelization is to distribute spectrum bandwidth to each user proportional according to their power capability, guarantee a specific power spectral density. Channelization actions are made only once per round.The coordination solve these problems by enhancing the bandwidth allocation and the randomization output solving certain conflicting reservations and sharing transmission to area that would otherwise be not utilized.. Finally, after each round of information transmission is over, each junction carryout power attribution to calculate the count of power contributed for communication of data by each node.

G. Securing VPN from insider bandwidth flooding attack

The insider attack is launched by users residing within the trusted zone of the VPN site. They are the legitimate users of the VPN service. Flooding packets are used for easily attacking the VPN service. Safeguarding from insider or internal cyber attack is more difficult then external cyber attack as it is launched by users who have authorized access to the VPN service. This type of flooding attack disrupts the VPN service to its other legitimate users. Network security deals on safeguarding network perimeter from outside threat even though internal attack is more serious. It's aim is to add a control mechanism for bandwidth to control the bandwidth each individual. The bandwidth control mechanism must ensure that the packet through the reserved bandwidth is within the allowable limit. Control mechanism has used to reduce dropping packets from the flooding source which protect authorized user from harmful attack. Saraswathi Shunmuganthan a et al. [7] describes Virtual Private Network (VPN) is an encrypted connection over Internet from a device to a network.It helps to transmit data from a branch office to main office.

Flooding is a routing algorithm present in computer network in which all arriving packet is passed through every other link not on the link from which it has came.

VPN site 1 and VPN site 2, are connected to gateway routers called customer edge (CE). CE1 and CE2 are interconnected to provider edge (PE) routers PE1 and PE2. Bandwidth is actually maximum data transfer rate over network. Customer Edge router ensure that bandwidth allocated to VPN site is being fairly distributed among users to avoid insider attack. It employs entropy based probabilistic model at CE router to rate limit of insider attack traffic. Entropy is used to measure the uncertainty. Entropy is used to calculate deviation of user from normal use age.

H. Insider threat risk prediction based on bayesian network

Bayesian network is a graphical model based on probability, consist of a number of variables via directed acylic graph (DAG) is used to show conditional dependencies. Nebrase Elmrabit a et al [8] demonstrate that the features which used by the graph are technological aspects, Organizational impact and Human Factors. Information are collected from organization and particular measure sealing to ensure insider threat breaches are kept to minimum. Investment balance is the balance between investment in insider and outsider threat is key to understand insider threat breaches. Detection level is the measurement of how accurate detection system with regards to previous insider attack. Security and privacy control include forensic evidence, network as well as email logs. Organizational Impact is the information related to the way in which organization is structured and how insider threat breaches are managed. Organizational impact deal with information like security breaches, Structure , security policy as well as employee work-related stress symptoms.

Security breaches include breaches that have occured historically with in the organization. Structure include information about recruitment procedure, previous employment screening. Security policy contain information related to organizational security policy. The fragile link in an information security chain is one and only human factors. It include motivation which include motivation for showing misbehavior, Opportunity is the factors which is available to perform attack. Capability include the power to do something by the fellow being.

I. Motivation And Opportunity Based Model

Situational crime prevention theory (SCPT) opportunities for misbehaviour is lowered to an extent.Social Bond Theory (SBT) can be used to help understand motivation to engage in misbehaviour. Raise in effort, risk and lower the rewards, stimulation, keep away exempt are the elements considered in SCPT. Nader Sohrabi Safaa et al. [9] explains SBT pivot on mainly four factors such as organisation attachment, realtion with institution or organisational , involve n a particular work, and personal standard. Increase the effort is used to raise the amount of effort which is taken to perform attack. Increase the risk is used to increase amount of risk that is faced by the attacker, when he/she do a malicious action which is harmful to organization. It also reduce the excuse which made by worker in doing mistake, since they fear to do it again. Reward which the attacker get by doing mistake is also reduce drastically.

Social bond theory include attachment with the organization. If their is any problem with the organization as well as worker, chance of performing attack is more. Commitment with the organization is also considered. If a person is commitment with organization, he/she will not do any negative thing to the organization. Workers involvement with the organization show that whether he is an attacker or normal user. If user is sensitive towards organization, he/she will not do any malicious activity.

J. User Behavior Modeling and Anomaly Detection Algorithms For Insider Detection

Junhong Kim et al. [10] demonstatre user behavior-modeling phase, where each user's behaviors are converted in to daily activity summary, e-mail contents, and e-mail communication network. Anomaly detection algorithm consist of Gaussian density estimation (Gauss), Parzen window density estimation (Parzen), principal component analysis (PCA) and K-means clustering (KMC) are algorithms used for separation of pattern. gaussian density estimation which is important anomaly detection algorithm is used exhibit probability distribution of variable which distributed randomly. Parzen window classification is used for density estimation. It find a point of interest. Only the features inside the window is considered to find which group the point of interest is present. It is used to calculate output probability when a point is given. Principal component analysis is used in dimensionality reduction for the reduction of noise or unwanted data. Dimensional Reduction consist of feature selection and feature extraction. PCA comes under feature extraction in order to reduce noise or error. As the number of feature decreases, processing will be fast. K-mean clustering is an unsupervised algorithm does not have labelled data. Set of data is put together in a group or cluster. cluster consist of object which is similar in nature. K denote the number of cluster or group.For best classification of data in to different group, appropriate cluster need to find.The attack observation model surrender at most 53.67% of the detection rate by only tracking the top 1% of malicious or suspicious instances.

The papers [11], [12] propose many insider detection methods like alarm filters and Psychological model to predict malicious behaviour.

V. PROPOSED SYSTEM

Insider Detection techniques have been developed to protect the system from wide variety of internal attack performed by current working employee, Pre-Working employee or Business Organization. It is used to safeguard the privileges, reputation, key documents and economics of the organization or institution. Several feature extraction techniques, Machine learning schemes, Psycho metrical and behaivour schemes are used to

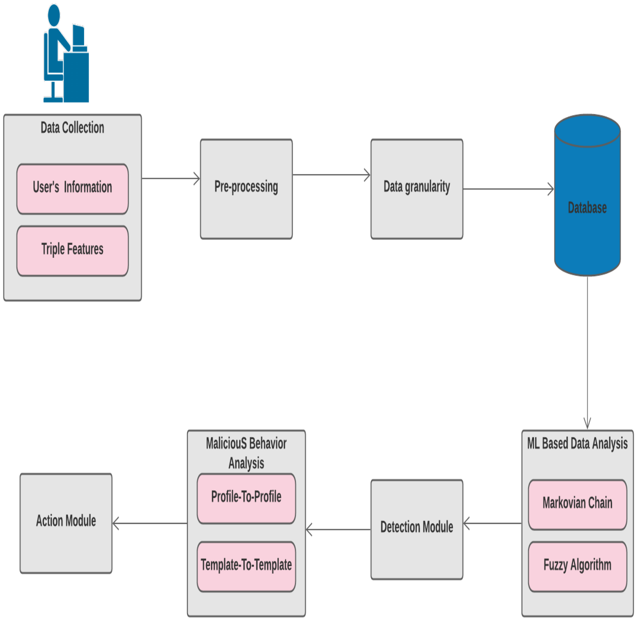


Fig. 1. Architecture Of Insider Detection Based on Two Stage Confirmation

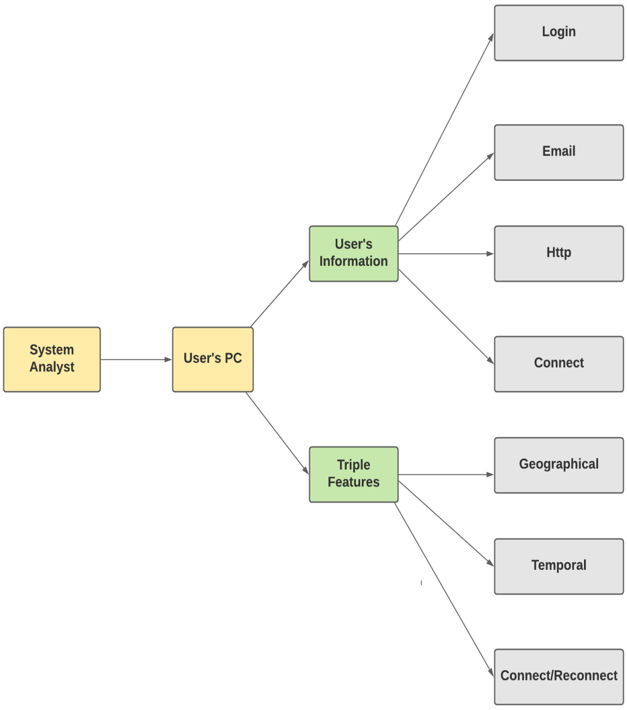


Fig. 2. Source Of Data Collection

detect insider. But, due to lack of proper arrangement or proper capturing of data, this technique remains ineffective or the performance is not up to the mark.

Feature based decision modelling is required for identifying more attack. So, a novel insider threat detection method using two tier, fuzzy logic and markov chain mechanism by collecting temporal feature, geographical feature and connection or re-connection feature is proposed.

The proposed system for malicious behavior and insider or internal cyber attack detection is shown in Fig 1. It has the following stages:

1) Data Collection: Data gathered from different sources are gathered and stored in a specified formats. The two main categories are

- User's Information.
- Triple features.

2) Pre-processing: Identification of features and filtering of best features from the aggregated data occurs.

3) Data granularity: Identification of collection of data segments is called granules.

4) ML engine based Data analysis: Two tier processing of data based on two important machine learning algorithm.

- Fuzzy logic (FL) - Fuzzy Logic (FL) uses the method of human reasoning to derive a solution.
- Hidden Midden Model (HMM) - It is a machine learning model in which current state depend on previous state.

5) Detection Module: It is peculiarly for identification of insider from the organization.

6) Malicious Behaviour Analysis or Behavior Analysis: This stage is primarily meant for the finalizing the insider as well as rejection of normal users.

7) Action Module: The insider who behaive as a normal user will face the consequences.

A. Data Collection

The entire system work based on the supervision of security analyst. A security analyst is a person who make detailed studies to protect the system from unauthorized attack or cyber threat. The process of aggregation of data from different sources and their further processing is done by system analyst. A good observation method in connection with proper collection of data leads to successful application of ML techniques and also assist security analysts in making correct decisions.System analyst mainly concentrate on collecting information related to the user's daily action on work hours and after he working hours on the user's PC, shared PC and Websites. Fig 2. represent the Data Collection process in proposed insider detection system. System analyst collect useful information for detection of insider from user's PC. They mainly concentrate on collecting two main categories of details. The User's information and Triple features. User's information mainly collected from Login, Http, Email and Connect features. They are Commo Separated file or .csv file. Triple features are mainly collected from geographical, Connect or Re-Connect features and Temporal features. These are three most important feature which is used to detect insider.Hence they are known as triple feature.

- User's Information: User's Information is collected mainly from Login, Email, Http and Connect dataset. These are background data contain idea about user's motive or work with in the organization. It gives a good idea about reality or abnormality of user's behavior. These are often actual data that need to be updated periodically. Since the user's behavior may change at any time. Above mentioned input dataset concentrate on the following contents:
  - Http: It contain ID, date, action, PC and Url information.
    Here ID means MAC-ID is generally machine access identification. It is not similar to any machine. So, MAC-ID IS A unique name for identification of user's PC. Different PC has different MAC-ID. Date is actually the system date in which data transfer takes place. PC denote the number of PC which perform the operation. Action denote the specified action user perform. Url information stands for Uniform Resource Locator. It include domain name, with other detailed information to direct the browser to certain webpage
  - Email: ID, date, pc, from, attachment, size and content, bcc and cc email address.
    ID means MAC-ID, Date is system date, PC denote the number of PC which perform the operation, From denote the from address, Attachment denote the count of details attached, Size denote the size of the file, Content indicate the details transferred, bcc indicate blind carbon copy allows the center of email to conceal the user's entered from bcc field from other recipients. CC means the actual carbon copy, that is recipient can see to whom all this message has been send.
  - Login: ID, date, pc and activity.
    ID means MAC-ID, date is the same system date, PC is the PC number, activity indicate the login and log off phenomenon.
  - Connect: ID, date, user, pc, activity. ID the MAC-ID, date is the same system date, user indicate the user name, pc indicate the pc number and activity indicate how many time the user connect or disconnect.
- Triple Features: Triple features means the three main features which contribute for insider detection and provide and extra miliage for detection. These are moral real time features. By adopting these features, attackers can be analyze from depth.
  - Geographical: It indicates the features of location, area or region. Here, longitude and latitude are considered. Black list area normally where the entries are blocked and not considered. It contain elements that are not automatically possible to access a certain area.
  - Temporal: Temporal feature helps to know the particular time in which attack has occurred. Time specification helps to know, which attacker logged in during the particular time. Since, it is an insider attack and it is performed by current working or pre-working employee of an organization or internal user, time specification helps to identify the internal attacker easily. It is based on time bound. Mainly to find time zone as well as time region.
  - Connection or Dis-Connection States: Connection and re-connection phase count helps to know the arrival of attacker, When insider or internal user misbehave, dis-connection occur, which helps to know the presence of abnormality. This will also contribute to the model building of threat profiles. It shows the indication of insider at particular moment. The effect of disconnection and reconnection states that to be logged in feature extraction module.

B. *Pre-Processing*

This stage actually delete non-continuous or records with no data. It identify all the features properly and filter or select best feature based on relevant values. It actually enhances the "garbage in, garbage out" process of the system. Analysing data carefully help to remove misleading results. It helps to improve the quality of data before running any analysis. DataSet with missing value lead to wrong results which can be removed by applying to pre-processing. If there are irrelevant, redundant, noisy and unreliable data, then knowledge discovery during the phase of training is more difficult. It increases the amount of processing time for preparation and filtering steps. Data preprocessing mainly includes cleaning, Instance selection, feature extraction and selection. The output of data preprocessing is the final training set.

C. *Data granularity*

Identifiable collection Of data segments is called granules. In a DataSet, certain field is combine to predict particular behavior. Such data is called granuled data.Data granularity is spliting or fragmenting data in to multiple pieces or granules.report.The greater the granularity, the deeper the level of detail. Increased granularity can help you drill down on the details of each organization and assess its efficacy, efficiency. Different datasets contain login, http, email, content and triple features are combine to generate the granule data. Here granule data is the training data. User-centric insider threat detection based on data granularity provide an additional advantage to the proposed approach. It actually considering microscopic feature to break down data. Generally, Multiple Granularity means hierarchically breaking up the database into blocks which can be locked and can be track what need to lock and in what fashion. Such a hierarchy can be represented graphically as a tree.

Hierarchical representation of data granularity is shown in Fig 3. Actually it's a tree, which is made of four levels of nodes. The highest level represents the entire data Set.

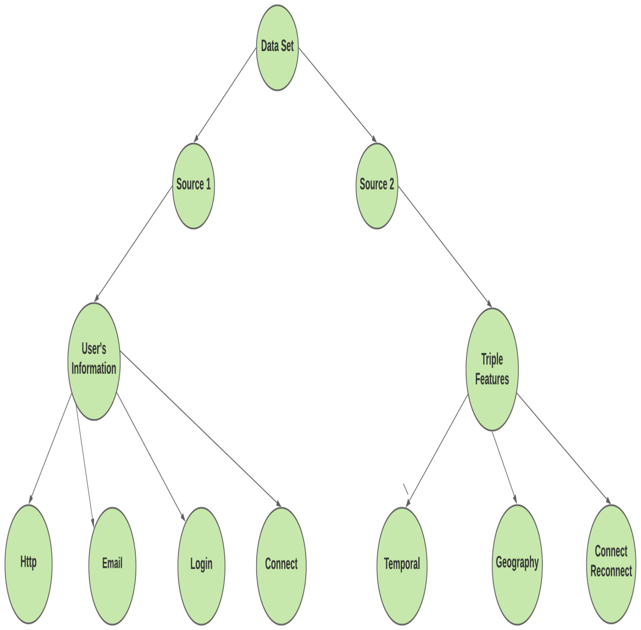


Fig. 3. Hierarchical representation of data granularity

Below it are nodes of type source, which denote the source of information. The dataset consists of exactly these source of information. Source 1 has child node which are called User's information. Source 2 has child node which is known as triple features. Finally, User's information has child nodes http, email, login and connect. Triple features has child nodes geographical, Connect or Reconnect, Temporal features. These are comma separated file and no file can be present in more than one Source of data. Hence, the levels starting from the top level are:

- DataSet.
- Source of Information namely source 1 and source 2.
- User's Information and Triple feature.
- Comma Separated files.

Example User-Week, User-Day, User-Session are granule data of user's login information.

D. Machine learning based Data Analysis

This stage uses machine learning based for the processing of data and detection of insider. Machine learning is from the knowledge that systems can grasp from data, understand patterns and make conclusion with reduced human intervention. Two stage filtering or two stage pruning is added advantage of this approach. Two important machine learning algorithm is used for this purpose. Hidden Markov Model (HMM) and Fuzzy logic (FL). Microscopic level of detection take place in two phase detection, where two prominent algorithm of machine learning helps in accurately classify the data has attackers and normal user.

Fuzzy logic is used for handling combination of attribute. It is used for feature aggregation and reduction of feature. So, efficiency and speed of insider detection increases. fuzzy logic is an important machine learning algorithm in which the real value of variables may be a real number which lies in between 0 and 1. It is working to use the partial truth concept, where value of truth varies between completely true and completely false. Fuzzy logic consider all possibilities and human way of decision making. If membership value of particular group is above a threshold then it is consider as important features for detecting insider. Attribute based comparison helps to know to insider at microscopic level. It helps to identify malicious user as well as malicious behavior. Fuzzy logic provide attention to Small false positive rate.

Hidden Markov Model (HMM), is assumed to be a markov process. It move through different state from the start state to end state. An important fact of Hidden markov model is that current state depends on the previous state. The markov process that is happening behind and hidden from rest of the world is actually Hidden markov process. Here, based on this fact a person is considered insider based on the previous suspecting action. The action such as attaching multiple mails per second is a malicious or doubtful action. This hint is considered in next step for detecting insider.

Markov chain is used in first phase. Remaining condition which occur is verified using fuzzy logic. This two-phase comparison helps to improves the accuracy of detection.

Fig 4. illustrate the process in developing the proposed architecture. Initially the dataset of http, login, connect , email and triple features will be extracted from .csv file format as excel file by the data collection module. After pre-processing and filtering the best feature it is converted in to granule data. The granule data will be split as training and testing data. Two stage detection model use fuzzy and markov is used to train the model with the training data. Once the model has been trained, the input data selected from the testing dataset will be given to the model. The model predict the MAC-ID of the insider as output. After generated MAC-ID, a second stage confirmation is done through Profile-to-Profile comparison or template-to-template comparison. Only after two stage confirmation, the final arrival in to the insider occurs. Based on that Alert or warning generated by the system analyst based on the decision of organization.

E. Detection Module

The MAC-ID generated by the fuzzy and markov is passed to the detection. In detection module, the system actually recognize the insider from the organization. MAC-ID is unique ID. Each electronic device has their own MAC-ID. It is a unique identification code.

F. Malicious Behavior Analysis

This module actually enhances the efficiency of decision marking process. An added advantage of Profile-to-Profile or template-to-template comparison occurs. Here, a two stage confirmation occurs. That is, it strength the decision which is made. Second level of comparison occur in malicious behavior analysis.

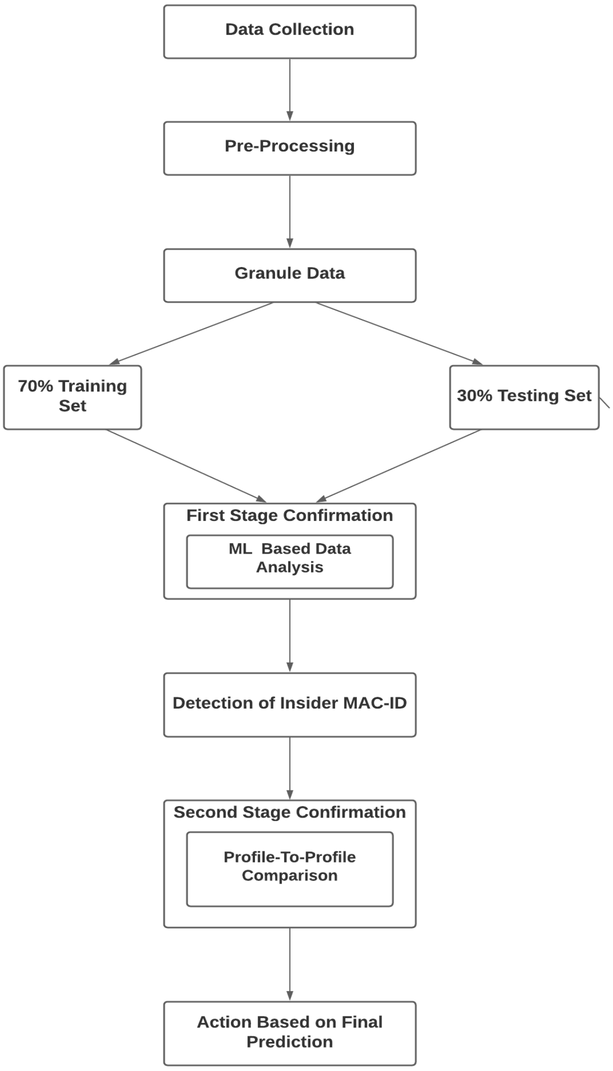


Fig. 4. Process of Insider Detection Based on Two Stage Confirmations

Profile-to-Profile or Template-to-Template comparison, an automatic profile creation of attackers occurs. In Profile-to-Profile Comparison an automatic profile of employees is created in the database based on the day to day activities. It is a real time feature, that get updated periodically. In template-to-template comparison, a template of particular individual is already created based on some expectation that particular individual will behaive in particular way. Actually it is already created expectation about an employee. It help to identify insider easily. Here, a concept of misuse detection and anomaly detection is used. Misuse detection is actually signature based which can only detect known insiders by matching the features of incoming insiders with the historical knowledge and predefined rules. In case of anomaly detection automatically constructs a normal behavior of the insiders and detects incoming insiders by computing deviations. It can detect new insider which is not detected by two stage of pruning of fuzzy and markov process.

Sudden Change in user behaviour can be identify using profile-to-profile or template-to-template comparison. Profile comparison help to identify attacker fastly and accurately. Using these feature an automatic profile creating of attackers will help to identify them very easily.

After two stage confirmation by machine learning algorithm and profile-to-profile comparison the chance of false rate will be reduced tremendously.

G. Action Module

In action module system analyst analysis the prediction by machine learning algorithm and their performance measure. After two stage confirmation, final decision of insider occur. System Analyst compare the predicted MAC-ID with the orginal report and identify the employee who behaive as an insider. They will forward the information with the organization. Based on the order from the organization system analyst generate alert, produce warning or blocking of certain url occur. For severe case, insider who behaive as a legitimate user need to face suspension. For, big lose, the insider will be send to prison and entire gang of insider will be find out and protect the reputation and secret files of organization. Mean while, increase the trust of users.

VI. Theoretical Analysis on Insider Detection

A theoretical analysis on the existing and the proposed systems is performed. The existing mechanism implements only the psychometric and behavioral features and certain machine learning algorithm with proper collection of features to predict insiders, which leads to decrease in performance measures. But the proposed method implements two stage confirmation method.The first stage uses novel method of detection using fuzzy logic and markov features. It is a two stage filtering or pruning methods. Machine learning is an advanced and efficient technique than the existing ones. It builds an effective and highly accurate model than the existing behavioral based ones. The second stage of confirmation using profile-to-profile comparison helps to reduce false positive rate.The proposed model also uses user-centric insider threat detection using data granularity, which is efficient to develop accurate models than the existing ones. Data granularity is used for microscopic level of detection. Each small feature for detection of insider is considered with high importance. Since accuracy level is comparatively higher for the proposed system, efficiency will also be higher for the machine learning based insider detection models using two stage confirmation, when compared with the existing insider detection models. Selection of real time features such as temporal features , geographical and connection or re-connection features which is the triple features help to isolate the attack model. These type of genuine filtering method is absent in existing system which leads to increase the miliage of proposed system.

VII. CONCLUSION AND FUTURE WORK

A insider detection model has been developed using novel approach of Fuzzy and Hidden markov model (HMM) for predicting the MAC-ID of insider in the organization. User-centric insider threat detection based on data granularity is important path for the detection of insider. Identical collection of data segments is called granules. It helps to drill down microscopic level of features for the detection of insiders. Two stage confirmation technique is used. In the first confirmation stage, a two stage detection techniques using two important machine learning fuzzy and markov improves the effectiveness of detection. Hidden Markov Model is used in the first stage and fuzzy is used in second stage. In the second stage of confirmation, profile -to-profile or template-to-template comparison. Two stage confirmation reduces false positive rate. and based on the identification of insider, change in internal policy occur.

Future scope of this work is that the markov model cannot be true in estimating conditional probability between two states. The current work can be enhanced in the direction, so that the limitation of markov analysis can be over-ridden. Modifying the existing markov model with a fuzzy relation of attributes to a novel system that can predict the risk full outcomes from existing attribute is a new direction for the research.

VIII. ACKNOWLEDGEMENT

This research was supported by Dr. K Krishnakumar, the head of the institution. We would also like to show gratitude to the head of our institution, Dr. S.V. Annlin Jeba for sharing her pearls of wisdom with us during the course of research. We thank our colleagues from Sree Buddha College Of Engineering who provided insight and expertise that greatly assisted us although they may not agree with all of the interpretations and conclusion of the paper.

REFERENCES

[1] Fang-Yie Leu, Kun-Lin Tsai, Member, IEEE, Yi-Ting Hsiao, and Chao-Tung Yang , “An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques,”IEEE SYSTEMS JOURNAL, 2015.

[2] Santosh Aditham and Nagarajan Ranganathan, “A System Architecture for the Detection of Insider Attacks in Big Data Systems ,” IEEE Transactions on Dependable and Secure Computing, 2017.

[3] Loukas Lazos and Marwan Krunz, ” Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks,”Scopus Indexed Journal,2011.

[4] Nathalie Baracaldo, Balaji Palanisamy, and James Joshi, “G-SIR: An Insider Attack Resilient Geo-Social Access Control Framework ,”IEEE Transactions on Dependable and Secure Computing, 2017.

[5] Baraq Ghaleb, Ahmed Al-Dubai, IEEE, Elias Ekonomou , Mamoun Qasem, Imed Romdhani , and Lewis Mackenzie, “Addressing the DAO Insider Attack in RPL’s Internet of Thing,” IEEE Communications Letters, Vol. 23, NO. 1, January 2019.

[6] Sang-Yoon Chang, Member, IEEE, and Yih-Chun Hu, Member, IEEE, “SecureMAC: Securing Wireless Medium Access Control Against Insider Denial-of-Service Attacks,” IEEE Transactions on Mobile Computing ,2016.

[7] Saraswathi Shunmuganathan a,* , Renuka Devi Saravanan b , Yogesh Palanichamy c , “Securing VPN from insider and outsider bandwidth flooding attack ,” Elsevier journal , 2020.

[8] Nebrase Elmrabit a, , Shuang-Hua Yang b , Lili Yangc , Huiyu Zhou, “ Insider Threat Risk Prediction based on Bayesian Network,” Elsevier Journal on Computers and Security, 2020.

[9] Nader Sohrabi Safaa,b, , Carsten Maplea , Tim Watsona , Rossouw Von Solms, “ Motivation and opportunity based model to reduce information security insider threats in organisations,” Journal of Information Security and Applications , 2017.

[10] Junhong Kim, Minsik Park, Haedong Kim, Suhyoun Cho and Pilsung Kang , “ Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms ,” Appl. Sci., 2019.

[11] Guang Yang , Lijun Cai , Aimin Yu and Dan Mengand , “A General and Expandable Insider Threat Detection System Using Baseline Anomaly Detection and Scenario-driven Alarm Filters,” IEEE International Conference On Trust, Security And Privacy In Computing And Communications, 2018.

[12] Guang Yang , Lijun Cai , yuaimi ,h JianGang ,h Dan Me and YuWu, ” Potential Malicious Insiders Detection Based on a Comprehensive Security Psychological Model,” IEEE Fourth International Conference on Big Data Computing Service and Application ,2018.

Ms. P. Varsha Suresh has completed B.Tech (CSE) from Sree Buddha College Of Engineering, Elavumthitta in 2018 and is currently pursuing M.Tech (CSE) from Sree Buddha College of Engineering, Pattoor.

Mrs. Minu Lalitha Madhavu pursued Bachelor of Technology from Rajiv Gandhi Institute of Technology (RIT). She received her M.Tech degree in Technology Management from Kerala University and undergoing PhD at University of kerala. She is currently working as an Assistant Professor in Computer Science and Engineering in Sree Buddha College of Engineering. She has published around 25 research papers in reputed international journals. Her main areas of research focus on Network and Security. She has more than 14 years of experience as Assistant Professor in Computer Science at Sree Buddha College Of Engineering.

MINDPAD: EEG BASED HUMAN-COMPUTER INTERFACE

1st Ruksana Jalaludeen
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

2nd Moses Jiji George
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

3rd Jestin George Varghese
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

4th Najma Abdul Sathar
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

5th Gopu Darsan
Assistant professor
Dept. of CSE
Sree Buddha College of Engineering
Alappuzha, India

***Abstract*—Brain Computer Interface (BCI) technology is a tremendously growing research area having various applications. Its involvement in the medical field lies with prevention and neuronal rehabilitation for severe injuries. BCI systems builds a pathway between human brain and external devices, providing the patients a media for communication with the world which eliminates the scope of depending on others to a less degree. To develop an integrated hybrid BCI system, a mouse control method by combining EEG signal and eye blink, in which the left/right-hand motor imagery (MI)-related EEG control the vertical movement of the mouse and the eye blinks control the mouse to select/reject a target.The horizontal movement of the mouse is controlled by head movement. With the hybrid BCI, users can input text, access the internet, communicate with others via email, and manage files in their computer using only EEG and eye blink without any body movements. Also provides a voice recognition-based system to enable easy interaction with the computer.**

***Index Terms*—Brain Computer Interface, Electroencephalography, Common spatial pattern, Support vector machine**

I. Introduction

The idea of interfacing brains with machines/robots has long captured the human imagination. Brain-computer interface (BCI) technology intend to build an interface between the brain and any electrical/electronic device (e.g., a wheelchair, smart home appliances, and robotic devices) using electroencephalogram (EEG) which is a non-invasive technique for measuring electrical potentials from electrodes placed on the scalp produced by brain activity. Nowadays, the EEG technique has been used to establish portable synchronous and asynchronous controls for BCI applications. Noninvasive EEG-based BCIs are the most promising interface for space of applications for people with severe motor disabilities because of their non-invasiveness, low cost, practicality, portability, and being easy to use. For some disabled patients with physical disability or paralysis while the brain function is still normal, although they have a normal large brain consciousness and thought, they cannot communicate with the external environment through the severely damaged muscle and nervous system and complete the daily work independently.

Brain Computer Interface (BCI) technology is a tremendously growing research area having various application. Its involvement in medical field lies with prevention and neuronal rehabilitation for severe injuries. BCI systems try to build a pathway between the human brain and external devices, providing the patients for communication with the world eliminating the scope of depending on others to a less degree. BCIs are often oriented at research, mapping, assisting, augmenting of human cognitive or sensory-motor functions. The growth of BCIs has increased in the recent years, paving way for research and aiming to be more accessible for the people [1].

The BCI technology is classified into two types based on the placement of electrodes- invasive and non-invasive systems. In invasive BCI systems the electrodes are implanted in the brain tissue. Thus, the patient's brain gradually adapts its signals to be sent through the electrodes. The non-invasive systems involves placing the electrodes on the scalp of the patient and taking readings. The non-invasive methods take Electroencephalogram (EEG) readings of the brain. An electroencephalogram is a measure of the brain's voltage fluctuations as detected from scalp electrodes. It is an approximation of the cumulative electrical activity of neurons [2].

A human-machine interface (HMI) system is a communication system that allows users to interact with external devices. In recent years, biological signals, such as electroencephalography (EEG) and electrooculography (EOG), have been widely used to augment or as alternatives to traditional HMIs (such as keyboards and mice) to help people with neuromuscular impairments (such as patients with disturbance of consciousness, amyotrophic lateral sclerosis, and stroke) to better interact with their environment. EEG-based BCIs, are usually developed based on event-related potentials (ERPs), including slow cortical potentials (SCPs), steady-state visually evoked potentials (SSVEPs), P300 potentials, and sensorimotor rhythms (mu and beta rhythms). In recent years, contemporary researchers have developed various types of asynchronous BCI spellers or BCI browser based on P300 potentials. Some researchers have also developed asynchronous HMI systems based on EOG.

II. Related Work

A noninvasive BCI using scalp-recorded electroencephalographic (EEG) activity and an adaptive algorithm , which can provide people, including people with spinal cord injuries, with two-dimensional cursor movement and target selection is proposed in [3]. Multiple targets were presented around the periphery of a computer screen, with one designated as the correct target. The user's task was to use EEG to move a cursor from the center of the screen to the correct target and then to use an additional EEG feature to select the target. If the cursor reached an incorrect target, the user was instructed not to select it. Thus, this task emulated the key features of mouse operation. The results indicate that people with severe motor disabilities could use brain signals for sequential multidimensional movement and selection.

Vasavi, K. et al.[4] focuses on movements of the mouse cursor controlled by a person with multiple disabilities. The mouse cursor movement would further be used by the disabled person to have a communication with his caretaker by means of the software developed by us. The proposed system uses discrete wavelet transforms for de-noising the muscular and cardiac signals. An independent component analysis is performed in order to extract the beta rhythms from the EEG signal. The mouse control is achieved by interfacing the mouse with a microcontroller which receives the operating voltages from the Data Acquisition System (DAS) which acquires and conditions the EEG signals coming from the user brain. The proposed system is tested on several young and elderly persons and is found to be working with more than 95% accuracy.

A new EEG-based intelligent teleoperation system was designed for a mobile wall-crawling cleaning robot. This robot uses crawler type instead of the traditional wheel type to be used for window or floor cleaning. For EEG-based system controlling the robot position to climb the wall and complete the tasks of cleaning, Lio et.al [5] extracted steady state visually evoked potential (SSVEP) from the collected electroencephalography (EEG) signal. The visual stimulation interface in the proposed SSVEP-based BCI was composed of four flicker pieces with different frequencies . To solve the multiclass problem, thereby achieving the purpose of cleaning the wall within a short period, the canonical correlation analysis (CCA) classification algorithm had been used. The proposed system was efficient in the classification and control phases with an obtained accuracy of 89.92% and had an efficient response speed and timing with a bit rate of 22.23 bits/min.

The paper [6] presents a new asynchronous hybrid brain-computer interface (BCI) system that integrates a speller, a web browser, an e-mail client, and a file explorer using electroencephalographic (EEG) and electrooculography (EOG) signals. More specifically, an EOG-based button selection method, which requires the user to blink his/her eyes synchronously with the target button's flashes during button selection. A mouse control method by combining EEG and EOG signals, in which the left-/right-hand motor imagery (MI)- related EEG is used to control the horizontal movement of the mouse and the blink-related EOG is used to control the vertical movement of the mouse and to select/reject a target. These two methods are further combined to develop the integrated hybrid BCI system. With the hybrid BCI, users can input text, access the internet, communicate with others via e-mail, and manage files in their computer using only EEG and EOG without any body movements.

III. Methodology

The most fundamental idea of BCI is to convert the brain patterns or the cerebral activity into respective scenarios which can be used for various control applications. In this project, we are using a non-invasive environment to develop a Brainwave Controlled Prosthesis gripper. Neurosky Mindwave Mobile headset is used to detect the brain waves in real time.

A. *Neurosky Mindwave mobile Headset*

The Neurosky Mindwave mobile 2 [8]headset, as shown in Fig. 1, is powered by AAA battery and communicates via Bluetooth. It has a Think Gear chip inside and uses a TGAM module (Think Gear Application specific IC). It detects raw brainwaves and outputs processed EEG signals consisting of Alpha, Beta, Delta, Theta and eSense parameters like Attention, Meditation, Blink strength shown in Fig.2. The blink values range from 0-255 and attention values ranges from 0-100. The frequency range of the headset is typically between frequency 2.42 – 2.472 GHz. Sampling rate of EEG signal is done at 512Hz and its maximum power is found to be 50mw.

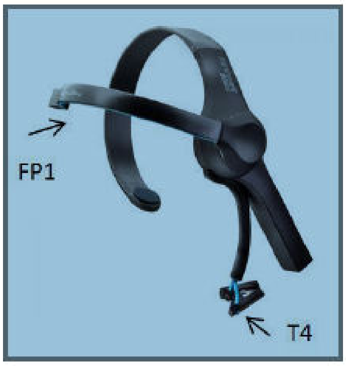


Fig 1. Neurosky Mindwave Mobile 2

B. *Signal Detection*

The different states of the brain corresponds to different patterns of the cerebral activity. These patterns give rise to waves which are distinguished with the help of amplitudes and frequency pattern generated. The interaction occurring between the neurons produce a microscopic electrical discharge. These patterns lead to waves characterized by different amplitudes and frequencies. These processed signals are then transmitted via Bluetooth communication to various applications.

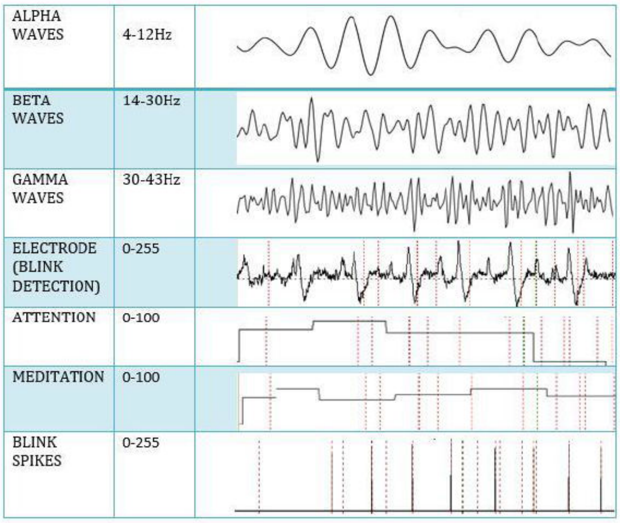


Fig 2. Plot of real time brain waves

C. Python interface- MQTT communication

A python module establishes connection between NeuroSky headset and Laptop using MQTT protocol with a NodeMCU interfacing between them. MQTT is an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth.

D. Signal Acquisition

The headset captured the EEG signals and are transmitted to the Laptop with the help of Bluetooth communication. The headset performs detection, analysis and processing of the signal and transmits the processed data to laptop.

E. Detection of eye blink signal

Eye blink play a critical role to people suffering from motor neuron diseases [9]. It helps to control many applications. Devices have been designed to understand the blinks and help people interact with the external world more effectively. Every eye blink has certain distinct feature such as frequency of operation, amplitude and time elapsed between closing and opening of the eyes. Attention values correspond to increased concentration levels. We are using the blink strength and attention values gathered from the processed signal from the NeuroSky Mindset headset.

The most common and widely used system is one consisting of multiple channels, which are located on the corresponding regions of the brain. these electrodes. In this system we are adopting a single electrode to measure the EEG signals. The channel A1 is related with sensor ear clip, FP1 relates to the sensor placed on the forehead which taps the brain waves and T4 is where the reference point of the headset is located. This is shown in Fig. 1.

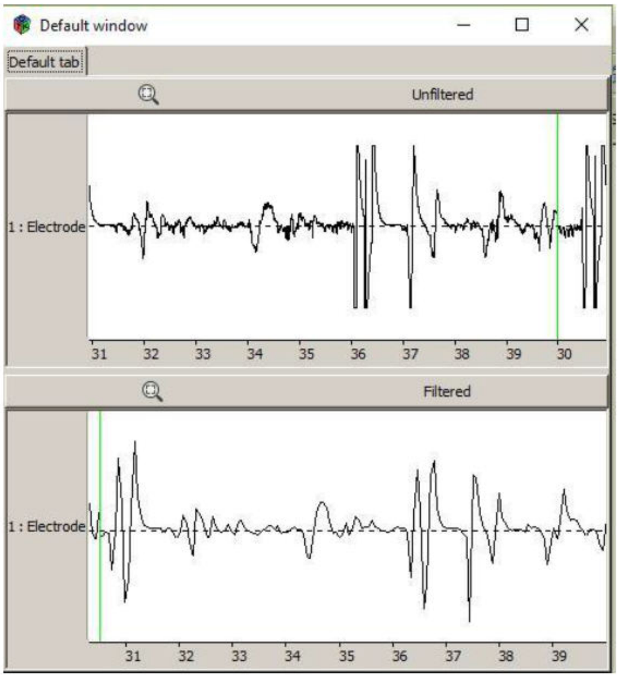
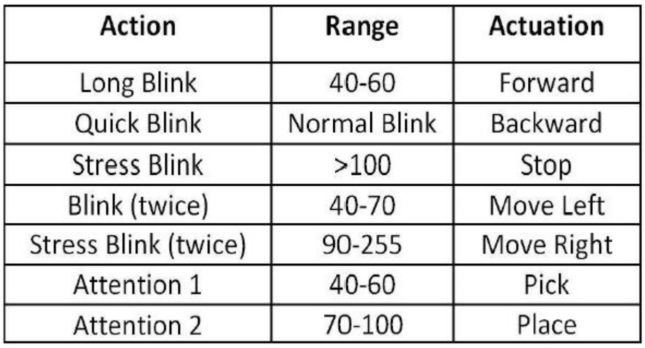


Fig 3. Signal Display

The brain signals detected from the headset is as shown in Fig.3. The signals measured from the sensor are decomposed and recorded. The blink spikes, shown in Fig 3, was plotted to filter the noise in the blink signal using OpenVibe Platform. The EEG signal was acquired in real time using an acquisition server which connects with the Neurosky headset by enabling the local host address. An OpenVibe design scenario was created using a simple temporal filter of an order N. Thus, distinct blink signals were captured and classified.

The blink strength values range from 0-255. A higher number indicates a strong blink while a smaller number indicates regular/lighter blink. The frequency of blinking is often correlated with nervousness. Based on these values, it is coded to perform the control applications as shown in Fig 4.[7].



Action	Range	Actuation
Long Blink	40-60	Forward
Quick Blink	Normal Blink	Backward
Stress Blink	>100	Stop
Blink (twice)	40-70	Move Left
Stress Blink (twice)	90-255	Move Right
Attention 1	40-60	Pick
Attention 2	70-100	Place

Fig 4. Blink and Attention status to perform control application

F. Common spatial pattern for feature extraction

Feature extraction is the signal processing step in which discriminative and non-redundant information is extracted from the EEG data to form a set of features on which classification can be carried out. The most basic feature extraction techniques use time-domain or frequency-domain analysis in order to extract features. Time-frequency analysis is a more advanced and sophisticated feature extraction technique which enables spectral information to be related to the time domain. Finally, analysis in the spatial domain using common spectral patterns is also a prevalent method for feature extraction.

Common spatial pattern (CSP) is one of the most common feature extraction methods used in MI EEG classification . CSP is a spatial filtering method used to transform EEG data into a new space where the variance of one of the classes is maximized while the variance of the other class is minimized. It is a strong technique for MI EEG processing since different frequency bands of the signal contain different information, and CSP enables the extraction of this information from particular frequency bands. However, pure CSP analysis is not adequate for high-performance MI classification because different subjects exhibit activity in different frequency bands and the optimal frequency band is subject-specific.

We are using the blink strength and attention values gathered from the processed EEG signal. The blink strength values range from 0-255. A higher number indicates a strong blink while a smaller number indicates regular/lighter blink. The frequency of blinking is often correlated with nervousness. Based on these values, it is coded to perform the control applications.

G. Support vector machine for classification

SVM is one of the most popular supervised learning algorithms for solving classification problems. It involves the adoption of a nonlinear kernel function to transform input data into a high dimensional feature space, which is more easier to separate data rather than at the original input space. Thus, depending on input data, the iterative learning process of SVM will finally devise an optimal hyperplanes with the maximal margin between each class in a high dimensional feature space. Here the attention level is considered for the vertical mouse movement, thus a greater attention concentration leads to upward movement and lower concentration level leads to a downward movement of the mouse pointer. Fig 5. summarizes the flow of feature extraction and feature selection process.

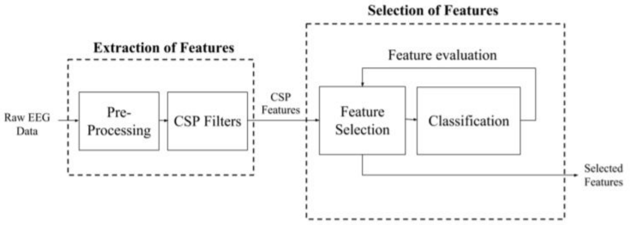


Fig 5. A diagram of the feature extraction and feature selection process

IV. DESIGN

The approach has two methods, image processing and EEG signal processing. In image processing, the facial first features are extracted using dlib library and is processed using OpenCV library. The position of nose (nose point) is at first taken as anchor point. Subsequent movement of nose produces difference between anchor point and nose point. This difference can be calculated in order to find the direction in which the head is moved and pointer movement is done accordingly.

The EEG signals on the other hand is recorded using EEG headset and the signals are transmitted to a computer using MQTT protocol with the help of NodeMCU. The EEG signal undergoes feature extraction using Common Spatial Pattern (CSP) algorithm. This again undergoes classification by using Support Vector Machine (SVM) classifier. This classified signal is then used to identify direction in which mouse pointer must be moved and to select a target.

Algorithm

step 1: Establish serial communication between the laptop and microcontroller.

Step 2: Establish MQTT communication to Neurosky headset and enable NodeMCU.

Step 3: Read and parse relevant eSense parameters like attention and blink strength values.

Step 4: Feature extraction is done using CSP algorithm and the signals are classified using SVM classifier.

Step 5: Direction parameters are extracted from the classified result

Step 6: Using the direction parameters, corresponding mouse movement is achieved.

CONCLUSION

The paper describes an asynchronous hybrid BCI system using MI-related EEG and blink-related signal. The proposed system consists of a web browser, speller, file explorer, and e-mail client, and all of these subsystems can work in asynchronous mode. While using the system, the user can control the mouse horizontal movement using face movement and EEG can control the mouse vertical movement, select targets using blink signal. Further more, a voice commanding system is implemented so that it becomes easier to access into folders and subfolders.

Further scope of improvement of this work involves increasing the accuracy of data acquisition by using multiple channel sensors, as accuracy plays a very important role in controlling real-time applications.

REFERENCES

[1] R. Prathibha, L. Swetha and K. R. Shobha, ”Brain computer interface: Design and development of a smart robotic gripper for a prosthesis environment,” 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), Thiruvananthapuram, India, 2017, pp. 278-283, doi: 10.1109/NETACT.2017.8076780.

[2] Nadakuduru, Padma Vasavi & Raju, Prssvraju & Radhika, S. & Prasad, G.D.K.. (2016), ”A Mind Operated Computer Mouse Using Discrete Wavelet Transforms for Elderly People with Multiple Disabilities”, Procedia Computer Science, 85. 166-175. 10.1016/j.procs.2016.05.205.

[3] McFarland DJ, Krusienski DJ, Sarnacki WA, Wolpaw JR. ”Emulation of computer mouse control with a noninvasive brain-computer interface”. J Neural Eng. 2008 Jun;5(2):101-10. doi: 10.1088/1741-2560/5/2/001. Epub 2008 Mar 5. PMID: 18367779; PMCID: PMC2757111.

[4] Vasavi, K., Raju, P., Radhika, S., & Prasad, G. (2016). ”A Mind Operated Computer Mouse Using Discrete Wavelet Transforms for Elderly People with Multiple Disabilities”. Procedia Computer Science, 85, 166-175.

[5] Lei Shao, Longyu Zhang, Abdelkader Nasreddine Belkacem, Yiming Zhang, Xiaoqi Chen, Ji Li, Hongli Liu, ”EEG-Controlled Wall-Crawling Cleaning Robot Using SSVEP-Based Brain-Computer Interface”, Journal of Healthcare Engineering, vol. 2020, Article ID 6968713, 11 pages, 2020. https://doi.org/10.1155/2020/6968713.

[6] S. He et al., ”EEG- and EOG-Based Asynchronous Hybrid BCI: A System Integrating a Speller, a Web Browser, an E-Mail Client, and a File Explorer,” in IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 28, no. 2, pp. 519-530, Feb. 2020, doi: 10.1109/TNSRE.2019.2961309.

[7] R. Prathibha, L. Swetha and K. R. Shobha, ”Brain computer interface: Design and development of a smart robotic gripper for a prosthesis environment,” 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), 2017, pp. 278-283, doi: 10.1109/NETACT.2017.8076780.

[8] Jozsef Katona, Tibor Ujbanyi, Gergely Sziladi,” Speed control of Festo Robotino mobile robot using NeuroSky MindWave EEG headset based Brain-Computer Interface “7th IEEE International Conference on Cognitive Info-communications (CogInfoCom 2016) Wrocław, Poland

[9] Wojciech SAŁABUN,West Pomeranian University of Technology, Szczecin, “Processing and spectral analysis of the raw EEG signal from the MindWave”

Detecting time synchronization error using machine learning

S Prasanthi
Computer Science and Engineering
Sree Buddha College of Engineering
Pattoor, India
prasanthis2014@gmail.com

Lakshmi S
Computer Science and Engineering
Sree Buddha College of Engineering
Pattoor, India
lakshmi.rnath@gmail.com

***Abstract*—Smart Grids are integrated systems that have connected entities having their own architecture. Because of the nature of the grid as distributed, complex, and connected system, it is vulnerable to any kinds of cyberattacks. This nature of the smart grid leads to the need for new solutions in order to monitor and react to the dynamics of the grid in a real-time environment. By using time synchronization, a pulse is introduced into a network, it enables to observe the real-time activity of the network. Time distribution mechanisms such as Precision Time Protocol (PTP) are used and are not designed with strict security and thus grid suffers from several security vulnerabilities. Compared to previous approaches in Precision Time Protocol, an extension of PTP gives the advantage of monitoring the status of time synchronization at end devices as they are more noticeable to attacks. The proposed model is simulated using a PTP server, Transparent clock(TC) and various slave clocks(SC). Also the model uses Machine learning technique GA with RNN for the prediction of sync differences over the clocks.**

***Index Terms*—Precision Time Protocol (PTP), Smart Grid, Transparent clock(TC), Slave Clocks(SC, Time synchronization, Genetic Algorithm (GA), Recurrent Neural Network (RNN)**

I. Introduction

From the year 1979, time synchronization protocols were in use. The first NTP was used in network time synchronization technology [10] and was used within the transatlantic satellite network. NTP uses a hierarchical, semi-layered system of time sources in which each level is called a stratum. NTP discovered many security issues. And therefore the protocol has been undergone revision and review. Stack Buffer Overflow, missing a return statement were basic errors in NTP which caused minimum access of the systems that run on different versions of NTP. A security audit in 2017 stated that NTP and NTPsec are more in danger of security issues.

To secure the time synchronization protocol which wasn't well served by NTP, Precision Time Protocol was introduced (PTP). PTP was defined within the IEEE 1588-2002 standard [10], and entitled as ”Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems”. The revised standard of IEEE 1588-2008 was released in 2008. It is also called PTP version 2 (PTPv2). It improves accuracy, precision, and robustness. PTPv2.1 was published in November 2019 and includes backward-compatible improvements.PTP was vulnerable to any kind of threats such as Denial of service, byzantine master, packet drop, manipulation, and insertion, and selective packet delay. Even having protection extensions such as Annex-K, PTP continues to be vulnerable to several attacks. In this paper, various attacks that affect the functionalities of PTP are addressed along with the proposed system to detect synch error in the system.

II. Attack Classification on IEEE 1588

A. Direct Attack on Nodes

It includes directly changing the data or the software which leads to the degradation of system performance. These are referred to as pitfalls which is an unsuspected danger. These attacks also occur when the resources are underrated. And being attacked by using a maliciously configured node that is connected to the network. These attacks are again classified as external attacks such as Denial of Service (DoS) attacks which occur from the network and blocks the capability to send and receive clock synchronization messages and internal sources such as concurrent protocol stacks or software competing for resources.

B. Byzantine Masters

Master selection algorithms are used in IEEE 1588. The algorithm is selected based on the mutual trust inhibited by the nodes. This trust is misused and unprotected in versions 1 and 2 of PTP. Every node announces its accuracy at the initial state but is not verified. The masters with the same class or stratum, the MAC address determines the selection of the master. A byzantine master gains control by inserting additional packets with high values in the sequence number field and therefore causes the packets of the legitimate master to be discarded [8].

C. Message manipulation

In this, the attacks on the messages transmitted over the network can be performed at multiple positions Physical interruption of the network, Removing of packets within switches, routers or gateways, Blocking of transmission by DoS attacks and Man-in-the-Middle attack on messages [8].

D. Message Delay and Insertion

As the individual packets can be deleted, likewise additional packets can be created and inserted in the control loop. Finally, malicious delays within the boundaries of the protocol cause clocks to be misaligned up to the cycle of sync messages. In this way differences in the range of seconds can be achieved [8].

III. MAJOR ATTACKS ON IEEE 1588

A. Denial of Service (DoS)

A small amount of DoS attack causes less accuracy in time synchronization [5]. DoS attacks cause flooding in traffic or sending data that causes a crash. In this, the attacked slave clock starts rejecting Sync and Follow Up messages. This is done by first spoofing the attacked slave clock with a Sync message which uses the original master clock address. DoS attack occurs [1] when the original master clock sends its next Sync message to the attacked slave clock. And the sync message is rejected by attacked slave clocks due to change in value without knowing the master.

B. Replay

The aim of a replay attack is to either create congestion in the network stacks of the clocks or to desynchronize clocks. The attack is carried out by recording real messages that are transmitted on the communication network and, after some time changing the real messages and then re-injecting the modified messages into the network [1].

C. Delay

The main aim of a delay attack in a PTP network is to delay the message arrives at the receiving nodes, which causes an increase in the values used in the offset and one-way delay calculations [1][4]. The attack can be performed by the usage of either hardware or software to get into the transmission of a message between nodes in a network. After some time re-inject the delayed message into the communication network. By delaying the receiving time of the Sync message by a certain slave clock, the attacker is able to increase the offset of the slave clock with respect to the master clock, which leads to the slave clock off synchronization with respect to the rest of the system [9][6].

D. Masquerading

The main aim of masquerading an attack in a PTP network is to pretend as the master clock and use a wrong identity to inject other attacks [1]. To inject the attack, the attacker first obtains information about the “true” master clock and then intrudes on Sync, Delay Req, and Delay Resp messages. These messages are sent to the slave clocks from the master. When required data are obtained, the attacker starts spoofing Sync, Delay Req, and Delay Resp messages to pretend as a master clock. Pretending as a master clock allows the attacker to transmit false timing and management messages to other slave clocks which in turn causes many other kinds of attacks.

E. Modification

The aim of a modification attack is to (a) cause denial of service, (b) cause slave clocks to incorrectly resynchronize, and (c) alter the hierarchy of the master and slave clocks [1]. The attack is done by changing the content of messages. Also, the modification of the messages sent by a master clock causes a great effect because a master clock can send messages used for both time synchronization and management [10][7].

IV. MEASURES FOR MAJOR ATTACKS

A. Denial of Service Attack (DoS)

DoS attack using sync-message is performed by spoofing the victim slave clock. It is done by having a sync message from the real master clock address, a sequence ID value that is greater than the previous sync message. By the usage of these data, the affected clock makes changes to its current data.

DoS attack is induced when the real master sends the next sync message to the affected slave clock. Parent-last-sync-sequence in the slave clock is updated by spoofed sync message. Thus, sync-message from the real master, the clock has less sequence ID value or greater than parent-last-sync-sequence. The affected slave clock discards this sync message without notified by the master clock. The process of synchronization does not take place until the real master sync message has a greater sequence ID than parent-last-sync-sequence in the slave clock. The affected clock will get out of sync with the master if the dispute sends sync message to increase the affected clocks parent-last-sync-sequence.

To reduce DoS attacks, port-level security can be used which helps to limit the set of authorized devices that are capable of sending synchronization messages [1]. Also, message authenticity and integrity protection can be implemented to reduce DoS attacks.

B. Replay Attack

Slave Clocks records the received time whenever the sync message is replayed to the slave clock. The replayed messages are overwritten if the storage location available is only one. And the records are queued if multiple storages is available.

To avoid message spoofing or message injection into the network, VPN connections can be used which helps in reducing replay attacks. VPN connections are used since they provide integrity protected path for the network [1].

C. Delay Attack

Introducing a backup plan into a PTP network helps in reducing delayed messages in the network. This can be implemented by calculating the averages of the Delay Request and Delay Response messages with a combination of previous values. This effect will reduce the postponed or time-out messages. In this way, delay attacks can be reduced in a communication network [1]. Another approach called game-theoretic analysis is used to detect delay attacks in a network [4].

Protocol Packet Exchange: The protocol messages are exchanged that conveys timestamps. By this method, TSP is executed in the model. The protocol is further proceeded by periodic message handshake. The model defines a single exchange as two protocol messages for analysis.

Players: 2 players participate in this game model referred to as M and B. The player M is located such that it can store and forward the packets after a delay attack. Player B is viewed as a security process which helps in detecting delay attack [4].

Defining Game: It is a noncooperative sequential game. First, M chooses its action and then B chooses its action. The decision taken by B depends on 4 timestamps and M and L take it independently. M represents the root of the tree and the outgoing edge from M represents M's actions. The outgoing edge is directed L which represents nature's decisions. The outgoing edge from L is directed to B.

D. Masquerading Attack

The goal of an attacker is to attack a PTP network to update the master clock and use the updated identity to launch other attacks. To launch the attack, the attack first obtains information about the "real" master clock and then eavesdrops on Sync, Delay Req, and Delay Resp messages that are sent to the slave clocks from the master. Once necessary data are obtained, the attacker can change Sync, Delay Req, and Delay Resp messages to masquerade as a master clock. Mimicking as a master clock could permit the attacker to transmit incorrect timing and management messages to other slave clocks, causing different kinds of damage to the system [1].

To reduce the masquerading attack, three measures can be used: chained process, centralized process, or port level security [1]. In the chained process, authentication information is given to the PTP network that is existing which uses a network component that is connected to the PTP network. In the centralized process, the position of the authentication server is given to the Grand Master clock(GM clock). Port level security is used to control the device which sends Sync, Delay Req, and Delay Resp messages [1].

E. Modification

The goal of a modification attack could be to (a) cause denial of service, (b) cause slave clocks to improper sync, or (c) alter the hierarchy of the master and slave clocks. The attack can be launched by manipulating the content of messages. Furthermore, the change in the messages sent by a master clock causes the greatest effect, since a master clock can send messages used for both time synchronization and management[1]

1) Attacking to deny service: In the analyzed version of the PTP, no methods are available for checking the authenticity of a message other than by checking the source of the message against the data set of the nodes. The data sets contain information such as the local and parent clock attributes, and information about the clock whose Sync messages are used for correcting time. Slave clocks check that a message arrived is from the correct master by comparing the source Communication Technology, sourceUuid and sourcePortId of the message with the corresponding fields in the parent data set of the slave clock. If the comparison fails, the message is discarded. By updating the above-mentioned fields of the Sync messages, an attacker can get the perfect match of Sync messages fail; thus, slave clocks would refuse to synchronize with the true current master. This can cause a denial of service (DoS) attack [1].

2) Attacking to cause incorrect resynchronization: Incorrect resynchronization of the slave clock(s) or a miscalculation of the network can be caused by the tampering with the timestamp clock and variance fields of Sync messages. The origin Timestamp field serves as the record of the time at which the Sync message leaves the master clock.

3) Attacking to alter the hierarchy of the master and slave clocks: Wrong information about the grandmaster clock within Sync messages leads the port setting to a different mode, e.g., slave or passive. Each slave clock executes the BMC algorithm for electing the best master clock for the next round of synchronization. Since the BMC algorithm uses information about the grandmaster clock, by altering the grandmaster clock information in a Sync message, an attacker can easily make this message "better" than other Sync messages that are received by the clocks in the given PTP subnet. Due to this, the manipulated Sync message becomes the best message for all local clocks from the attacker's subnet. Then, by correcting all the comparisons used in the BMC algorithm, the attacker can make the victim clocks switch into the passive mode or slave mode. As a result, the attacker destroys the synchronization hierarchy of clocks on the victim PTP network.

To reduce modification attacks, the usage of a technique called cryptographic integrity can be employed on all PTP messages for protection against modifications [1]. A modification attack is also termed a data integrity attack [7].

V. Proposed System

A. Background

The smart grid is a network that enables the flow of electricity in two-way. The data using digital communication technique enables to detect, react, and proact to changes. Self-healing capabilities is one of the main capabilities of grids and enable electricity customers to become active participants. The Smart grid provides opportunities to transmit the energy industry into a new requirement of reliability, availability, and efficiency. This helps in contributing to economic and environmental health. The Smart Grid is not just about utilities and technologies; it is about giving the information and tools that are needed to make choices about energy use.

The Smart Grid consists of new technologies and equipment. The grid needs a particular time for getting the technologies to be perfected, equipment's to get installed, and systems to be tested before it is implemented completely. And this is not possible at once when the Grid is evolving. The smart grid are integrated systems that needs new solutions to monitor and react to the grid dynamics in real-time environment.

Smart grid infrastructure will be in great demand in the coming generations due to their accurate timing signals. The increased demand for better reliability in the grid results in higher accuracy requirements and is reflected through standards that define the needs of various grid applications. Precision Time Protocol(PTP) is used in grids to achieve synchronization. But PTP is under cyberattacks, and its availability and end devices are targeted for attacks. Even after having a security extension called ANNEX-K, the smart grids are vulnerable to attacks as it does not consider all vulnerabilities related to PTP. The availability of synch error, injected by a threat agent circulates in the network, which has a greater impact on-time accuracy at synchronized devices.

The concept of time synchronization has a major role in managing, debugging, securing and planning network events. The key to achieve this functionality is by having precise synchronization between devices. The small-time delay error can cause the data collected to be out of sync, affect the data analysis and application, endanger the safety production, and cause the immeasurable economic loss. For performing synchronization various time protocols are used among which Precision Time Protocol (PTP) is the newest one which outpaces Network Time Protocol (NTP) by providing timing solutions in terms of accuracy, scalability and cost. Even though the PTP is enabled with security extensions, it is still open to synchronization attacks. To predict these synchronization attacks machine learning techniques are used. By employing machine learning techniques, it allows the system to predict the future responses from past data availability. This enables the detection of synchronization differences precisely over the network.

B. Peer-Delay Mechanism

The master clock (MC) sends the timestamped messages and the path between master and slave clock (SC) is connected by a transparent clock (TC). A Peer-delay mechanism is implemented over each segment to get link delay over the particular link. Timestamped messages (pdelay-request and pdelay-response) are exchanged by the devices at the two ends of the link (fig 1).

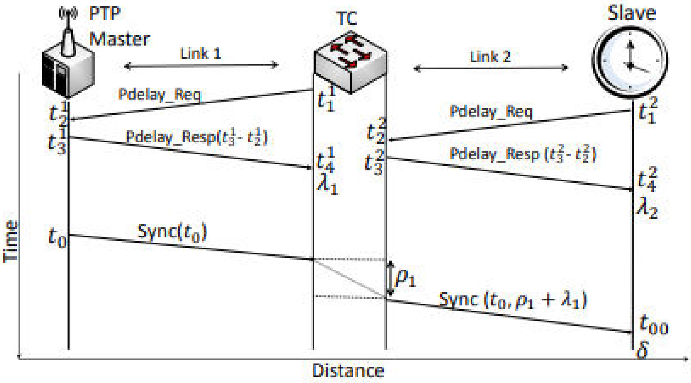


Fig. 1. peer-delay mechanism

C. Attack Surfaces

- Grand Master Clock (GMC): PTP arranges the network in a hierarchy with the GMC as its only root, targeting the GMC will present a bad time reference for synchronization and impact all the connected devices.
- Transparent Clocks (TCs): Through targeting a TC, an attacker leverages the functionality of the TC to perform the attack, and avoid integrity-based detection mechanisms. The TC is allowed by PTP to reconstruct PTP event messages after updating the correction Field, among other modifications, to reflect the PTP event message residence time.
- Slave Clocks: Attacks on a slave clock affect only the targeted slave. Such an attack causes impact on the applications that use timestamped data from the targeted slave.

D. System Architecture

The system consist of three types of clocks and are considered inside a PTP simulator. The attacker tries to create a change in time, it is handled by the request handler block . The features are extracted from the request collected from the attacker.
The corresponding dataset from the feature collected is generated. From the collected dataset attack detection and analysis is done. Genetic Algorithm is used to select the best features that satisfy the fitness function. The features of packets are collected and are given to RNN. Different layers of RNN helps in filtering out the attacked features for prediction (fig 2).

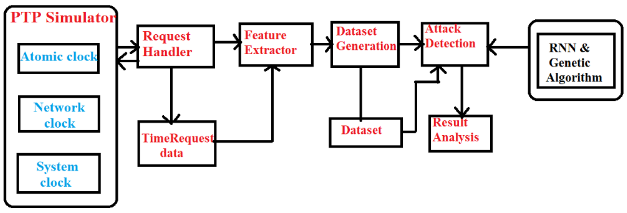


Fig. 2. System Architecture

E. Data Flow

The three types of clocks interacts with the precision type protocol (PTP). TC and Sc clocks are set up under the master clock. The synch request are handled by the slave clocks via PTP.

The attack attributes obtained from setting up TC and SC under the master clock are collected and are saved as log file. The data in log file is considered as attack log that saved all the sync difference occurred in the respective clocks.

A dataset is generated from the data obtained in the attack log and stored as table data containing sync differences. The generated dataset is used for attack prediction by applying machine learning algorithms. Genetic Algorithm (GA) is used for getting the fittest attributes. The fittest attributes are fed to RNN for predicting the attacks. The obtained information is stored as threat log used for determining the precision and recall of the process (fig 3).

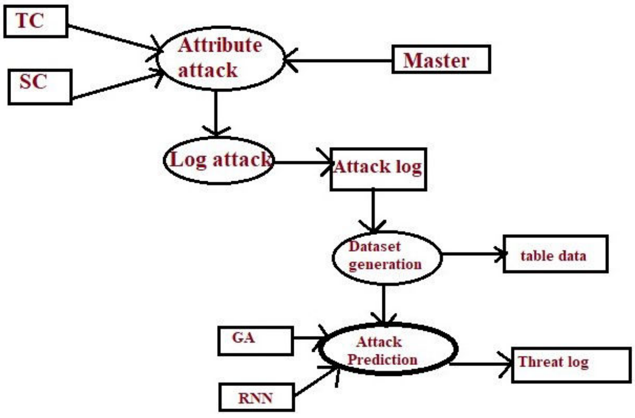


Fig. 3. Data Flow Diagram

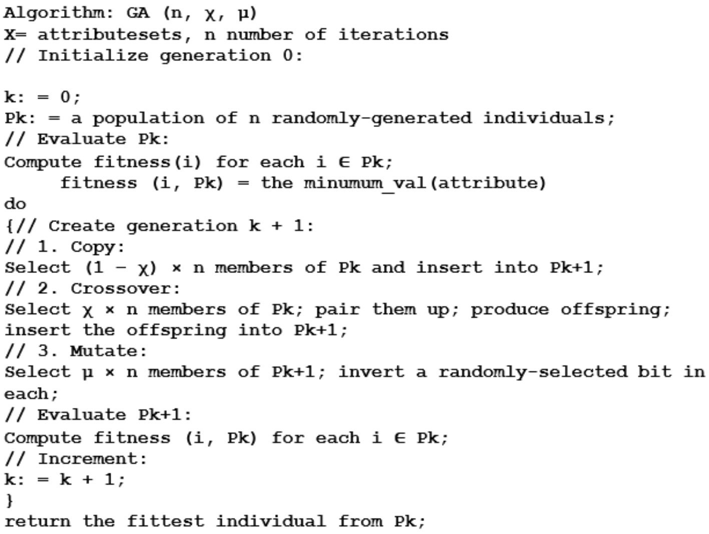
VI. System Implementation

A. Dataset

This module deals with generation of sync differences from respective clocks as dataset stored as table data. The sync difference data taken is below the range of [100] which is stored to table tbl-log. The clock synch error dataset is used as input along with attributes such as time to live (ttl), synch error, time delay, protocol, network overhead for the machine learning algorithms.

B. Applying Algorithm

This module deals with applying machine learning to the system for predicting the attacks. The synch error dataset is loaded with ttl, synch error, time delay, protocol, network overhead attributes displayed in a grid in UI interface. The Genetic Algorithm (GA) parameters includes population size and fitness values [2]. When applying Genetic algorithm, it filters out the fittest attributes which are above the fitness value taken as threshold. For the purpose of getting the best features from loaded attack dataset, GA is applied. For getting the fittest attribute GA is called first where [GA ga = new GA()] . A fitness function is also defined by[fitness function define] . Also [ga.Go()] is used to run the GA. [ga. GetBest] gives the best fittest value of the loaded attack attribute. The output is displayed using a out variable [out variable:].



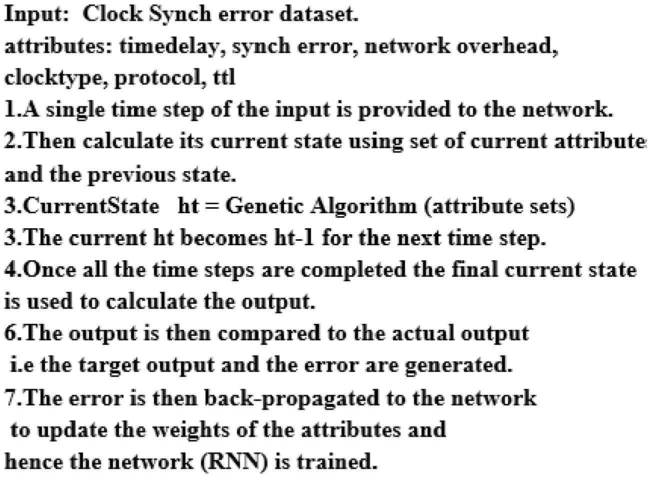
```
Algorithm: GA (n, χ, μ)
X= attributesets, n number of iterations
// Initialize generation 0:

k: = 0;
Pk: = a population of n randomly-generated individuals;
// Evaluate Pk:
Compute fitness(i) for each i ∈ Pk;
     fitness (i, Pk) = the minumum_val(attribute)
do
{// Create generation k + 1:
// 1. Copy:
Select (1 − χ) × n members of Pk and insert into Pk+1;
// 2. Crossover:
Select χ × n members of Pk; pair them up; produce offspring;
insert the offspring into Pk+1;
// 3. Mutate:
Select μ × n members of Pk+1; invert a randomly-selected bit in
each;
// Evaluate Pk+1:
Compute fitness (i, Pk) for each i ∈ Pk;
// Increment:
k: = k + 1;
}
return the fittest individual from Pk;
```

Fig. 4. GA pseudocode

C. Predicting Attacks

For analysis GA based RNN is used. RNN contains input layer, hidden layer and an output layer [3]. A single step of input is provided to the network. It checks the current state by comparing with the previous state. The current state is evaluated by GA using fittest attribute and completely crosscheck. It returns the row that can generate the most error. Current state calculated using GA is given to RNN. Once all time steps are completed, final current state is used to calculate the output. The output is then compared to target output and error is generated. The error is then back-propagated to the network to update the weights. The softmax layer is used to read the weights and weighted attacks will be predicted and are given to the output layer.



```
Input:  Clock Synch error dataset.
attributes: timedelay, synch error, network overhead,
clocktype, protocol, ttl
1.A single time step of the input is provided to the network.
2.Then calculate its current state using set of current attribute
and the previous state.
3.CurrentState   ht = Genetic Algorithm (attribute sets)
3.The current ht becomes ht-1 for the next time step.
4.Once all the time steps are completed the final current state
is used to calculate the output.
6.The output is then compared to the actual output
 i.e the target output and the error are generated.
7.The error is then back-propagated to the network
 to update the weights of the attributes and
hence the network (RNN) is trained.
```

Fig. 5. RNN pseudocode

VII. CONCLUSION

In this, attacks on PTP are classified into different categories. Various attacks affecting the security of time synchronization protocol are addressed. Various measures to reduce these attacks on the PTP network are also addressed. Still, these approaches are in current use, threats to PTP are not completely avoided. Usage of addressed countermeasures is compromised to certain levels in PTP networks. Employing these measures against major attacks does not strictly secure a time-synchronized network. Since time Synchronization protocols are growing immensely in the field of the networks, smart grids, and other time-synchronized applications they are still in danger of getting affected by many kinds of cyber attacks. The proposed system introduces machine learning along with PTP to predict the synch errors at various clocks.

REFERENCES

[1] https://www.researchgate.net/publication/220739067 ”A Security Analysis of the Precise Time Protocol Short Paper”.

[2] https://towardsdatascience.com/introduction-to-genetic-algorithms.

[3] https://www.geeksforgeeks.org/introduction-to-recurrent-neural-network.

[4] T. Mizrahi, “A Game Theoretic Analysis of Delay Attacks Against Time Synchronization Protocols,” in Proceedings of the IEEE International Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS), 2012.

[5] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” SANS ICS Report, 2016.

[6] M. Ullmann and M. Vogeler, “Delay attacksimplication on NTP and PTP time synchronization,” in 2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, 2009.

[7] L. Xie, Y. Mo, and B. Sinopoli, “Integrity data attacks in power market operations,” IEEE Trans. Smart Grid, vol. 2.

[8] A. Treytl, G. Gaderer, B. Hirschler and R. Cohen, “Traps and pitfalls in secure clock synchronization”, International Symposium for Precision Clock Synchronization for Measurement, Control and Communication, ISPCS 2007.

[9] Q. Yang et al., “On time desynchronization attack against IEEE 1588 protocol in power grid systems,” in Energytech, 2013 IEEE.

[10] B. Moussa, M. Debbabi, and C. Assi, “Security Assessment of Time Synchronization Mechanisms for the Smart Grid,” IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1952–1973, 2016.

Smart Traffic Control System

*

Abhikrishna T
Department of Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
abhikrishna131@gmail.com

Binsu Susan Thomas
Department of Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
binsusanthomas@gmail.com

Merin Sara Thomas
Department of Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
merinsarathomas11@gmail.com

Surya R
Department of Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
suryasurabhi5@gmail.com

Dhanya Sreedharan
Department of Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
dhanu.sree@gmail.com

***Abstract*—In the era of advancing technologies, people urge for technological advancement. Compared to the past decade, the increase in the quantity of automobiles delivered by the industry is increasing at an immense rate. Due to which the society is now facing a potential issues of Traffic congestion. The particular reason for this circumstance is due to the outdated traffic control system. Further, the lifestyle of people is affected due to the heavy traffic system as it causes time delays, economic losses, fuel consumption at high levels, air pollution and the stress while driving the vehicle. In order to overcome this crisis, there should be advancement in the traffic control system. A well-defined traffic control system eliminates the problems mentioned above to a particular extent. Here the conventional system is replaced by a new technology, where the density of vehicles in real-time is to be detected accurately which is then used for image processing. Our proposed system aims to design a smart traffic light control system based on image processing that could be adapted to the existing traffic system there by giving the priority based on density and also a provision for pedestrians to reduce their waiting time in this huge traffic.Inseption V3 is used to classify the objects. The classified objects are detected using SSD algorithm. The dataset used here is MobileNet.After processing data is stored in the AWS cloud.**

***Index Terms*—SSD, formatting, style, styling, insert**

I. Introduction

Traffic congestion is one of the issues faced by most of the urban cities. This is mainly due to the sudden rise in traffic volume and also the malfunctioning of Traffic signals. Traffic congestion not only causes extra time delay and stress for the drivers, but also increases fuel consumption, increase air pollution.The conventional methods for the traffic control are manual and automatic traffic signals. There are lot many drawbacks in this conventional methods. The manual controlling system requires a large number of manpower and also most the traffic signals are preprogrammed by a timer value which delays the traffic by stopping the vehicles during peak hours. If a signal break down occurs it can also cause difficulties for the traffic flow. Traffic signals are most needed in peak hours for avoiding congestion and saving time. As we see in today's scenario most traffic signals are giving more importance to the vehicles than the pedestrians which causes so much difficulties to them and also causes accidents at the time of crossing the roads. The conventional system has to be upgraded in order to reduce the traffic congestion, time delay etc. In this paper we are introducing a smart traffic light control system using image processing techniques based on the density of the vehicle and the pedestrian the traffic signal is allocated. By implementing this system which aims to reduce the congestion by computing the optimal green signal time by calculating the density in each lane. This system will override the older system of preprogrammed traffic signals which causes unwanted delays.

II. Literature Survey

In this section we will discuss the recent technologies that deal with traffic congestion.

This work introduced in Refernce[1] The proposed system is implemented in Matlab with an objective to reduce the traffic based on density. The vehicles are detected by considering the captured images instead of using timers or electronic sensors which are placed on the pavement. A web camera is placed at the traffic light which captures images of the road through which the vehicle count is estimated and traffic is controlled. Four main steps are considered for the system: image acquisition, RGB to grayscale transformation, image enhancement and morphological operations. A camera is installed and used to capture video of the highway. The video is recorded continuously in consecutive frames and each frame is compared to the initial captured image. The total number of cars present in the video is found out using image processing algorithms. If the total number of cars exceeds a predefined threshold, heavy traffic status is displayed as a message. It helps decrease traffic congestion without any wastage of time caused by showing green signal on an empty road without any vehicles. It is a better way to determine the presence of vehicles since it makes use of real-time images which makes it better than systems depending on the vehicle's metal content only. Drawback with this method is that during weather conditions image quality is affected.

In Reference [2] is a real-time traffic control system which can easily keep traffic in control using image processing techniques. This system consists of video cameras on the traffic junctions for each side as if it is a four way junction. Therefore four video cameras will be installed over the red lights facing the road. Cameras would be capturing video and broadcasting it to the servers where using video and image processing techniques the vehicle density on every side of the road is calculated and an algorithm is employed to switch the traffic lights accordingly. Hardware includes connection of these cameras to the server to receive live feed and a server capable enough for handling the processing requirements. Software used in the system includes MATLAB video and image processing toolbox and C++ compiler to generate algorithmic results. This provides the approximate density of vehicles on road considering that a vehicle larger in size will have higher density as it will cover relatively more area and more time to pass the traffic junction. This process is repeated for every second and for all the sides. Now, with the real time density of vehicles at every side of traffic junction and density is added to the algorithm as a variable stated below to switch the traffic lights. It doesn't provide the number of vehicles. It provides the density of traffic, for instance the vehicle density of a truck could be equivalent to two medium sized cars and the benefit of calculating the vehicle density is the amount of time a truck will take to pass the light which would be equivalent to the total amount of time two cars will take one after another. Although this method is cost effective it also has some disadvantage that it cannot be used in low light conditions and due to shadows and weather it will affect the accuracy of the results.

In Reference [3] A system to control the traffic by measuring the real time vehicle density using canny edge detection with digital image processing is proposed. Edge detection technique is imperative to extract the required traffic information from the CCTV footage.It can be used to isolate the required information from rest of the image. It has been observed that the Canny edge detector depicts higher accuracy in detection of object with higher entropy, PSNR(Peak Signal to Noise Ratio), MSE(Mean Square Error) and execution time compared with Sobel, Roberts, Prewitt, Zero crossing and LOG [10-12].A system in which density of traffic is measured by comparing captured image with real time traffic information against the image of the empty road as reference image is proposed. Each lane will have a minimum amount of green signal duration allocated. According to the percentage of matching allocated traffic light duration can be controlled. The matching is achieved by comparing the number of white points between two images. The entire image processing before edge detection i.e. image acquisition, image resizing, RGB to gray conversion and noise reduction is explained in Image Processing. At Edge Detection and white point count, canny edge detection operation and white point count are depicted. Canny edge detector operator is selected because of its greater overall performance. Percentage matching for different sample images and traffic time allocation for them are demonstrated in section Percentage matching and Time allocation. The content of this paper completely serves the purpose of demonstrating the limitations of current traffic control techniques and the solution of this limitations with detailed explanation. Image matching by comparing detected edges is a novel approach to identify the vehicular density with propitious accuracy. As far as we know, matching images by comparing detected edges has not been used before for smart traffic control application. Drawback of this method is while calculating the number of vehicles may give false results if the intravehicular spacing is very small.

III. Proposed System

A. Methodology

The system consists of video cameras which is already installed on the street poles. These cameras will be focusing on the vehicles as well as pedestrians. The input to the system will be a realtime traffic which is used for density calculation using image processing and object detection. The video is converted to frames using image processing techniques and from the input image the objects are detected using SSD algorithm. The number of vehicles is calculated which is used for density calculation. Similarly, the density of the pedestrian is calculated. This density is given to the traffic management for setting the green signal timer to the each lane.

B. Object Detection Module

Classification of objects is done using Inception V3. It consists of 48 convolution layers, in which feature extraction is done within each layer. Average pooling and max pooling are used for image classification, for tracking the images and objects. Object detection is done using SSD(Single Shot Detection Algorithm), in which, it uses multiple layers to detect objects. Faster R-CNN is used to create boundary boxes to classify the objects. Objects can be classified in a single

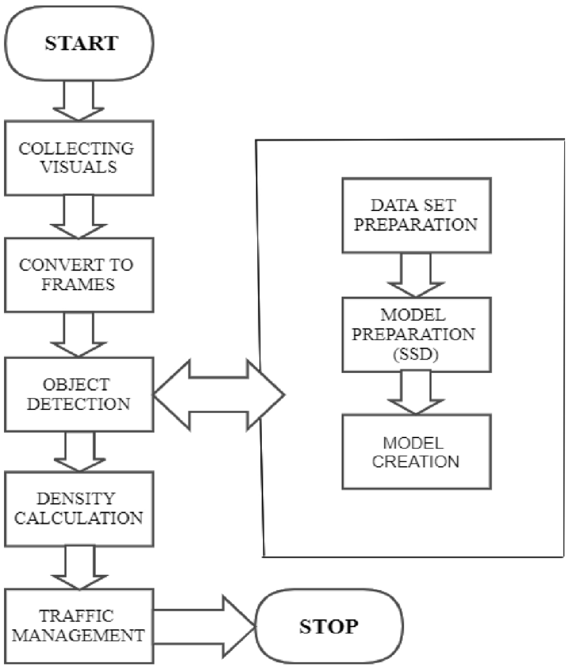


Fig. 1. flowchart of proposed method

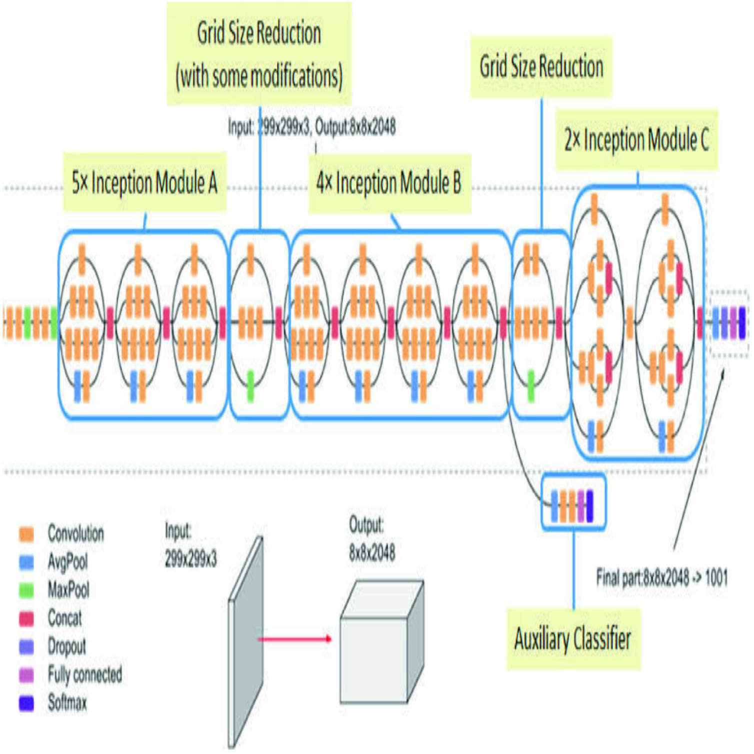


Fig. 3. Structure of inception v3

shot. More default boxes in the algorithm results in more accuracy in object detection.

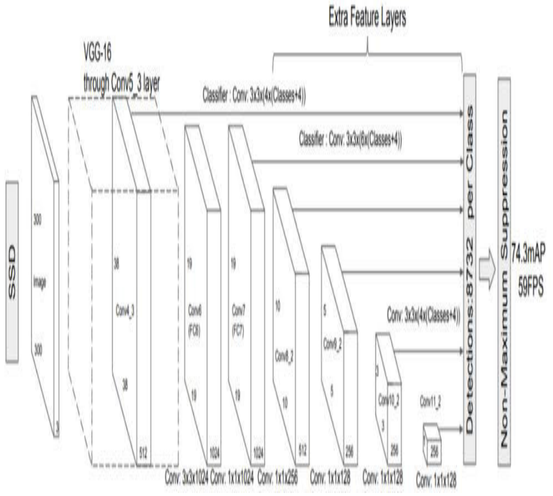


Fig. 2. Structure of SSD algorithm

Conclusion

In this paper we introduced a smart traffic light control system based on image processing.It provides solution to the current traffic system.The system uses a dynamic approach in which both the peak and non peak hour traffic light is controlled.The proposed system is implemented and delivers an accuracy of 90-93 percent in estimating the density of traffic and controlling the signal.Based on the results the system is more efficient and is capable of reducing traffic congestion during peak and non-peak hours.The image processing techniques are always much cheaper than compared to other techniques and it doesn't require any implementation cost.

References

[1] U. E. Prakash, "Density Based Traffic Control System Using Image Processing," pp. 1–4, 2018.

[2] A. Kanungo, "Smart Traffic Lights Switching and Traffic Density Calculation using Video Processing," pp. 6–8, 2014.

[3] T. Tahmid and E. Hossain, "Density Based Smart Traffic Control System Using Canny Edge Detection Algorithm for Congregating Traffic Information," no. December, pp. 7–9, 2017.

2021 Recent Trends in Advanced Computing Technologies

JPEG Steganalysis Using Deep Learning

1st Athira Madhusoodan
Dept. of Computer Science,
Sree Buddha College of Engineering
Alappuzha, India

2nd Elizabeth Jose
Dept. of Computer Science,
Sree Buddha College of Engineering
Alappuzha, India

3rd Linta Thomas
Dept. of Computer Science,
Sree Buddha College of Engineering
Alappuzha, India

4th Aneena Susan Saji
Dept. of Computer Science,
Sree Buddha College of Engineering
Alappuzha, India

5th Minu Lalitha Madhavu
Dept. of Computer Science,
Sree Buddha College of Engineering
Alappuzha, India

***Abstract*—Steganography is simply defined as the technique of hiding a message. In this digital media ,it is referred as the method of encrypting a message in form of text , image,video,audio etc. within an image ,or video. While on the other hand steganalysis is the approach of analyzing whether an image is stego or not. There are several for encrypting message in an image. This method widely depends on the handcrafted features. But This method becomes more and more inefficient due to the rapid growth of advanced steganography, manual design of complex features has becomes a tedious process and time consuming process. With deep learning approach, it can greatly reduce this complex task. Since deep learning works in such a way that ,it works on user input data and corresponding labelled output and network automatically decides the rules for the model .This in comparison to convectional programming strategy were user inputs data and sets the rules ,performance of this type of models thus greatly depends on handcrafted features.**

In this model ,we propose a jpeg steganalysis deep learning model that predicts the percentage whether an image is stego or not. For this proposed model we consider steganography in JPEG images, since it is the most widely used image format that supports all devices. The proposed model learns feature automatically since the filters in their convolutional layers are able to recognize a great diversity of shapes,textures, noise patterns, processing and image-development traces, which are exactly the attributes that modulate the stego signal of modern content-adaptive steganographic schemes which in turns results in the detection of stego image.In the proposed model ,we use transfer learning concept with EfficientNet to increase the accuracy of the model with limited computational resources. In final phase ,we deploy our model on website which is hosted on local computer.

***Index Terms*—Deep Learning,Convolutional layer,EfficientNet, Steganography,Steganalysis.**

I. Introduction

With the fast improvement of information technology and the quick promotion of the Internet, computerized media has gotten a significant transporter for military, business and different associations just as people to acquire and communicate information. In any case, at a similar time, on the grounds that the computerized correspondence in the Internet is powerless against the danger of listening in, noxious impedance what's more, different exercises, individuals focus closer on the [7]security issues like security assurance and information honesty simultaneously of information transmission than at any other time. The customary arrangement utilizes encryption technology to change the information over to ciphertext for transmission. Yet, its deficiency is that the scrambled ciphertext is normally cluttered. Simultaneously, it might additionally lead to information being meddled or captured, coming about in the disappointment of information transmission. In the above setting, a new idea of correspondence security has been progressively acknowledged and perceived: correspondence security implies not just that the substance of information to be sent is secure, yet additionally that the presence of the demonstration of sending privileged intel is obscure. Hence, steganography, which is described by ”camouflage” in the transmission of information, has pulled in increasingly more consideration Steganography is the art of hiding information in a non-suspicious medium so that the very existence of the hidden information is statistically undetectable from unaware individuals. The objective is to make steganographic correspondence vague from customary trade of data during which no insider facts are passed between imparting parties. Advanced media, like pictures, are especially reasonable cover objects in view of their omnipresence and on the grounds that they can be somewhat adjusted without changing their appearance, possibly along these lines ready to hold huge messages. JPEG images are more oftenly used since this image formats are greatly utilized in digital cameras, smart phones devices and in all media of communication over the Internet and social networks.

While on the other hand,steganalysis is the technique of detecting the appearance of hidden data in such supports. The purpose of finding the presence of embedding changes is tedious due to the reason that images contain an indeterministic component, the acquisition noise, and by wide range of diversity and complexity introduced during acquisition, development from the RAW capture, post-processing, editing, and sharing. When designing steganalysis detectors, researchers commonly consider a rather sand-boxed environment: a known steganographic scheme, known payload, and a known cover source typically consisting of grayscale images of a fixed size.

II. Background

A. Traditional Methods

Due to the popularity of images in digital society, images are more likely to be used for carrying secret messages and therefore more attention is paid on image steganalysis. In any case, it is a difficult undertaking in light of the fact that the stego signal acquainted with pictures is somewhat weak. Traditionally, existing steganalysis methods rely on handcrafted features to [1] model the statistical changes of an image caused by embedding operation. In early period, insights, for example, picture quality measures (IQMs), amplitudes of nearby extrema in the dark level histogram are utilized as [8] Afterward, analysts followed a worldview of model-ing the measurable conditions between neighboring pixels or coefficients by figuring Markov interaction or co-events from the commotion leftover. The [5]noise lingering is acquired by utilizing high-pass filters to reinforce the stego commotion, subsequently making highlight portrayals more delicate to installing tasks. As of late, with the expanding refinement of steganographic strategies, it is getting more earnestly to identify precisely when simply utilizing straightforward picture models. Subsequently, scientists proposed to utilize unpredictable and high request insights to improve the location performance. So far, the most representative handcrafted features are the so-called rich image representations. These features are extracted by firstly using a large number of designed high-pass filters [10] to obtain a family of noise residuals, and then merging features computed from different noise residuals to obtain a high dimensional feature set.

When designing the above handcrafted features, steganalyzers need to specify all of the image statistics that steganalysis systems need, which is time-consuming and laborious. Unfortunately, it is rather difficult to know what features should be extracted for detecting embedding changes because natural images are difficult to model accurately. Moreover, increasing sophistication of embedding algorithms makes the task even more challenging.

B. Steganographic Methods

Stenographic methods can be classified mainly into five categories which is mentioned below.

a) Spatial Domain : This stenographic method is also known as substitution techniques, are a group of interconnected simple techniques that produces a covert channel in the areas of the cover image in which alters in such a way that a bit scant when compared to the human's eyes.One of the ways to do so is to hide information in the Least Significant Bit (LSB) of the image data. This embedding approach is generally based on the fact that the least significant bits in an image is considered as random noise, and generally, they become unresponsive to any alterations on the image.

b) Transform Domain : Transform Domain In Transform domain, images are first transformed and then the message is embedded into it.This approach is more tedious to hide secret message into an image. It carrys out data hiding by altering mathematical functions and image transformations. Transformation of cover image is carried out by tweeking the coefficients and inverts the transformation. Most well known transformations include the two-dimensional discrete cosine transformation (DCT), discrete Fourier transformation (DFT) and discrete wavelet transformation (DWT).

c) Statistical Method : : This method is known as model-based approaches, these approaches tend to alter the statistical properties of an image in addition to preserving them in the embedding process. This modification is generally small, and it is hence able to take advantage of the human inability in detecting luminance variation.

d) Distortion Techniques : Distortion techniques needs information of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder, on the other hand, adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion.

C. Jpeg Steganography

- Working of Jpeg Algorithm

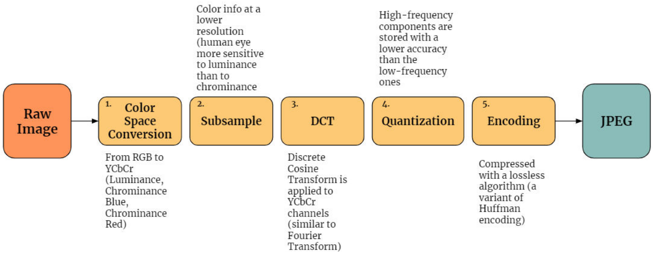

Color info at a lower resolution (human eye more sensitive to luminance than to chrominance
High-frequency components are stored with a lower accuracy than the low-frequency ones
Raw Image
1. Color Space Conversion
2. Subsample
3. DCT
4. Quantization
5. Encoding
JPEG
From RGB to YCbCr (Luminance, Chrominance Blue, Chrominance Red)
Discrete Cosine Transform is applied to YCbCr channels (similar to Fourier Transform)
Compressed with a lossless algorithm (a variant of Huffman encoding)

Fig. 1. Figure representing the working of Jpeg Algorithm

Firstly the image is converted into YCbCr from RGB channels. YCbCr and RGB are both colorspaces having different channels where YCbCr consists three channels as Luminance(Y) , Cb(Cb is blue minus luma (B-Y)) , Cr(Cr is red minus luma (R-Y).Then DCT is applied on the pixels of these channels , using DCT coefficients.The image encoded using JPEG algorithm stays in YCbCr colorspace untill it is decoded by an Image viewer software. When a JPEG is read it is decoded and converted back to RGB colorspace to be rendered on screen using the techniques described the above in Fig.1

- Steganography in Jpeg
  For hiding secret messages in jpeg images,DCT coeffcients of different channels of images are altered.There are several approaches for doing this which is mentioned in traditional methos section.Most advanced form [15] of this method is the use of adpative stegongraphy techinques like JUNIWARD,JMiPOD which uses deep learning techniques too hide messages in Jpeg images and are very difficult to track down traditional steganalysing methods.

D. Steganalysis with Deep Learning

Deep learning is a subset of machine learning in artificial intelligence that has networks capable of learning unsupervised from data that is unstructured or [6] unlabeled. Apart from conventional programming concept which works on input data and rules which are explicitly set by user, deep learning works on input and corresponding output data which is feeded by user and network automatically sets the rules. Due to this reliable and scalable nature of deep learning, it is used in wide variety of applications.

The problem of feature representation for steganalysis can be solved by using deep learning, since this [11] approach automatically learns patterns from raw data. Since this steganalysis deals with images, Convolutional Neural Network (CNN) in deep learning is employed for this problem. Pibre et al. present a CNN architecture for steganalysis with fewer convolutional layers, and without the pooling operation. But such architecture is designed especially for steganalysis in the scenario where the embedding changes occur roughly in the same locations over images caused by the fixed embedding key. However, the scenario hardly happens in practice.In [12] propose to use absolute activation layer, Tanh activation function and 1×1 convolution in CNN architecture for steganalysis. In ,the authors propose a method based on Deep Residual Network, a kind of very deep CNN model. In [14], a transfer learning procedure was applied to improve the exhibition of CNN on distinguishing steganography with a low installing rate. Here, in an unexpected way, the model blend procedure is successful on improving the discovery execution against steganography with high payload too. In [2], the authors devised to regularize CNN model with auxiliary functions. Different from this method, the proposed model combination strategy does not need extra explicit feature representation.

III. The proposed model Architecture

A. Defining the model

The Fig.2 represents the proposed deep learning model for carrying out steaganalysis. In the first phase data collection of model was carried out. For this model, we take cover images and its corresponding stego images of 60,000 images on each label from ImageNet Dataset which contains over 14 million color images. The stego label contains jpeg images on which adaptive [4] stenographic algorithms such as JUNIWARD,JMiPOD are applied. In the second phase processing of the supplied images was carried out. To make dataset uniform, the input images are resized to size 224 x 224 .Then in training set data, data augmentation process is carried out. Data augmentation refers to the modifications applied to dataset inorder to reduce the phenomenon of Overfitting, which refers to situation in which model [14] performs well on train data ,but fail on test data. Here in this case, random cropping ,horizontal and vertical flips are carried out. After that normalization operation is carried out

The proposed steganalysis model is based on EfficientNet [13] which is a state of art network model developed by google. We use transfer learning strategy on Efficient network model and fine tune the model for our proposed network model.

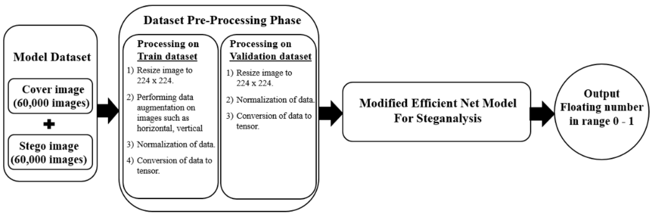

Model Dataset
Cover image (60,000 images)
+
Stego image (60,000 images)
Dataset Pre-Processing Phase
Processing on Train dataset
1) Resize image to 224 x 224.
2) Performing data augmentation on images such as horizontal, vertical
3) Normalization of data.
4) Conversion of data to tensor.
Processing on Validation dataset
1) Resize image to 224 x 224.
2) Normalization of data.
3) Conversion of data to tensor.
Modified Efficient Net Model For Steganalysis
Output Floating number in range 0 - 1

Fig. 2. Model Architecture

a) EfficientNet Model: For reducing the computational time, the amount of resources for training and deployment complexity [3] of deep learning state of art models like ResNet,NasNet ,Inception networks, google research labs devised a new method called Efficient Net. This network outperforms all state of models with accuracy and reducing the computational cost for modelling network to the ratio of 1:5. This method provides a compound scaling scaling method, which use a compound coefficient to uniformly scales network width, depth, and resolution in a principled way. Since'd' depth can capture richer and more complex features, and generalize well on new task, width 'w' wider networks tend to be able to capture more fine-grained features and are easier to train and With higher resolution 'r' input images, potentially capture more fine-grained patterns.The below Eq.1, represents the equation for compound scalling

$$\begin{aligned} &\text{depth: } d = \alpha^{\phi} \\ &\text{width: } w = \beta^{\phi} \\ &\text{resolution: } r = \gamma^{\phi} \\ &\alpha \cdot \beta^2 \cdot \gamma^2 \approx 2 \\ &\text{where} \quad \alpha \geq 1, \beta \geq 1, \gamma \geq 1 \end{aligned} \tag{1}$$

b) Transfer learning: In deep learning, transfer learning [9]is a method by which a neural network model is first trained on a problem similar to the problem that is being solved. In this approach one or more layers from the trained model are then reused in a new model trained on the problem of interest. With this transfer learning approach model can achieve better accuracy as compared [16] to the model that is built from scratch and also results in decreasing the training time for a neural network model and resulting in lower generalization error. For the proposed model, the last layer of EfficientNet model is dropped out we add average pooling layer and dense layer with SoftMax activation function at end .The weights of the EfficientNet model is kept constant and untrained. The modified model is then trained on our training dataset.

B. Working of the Proposed Model

The above Fig.3 shows the working of the proposed model. After preprocessing images in train dataset which is of size

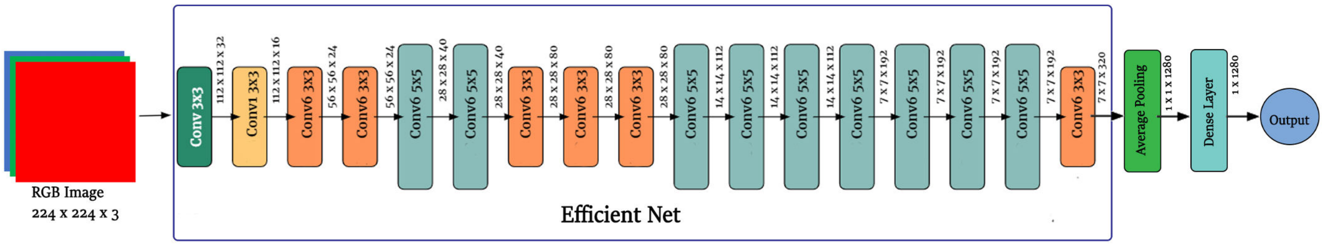


Fig. 3. Proposed model network for steganalysis

512 x 512 x 3, we get image 224 x 224 x3 which is to the efficient Net. The Efficient Net is a convolutional layer of type inverse residual block. Inverse residual is a type of residual block which is utilized for picture classification models that uses an inverted structure for achieving higher accuracy of model with limited resources. A traditional Residual Block has a structure of wide - narrow - wide with the number of channels. The input has a large number of channels, which are compressed with a 1x1 convolution. The number of channels is then increased again with a 1x1 convolution so input and output can be added. But in case of an Inverted Residual Block structure is narrow - wide - narrow, hence the inversion. We first widen with a 1x1 convolution, then use a 3x3 depth wise convolution which results in reduction of the parameters used then we use a 1x1 convolution to decrease the number of channels so input and output can be added.

Here we apply transfer learning approach, the weights of efficient network layer is kept constant and make also make training of dataset in this layers are set to false. For this proposed model the layer of Efficient Net is dropped out and we add additional layers which is required to meet our purpose. Average Pooling layer and dense layer is added. The average pooling layer pools average over all layers that is output by efficient net converts layer to equivalent 1D network. This network later connects to the dense layer of size 1280 x 1 and then this layer are densely connected to a softmax layer ,which outputs the results in form of probability value ranging from 0 to 1.This decimal value represents the percentage that model predicts the image contain stego message.

C. *Implementation of the Proposed Model*

The proposed model was done on PyTorch, which is a deep learning framework written on python language. The model was trained on local computer with support of GPU to speed up training of the model.To visualize the model accuracy, we use matplotlib library of python. For optimization of model, we use Adam optimizer which is a module built over stochastic gradient descent method. The model ran for 100 epochs and result was analyzed. Finally, deployment of model was carried with help of Flask, python web framework with setting server as our local computer with help of ngrok.

IV. Results

The Fig. 4. shows the training loss and validation loss curve when the model run for 100 epochs or iterations. From figure it is clear that the losses of model decrease with increasing epochs which shows that model is training well on the given dataset.The convergence of training curve and validation curve shows that the model generalizes very well, that is model will give good performance on real world data.

The Fig. 5. shows the accuracy curve of the proposed model. It is clear from graph that, the validation accuracy of model increases with increase in epochs which implies that model generalizes well. From graph, it clear that the accuracy of proposed model ranges between 75% - 85% which shows the performance of model.

V. Conclusion

In this paper we propose a deep learning model, that predicts if a jpeg image is stego or not. In section 2 of the paper, we discussed about the traditional steganalysis approaches. From that, it was clear that feature extraction in traditional like rich models, support vector approaches was handpicked one which is a tedious task. As steganography approaches are improving, such as adaptive steganography methods like JUNIWARD, JMiPOD are very difficult to implement feature extraction explicitly. Due to this we proposed a deep learning steganalysis model. For better computation with limited resources and for achieving good accuracy we use transfer

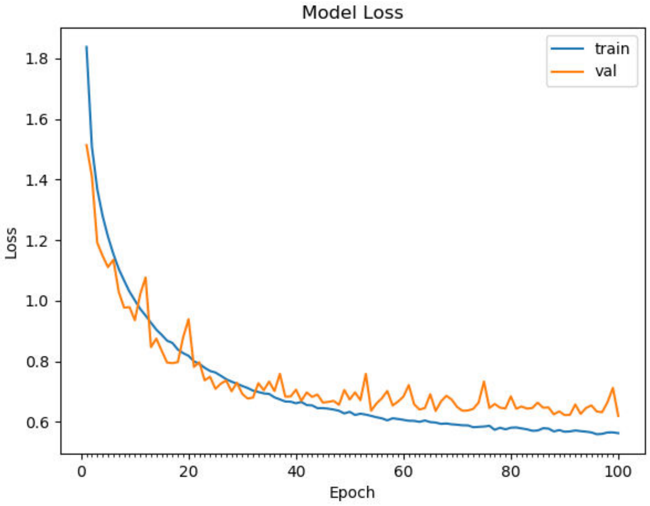


Fig. 4. Loss Curve of the proposed model

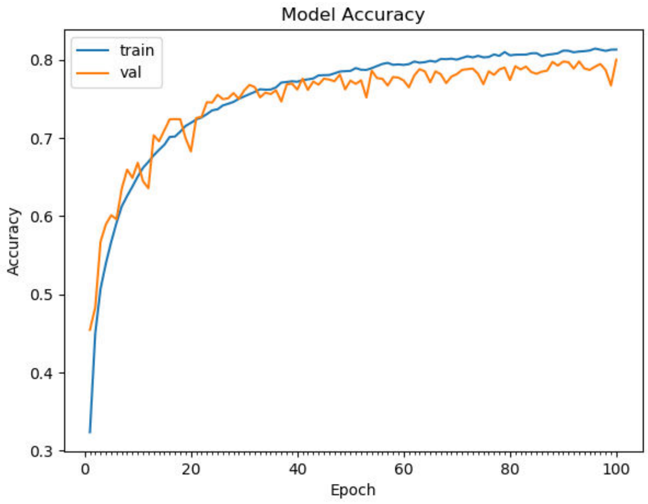


Fig. 5. Accuracy Curve of Proposed model network

learning approach and fine tune the model. For the proposed model we use EfficientNet and fine tune this network model to make it suitable for our purpose. After training and testing the proposed model we get an accuracy around 75 %.With this approaches the model performs very well with limited amount of work as compared to hand -crafted features in traditional methods.

References

[1] High-dimensional steganography blind detection method based on improved support vector machine. *Computer Engineering*, page 06, 2015.

[2] Mehdi Boroumand, Mo Chen, and Jessica Fridrich. Deep residual network for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, 14(5):1181–1193, 2019.

[3] Marc Chaumont. 14 - deep learning in steganography and steganalysis. In Mahmoud Hassaballah, editor, *Digital Media Steganography*, pages 321–349. Academic Press, 2020.

[4] Mo Chen, Vahid Sedighi, Mehdi Boroumand, and Jessica Fridrich. Jpeg-phase-aware convolutional neural network for steganalysis of jpeg images. In *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, IHamp;MMSec '17, page 75–84, New York, NY, USA, 2017. Association for Computing Machinery.

[5] Jessica Fridrich and Jan Kodovsky. Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, 7(3):868–882, 2012.

[6] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778, 2016.

[7] Konstantinos Karampidis, Ergina Kavallieratou, and Giorgos Papadourakis. A review of image steganalysis techniques for digital forensics. *Journal of information security and applications*, 40:217–235, 2018.

[8] Jan Kodovsky, Jessica Fridrich, and Vojtěch Holub. Ensemble classifiers for steganalysis of digital media. *IEEE Transactions on Information Forensics and Security*, 7(2):432–444, 2011.

[9] Selim Ozcan and Ahmet Fatih Mustacoglu. Transfer learning effects on image steganalysis with pre-trained deep residual neural network model. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 2280–2287. IEEE, 2018.

[10] Tomáš Pevny, Patrick Bas, and Jessica Fridrich. Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security*, 5(2):215–224, 2010.

[11] Yinlong Qian, Jing Dong, Wei Wang, and Tieniu Tan. Deep learning for steganalysis via convolutional neural networks. In *Media Watermarking, Security, and Forensics 2015*, volume 9409, page 94090J. International Society for Optics and Photonics, 2015.

[12] Yinlong Qian, Jing Dong, Wei Wang, and Tieniu Tan. Learning and transferring representations for image steganalysis using convolutional neural network. In *2016 IEEE international conference on image processing (ICIP)*, pages 2752–2756. IEEE, 2016.

[13] Mingxing Tan and Quoc Le. Efficientnet: Rethinking model scaling for convolutional neural networks. In *International Conference on Machine Learning*, pages 6105–6114. PMLR, 2019.

[14] Guanshuo Xu. Deep convolutional neural network to detect j-uniward. In *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, pages 67–73, 2017.

[15] Weike You, Hong Zhang, and Xianfeng Zhao. A siamese cnn for image steganalysis. *IEEE Transactions on Information Forensics and Security*, 16:291–306, 2020.

[16] Barret Zoph, Vijay Vasudevan, Jonathon Shlens, and Quoc V Le. Learning transferable architectures for scalable image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 8697–8710, 2018.

BOBtheBOT: An Intelligent Chatbot to Detect Mental Illness by Recognizing Emotion Through Text

Ashwin
Department of Computer Science and Engineering,
Sree Buddha College of Engineering, Pattoor,
Alappuzha, Kerala, India - 690529
Email: Ashwindavid11@gmail.com

Vidya Prasannan
Department of Computer Science and Engineering,
Sree Buddha College of Engineering, Pattoor,
Alappuzha, Kerala, India - 690529
Email: Vidyaprasannan1999@gmail.com

Megha P S
Department of Computer Science and Engineering,
Sree Buddha College of Engineering, Pattoor,
Alappuzha, Kerala, India - 690529
Email: Gem.ps14@gmail.com

Vishnu B Dev
Department of Computer Science and Engineering,
Sree Buddha College of Engineering, Pattoor,
Alappuzha, Kerala, India - 690529
Email: Bdevbdevbdev@gmail.com

Lakshmi S
Assistant Professor
Department of Computer Science and Engineering,
Sree Buddha College of Engineering, Pattoor,
Alappuzha, Kerala, India - 690529
Email: Lakshmi.rnath@gmail.com

A*bstract* – A chatbot is an intelligent piece of software that is capable of communicating and performing actions similar to a human by artificially replicating the patterns of human interaction. It allows a form of interaction between a human and a machine. Social chatbots are designed to form a social-emotional relationship with the end user. The main notion behind this chatbot is to predict if the user has an underlying mental health issue. This paper provides a solution as a system which can communicate and find the intensity of various emotions such as joy, sadness, fear, anger, guilt, disgust, shame. Further, based on the obtained intensity of each emotions, the chatbot predicts if the users suffering from mental illness by using users chat data. The chatbot uses Long–Short Term Memory (LSTM) for emotion detection.

Key words: Artificial Intelligence, Mental Illness, Chatbot, Emotions.

I. INTRODUCTION

Chatbots are special agents that respond with the user in natural language just as a human would reply [1][7]. Pointedly, social chatbots are the ones which builds a strong emotional relationship with the user [1]. The primary goal of a social chatbot is not necessarily to solve all the questions the users might have, but rather, to be a virtual companion to users [4].

Early conversational systems, such as Eliza (Weizenbaum, 1966), Parry (Colby, 1975), and Alice (Wallace, 2009), were designed to mimic human behaviour in a text-based conversation, hence to pass the Turing Test (Turing, 1950; Shieber, 1994) within a controlled scope [5][6]. Despite impressive successes, these systems, which were precursors to today's social chatbots, were mostly based on hand-crafted rules. As a result, they worked well only in constrained environments.

In the area of mental health, there are still open questions about how to use technology to sense affective states of mind [4]. A recent analysis implies that many people may actually would rather "talk" to a chatbot or other AI program about their mental health struggles than to a therapist themselves. In fact, only 18% of people surveyed preferred to talk to a human about their problems, meaning that 82% would prefer to talk to a robot [7].

In this paper, we proposed an intelligent chatbot which can help to detect the intensity of emotions in textual data from users' chat. Likewise, the bot can suggest whether the user needs an immediate medical attention, for that the user needs to converse with the bot, in this process the bot will try to form a bond between itself and the user. Based on the chat data collected from the conversation the bot will try to identify the emotion associated with each text. Subsequently, the overall intensity of each emotions will be calculated and whether the user is suffering from a mental illness is predicted**.**

The two algorithms are used in the model training. Long short-term memory (LSTM) is used for chatbot training while emotion analysis is done using Linear Support Vector Machine (LSVM). LSTM is applicable to tasks such as unsegmented, connected handwriting recognition, speech recognition and anomaly detection in network. A common LSTM unit is comprised of a cell, an input gate, an output gate and a forget gate [8]. LSVM on other hand is particularly suited for use with wide datasets, that is, those with a large number of predictor fields [9].

These two algorithms are deployed further for completing the training.

II. RELATED WORKS

Continual refinement of emotion recognition and natural language processing techniques has allowed for chatbot systems to be successfully used in therapy and counselling.

One study attempted to redefine emotion recognition by distributing text into emotion labels and based on the labels it identifies users' mental state as stress or depressed using users' chat data. Further, based on the emotions, it calculates the positivity and negativity percentage to classify the mental state of the user using negativity percentage. For emotion detection, they deployed three popular deep learning classifiers namely, Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), and Hierarchical Attention Network (HAN) [1].

Another approach to textual emotion analysis was by building an emotion embedding model using Convolution Neural Network. In this paper, a further classification of emotion is added so as to provide more descriptive output from the model. Emotions embedding model here only refers to an embedded layer trained in CNN emotional classification learning process and cannot identify the presence of emotion shift in statements [2].

A different research summarized many recent advances and several key research challenges associated with NLP research area. It suggests an effective emotion-shift recognition model and context encoder can yield significant performance improvement over chit-chat dialogue, and even improve some aspects of task-oriented dialogue [3].

III. PROPOSED METHOD

In this work, we proposed a chatbot which takes users' chat as input and predicts the percentage of various emotions such as Joy, Shame, Anger, Disgust, Sadness, Guilt, and Fear involved in it. The chatbot is trained to handle simple conversations and meanwhile passing the users' chat to emotion detection model which classify the users' chat into the emotions mentioned above and further based on this classification, the percentage of each emotion is calculated by taking the total number of conversations into account.

A. Dataset Description

In this work, we have used the International Survey on Emotion Antecedents and Reactions (ISEAR) dataset for emotion detection from the chat text. The dataset consists of 7652 phrases and 1542 emotional words. It is categorized into several categories of emotions such as Joy, Shame, Anger, Disgust, Sadness, Guilt, and Fear.

The dataset used for chatbot is a collection of YAML files with each of them handling various contexts in the conversation.

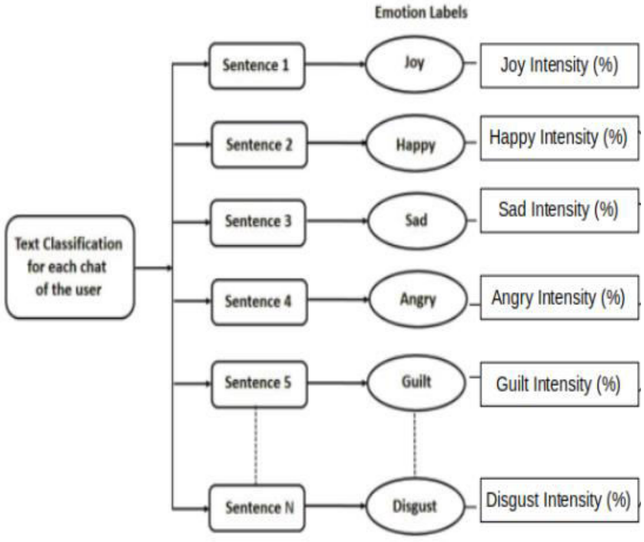


Fig 1.1: Proposed model

B. Training and Testing

We trained and tested two models. One for emotion detection and the other for chatbot. To identify the emotion from text, LSVM algorithm is deployed. And the chatbot is trained with LSTM, a deep learning algorithm.

i. *Emotion detection model*

a) Data cleansing: This process involves removing unwanted characters, converting entire text into lowercase, spelling correction, rare word removal and the removal of stopwords using NLTK.

b) Label Encoding: The emotion label corresponding to each sentence of the dataset is encoded into integer values.

c) Splitting the dataset: The dataset is split into two for training and testing in a 9:1 ratio.

d) Lemmatization: This process groups together the inflected forms of a word so they can be analysed as a single item. Word.lemmatize() function in the TextBlob package is used.

e) Forming Word Vector: Scikit-learn's CountVectorizer is used for obtaining vector representation for words. It is used to transform a given text into a vector on the basis of the frequency of each word that occurs in the entire text.

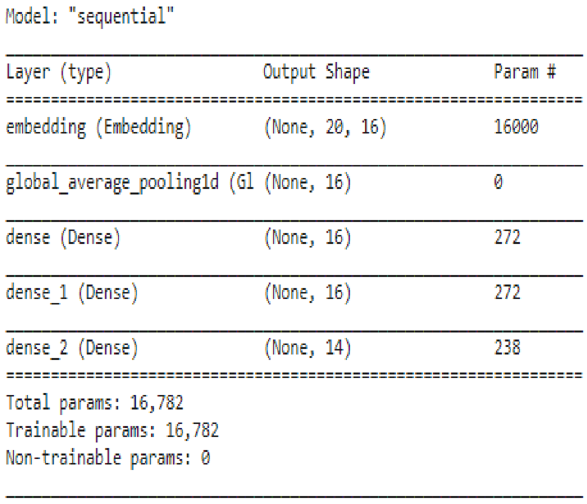
f) Training: The LSVM Model is trained with SGDClassifier followed by testing. An accuracy of 56% is obtained.

ii. Chat-Bot Model

a) Data Pre-processing: As Deep learning techniques are used for the training of the chat model, there are only few pre-processing done manually to the dataset. The collection of YAML files is converted to a single YAML file. These data are then tokenized.

b) Label Encoding: The intent corresponding to each conversation text is encoded into integer value.

c) Training: The model is trained using the LSTM model and an accuracy of 99% is achieved.



```
Model: "sequential"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
embedding (Embedding)        (None, 20, 16)            16000
_________________________________________________________________
global_average_pooling1d (Gl (None, 16)                0
_________________________________________________________________
dense (Dense)                (None, 16)                272
_________________________________________________________________
dense_1 (Dense)              (None, 16)                272
_________________________________________________________________
dense_2 (Dense)              (None, 14)                238
=================================================================
Total params: 16,782
Trainable params: 16,782
Non-trainable params: 0
_________________________________________________________________
```

Fig 1.2: Chatbot Model

C. Emotion Percentage Calculation

After the training and testing of both the model is completed, the two models are pipelined together in such a way that the users' chat input is first fed into the emotion detection model and the result is stored till the end of the chat.After this, the users' chat input goes to the chatbot model itself from where the model finds the apt reply output by calculating cosine similarity between the sentences which belongs to the same intent as the input.

The chatbot stops taking input after receiving the 'quit' command. At this stage, all the results stored by the emotion detection model are now used to calculate the percentage of each emotion.

$$Emotion\ percentage(joy) = \frac{Emotion\ count(joy)}{Total\ no.of\ chat\ sentences}$$

The calculated percentages are finally printed on the screen as output.

IV. CONCLUSION

In this paper we proposed an intelligent chatbot for detecting user's emotion and to predict whether there is an underlying mental health issue. For the purpose of analysing emotions from user's text, machine learning algorithm namely, LSVM was deployed. Furthermore, deep learning algorithm namely, LSTM was used for chatbot training.

When any type of mental health or emotional concern affects daily life and function, it is important for people to choose to seek help on their own. But most often people don't recognize if there is anything worth of a concern. The chatbot promotes a mode to make the user understand the problem that they themselves wasn't able to.

Whether AI chatbots can become a placeholder for emotional relationship with real humans is still a question but already, AI researchers and robotics are developing products for exactly this purpose, testing the limits of how much a machine can learn to mimic and respond to human emotions.

V. REFERENCES

[1] Falguni Patel, Ishita Nandwani, Riya Thakore and Santosh Kumar Bharti, "Combating Depression in Students using an Intelligent ChatBot: A Cognitive Behavioral Therapy", 2019 IEEE 16th India Council International Conference (INDICON).

[2] Seo-Hui Park, Byung-Chull Bae and Yun-Gyung Cheong, "Emotion Recognition from Text Stories Using an Emotion Embedding Model", 2020 IEEE International Conference on Big Data and Smart Computing (BigComp).

[3] Soujanya Poria, Navonil Majumder, Rada Mihalcea and Eduard Hovy, "Emotion Recognition in Conversation: Research Challenges, Datasets, and Recent Advances", 2019 IEEE Access, Vol.7.

[4] Asma Ghandeharioun, Daniel McDuff, Mary Czerwinski and Kael Rowan, "EMMA: An Emotion-Aware Wellbeing Chatbot", 2019 8th International Conference on Affective Computing and Intelligent Interaction (ACII).

[5] Kerstin Denecke, Sayan Vaaheesan and Aaganya Arulnathan, "A Mental Health Chatbot for Regulating Emotions (SERMO) - Concept and Usability Test", 2020 IEEE Transactions on Emerging Topics in Computing.

[6] Lin, Z., Xu, P., Winata, G. I., Siddique, F. B., Liu, Z., Shin, J., & Fung, P, "CAiRE: An End-to-End Empathetic Chatbot", Proceedings of the AAAI Conference on Artificial Intelligence, 2020 34(09), 13622-13623.

[7] Forbes. (2021, April 2). Opening up to a robot? How mental health tech can help patients [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2021/04/02/openi

ng-up-to-a-robot-how-mental-health-tech-can-help-patients/?sh=7a033831722c

[8] Felix A. Gers, Jürgen Schmidhuber and Fred Cummins, “Learning to Forget: Continual Prediction with LSTM”, Neural Computation, Volume: 12, Issue: 10, Oct. 1 2000.

[9] Shu-Xia Lu and Xi-Zhao Wang, “A comparison among four SVM classification methods: LSVM, NLSVM, SSVM and NSVM”, Proceedings of 2004 International Conference on Machine Learning and Cybernetics.

MF-CNN for Low Rate DDoS Attack Detection

Selma B
PG Student
Department of CSE
Sree Buddha College of Engineering
Pattoor, India
selmabasheer30@gmail.com

Reeba R
Assistant Professor
Department of CSE
Sree Buddha College of Engineering
Pattoor, India
reeba.amjith@gmail.com

***Abstract*—Distributed Denial of Service (DDoS) attacks are one of the most harmful threats in today's Internet, disrupting the availability of essential services. Among this the Low Rate DDOS(LR-DDOS) attacks are more difficult to detect due to the behaviour of attack flows which is similar to normal flows. The explosive growth of network traffic and its multitype on Internet have brought new and severe challenges to LR-DDoS attack detection. Numerous LR-DDoS attacks, which have been launched against various organizations in the last decade, have had a direct impact on both vendors and users. In recent years, LR-DDoS attacks have become more difficult to detect due to the many combinations of attack approaches. In order to combat the diversity of attack techniques, more acCcurate and more robust defence techniques are required. So here proposes a LR-DDoS attack detection method based on multi-feature fusion and convolution neural network(CNN) in resource constrained environment. This method compute a variety of network features and fuse them into a feature map, which will be used to characterize the state of the network. The system targets a practical, lightweight implementation with low processing overhead and attack detection time. It is a practical, lightweight deep learning LR-DDoS detection system, which exploits the properties of Convolutional Neural Networks (CNNs) to detect and classify traffic flows as either malicious or benign.**

***Index Terms*—DDoS Attack, LR-DDOS, DDoS Detection, Convolutional Neural Network, Feature fusion.**

I. Introduction

Distributed Denial of Service (DDoS) is a cyber attack that makes services unavailable or only partially available. It is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. Low-Rate Distributed Denial-of-Service (LR-DDoS) attacks are a new challenge to cyberspace, as the attackers send a large amount of attack packets similar to normal traffic, to throttle legitimate flows. The main goal of a LR-DDoS attack is to exhaust the network with a high volume of traffic, thus denying access to services by legitimate users. DDoS attacks have been the major threats for the Internet and can bring great loss to companies and governments. With the development of emerging technologies, such as cloud computing, Internet of things, artificial intelligence techniques, attackers can launch a huge volume of DDoS attacks with a lower cost, and it is much harder to detect and prevent DDoS attacks. Because DDoS traffic is similar to normal traffic. Numerous DDoS attacks have been launched against various organizations in the last decade, resulting in revenue losses as well as increased costs to defend the availability of services.

LR-DDoS attacks are currently the most prevalent and sophisticated threat for organizations, and are increasingly difficult to prevent. In 2018, GitHub was hit with one of the largest DDoS attacks ever. This impactful attack comes in one of the most highlighted cyber attacks of the current cyber age, shaking the ground basis of one of the pillars of the CIA security triad. Attackers use thousands of dump terminals, machines, and botnets to concurrently launch DDoS attacks that subsequently exhaust the target system main resources, making the entire services unavailable. There are a potentially extreme number of legitimate and powerful tools available, which can be abused to launch DDoS attacks on large and small scales accordingly. In another recent DDoS attack, attackers misused the legitimate Memcached tool, whose primary purpose is to reduce strain over the underlying network resources. The attacker abused Memcached objects and spoofed IP addresses, allowing Memcached responses to be directed to the target addresses with 126.9 million packets/second to largely consume target resources. Moreover, the use of spoofed IPs makes the trace-back next to impossible in DDoS attacks. Therefore, the efficient and early detection, mitigation, and prevention of DDoS attacks remain a challenging task. However, strong novel measures can be taken towards timely detection, to allow subsequent countermeasures to prevent or mitigate sophisticated DDoS attacks. There have been interest in utilizing artificial learning approaches (e.g., machine learning and deep learning techniques) to prevent or mitigate sophisticated DDoS attacks, although designing efficient and effective DDoS mitigation strategies remain an ongoing challenge.

Nowadays, LR-DDoS attacks have become so dynamic and sophisticated, in that they are launched in a variety of patterns, making it difficult for static solutions to detect. However, existing research has many problems, including the performance of the detection system, that is, the success in detecting a DDoS attack, computation cost of detection, as well as the ability to deal with large amounts of data. A new approach is therefore needed to detect DDoS attacks dynamically, to handle dynamic DDoS attack patterns and the large volume of data effectively.

Convolutional Neural Networks (CNNs), a specific DL technique, have grown in popularity in recent times leading to

major innovations in computer vision and Natural Language Processing , as well as various niche areas such as protein binding prediction, machine vibration analysis and medical signal processing. Whilst their use is still under-researched in cyber security generally, the application of CNNs has advanced the state-of-the-art in certain specific scenarios such as malware detection, code analysis, network traffic analysis and intrusion detection in industrial control systems. These successes, combined with the benefits of CNN with respect to reduced feature engineering and high detection accuracy, motivate to employ CNNs in this work.
The main contributions of this paper are:
- Here propose a new LR-DDoS attack detection method based on MF-CNN in resource constrained environment.
– The method uses a variety of network features to describe the state of the network. The calculated network eigenvalues are fused into feature maps. These feature maps are used for training CNN model and detecting LR-DDoS attack.

The remainder of this paper is structured as follows:: Sec. II details different DDoS attacks, Sec. III discusses the related work, Sec. IV explains the proposed system. Finally, the conclusion of this paper is provided in Sec. V.

II. DDoS Attacks

DDoS attacks aim to decrease the availability of service by exhausting the network or computational resources available for traffic or computation and thus preventing the legitimate users from accessing their services. There are many techniques to launch a DDoS attack such as the following:

A. UDP flood attack

In the User Datagram Protocol (UDP), unlike in the Transmission Control Protocol (TCP), the packet is sent directly to the target server without any handshake. The attacker uses this protocol property to send a large volume of traffic and thus exhausts the network resources of the target server.

B. SYN flood

The connection in TCP protocol is established after the three-way handshake process in which the server and client exchange synchronize (SYN) and acknowledge (ACK) messages. The SYN attack happens when a client responds to the server with an incorrect ACK message with a spoofed IP address. The server replies to wrong IP address SYN message and waits to get a reply back from the client. This wait time makes the connection open for some time causing the server resource to be unavailable.

C. Ping of Death

Ping Of Death (POD) is an old version of ICMP ping flood attack. The IP protocol has a maximum packet size, to be sent between two devices, which is 65,535 bytes for IPv4. Using a simple ping command to send malformed or oversized packets can have a severe impact on an unpatched system.

D. Denial of sleep attack

In wireless sensor nodes, the Media Access Control (MAC) layer protocol plays an essential role in controlling and saving the power consumption. Denial of sleep attack occurs when the attacker has obtained information about MAC protocol, which allows bypassing the authentication and the encryption protocols.

III. LR-DDOS attack

LR-DDoS attacks are hard to detect since they have the same characteristics as legitimate traffic and are hidden in background traffic. Attacks are launched through a single attack source and its average rate is low enough, so the number of packets sent is very small and challenging to detect. Thus, common DDoS attack detection mechanisms are not effective in detecting LR-DDoS attacks.

IV. RELATED WORK

DDoS detection and mitigation techniques have been explored by the network research community since the first reported DDoS attack incident in 1999. In this section, the DDoS detection techniques based on different approaches, with a specific focus on deep learning techniques were reviewed and discussed.

A. CPSS LR-DDoS Detection and Defense in Edge Computing

Existing intrusion detection and defense models for Cyber-Physical Social Systems (CPSS) rely on the analysis of static intrusion characteristics, which cannot effectively detect Low-Rate Denial-of-Service (LRDDoS) attacks on large scale, especially in the edge environment. Liu et al. [7] explained the development of a novel hybrid defense and intrusion detection method for the previous CPSS LR DDoS scenario in a fringe environment using the location-sensitive feature extraction and the Deep Convolutional Neural Network (DCNN) to automatically learn the optimal value properties of the original data Distribution and implements profound learning Q Network as a powerful decision maker to defend against attacks. The experimental results in the detection phase show that the proposed method can differentiate abnormal network attack streams with higher detection accuracy and faster response time than the Support Vector Machine (SVM), K-means and K-means types. Surface Learning Neural Network etc. a certain detection rate for new unknown attacks, which means that the method is efficient and suitable for the real network environment. Experimental results in the defense phase show that LR DDoS attacks can be defended without any problems.

B. Deep Cnn Ensemble SDN Framework

In a Flow-based benchmark dataset, which solely reflects software-defined networks, Haider et al.[8] suggests a novel approach to using DL-based ensemble and hybrid approaches to detect large-scale DDoS attacks. This proposed paradigm leverages novel CNN ensemble models for enhanced Flow-based data detection. To add to the issue of the most prevalent and advanced DDoS attack detection in SDNs, they implemented an effective and scalable deep CNN ensemble architecture. On a flow-based SDN dataset, the architecture was tested with benchmark deep learning sets and hybrid state-of-the-art algorithms. The proposed algorithm shows improvements in both the accuracy of detection and the complexity of computing. Finally, they endorse varied deep learning ensemble based detection and prevention mechanisms for the emerging large-scale distributed networks.

C. DeepDefense: Deep Learning based Approach

Xiaoyong et al.[9] suggested a DDoS attack detection method focused on deep learning called Deep Defense. The deep learning method will automatically extract the high-level features from the low-level ones and get powerful representation and inference. To learn patterns from network traffic sequences and track network attack events, they developed a recurrent deep neural network. Compared to traditional machine learning models, the experimental findings show better model efficiency. With a broad dataset, they train deep learning models to solve complicated recognition issues. Different neural network models are used by Deep Defense: Convolutionary Neural Network (CNN), Recurrent Neural Network, Long Short-Term Memory Neural Network (LSTM) and Gated Recurrent Neural Network Unit (GRU). These methods are proved to greatly improve the performance in many domains when training large data sets. They reduce the error rate from 7.517% to 2.103% compared with conventional machine learning method in the larger data set.

D. DDoS Detection and defense based on deep learning

Chuanhuang et al[10] introduced a new DDoS attack detection model and defense system based on emerging deep learning technology in the Software Defined Network environment. The model can learn patterns in a historical way from sequences of network traffic and trace network attack activities. Through using the model-based protection framework, the DDoS attack traffic in the Software Specified Network can be cleaned efficiently. The experimental results demonstrate the much better performance of this model compared with conventional ways. It also decreases the degree of environmental dependency, makes it easier to upgrade the detection system in real time, and reduces the complexity of updating or modifying the detection strategy.

E. TCP-based Detection in Cloud Computing Data Centers

Cloud computing data centers have become one of the most important infrastructures in the era of big data. When considering data center security, one of the most serious issues is Distributed Denial of Service (DDoS) attacks[11]. This takes into account DDoS attacks that use TCP traffic, which is increasingly common but difficult to detect. Two attack modes are defined to detect DDoS attacks: fixed source IP attacks (FSIA) and random source IP attacks (RSIA), based on the source IP address that attackers use.The TCP-based DDoS detection approach, which extracts efficient TCP traffic characteristics and distinguishes malicious traffic from normal traffic by two decision tree classifiers, is also proposed here. Using a virtual dataset and actual datasets, including the ISCX IDS dataset, the CAIDA DDoS Attack 2007 dataset, and a Baidu Cloud Computing Platform dataset, the proposed solution is evaluated. Experimental results show that the proposed approach can achieve attack detection rate higher than 99% with a false alarm rate less than 1%. This approach were implemented in the DDoS defense system of Baidu's cloud computing data center.

F. Semi-Supervised K-means Detection Algorithm Using Hybrid Feature Selection Method

An attempt to make an online service inaccessible by flooding it with traffic from multiple sources is a distributed denial of service (DDoS) attack. There are some drawbacks to the current againt ddos attack schemes, including that supervised learning methods require large numbers of labeled data and relatively low detection rate and high false positive rate of unsupervised learning algorithms. They suggested a semi-supervised method of weighted k-means detection in order to resolve these problems. Gu et al.[12] proposed a hybrid feature selection algorithm based on Hadoop to find the most efficient feature sets and suggest an enhanced initial cluster center selection algorithm based on density to solve the problem of outliers and optimal place. Using hybrid feature selection (SKM-HFS) to detect attacks, they include the Semi Monitored K-means algorithm. The results of their experiments shown that in terms of detection efficiency and order preference technique, the proposed approach exceeds the benchmark by similarity to an ideal solution (TOPSIS) evaluation factor.

G. Detection Based on Improved KNN With the Degree of DDoS Attack in SDN

The emerging networking in Software Defined Networks provides a new way to reconsider the defense against DDoS attacks. Dong et al.[13] proposed two methods to detect the DDoS attack in SDN. The degree of DDoS attack to classify the DDoS attack is adopted by one process. The other approach uses the enhanced Machine Learning (ML)-based K-Nearest Neighbors (KNN) algorithm to discover the DDoS attack. Here they have proposed four features (called flow length, flow duration, flow size, and flow ratio) in order to evaluate the DDoS attack detection performance when the SDN controller is attacked by the DDoS attack. A new concept called the degree of attack is proposed to detect the DDoS attack was also introduced. A detection algorithm based on the degree of the attack (called DDADA) was proposed based on this concept. And also inorder to further improve the detection efficiency, another detection algorithm based on machine learning (called DDAML) was introduced to identify the DDoS attack.

H. A Hybrid Deep Learning based Model for Anomaly Detection in Cloud Datacentre Networks

Garg[14] proposed a hybrid data processing model for network anomaly detection is proposed that leverages Grey

Wolf Optimization (GWO) and Convolutional Neural Network (CNN). This work presents a robust hybrid model for network anomaly detection in cloud environments, particularly for streaming data. The model leverages the advantages of multiobjective optimization and deep learning, particularly for feature extraction and anomaly detection on real-time network traffic streams. For this purpose, two computationally efficient techniques were employed namely-GWO and CNN. The amalgamation of these techniques is further improved by revamping their respective standard strategies. For instance, GWO is improvised with respect to enhance initial population, exploration and exploitation capabilities, while CNN is modified in terms of dropout layer functionality. Additionally, the proposed hybrid model was extensively evaluated on benchmark and synthetic datasets. But the inherent complexity in the cloud environment is induced due to the heterogeneity of incoming traffic and underlying hardware; which makes the task of anomaly detection more cumbersome.

I. DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark

Alsirhani et al.[15] proposed a dynamic DDoS attack detection system based on three main components: classification algorithms, a distributed system, and a fuzzy logic system. Their framework uses fuzzy logic to dynamically select an algorithm from a set of prepared classification algorithms that detect different DDoS patterns. Out of the many candidate classification algorithms, they use Naive Bayes, Decision Tree (Entropy), Decision Tree (Gini), and Random Forest as candidate algorithms. Their results show that there is a tradeoff between the precision of the classification algorithms used and their delays. In this case, this is not always the case, because the model training times are inversely proportional to the number of nodes in the Spark cluster. The fuzzy logic system, on the other hand, can efficiently select the right classification algorithm from among the others at the right time.

J. Learning Multilevel Auto-encoders for DDoS Attack Detection in Smart Grid Network

Ali, S et.al[16] proposed an efficient DDoS attack detection technique based on multilevel auto-encoder based feature learning. They learned multiple levels of shallow and deep autoencoders in an unsupervised manner which are then used to encode the training and test data for feature generation. A final unified detection model is then learned by combining the multilevel features using and efficient Multiple Kernel Learning (MKL) algorithm. The overall system is targeted towards more accurate and more efficient DDoS attack detection in the smart grid network. The algorithm exploits both shallow and deep auto-encoders for learning powerful features in an unsupervised manner. Features from multilevel auto-encoders are combined using Multiple Kernel Learning (MKL) that automatically learns the weights of the features in the ensemble. Experiments are performed on two benchmark DDoS attack detection databases (and their subsets) and the results are compared with six state-of-the art methods. Our results show that the proposed method outperforms the compared methods in terms of accuracy and simplicity.

V. PROPOSED SYSTEM

This paper introduce a new architecture for Low Rate DDoS attack detection and mitigation in an emerging paradigm called SDN environment using deep learning technique. CNN encapsulates the learning of malicious activity from the network traffic to enable the identification of DDoS patterns regardless of their temporal positioning. This is a fundamental benefit of CNN to produce the same output regardless of where a pattern appears in the input. This encapsulation and learning of features while training the model removes the need for excessive feature engineering, ranking and selection. To support an online attack detection system, here use a novel preprocessing method for the network traffic that generates a spatial data representation which is subjected to feature fusion and the resultant feature maps is used as the input to the CNN.

In deep learning, CNN is a feed-forward neural network that contains a complex arrangement of cells interconnected by a relation inspired from the organization of the animal visual cortex. It is a classic algorithm which is widely used in image recognition and image classification. The basic idea behind this model is that here extract multiple features from network traffic with a network traffic preprocessing algorithm and then fuse them into feature maps. Based on the feature maps, here build a CNN model to detect LR-DDoS attack. The architecture of the proposed method is shown in Fig.1

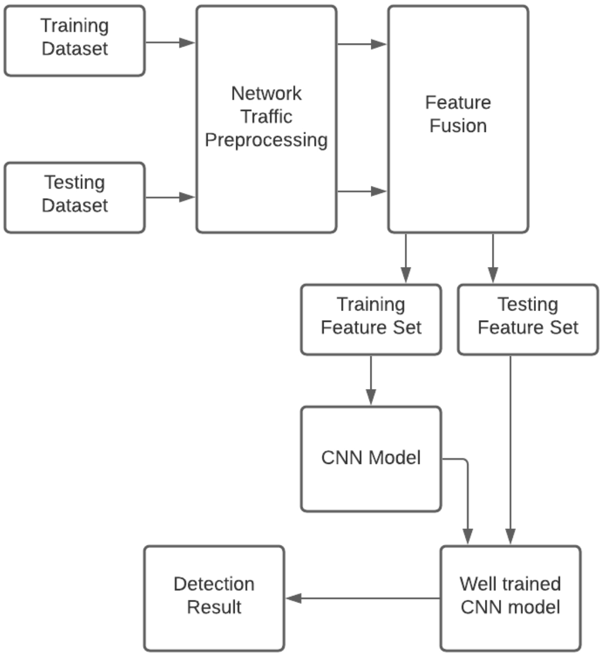


Fig. 1. Proposed architecture

A. Input data

Input is the network traffic data. The network traffic comprised of data flows between the end points. The network traffic data is divided into two as training data and testing data. The training data is used to train the CNN model. Training contains both attacked data and non-attacked data. Training data and testing data are converted into corresponding feature maps by feature extraction and feature fusion. During the stage of training the CNN model, model acquires the ability to identify LR-DDoS attack by learning and remembering feature maps of training data. In the detection of LR-DDoS attack stage, the well-trained CNN model classifies the feature maps of testing data. Shaping the input data in this manner allows the CNN to learn the characteristics of LR-DDoS attacks and benign traffic through the convolutional filters sliding over such input to identify salient patterns.

B. Network Traffic preprocessing

For preprocessing, here an algorithm is used called Network Traffic Preprocessing Algorithm that converts the traffic flows extracted from the network traffic traces of a dataset into array-like data structures and splits them into sub-flows based on the time windows. The input to the algorithm are network traffic trace, flow-level labels, time window and maximum packets/sample.

C. Feature Extraction

From the given a traffic trace file of the dataset and the pre-defined time window of length t seconds, the algorithm collects all the packets from the file with capture time between t0, the capture time of the first packet, and time t0 + t. From each packet, the algorithm extracts 11 attributes. The more accurate and precise attributes for the generalization of model are selected. Others are excluded intuitively.

D. Data processing

Here the traffic is collected for a particular amount of time before it being sent to the anomaly detection algorithm. Without the knowledge of theIR whole life, such algorithms must base their decisions on portions of traffic flows. To simulate this process, the attributes of the packets belonging to the same bi-directional traffic flow are grouped in a chronological order to form an example of shape [n, f], where f is the number of features (11) and n is the maximum number of packets the parsing process collects for each flow within the time window. t and n are hyper-parameters for the CNN model. Flows longer than n are truncated, while shorter flows are zero-padded at the end during the next stage after normalization. The same operations are repeated for the packets within time window [t0+t, t0+2t] and so on, until the end of the file. The output of this process is a bi-dimensional array of samples. The row of array represents the samples whose packets have been captured in the same time window, while the column represents the samples whose packets belong to the same bi-directional flow.

E. Normalization

Normalization is a scaling technique in which values are shifted and rescaled without distorting differences in the ranges of values or losing information. Here each attribute value is normalized to a [0, 1] scale.

F. Padding

Padding is the process of adding extra values outside of it. Here the data is zero-padded so that each sample is of fixed length n, since having samples of fixed length is a requirement for a CNN to be able to learn over a full sample set.

G. Feature Fusion

Feature fusion is the process of converting a feature matrix obtained into the image data. The advantage of the feature fusion is obvious. Different feature vectors that are extracted from the same pattern always reflects the different characteristic of patterns. By optimizing and combining these features, it not only keeps the effective discriminant information of multi-feature, but also eliminates the redundant information to certain degree. This is especially important to classification and recognition process. There are the two existing feature fusion methods. One is to group two sets of feature vectors into one union-vector , and then to extract features in the higher-dimension real vector space. Another one is to combine two sets of feature vectors by a complex vector, and then to extract features in the complex vector space. Both feature fusion methods can increase the recognition rate, the feature fusion method based on the union-vector is referred as serial feature fusion and the one based on the complex vector is called parallel feature fusion.

Feature fusion helps to fully learn the features of image for description of their rich internal information. It integrates the related information extracted from a group of Training and Testing data without losing any information. Network traffic is also called as data traffic which is the amount of data moving across the network at any given amount of time. The data traffic is broken down into different data packets that are sent over a network before being reassembled by the destination device. The network traffic is divided into several detection windows, and each detection window can obtain a feature matrix by feature extraction. Feature matrix is the n-dimensional array or matrix of features. The feature matrix is processed to get the feature maps. The obtained feature maps are the input to the CNN model. The feature maps of the normal traffic is different from the feature maps with LR-DDoS attack.

H. Convolutional Neural Network

Convolutional neural network (CNN) is a class of Deep Neural Networks in deep learning that is commonly applied to computer vision and natural language processing. CNN is a class of neural network that allows greater extraction of features from the captured input data. Unlike classical models, CNNs can take image data, train the model, and then classify the features automatically for healthier level classification.

CNNs are used in many applications like image recognition, face recognition, and video analysis. CNN performs two basic operations, namely convolution and pooling. The convolution operation using multiple filters which is able to extract features called feature maps from the given dataset, through which their corresponding spatial information can be preserved. The pooling operation, also called subsampling, is used to reduce the dimensionality of feature maps from the convolution operation. The pooling operations are max pooling, min pooling and average pooling. Max pooling and average pooling are the most common pooling operations used in CNN. The structure of a CNN model consist of input layer, convolution layer, pooling layer, full-connection layer and the output layer.

Input layer: The original image data is processed in the input layer.

Convolution layer: The convolution layer is used to convolute the input image data. CNN model has one or more convolution layers, each of which consist of several convolution planes. Each convolution plane contains a group of convolution units. A convolution plane is also called a channel. Convolution unit performs linear weighting operation on the input data through the activation function. The local perception and weight sharing mechanism are the biggest difference between CNN model and ordinary neural networks. Local perception means that the picture information has the local similarity. Based on the principle of local perception, the input data of each convolution unit is only part of the image data. The input data size of the convolution unit is determined by the convolution kernel. The convolution kernel is a set of weights. The size of convolution kernel mainly includes 5×5 and 7×7. All convolution units in a convolution plane share a convolution kernel is called weight sharing.

Pooling layer: The pooling layer is used to reduce the data size and improve the over-fitting problem. Pooling methods include max pooling, mean pooling and average pooling.

Full-connection layer: The fully-connection layer consists of a series of neurons. It plays the role of classifier in the CNN model.

Output layer: This layer outputs the final classification results. A neuron in the output layer corresponds to a classification type. Each neuron outputs a probability value representing the score of the corresponding category. Finally, the model selects the category with the highest score as the result of the classification.

The method consists of two stages such as building of CNN model and attack classification.

VI. CNN Model Training

The training of CNN model consist of two stages ; forward propagation stage and backward propagation stage. In the forward propagation stage, the CNN model calculates the actual classification results of samples. In the backward propagation stage, the CNN model adjusts the convolution kernel weights by calculating the error rate of classification results. The error calculation function includes mean square error function, logarithmic likelihood error function and crossentropy function. In this paper, the mean square error function is used to train the parameters of CNN model.

The CNN model parameters are;

A. Activation function

The activation function is used for feature mapping of image data in convolution unit. The closer the output is to 1, the stronger the image data feature of the corresponding region is, and the closer the output is to 0, the weaker the image data feature of the corresponding region is. The full-connected layer and the output layer also contain activation function, which is mainly used for non-linear mapping of data. Activation functions include Sigmoid, ReLU and Tanh.

B. Learning rate

It is used to control the learning progress of the model during the training process. The learning rate includes fixed learning rate and variable learning rate. Fixed learning rate is simple to implement, but it tends to cause slow convergence of the model. Therefore, the CNN model constructed in this paper uses a variable learning rate. The variable learning rate can be adaptively reduced during the training process to accelerate the convergence speed of the model and get the optimal detection model.

C. Number of iteration

It represents the number of training the model needs. Each iteration will modify the weight to improve the classification ability of the model.

VII. Construction of CNN model

The CNN model consists of one input layer, two convolution layers, two pooling layers, two full-connection layers and one output layer. The input layer is a 28×28 feature map. In the first convolution layer, it includes 6 convolution planes and the size of convolution kernel is 5×5. In the second convolution layer, it includes sixteen convolution planes and the size of convolution kernel is 5×5. Convolution kernel uses Rectified Linear Unit function as activation function. The pooling horizon of the pooling layer is 2×2, and the max pooling mode is used. In the full-connection layers, the number of neuron in the first layer is 120, and the number of neuron in the second layer is 84. The output layer consists of two output nodes, which represent attacked and non-attacked respectively. The Sigmoid activation function is used for both the fullconnection layers and the output layer.

A sample data sequence over a period of time is referred to as Detection window (DW). A DW can be equally divided into several segments is termed as Data slice(DS). Each segment is called a data slice.

In this method, the DW is the detection unit and the DS is the feature calculation unit. One DW contains several DSs. One DS extracts network traffic eigenvalues and forms a feature vector. Therefore, One DW forms a feature matrix. Feature matrix is used to generate feature map by feature fusion.

The detection algorithm consists of two parts: the training of CNN model and the detection of LR-DDoS attack.

The construction of CNN model is performed by inputting the training data, sampling interval, size of DW, size of DS, and number of iterations. Then the splitting of training data is performed in the data is divided into several DWs by the size of DW, and is divided into several DSs by the size of DS. This is followed by Calculating the eigenvalues of each DS and generating the feature maps of each DW. With these feature maps training of the CNN model is performed. This is repeatedly done in a loop and will exit from the loop when the current number of training has reached the preset number of iteration. If so, training program will exit.

VIII. Detection of LR-DDoS Attack

Procedure for detection algorithm are;

Step 1: The detection algorithm takes sampling interval, the size of detection window, the size of data slice, and the end condition as the input.
Step 2: Then obtaining the detection data of a detection window in real time.
Step 3: Dividing the detection data into several data slices by the size of data slice.
Step 4: Calculating the eigenvalues of each data slice.
Step 5: Generating a feature map of the current detection window.
Step 6: Inputting the feature map into the CNN model.
Step 7: Outputting the detection result.
Step 8: Judging the end condition.
If the condition is met, the detection program will exit. Otherwise, return to the step 2 and continue to detect network traffic.

IX. LR-DDoS Classification

The nput to the fully-connected layer of CNN is of the same size, and the output layer has a sole node. This output is passed to the sigmoid activation function such that. This constrains the activation to a value of between 0 and 1, hence returning the probability, p[0, 1] of a given flow being a malicious DDoS attack. The flow is classified as LR-DDoS when p greater than 0.5, and benign otherwise.

X. Conclusion

The challenge of DDoS attacks continues to undermine the availability of networks globally. This paper proposed a CNN-based DDoS detection architecture based on feature fusion. The design has targeted a practical, lightweight implementation with low processing overhead and attack detection time. The benefit of the CNN model is to remove threshold configuration as required by statistical detection approaches, and reduce feature engineering and the reliance on human experts required by alternative ML techniques. This enables practical deployment. The proposed method calculates 17 kinds of characteristics of network traffic and fuses them into feature maps, which representing the state of the network. In order to detect network anomalies, here construct an eight-layer CNN model to classify network traffic. The generated feature maps will be used as input data of CNN model to train the model and detect the LR-DDoS attackS.

XI. Acknowledgement

This research was supported by Dr. K Krishnakumar, the head of the institution. We would also like to show gratitude to the head of our institution, Dr. S.V. Annlin Jeba for sharing her pearls of wisdom with us during the course of research. We thank our colleagues from Sree Buddha College Of Engineering who provided insight and expertise that greatly assisted us although they may not agree with all of the interpretations and conclusion of the paper.

References

[1] Liu, Z., Yin, X., Hu, Y. (2020). ”CPSS LR-DDoS Detection and Defense in Edge Computing Utilizing DCNN Q-Learning”. IEEE

[2] Haider, S., Akhunzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Choo, K.-K. R., Iqbal, J. (2020). ”A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks”. IEEE Access, 1–1.

[3] Yuan, X., Li, C., Li, X. (2017). ”DeepDefense: Identifying DDoS Attack via Deep Learning”. 2017 IEEE International Conference on Smart Computing (SMARTCOMP).

[4] Bhardwaj, A., Mangat, V., Vig, R. (2020). Hyperband Tuned Deep Neural Network With Well Posed Stacked Sparse AutoEncoder for Detection of DDoS Attacks in Cloud. IEEE Access, 8, 181916–181929. doi:10.1109/access.2020.3028690

[5] Ali, A., Yousaf, M. M. (2020). Novel Three-Tier Intrusion Detection and Prevention System in Software Defined Network. IEEE Access, 8, 109662–109676. doi:10.1109/access.2020.3002333

[6] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, “Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN,” Future Gener. Comput. Syst., vol. 111, pp. 763–779, Oct. 2020.

[7] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, “Autoencoder-based feature learning for cyber security applications,” in Proc. Int. Joint Conf. Neural Netw. (IJCNN), May 2017, pp. 3854–3861.

[8] M. Wang, Y. Lu, and J. Qin, “A dynamic MLP-based DDoS attack detection method using feature selection and feedback,” Comput. Secur., vol. 88, Jan. 2020, Art. no. 101645.

[9] Li, C., Wu, Y., Yuan, X., Sun, Z., Wang, W., Li, X., Gong, L. (2018). ”Detection and defense of DDoS attack-based on deep learning in OpenFlow-based SDN”. International Journal of Communication Systems, 31(5), e3497.

[10] Jiao, J., Ye, B., Zhao, Y., Stones, R. J., Wang, G., Liu, X., … Xie, G. (2017). ”Detecting TCP-Based DDoS Attacks in Baidu Cloud Computing Data Centers”. 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS).

[11] Gu, Y., Li, K., Guo, Z., Wang, Y. (2019). ”Semi-supervised K-means DDoS Detection Method Using Hybrid Feature Selection Algorithm”. IEEE Access, 1–1.

[12] Dong, S., Sarem, M. (2020). ”DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks”. IEEE Access, 8, 5039–5048.

[13] Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y., Ranjan, R. (2019). A Hybrid Deep Learning based Model for Anomaly Detection in Cloud Datacentre Networks. IEEE Transactions on Network and Service Management, 1–1.

[14] Alsirhani, A., Sampalli, S., Bodorik, P. (2019). DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark. IEEE Transactions on Network and Service Management, 1–1.

[15] li, S., Li, Y. (2019). Learning Multilevel Auto-encoders for DDoS Attack Detection in Smart Grid Network. IEEE Access, 1–1. doi:10.1109/access.2019.2933304

NOVEL FEATURE OF COMPUTER SECURITY OVER ENCRYPTED CLOUD DATA

Renu Sara Thomas
Student, Dept of CSE
Sree Buddha College of
Engineering, Pattoor
Pattoor , India
renusaramannil@gmail.com

Minu Lalitha Madhavu
Ass.Professor ,Dept. of CSE
Sree Buddha College of
Engineering, Pattoor
Pattoor, India
minulalitha@gmail.com

Abstract— **Encrypted technology is Encoded search innovation has been concentrated broadly lately. For that here methods called NLP (Natural Language Processing) and AES (Advanced Encryption Standard) are used. It helps to increase the search accuracy and security in search. With to an ever increasing extent data being put away in cloud, making records with free catchphrases has brought about tremendous capacity cost and low pursuit exactness, which has become a critical issueto be tackled. Subsequently, some scientists propose a component coordinating with positioned search instrument (FMRSM) for encoded cloud information. But there arises some problems like accuracy and security. In this security in search is not provided. For that here methods called NLP (Natural Language Processing) and AES (Advanced Encryption Standard) are used. It helps to increase the search accuracy and security in search.Through this method search can be protected.**

Keywords— ***NLP , AES ,FMRSM, VSSE, SSARES***

I. INTRODUCTION

Data security is a protective digital privacy measures that is applied to prevent unauthorized access to computers, databases and websites. Data security protects data from corruption. Information security is a basic viewpoint of IT for organizations of each estimate and type. Data security is also known as information security (IS) or computer security. Storage in cloud has resulted in enormous storage cost and low search accuracy, which has become an urgent problem to be solved. NLP(natural language processing) based Indexing for accurate keyword selection. A network server based mechanism for security of data's inside network. User side data security for end to end transfer. NLP and AES are two technologies that is used here.

II. RELATED WORKS

The paper "Verifiable Symmetric Searchable Encryption For Semi-honest-but-curious Cloud Servers "[1] discuss about how to mediate the conflicts between data usability and data privacy in today's world. This put forward the first verifiable SSE scheme . Also if offers data privacy, verifiable searchability and efficiency. VSSE scheme composes of five algorithms. They are : .Keygen, pre-process ,querygen , search, verify . VSSE is a promising solution to mediate the conflicts between data usability and data privacy.

The paper "Privacy Preserving Keyword Searches on Remote Encrypted Data" [2] briefs about a problem and the problem is : user U wants to store his files in an encrypted form on a remote file server. The file server is V. Later the user U wants to efficiently retrieve some of the encrypted files containing specific keywords. It is free of encryption method. No public-key cryptosystem is required in the solution scheme only pseudo-random functions are used. For completeness they define pseudo-random permutations and functions for this.

The paper "Practical Techniques for Searches on Encrypted Data" [3] briefs about storage servers. It is desirable to store data on data storage servers. Storage servers like mail servers and file servers in encrypted form and it is for reduce security and privacy risks. The new technique have some features. The technique is probably secure . These schemes are efficient and practical. Advantages of this method is they are provably secure, they support controlled and hidden search and query isolation they are simple and fast .

The paper "SSARES: Secure Searchable Automated Remote Email Storage" [4] briefs about the increasing centralization of networked services had places user data at considerable risk. Secure Searchable Automated Remote Email Storage (SSARES) helps to address this problem. Email "at rest" (stored on the server) remains at risk. SSARES contains three major components. The first two components handle the encryption The third component handles the composition and issuance. SSARES helps improve the security of server–side email storage. The paper "Privacy-Enhanced Searches Using Encrypted Bloom Filter" [5] is often necessary for two or more parties that do not fully trust each other to share data selectively. Proposed a search scheme based on Bloom filters and group ciphers . The actual document retrieval can be a crucial feature .It is about total system design: by seeing which documents are actually retrieved. Here described a scheme for protected searches among mutually suspicious parties. It doesn't need a trusted intermediary. This technology provides an efficient scheme for performing such searches.

III. PROPOSED SYSTEM

A. METHODOLOGY

NLP (Natural Language Processing) based Indexing for accurate keyword selection. A network server based mechanism for security of data's inside network. User side data security for end to end transfer . By using these technologies the existing flaws in this field like search accuracy and search in keyword selection. All the encrypted words and those keywords that are encrypted after finding the accurate keyword using NLP is stored in cloud server.

B. SYSTEM IMPLEMENTATION

In many existing systems the words are extracted from the document can't predict the proper accuracy of the keywords. Normally when we search for something it won't give meaningful keyword but also unwanted or bad keywords too. The accuracy of words are so poor. But this proposed method extracts only meaningful words and provide higher accuracy. Many NLP's are present in stanford datasets like human trafficking NLP . That system already classified words into good ,bad and neutral. When we apply such NLP's we get the keywords with higher accuracy. If any bad words like words from sexual harassment NLP is used then it detects that the word is from that NLP which is classified as bad. Then the user gets only standard or good words.It is given to cloud server and it contains encrypted data and indexing. In this way the search accuracy can be done.

Security to the keywords that we are searched. Google stores keywords that we uses to search and with this it ranks the keywords. Encrypt the keyword and decrypt it at the server it prevents the hackers who tries to find out about our searches using these keywords. When the user is given some keyword for searching first then the keyword is encrypted using AES. Then give that encrypted word to cloud server. In cloud server there present encrypted data and indexing. The keywords are divided into 3 parts A,B,C.

Keyword encryption with XOR operation for securing keywords from access by public domains. By diving the encrypted keyword and keep it like keyword A, keyword B and keyword C we can make the word protected. For encryption AES is used. In this way the recipient or the person which whom the sender wants these messages to receive. By applying this technique nobody can understand or find out what exactly the user searched and what about the user searched. In this way the keywords that we searched can be protected.

It consists of data user ,data owner and cloud server. It have different functionalities and uses. Information Proprietor register the clients and circulate username and secret key so they can login and get to files..Then transferring the vital records into the cloud worker. Computing rank scores of the watchwords in the documents utilizing different measurable methods and store in the data set. Then comes the data user . The client will sign into the application through the username request of the position score of the specific catchphrase. The client can choose the necessary documents that from the rundown. Finally the cloud server that stores all the datas . Here the NLP searched data and AES encrypted data. Actually it contains all kinds of data or information that a user needs.

In this way we get only meaningful words or meaningful search results that are not bad or abusive. Other case that is present Today different mechsanisms give results that contains both good ,bad and neutral words. Words can be of any type and it creates some problem in result. According to this method the user only gets useful and meaningful results for the user's query. The advantages of the system is that we get accurate search result and no interruption or others can't get any idea about what we searched.

The Figure .1 represents the structure of proposed system. If user selects using a keyword then the keyword is encrypted using AES algorithm. This algorithm encrypts data. The data is divided into 3 keywords. Then the encrypted keyword is stored in cloud server. If we search for a word then the keyword is checked using the NLP present. Through this way only accurate keyword is encrypted and stored in cloud server. Therefore when a user search for a keyword then only accurate keyword is provided as result and nobody will get any idea about what actually the user searched and what the exact keyword is. The stored data will get within seconds and nobody can hack our system by finding keywords. NLP and AES provides safety and security in data search and data safety.

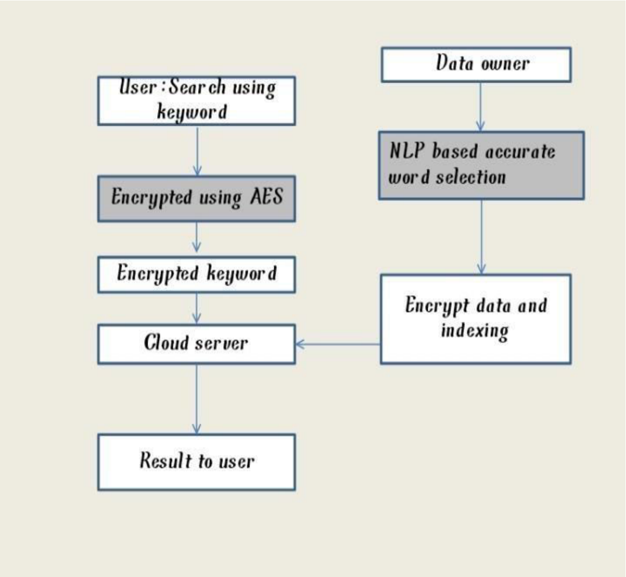

User :Search using keyword
Encrypted using AES
Encrypted keyword
Cloud server
Result to user
Data owner
NLP based accurate word selection
Encrypt data and indexing

Fig 1: Proposed System

IV. CONCLUSION

Theoretically this proposed system provides high search accuracy from bad words or that have bad meaning and save storage cost. It also reduce index dimension .It's efficiency of encryption can be improved ,it reduces the risk of keyword recognition. Storage cost of indexes can be reduced It is more feasible and effective.

REFERENCES

[1]. Q. Chai and G. Gong, ''Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers,'' in Proc. IEEE Int. Conf. Commun.(ICC), Ottawa, ON, Canada, Jun.2012, pp. 917–922.

[2]. Y. Chang and M. Mitzenmacher, ''Privacy preserving keyword searches on remote encrypted data,'' in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.,vol. 5. Berlin, Germany:Springer, 2005, pp. 442–455.

[3]. D. X. Song, D. Wagner, and A. Perrig, ''Practical techniques for searches on encrypted data,'' in Proc. IEEE Symp. Secur. Privacy (S&amp;P), Berkeley,CA, USA, May 2000, pp. 44–55.

[4]. A. J. Aviv, M. E. Locasto, S. Potter, and A. D. Keromytis, ''SSARES: Secure searchable automated remote email storage ,'' in Proc. 23rd Annu. Comput. Secur. Appl. Conf. (ACSAC), Miami Beach, FL, USA, Dec. 2007, pp. 129–139. storage,'' in Proc. 23rd Annu. Comput. Secur. Appl. Conf. (ACSAC), Miami Beach, FL, USA, Dec. 2007, pp. 129–139.

[5]. S. M. Bellovin and W. R. Cheswick, ''Privacy-enhanced searches using encrypted Bloom filters,'' IACR Cryptol. ePrint Arch., Tech. Rep., 2004, vol. 22.

[6] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, ''Enabling personalized search over encrypted outsourced data with efficiency improvement,'' IEEE Trans. Parallel Distrib. Syst.,vol. 27, no. 9, Sep. 2016, pp. 2546–2559.

[7]. Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, ''Enabling personalized search over encrypted outsourced data with efficiency improvement,'' IEEE Trans. Parallel Distrib. Syst.,vol. 27, no. 9, Sep. 2016, pp. 2546–2559.

[8]. Z. Fu, X. Sun, Z. Xia, L. Zhou, and J. Shu, ''Multi-keyword ranked search supporting synonym query over encrypted data in cloud computing,'' in Proc. IEEE 32nd Int. Perform. Comput. Commun. Conf. (IPCCC), San Diego, CA, USA, Dec. 2013, pp. 1–8.

[9]. H. Yin, Z. Qin, J. Zhang, W. Li, L. Ou, Y. Hu, and K. Li, ''Secure conjunctive multi-keyword search for multiple data owners in cloud computing,'' in Proc. IEEE 22nd Int. Conf. Parellel Distrib. Syst. (ICPADS), Wuhan, China, Dec. 2016, pp. 276–286.

[10]. Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, ''Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement ,'' IEEE Trans . Inf . Forensics Security,vol.11,no.12, Dec 2016, pp. 2716-2716.

MedBot:AI Powered Virtual Doctor

1st Aiswarya Prabhalan
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

2nd Bini Abraham
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

3rd Jisha Saji
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

4th Kevin Jacob Biju
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

5th Reshmi S
Assistant professor
Dept. of CSE
Sree Buddha College of Engineering
Alappuzha, India

***Abstract*—Nowadays, due to the busy-scheduled life people forget to take suitable measures to maintain their health and are less aware of their health status. Most people including the working section of the society claims that their hectic schedule gives them no time for periodic medical check-ups. Moreover, it is very difficult to get the consultation with the doctor in case of any health issues. Thus, the proposed system is to create an alternative for this conventional method. Medical chatbots have a high impact on the health culture of the state. It can improve reliability and is less prone to human errors. People can communicate with the chatbot just like they would with another human, and the chatbot will identify the user's symptoms and, as a result, diagnose the condition through a series of questions.This approach can be very useful in doing check-ups, making individuals aware of their health state, and encouraging them to take the necessary precautions to stay healthy.The main objective of the system is to have the importance of health in life reach out to people.**

***Index Terms*—Artificial Intelligence, Chatbot, Disease Prediction, CNN**

I. Introduction

A chatbot is an Artificial Intelligence (AI) software that is commonly referred to as one of the most advanced and promising ways of human-machine interaction. Chatbots are taking on some of the tasks that were usually performed by humans. When it comes to the healthcare industry, there are a lot of opportunities for chatbots to expand. Despite the fact that adoption is not yet widespread. Healthcare is very important to lead a good life. However, obtaining a doctor's appointment in the case of any health problem is extremely difficult.

This idea focuses on creating a chatbot which is free of cost and is available throughout the day. The fact that the chatbot is free and can be accessed wherever the user is, be it their working environment, prompt the user to have it and use it. It saves the overhead involved in consulting specialized doctors and if necessary it places an appointment with an efficient doctor based on their schedule. In addition to this the symptoms and disease identified by the chatbot is made into a report and automatically forwarded to an available doctor where he can further aid the user with more advices and future measures to keep up their health. For this the chatbot is trained on symptoms-disease dataset. The CNN algorithm used can predict the disease depending on this dataset which then helps the system to recognize the disease and recommend suitable treatment.

II. Background

At some point in their lives, everyone must see a doctor. Their problems, settings, and even the expert doctors they need to contact may all be unique. However, the requirement to see a doctor remains constant regardless of the circumstance. It is possible that the patients will die if they do not receive the proper medical therapy.A skilled and well-known doctor is always in high demand. As a result, getting an appointment can be challenging at times. Even if you are given an appointment, you must consult at the time set by them. If the patients are not treated as soon as possible, this can be very time consuming and deadly.Fortunately, there is a solution to all of the patients' difficulties. This is done with the use of a medical chatbot that can reliably predict diseases and provides a 24/7 support.

III. RELATED WORKS

The proposed idea of the paper 'chatbot for disease prediction and treatment recommendation using machine learning' by Rohit Binu Mathew [1] is to build a chatbot which is an android programme used to chat with user to find the disease. The user sends messages, and the chatbot responds with the required message. Text processing will begin when the user sends a message. The chatbot is programmed using a database of disease symptoms. KNN algorithm will predict the disease based on the user's symptoms and will also provide a link where the user can search for the treatment required for the disease predicted, depending on the dataset.

The proposed idea of the paper 'chatbot utilization for medical consultant system' by Nudtaporn Rosruen [3] is to implement a medical consultant system using the chatbot technology. The chatbot was developed by using Dialogflow powered by Google's machine learning and is an intent based approach.User interacts with the application. The application thus transfers the message to Dialog flow. The message is then extracted to obtain the intent. From the training phrase in the fulfilment, the response is predefined according to the message intent. The system will then produce actionable data which the user can understand and send back to the application. Finally, the user will receive text, picture, speech and video responses. The chatbot has 34 intents, including 16 for symptoms, ten for sub-details of a stomach ache, five for sub-details of a headache, one for greeting, one for no illness, and one for finding a hospital by getting the link.

The proposed idea of the paper 'a novel approach for medical assistance using trained chatbot' by Divya Madhu [2] is to create a chatbot model that can assist people in determining the best treatment for their illness and also gives age-based medicine dosage details. Also, the chatbot is a dedicated system which is able to solve all the queries regarding a medicine. The system can describe the medicine given the name and manufacturing company. It will give the chemical composition, the dosage for each age group, prescribed uses and side effects. The users can ask almost any query regarding the medicine. Then the users can verify the doctor's opinion and be sure of the treatment suggested.The chatbot can also can effectively predict diseases based on symptoms. Each disease has a signature. So, by reading the symptoms and analysing them, any possible health problem can be predicted.

The proposed idea of the paper 'pharmabot: a pediatric generic medicine consultant chatbot' by Benilda Eleonor V. Comendador [4] is a paediatric generic medicine consultant chatbot that can prescribe, recommend, and provide information on generic medicines for kids.In order to arrive at the desired result, the researchers employed Left and Right Parsing Algorithms.The main menu will appear, which consists of four buttons: Start, Instruction, Guidelines, and Exit. If the user selects the instruction button, the device will display the steps for accessing the entire program. If the user clicks the Guidelines button, the rules for input/question format will be shown. However, if the user wishes to begin the chatbot consultation right away, he/she should press the Start button. The user should enter the patient's age on the chatbot tab. The user inputs will be evaluated "word by word in the Chatbot's database" using the Left-Right Parsing Algorithm. The chatbot will administer generic medicines after a series of conversations and consultations, including correct consumption, dosage, drug reaction, precaution, and indication of medicines.

The proposed idea of the paper 'sanative chatbot for health seekers' by V.Manoj Kumar [5] is a system for coding medical records that incorporates local and global approaches. The user enters the query which is pre-processed by extracting noun phrase by eliminating noisy, filler and steaming words. Then the medical terms are detected from noun phrase by using medical concept detection. The solutions are extracted by applying a technique based on comparing the medical keywords in the query and those data sets that at least contain a keyword extracted and are evaluated by this answer extraction module that decides if it correctly answers the user question. If the extracted keyword doesn't present in the dataset, then the contact of specialist is provided. Now the user is asked to rate for the solution produced, based on which question answer pairing would take place for later queries by different user.

IV. Proposed method

The MedBot is an auto-response system also known as a chatbot which is a disease prediction chatbot. It interacts with the user, takes the symptoms from the user as input, maps it to appropriate disease and also places an appointment with the doctor if required. It not only does the disease prediction but also makes a detailed report of the prediction made by the chatbot and forwards it to the doctor when an appointment is made so that the doctor can further aid the user.

MedBot is useful for someone who wants to learn more about health and wellness. It is a web-based programme in which the user must first register before being approved using a one-time password sent via email. After that, they need to submit some personal details which will be confidential.Then the user communicates with the application, and the chatbot responds with the required message. For this to happen smoothly the chatbot is trained with some possible questions to which the user can respond. When the input is received from user the chatbot tries to converge it to that available in the dataset and this is done with the help of CNN algorithm.The algorithm then maps it to the appropriate disease and a report is made. The report consists of the disease predicted by the chatbot, risk factor, and an option to book an appointment with the doctor. If the user chooses to book an appointment , the chatbot will then provide the user with the facility to search for the doctor according to their location and specialization. Once the appointment is placed the doctor will receive the appointments and will get the reports of the patients who have the appointment.

A. Convolutional Neural Network

The Medbot's chat dataset is the primary source of data used as the CNN testset[6]. The algorithm develops a feature model with its layers and uses the Training set to forecast the disease. In both the test and training sets, there are N instances with a set of attributes. The majority of the data is of a nominal character.

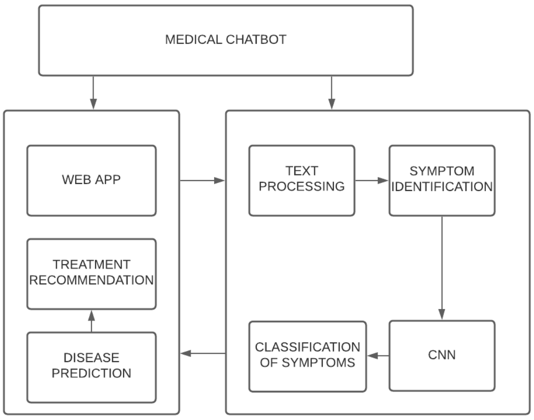


Fig. 1. Proposed Method.

A sample in the form of a feature vector (i.e., a column vector of dimension p x 1) is required by traditional machine learning (ML) algorithms for classification or detection problems.A transformation T transforms a disease feature vector x made up of expression values into a feature matrix M. The similarity of features determines the position of features in Cartesian coordinates. Features g1, g3, g6, and gd, for example, may be closer together. The expression values or feature values are mapped once the positions of each feature in a feature matrix have been identified. Each sample will have its own image as a result of this (or feature vector).There will be N samples of m x n feature matrices from N samples of d features. All of the d characteristics will be present in this 2D matrix form. Following that, this collection of N feature matrices is fed into the CNN architecture, which learns the model and makes predictions.

1) Convolution Layer: The convolution layer is the first layer. The layer keeps track of the relationships between the instances' attributes. It accomplishes this by gaining an understanding of its qualities. This action is carried out by calculating the probability of data values falling within the range of the attribute column. It is a mathematical operation that accepts a data vector as input.

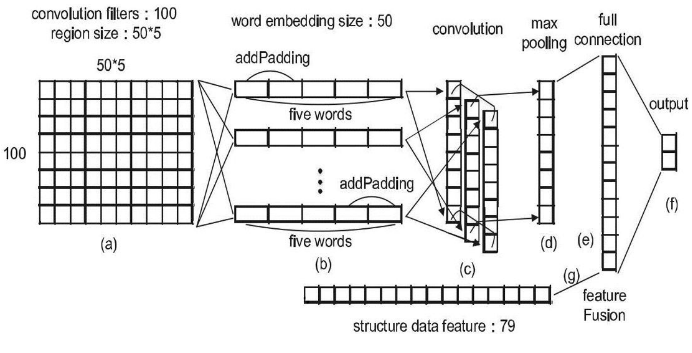


Fig. 2. CNN

2) Pooling: When appropriate, the pooling section is utilized to remove unnecessary parameters from a disease dataset. Spatial pooling decreases the dimensionality of disease data while preserving its key characteristics. There are various varieties of this are 1) Max Pooling: It uses the disease feature map's largest element. 2) Average Pooling: This is where the most significant element comes into effect. 3) Sum Pooling: The sum of all disease feature map elements is calculated and used.

3) Fully Connected Layer: The fully connected (FC) layer takes the matrix once it has been turned into vectors. The feature map matrix is transformed into a vector format (v1, v2, v3, etc.) and fed into a neural network. These vectored characteristics are combined in the FC layer to produce a model.Finally, for categorization, another activation function is used. In CNN, the activation function is often sigmoid or SoftMax.

4) Sigmoid Function: It's a mathematical function with a "S"-shaped curve, sometimes known as a sigmoid curve. It is primarily employed in binary classifications.The key benefit of this activation function is that its derivative is simple to calculate. We can expect an output value in the range of -1 to 1 based on the convention.

5) SoftMax Function: The Softmax function determines the event's probability distribution across a set of n events. The following are a handful of the softmax function's features.1)Probabilities calculated will range from 0 to 1.2)The total of all computed probabilities will equal one.

6) Dense Layer: A matrix vector multiplication is represented by a dense layer. The trainable parameters are represented by the values in the matrix, which are updated during back propagation.

7) Dropout Layer: For regularisation, a dropout layer is utilised, in which you change some of the dimensions of your input vector to zero at random with probability keep_probkeep_prob. There are no trainable parameters in a dropout layer. The layer uses the keep_probkeep_prob to stop or block features (a threshold for keeping the attributes).

B. Modules

The chatbot consists of three modules. Admin Module, User Module, Doctor Module. The Admin Module manages the users associated or logged in to the prediction system. It also manages the dataset taken from Kaggle. The normalization of data is done in this module. The Admin Module has the following components. Test set Generation which is a periodical process where the data captured from one user is collected and formed as a Test set. This is used with the training set to predict the disease. The Chatbot Configuration is associated with a series of queries to the user. A hierarchy of question words are prepared and configured in this section. Next is the prediction. Here we use the CNN algorithm for the prediction purposes. In the Evaluation process the performance of an algorithm is associated with many measures like accuracy, precision and recall of an algorithm. This data is generated from the algorithm evaluation process. In Health Statistics part it generates a disease history in terms of percentages or charts. In the Feedback View part, the user reported feedbacks will be analysed.

The User Module has the following components. User Registration is done by providing some details and authenticating by one-time password. In Chatbot Interface the preconfigured questions will be asked to the user and the results are saved. In the Test set Validation part, the user answers and questions will be saved for each patient session. In Result and Feedback section the user will get the prediction results and a feedback facility will be available.The Doctor Module has the following components.

Doctor Registration is done by providing details of doctor from the authorized hospitals. In the Chatbot Interface of doctor he will receive the appointments and will get the reports of the patients who have the appointment.

V. Conclusion and Future Works

A. Conclusion

Nowadays, the busy schedule of the people makes them forget to take care of their health. Many of them are also affected by occupational illness. So, it is difficult to get time for periodic medical check-ups. Thus, the proposed system is to create a chatbot which can improve the reliability and is less prone to human errors. The chatbot is based on Artificial Intelligence and it can identify the diseases according to the symptoms provided by the user. It can also assist in the availability of medical services. The chatbot also makes it possible to book an appointment with a doctor. The fact that the chatbot is free and also it can be accessed wherever the user is. Hence it prompts the user to have it and use it.

B. Future Works

In the future, the CNN can be trained with more datasets to increase reliability, and a facility for making video call with the specialized doctor can also be made depending on the availability of the user and not based on the availability of doctors.

References

[1] Rohit Binu Mathew, Sandra Varghese, Sera Elsa Joy, Swanthana Susan Alex “Chatbot for Disease Prediction and Treatment Recommendation using Machine Learning,” Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019).

[2] Divya Madhu,Neeraj Jain C. J, Elmy Sebastain, Shinoy Shaji, Anandhu Ajayakumar. “A Novel Approach for Medical Assistance Using Trained Chatbot”, International Conference on Inventive Communication and Computational Technologies (ICICCT 2017).

[3] Nudtaporn Rosruen and Taweesak Samanchuen. “Chatbot Utilization for Medical Consultant System”, The 2018 Technology Innovation Management and Engineering Science International Conference (TIMES-iCON2018).

[4] Benilda Eleonor V. Comendador, Bien Michael B. Francisco, Jefferson S. Medenilla, Sharleen Mae T. Nacion, and Timothy Bryle E. Serac. “Pharmabot: A Pediatric Generic Medicine Consultant Chatbot”, Journal of Automation and Control Engineering Vol. 3, No. 2, April 2015.

[5] V.Manoj Kumar, A.Keerthana, M.Madhumitha, S.Valliammai, V.Vinithasri “ Sanative Chatbot For Health Seekers,” International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume – 5 Issue -03 March, 2016 Page No. 16022-16025.

[6] Sayali Ambekar,Rashmi Phalnikar ”Disease Risk Prediction by Using Convolutional Neural Network”,2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)

A Blockchain Based Secure Inter Medical Data Access System for Hospitals

Anjana J Suresh, Devaprem S, Febin Jose, Gopika Gopal, Gopu Darsan
Department of Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
anjanaslekshmi@gmail.com
devaprems@gmail.com
febinjosefj999@gmail.com
gopikagg014@gmail.com
cs.gopud@sbcemail.in

Abstract—Electronic medical records (EMRs) are critical, sensitive non-public info in healthcare, and need to be frequently shared among peers. In this work, a great deal of emergency clinics will be a part of the organization with varied forms of illness. Indeed, a couple of hospitals are having specific specialists who understand a large scope of illness and provides higher medical aid to the patients. The planned technique shares the patients' subtleties to alternative hospitals. It will be a great help once a patient has manifestations of diseases that once in a very whereas happen and moreover to tell apart if another medical clinic has patients with similar indications and experiencing problem to analyse. On the off probability that the medical clinics contain specific specialists who can facilitate the specialists of various clinics to treat the patient. Thus, a lot of patients can endure while not obtaining applicable therapy. The specialist has to enter all the user accreditations to the framework. The medicos can transfer the information concerning treatment when the registration method completes. If the emergency clinic needs to be approved on this document, the specialist will need to enter and verify the client's CSP key and request the registration key. On the off probability that the 2 keys are right, the client can transfer the particular document.

Index Terms—Treatment, Database, Authenticate, Symptoms, Encryption, Electronic Medical Record (EMR)

I. Introduction

Blockchain is one of the most secure technique for medical data storage. Security is a major concern in the medical industry because millions of patients' data are being exposed in data breaches. The immutability of data stored in a blockchain draws the attention of healthcare sectors. The functionalities like decentralized management, data lineage, robustness, and improved security and privacy all makes blockchain a better option for health care.

A blockchain-based EMR solution will also improve data consistency and inter-operability while reducing the time it takes to access a patient's details. The blockchain concept was initially developed to manage a financial ledger; however, it can be expanded to provide a generic structure for integrating decentralized computing services in any industry, including healthcare. In the long run a nationwide blockchain network for electronic medical records may improve efficiencies and help patients to achieve improved health outcomes.

Blockchain-based systems have the ability to lessen or remove the friction and costs of recent mediators. Data sent via email is regarded as a security risk because this data contains details of patients such as diagnoses, medicines, tests, allergies, immunizations, treatment plans and scanning reports which are the most sensitive information regarding an individual and they are easily prone to attackers when they are transferred through emails, by using blockchain technology we don't want to consider this issue.

The data stored here are available only to the doctors in that particular framework and used only for medical clarifications and treatment assistance. Patients will get more reliable diagnosis; fatal mistakes will be reduced. The promise of blockchain technology is enormous, and integrating it with EMR would ensure that we all profit from a better, more equitable and healthier future.

II. Background

A. Reducing Delays for Medical Appointments: A Queueing Approach

Long delays for appointments can be found in several medical assistance offices and healthcare facilities. Patients may face medication delays and may be treated by somebody else like a primary care provider, possibly resulting in negative health outcomes, patient dissatisfaction and financial losses. Long delays can necessitate additional human and material resources to deal with patients trying to get same day appointments, and are often characterized by high rate of cancellations or no-shows.

There have been a number of strategies for lowering no-show rates including sending pre-appointment notifications, imposing financial penalties and delivering programs make things easier for patients to hold appointments. Advanced access is a method that focuses on the inefficiencies of many current patient scheduling processes. The basic concept is to "do all of today's work today," so patients don't have to wait for an appointment practices and don't lose capacity by scheduling appointments in advance of same day needs and patients are more likely to see their own doctor.

In this paper, they appear to imagine an appointment system like a single-server queueing system. They introduce two queueing models. The first model is to explicitly include a backlog-dependent termination rate, which has been widely observed. As they have shown, this cancellation aspect and its related rescheduling probability have a considerable impact on its performance and the maximum patient panel size. Although no model can perfectly reflect reality, they believe these are useful for guiding patient panel decisions because they reflect the key dynamics of a patient appointment system. They derive fixed queue size distributions, assuming that each is settled in addition as cumulative service times and compare the output metrics to the results of an appointment system simulation. Their findings show that when patients take the next available appointment, the deterministic service model built here is extremely reliable.

Some practices that are attempting to introduce advanced access limit the number of days in advance that they can book an appointment and allow their patients to take one of the first few appointments available. More broadly, their findings from the MRI facility suggest that using both deterministic and exponential models to limit the maximum panel size can be very useful. It may be useful in pediatrics, gynecology, and cardiology, among other specialties.

B. Health Information Technology: Benefits and Problems

In this paper, they suggest a method to use blockchain technology to incorporate EHRs and make them safer and more private. Using cryptographic techniques and decentralization, blockchain technology can maintain control over information access. It will also strike a balance between data security and data accessibility.

The project's primary goal is to frame data privacy and security problems in electronic healthcare. Clinicians were able to make more accurate diagnosis of patients, contact between doctors and patients improved, and doctors were more readily accessible to patients in an emergency. Patients could contact their doctors even from far away thanks to electronic records. Blockchain is a decentralized ledger framework that can effectively record transactions between two parties. Each transaction is saved as a record, which is then linked together using cryptography to form a list or blockchain. In a blockchain network, each block contains transaction data, a cryptographic hash, the previous block's hash and a timestamp. The blockchain is designed in such a way that it is impervious to alteration. Participants, Assets and Transactions are the three key components of this scheme. Patients, Clinicians/Doctors, Labs, and Admin are the three key players in this blockchain-based EHR implementation. The transactions are often acts performed on the network asset, such as adding a participant to the network, creating a medical record, extracting relevant information from the network, changes in the participant's information and granting or revoking access to clinicians or labs.

In this scheme, the permission rules are also specified. These guidelines determine which participants have access to which services and what kind of access they have. This aids in limiting access to all of the system's resources. The permission rules are also stated in this scheme. These rules decide which participants have access to which programs and to what extent they have access. This helps to restrict access to the entire system's resources. It can be combined with a web application to make it more interactive. Through introducing pharmacists to the system as a member, EHRs can be rendered useful for pharmacists in tracking medical sales.

C. Functionality of Hospital Information Systems: Results from a Survey of Quality Director at Turkish Hospitals

Since the early 2000s, there have been consistent attempts to improve healthcare quality, which were sparked by two Institute of Medicine studies. The first study claims that healthcare isn't as healthy as it should be, citing a large body of evidence that medical errors are a major cause of morbidity and mortality in the US (U.S.). The second study looks at how the healthcare delivery system can be redesigned to be more innovative and provide better care. Both reports recommend that one of the six necessary strategies for the modernization of healthcare systems is to make efficient use of information technologies, and they express concern about the slow adoption of information technology in healthcare.

Healthcare is an information-based science, and in order to deliver reliable, high-quality care, providers must provide timely and accurate information. The majority of stakeholders believe that information technologies, such as electronic health records (EHRs) and computerized provider order entry (CPOE), will be essential to the healthcare industry's transformation.

The aim of this study is to establish the availability of core Hospital Information Systems (HIS) functions in Turkish hospitals, as well as their perceived value in terms of quality and patient safety. Quality Directors (QDs) at civilian hospitals across Turkey were surveyed. Data was gathered via a web survey using a 50-item instrument that defined HIS core functionality. They measured the average availability of each feature, as well as the mean and median values of perceived quality effects, and looked into the relationship between availability and perceived importance.

They received responses from 31% of qualified organizations, which represented all of Turkey's major geographic regions. The average availability of 50 HIS functions was 65.6 percent, with a range of 19.6 percent to 97.4%. The average significance score was 7.87 (on a scale of 1 to 9) with a range of 7.13 to 8.41. The highest and lowest recorded availability is for functions related to outcome management (89.3%) and decision support systems (52.2%), respectively. The availability of information and the perceived value of that information were moderately correlated (r = 0.52). The relevance of the HIS functions surveyed to quality and patient safety is emphasized by QDs. These results could help to direct future investments and policy changes in Turkey's healthcare system. Financial incentives, legislation around accredited HIS, updates to accreditation manuals and training interventions are all policies that will aid in the integration of HIS functions in Turkish hospitals to promote quality and patient safety.

III. Proposed System

The fundamental intention of the proposed system is to build a secure network to access medical information and provide patients with better treatment as expected. The system is equipped with a server having common database to beat the downsides of existing systems. Every hospital management needs to enlist in this framework. This frame generates a CSP key during the registration process. Thereafter, doctors should involve all client accreditations to the framework. Once the registration cycle is fully completed, the doctor will be able to submit all the information about the illness and medicine and how to take care of that issue.

While uploading, the server provides security by encrypting the data set using the AES algorithm and storing it in the database, so that the client on the worker thread can undoubtedly identify the corresponding document. If doctors need information about the disease, they can select the disease and send a clarification request. On that occasion, the request for the file will be transferred to the corresponding hospital. The customer can receive this record and document key only when the hospital accepts this request. If the clinic needs to access the record, the clinician must enter the client's CSP key, confirm that it is correct and request the file key. If the two keys are correct, the customer can download the specific document.

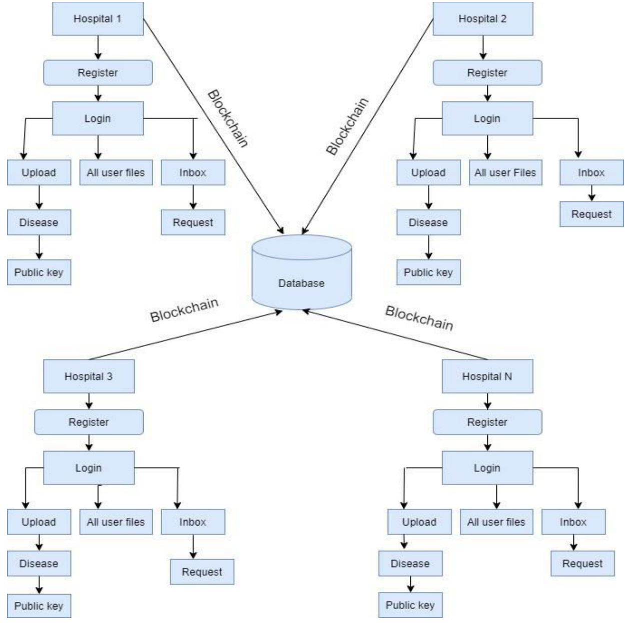


Fig. 1. Structure of Proposed Scheme

A. Working

The software's main page has two choices, which are represented as buttons. The first button allows you to register, while the second allows you to log in. The hospital administration must first register for this framework by clicking the register button. There are different parts inside the register button to fill in the hospital management's details such as name, address, pin code, and phone number, and then press the register button. This request is on hold until the central authorities confirm that the hospital information is valid, then they will grant access to the framework. A Cryptographic Service Provider (CSP) Key is generated automatically at this point, with a public key for the user and a corresponding private key stored in the database with the hospital's information which is used for final authentication purpose.

The dashboard button appears at the top of the screen after the user has successfully logged in. This button includes three additional buttons for upload, download, and request. The patient's information can be uploaded in PDF or Excel format. This information is encrypted by the 256-bit Advanced Encryption standard algorithm (AES) and stored in a database with an ID number that is assigned to each patient's data at the uploading time.

If a hospital requires information about a specific disease, they can use the request button associated with the file. The central authorities will verify the request for approval before deciding whether or not to grant permission to access the file record. If they grant access, the request is forwarded to the inbox of the admin hospital. When the file request shows up, the admin hospital has an approval option; when they select it, the specific file is sent to the needy hospital along with the file key. The hospital can only download the specific file only after authenticating the CSP key and the file key. Since the blockchain is a distributed ledger, the patient's information is also accessible in the block, but the data is only visible until the unique keys are obtained. The attackers would require at least 12 years to crack the key.

B. Modules

1) *User interface:* Here the hospital management has to register in one account under the database, while registering time itself for each and every user gets one private key called CSP key that is generated automatically by random key generation.

2) *Admin upload details about treatment:* After the registration process, the doctors in that hospital have to login with their respective user credentials. The doctors who have knowledge about the treatment for that particular disease will enter complete details regarding this in a single document and during the uploading time the contents will be encrypted and a private key is generated and stored in a database.

3) Doctors can search for new treatment documents: Doctors can login into the system and if they need any details about the treatment document, they are able to view the details about all hospital data.

4) Send request for document: When they find their required document and need access to view it, they have to send a request to the file owner.

5) Request accepted by the hospital admin by authentication: After getting the file view request by the other hospital the admin hospital can decide whether to accept it and give them public access. When they get the file granted permission from the owner first, they have to enter their user CSP key if it was authenticated correctly then it will ask to enter your file view key if both were correct then only, they are able to view that particular document.

IV. Conclusion

Nowadays, the majority of people have lost their valuable lives due to a lack of timely medical treatment. As a result, the proposed method will create a secure network using blockchain technology for medical data access, as well as provide patients with better treatment than expected. To do so, the doctor must transfer the patient's medical record to another hospital and request data related to it. Cybercriminals may be interested in healthcare data because it contains personal and sensitive information. While entering data into the database, we use AES encryption calculation to keep the data secure. By combining all of these, the doctor can provide a superior treatment to the patient and potentially save many lives.

References

[1] Suboh M Alkhushyni, M Alzaleq Du'a, and NadineL Gadjou Kengne. "Blockchain Technology applied toElectronic Health Records". In:Proceedings of 32ndInternational Conference on. Vol. 63. 2019, pp. 34–42.

[2] Asaph Azaria et al. "Medrec: Using blockchain formedical data access and permission management". In:2016 2nd International Conference on Open and BigData (OBD). IEEE. 2016, pp. 25–30.

[3] Lanxiang Chen et al. "Blockchain based searchable en-cryption for electronic health record sharing". In:FutureGeneration Computer Systems95 (2019), pp. 420–429.

[4] Mario Ciampi et al. "A federated interoperability ar-chitecture for health information systems". In:Inter-national Journal of Internet Protocol Technology7.4(2013), pp. 189–202.

[5] Alevtina Dubovitskaya et al. "Secure and trustableelectronic medical records sharing using blockchain".In:AMIA annual symposium proceedings. Vol. 2017.American Medical Informatics Association. 2017,p. 650.

[6] Christian Esposito et al. "Blockchain: A panacea forhealthcare cloudbased data security and privacy?" In:IEEE Cloud Computing5.1 (2018), pp. 31–37.

[7] J Goodman, L Gorman, and D Herrick. "Health in-formation technology: Benefits and problems". In:Na-tional Center for Policy Analysis, Washington(2010).

[8] Linda V Green and Sergei Savin. "Reducing delaysfor medical appointments: A queueing approach". In:Operations Research56.6 (2008), pp. 1526–1538.

[9] Reinhold Haux. "Health information systems–past,present, future". In:International journal of medicalinformatics75.3-4 (2006), pp. 268–281.

[10] Kristiina H ayrinen, Kaija Saranto, and Pirkko Nyk anen."Definition, structure, content, use and impacts of elec-tronic health records: a review of the research litera-ture". In:International journal of medical informatics77.5 (2008), pp. 291–304.

[11] Marko H olbl et al. "A systematic review of the use ofblockchain in healthcare". In:Symmetry10.10 (2018),p. 470.

[12] Mohamad Kassab et al. "Blockchain: A panacea forelectronic health records?" In:2019 IEEE/ACM 1stInternational Workshop on Software Engineering forHealthcare (SEH). IEEE. 2019, pp. 21–24.

[13] Harleen Kaur et al. "A proposed solution and futuredirection for blockchain-based heterogeneous medicaredata in cloud environment". In:Journal of medicalsystems42.8 (2018), pp. 1–11.

[14] Jingwei Liu et al. "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records".In:2018 IEEE Global Communications Conference(GLOBECOM). IEEE. 2018, pp. 1–6.

[15] Andr e Henrique Mayer, Cristiano Andr e da Costa, andRodrigo da Rosa Righi. "Electronic health records in ablockchain: a systematic review". In:Health informaticsjournal26.2 (2020), pp. 1273–1288.

[16] Montse Moharra et al. "Implementation of a cross-border health service: physician and pharmacists' opin-ions from the epSOS project". In:Family practice32.5(2015), pp. 564–567.

[17] Mehmet Saluvan and Al Ozonoff. "Functionality ofhospital information systems: results from a survey ofquality directors at Turkish hospitals". In:BMC medicalinformatics and decision making18.1 (2018), pp. 1–12.

[18] Ayesha Shahnaz, Usman Qamar, and Ayesha Khalid."Using blockchain for electronic health records". In:IEEE Access7 (2019), pp. 147782–147795.

[19] Yogesh Sharma and B Balamurugan. "Preserving theprivacy of electronic health records using blockchain".In:Procedia Computer Science173 (2020), pp. 171–180.

[20] Melissa Steward. "Electronic medical records: privacy,confidentiality, liability". In:The Journal of legalmedicine26.4 (2005), pp. 491–506.

[21] Thein Than Thwin and Sangsuree Vasupongayya."Blockchain based secret-data sharing model for per-sonal health record system". In:2018 5th InternationalConference on Advanced Informatics: Concept Theoryand Applications (ICAICTA). IEEE. 2018, pp. 196–201.

[22] Dara Tith et al. "Application of blockchain to maintain-ing patient records in electronic health record for en-hanced privacy, scalability, and availability". In:Health-care informatics research26.1 (2020), p. 3.

[23] Guang Yang, Chunlei Li, and Kjell E Marstein. "Ablockchainbased architecture for securing electronichealth record systems". In:Concurrency and Compu-tation: Practice and Experience(2019), e5479.

[24] Alex Yovera-Loayza, Rajhut Fernandez-Nevado, andPedro ShiguiharaJu arez. "Architectures for Blockchainin the Management of Medical Records: A Compar-ison". In:2019 IEEE XXVI International Conferenceon Electronics, Electrical Engineering and Computing(INTERCON). IEEE. 2019, pp. 1–4.

[25] https://technorely.com/emr-using-blockchain/

DETECTION OF CYBERBULLYING USING DEEP LEARNING

Anoop S Nair
Department of Computer Science
Sree Buddha College of Engineering
Kerala, India
nairanoop59@gmail.com

Jobiya C Johnson
Department of Computer Science
Sree Buddha College of Engineering
Kerala, India
jobiya1999@gmail.com

Merin Mathew
Department of Computer Science
Sree Buddha College of Engineering
Kerala, india
merinm2017@gmail.com

Vignesh S N
Department of Computer Science
Sree Buddha College of Engineering
Kerala, India
vsn.fun@gmail.com

Asst. Prof. Lakshmi S
Department of Computer Science
Sree Buddha College of Engineering
Kerala, India
lakshmi.rnath@gmail.com

***Abstract*—In the era of social media and networking, the usage of bad words and aggressive words has increased significantly. The young population is playing a major role in it. Cyberbullying affects more than half of the young population using social media. Insults in social media websites create negative interactions within the network. These remarks build up a culture of disrespect in cyberspace. Tools and technologies geared to understand and mitigate it are scarce and mostly inactive. Also, current implementations on insult detection using machine learning and natural language processing have very low recall rates. In short, this paper involves determining ways to identify bullying in text by analysing and experimenting with different methods to find the most suitable way of classifying bullying comments. We are going to propose an efficient hybrid model that can identify the bullying and aggressive comments from text and emotion icons that are produced in English and one of the Indian language Malayalam. The end users of this model can input the confusing words and can receive the output whether the word/comment is bully or not. A Convolution Neural Network (ConvNet/CNN) is a Deep Learning algorithm which can take in an input image, assign importance (learn able weights and biases) to various aspects/objects in the image and be able to differentiate one from the other.**

***Index Terms*—Cyberbullying, deep learning, machine learning, convolutional neural network, Malayalam**

I. Introduction

The Internet gave users the opportunities to express an opinion on any topic in the form of user reviews or comments. The comments are usually of an informal style, mostly in social media forums such as YouTube, Facebook, and Twitter, which opens up the ground for mixing languages in the same conversation for multilingual communities. Some people with different linguistic backgrounds and cultures mark their impressions about a subject with the individual feeling. Due to the ease of posting the content of these social media, cyberbullying empowers a bully to humiliate and hurt the victim in online communities without ever getting recognized[1].

So, this paper proposes a hybrid Multilingual Cyberbullying Detection System for detection of cyberbullying in Malayalam and English languages. Even though English is one of the most popular languages in the world, in addition to that we choose Malayalam because most of the current approaches to identify cyberbullying are focused on English text, and a very few approaches are venturing into other languages. Malayalam is one of the Dravidian languages spoken in the southern region of India with nearly 38 million Malayalam speakers in India and other countries. Malayalam is a deeply agglutinating language[2].

II. PREVIOUS WORKS

A. *Detecting A Twitter Cyberbullying Using Machine Learning[3]*

In this work it identified word similarities in the tweets made by bullies and make use of machine learning and can develop a machine language model that can automatically detect social media bullying action contents. The problem can be tackled by detecting and preventing it by using a machine learning approach, this needs to be done using a different perspective. The main purpose of this paper is to develop an ML model so it can detect and prevent social media bullying, so nobody will have to suffer from it. The proposed technique is implemented on the social media bullying dataset which was collected from various sources like Kaggle, GitHub, etc. The performance of both Naive Bayes and Support Vector machine is compared to TFIDF. Twitter API is used to fetch a particular location's tweets to detect whether they are Bullying or not. Furthermore, the probability of each tweet is calculated to predict the result and the result of each tweet is stored into the database with bullies username.

B. Multilingual Cyberbullying Detection System Detecting Cyberbullying in Arabic Content[4]

This proposed methodology presented a solution for the problem of cyberbullying in both English and Arabic languages. As seen in the other sections, there is some work done for detection in English, but none in Arabic. Proving the hypothesis that Arabic cyberbullying can be detected was a challenge. This paper presents a system capable of detecting and stopping cyberbullying attacks using different stages. Thus in the first stage of the system the focus was on detecting cyberbullying in Arabic language. Since the proposed system employs ML, a dataset had to be prepared to be used for training and testing the system. Two toolkits were tested for Machine Learning, Dataiku DSS and WEKA. The decision was to use WEKA toolkit because it supports Arabic language.

C. Multilingual Cyberbullying Detection System[5]

This work describes a Multilingual Cyberbullying Detection System for detection of cyberbullying behavior in two Indian languages – Hindi and Marathi. These two languages have 293 million (4.46 per cent of world's population) and 73 million (1.1 per cent of world's population) native speakers. Hence, the proposed system has a potential of creating a significant impact in making online forums safer for the users of these two languages. Hindi and Marathi languages use the 'Devanagari' script and hence, some of the words are common in both the languages. However, the grammar of both the languages is a bit different. The system employs principles of ML, and thus, as a first step, they had to create a dataset for training and testing the ML models. They created out ML model using python's ML framework i.e., scikit-learn.They have chosen three models, Multinomial Naive Bayes (MNB), Logistics Regression (LR), and Stochastics Gradient Descent (SGD). These algorithms were selected as they perform well on Topic Modeling and Text Classification, as indicated in our past work as well as in literature. These machine-learning algorithms were trained to create models that were used for the classification of the cyberbullying tweets. They used 80 per cent of the data for the training purpose and remaining 20 per cent for the testing purpose.

III. PROPOSED SYSTEM

As already mentioned our proposed system intends to find the bullying words and emotion icons from text, tweets or social media contents by using a hybrid approach of knowledge based learning and machine learning. This system being a combination of knowledge based and machine learning based methods can effectively trace and track these abuses is the need of the hour.

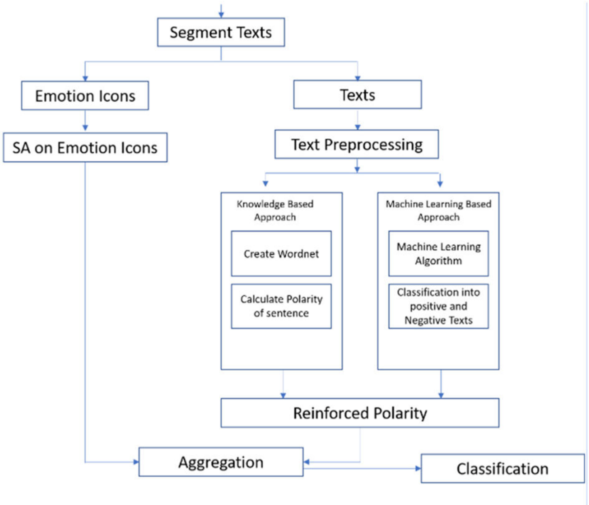
A. DATA PREPARATION

The emotion icons and text contents are separated first from the provided sentence, where the emotion icons undergo a structure analysis to analyze the content, then a word-net bag of contents is created where the polarity score for each words or contents will be estimated[6], similarly on parallel thread each words undergo a machine learning scanning which classifies into positive and negative words[7].

B. SYSTEM TRAINING AND TESTING

The system is a combination of knowledge based and machine learning based methods can effectively trace and track these abuses is the need of the hour. The emotion icons and text contents are separated first, where the emotion icons undergo a structure analysis to analyze is content, then a word-net bag of contents is created where the polarity score for each words or contents will be estimated, similarly on parallel thread each words undergo a machine learning scanning which classifies into positive and negative words, the knowledge based analysis and the machine learning based analysis is aggregated and final classification is made.

C. ARCHITECTURE



The proposed system is a combination of machine learning and knowledge base, where initially the segmented text is divided into two groups of data. One is the set of emotion icons and the other is the set of textual data. The emotion icons undergo a structure analysis to analyze is content. With the help of world-net bag the polarity of words and content is been checked. One the other side each words will undergo a machine learning scanning which classifies into positive and negative words. The knowledge based analysis and the machine learning based analysis is aggregated along with the structural analysis result and then the final classification is made.

IV. CONCLUSION

Many Cyberbully detection systems are accomplished in English textual comments. Extending this idea for some more languages may help several people to identify the bullying texts. Hence that was the reason we proposed an idea for bringing up with Malayalam language. Our model can identify and classify the bullying comments produced from text and emotional icons can also be identified. Considering these special cases we can improve the identification and reduce various threat which were occurring all around the world. Our proposed methodology, can come useful in handling crises and can even be enhanced to provide full-time support. Also we are looking forward for bring up with some more regional languages.

V. REFERENCE

[1] Sourabh Parime,Vaibhav Suri,"Cyberbullying Detection and Prevention: Data Mining and Psychological Perspective",2014 International Conference on Circuit, Power and Computing Technologies [ICCPCT]

[2]Bharathi Raja Chakravarthi1, Navya Jose2, Shardul Suryawanshi1 ,Elizabeth Sherly2, John P. McCrae1,"A Sentiment Analysis Dataset for Code-Mixed Malayalam-English",Proceedings of the 1st Joint SLTU and CCURL Workshop (SLTU-CCURL 2020), pages 177–184 Language Resources and Evaluation Conference (LREC 2020), Marseille, 11–16 May 2020c European Language Resources Association (ELRA), licensed under CC-BY-NC

[3] Rahul Ramesh Dalvi,Sudhanshu Baliram Chavan,Aparna Halbe, "Detecting A Twitter Cyberbullying Using Machine,Learning", Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2020) IEEE Xplore Part Number:CFP20K74-ART; ISBN: 978-1-7281-4876-2

[4]Batoul Haidar,Maroun Chamoun,Ahmed Serhrouchni,"Multilingual Cyberbullying Detection System Detecting Cyberbullying in Arabic Content"

[5]Rohit Pawar, Rajeev R. Raje,"Multilingual Cyberbullying Detection System in hindi and marathi"

[6] Josephine E. Petralba,"An Extracted Database Content from WordNet for Natural Language Processing and Word Games"

[7] S. Dinakar, P. Andhale and M. Rege, "Sentiment Analysis of Social Network Content," in IEEE 16th International Conference on Information Reuse and Integration, 2015

Automatic Number Plate Detection,If a Person is Not Wearing Helmet

1st Lekshmi Priya
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

2nd Adithya R
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

3rd Pranav Prasad
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

4th Harimurali M
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

5th Reeba R
Assistant professor
Dept. of CSE
Sree Buddha College of Engineering
Alappuzha, India

***Abstract*—This paper is about identifying two-wheeler riders who are travelling without wearing helmets with the help of machine learning and provide them with a user interface to pay challans. The proposed approach first captures the real time video footage from traffic cameras and then isolates videos into frames of images to differentiate the two wheelers from other vehicles in the road. It then processes to check whether the rider and pillion rider are wearing a helmet or not; this is done by processing their vehicle number plate using optical character recognition.**

***Index Terms*—machine learning,traffic cameras,optical character recognition**

I. Introduction

Almost everywhere in the world, two-wheeler vehicles are a popular means of transport. However, due to reckless driving and use of less protective gear had increased the risk of riders getting involved in accidents. Thus use of helmets are widely desirable for two-wheeler riders to reduce the risk of accidents. Considering the data related to accidents most of the deaths in the last few years are due to head injury hence it is a punishable offense to ride a bike without a helmet and there are many methods the traffic authorities use to catch the offenders still there are many violators of this offense. An automated mechanism needed to be implemented in the present day and time so a real time and accurate monitoring of these violators can be detected thus significantly reducing the amount of human intervention.In most countries different techniques and infrastructures are implemented for surveillance; using different types of CCTV cameras which captures footage of traffic.

Almost everywhere in the world, two-wheeler vehicles are a popular means of transport. However, due to reckless driving and use of less protective gear had increased the risk of riders getting involved in accidents. Thus use of helmets are widely desirable for two-wheeler riders to reduce the risk of accidents. Considering the data related to accidents most of the deaths in the last few years are due to head injury hence it is a punishable offense to ride a bike without a helmet and there are many methods the traffic authorities use to catch the offenders still there are many violators of this offense. An automated mechanism needed to be implemented in the present day and time so a real time and accurate monitoring of these violators can be detected thus significantly reducing the amount of human intervention.In most countries different techniques and infrastructures are implemented for surveillance; using different types of CCTV cameras which captures footage of traffic.

The paper is organized as follows. Section 2 considers the bachground. Section 3 describes the developed technique. Section 4 presents the modules and its description. Section 5 discusses the advantages and disadvantages of the proposed solution, and the experimental results Section 6 contains the main conclusions.

II. Background

Automatic detection without helmet is it first detect the riders from surveillance video using background substraction and object segmentation[1]. Using visual feature and binary classifier, the rider is detecting having helmet or not. It provides three widely used feature representation using histogram of oriented gradients, scale invariant feature transform and local binary platform for classifications. It shows an accuracy of 93.80expensive. To detect the moving and static object the background subtraction is done on grey-scale. Background substraction is used to separate the objects in motion such as human, bike, etc. This method is also used to detect the number plates of violators.

The proposed approach for the detection works in two-phases[2]. In first step video frame are detected and in second step is used to detect whether the rider is wearing helmet or not. Background substraction is done on grey-level to distinguish between moving and static objects. In certain cases single Gaussian is not sufficient and for this reason each pixel is given to variable numbers of Gaussian model. It has feature extraction and classification. Both are computationally complex in case of large visual data. In order to locate unusual pattern it is used t analyze large amount of video footage. The framework also assist the traffic to detect in odd environmental conditions. It is also used to detect the number plate of the violators.

Detection of traffic riders are challenging due to various difficulties such as illumination, occlusion etc[3]. Moving objects are detected by using convolutional neural networks. The approach is evaluated in two datasets containing spare traffic and dense traffic. The usage of less discriminative representation for object classification is the main reason for the poor performance of existing methods. CNN improves the classification task and helpful in detecting the riders not wearing helmet. Deep learning improves the detection rate and reduces false alarm. It successfully detects 92.87 percent vialators and false alarm of 0.50 percent on two real datasets and shows the efficiency of the mdel.

III. Proposed Method

In our system architecture we are beginning by placing the Traffic cameras in the intersections of street and at the traffic lights for catching the pictures of the individual who isn't wearing helmet. The taken pictures is given as the input to the YOLO algorithm. Here we are utilizing YOLOV3 calculation. YOLOv3 (You Only Look Once, Version 3) is a continuous article recognition calculation that recognizes explicit items in recordings, live feeds, or pictures. This algorithm is utilized here to discover the individual without wearing Helmet. This cycle is finished by drawing bounding boxes to every one of the articles found on that picture. On the off chance that an individual isn't wearing head protector, we identify the number plate of that vehicle by utilizing the OCR innovation. OCR innovation is utilized to change over for all intents and purposes any sort of picture containing composed content (composed, written by hand, or printed) into machine-clear content information. OCR Technology got famous in the mid-1990s while endeavouring to digitize memorable papers. From that point forward, the innovation has gone through a few upgrades. In reality, Interlacing Technique is done here for the number plate identification. After that we gather the data of the individual who isn't wear the helmet by utilizing the assistance of identified vehicle number. Finally, Challan is created for comparing individual without protective cap.

IV. Modules and Description

The different modules are:

- Dataset Preparation
  We can download the dataset from the Kaggle website. In dataset preparations, different angle pictures of helmet is added.
- Training Phase
  Collected the set of 100 images from the sources such as Google Images and Flickr. Then annotated the set of images by drawing the boundary box over the number plates to send it for the training phase.In this module, the data is splitted into two parts,80 percent is used for training and 20 percent is used for testing. Here, The data collected for testing and training phase is done in a random manner.
- Model Creation
  In this module, a model is implemented by using Yolo algorithm which is used for tracking moving objects and OCR is used for number plate detection
- Prediction
  Prediction model predicts the future outcome rather than the current situation that is it predicts the next weeks closing price for the google share price per unit
- Deep Learning
  Deep learning is a subset of machine learning, which is essentially a neural network with three or more layers. These neural networks attempt to simulate the behavior of the human brain far from matching its ability to allowing it to learn from large amounts of data. While a neural network with a single layer can still make approximate predictions, additional hidden layers can help to optimize and refine for accuracy.This module contains a neural network.

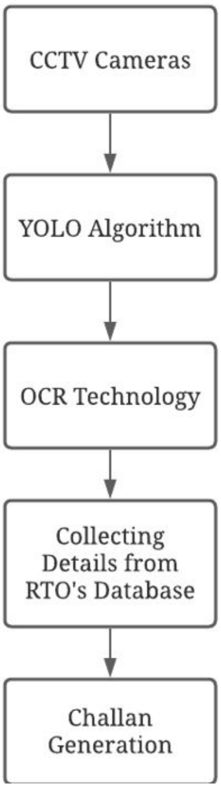


Fig. 1. System Architecture.

A. Optical Character Recognition

Optical character recognition or optical character reader (OCR) is the electronic or mechanical transformation of pictures of composed, transcribed or printed text into machine-encoded text, regardless of whether from a checked record, a photograph of an archive, a scene-photograph (for instance the content on signs and boards in a scene photograph) or from caption text superimposed on a picture (for instance: from a transmission). Broadly utilized as a type of information passage from printed paper information records – regardless of whether identification

records, invoices, bank explanations, modernized receipts, business cards, mail, printouts of static-information, or any appropriate documentation – it is a typical strategy for digitizing printed messages so that they can be electronically altered, looked, put away more minimalistically, showed on-line, and utilized in machine cycles like intellectual registering, machine interpretation, (removed) textto-discourse, key information and text mining. OCR is a field of examination in design acknowledgment, counterfeit insight and PC vision.

B. *YOLO (You Look Only Once) Algorithm*

YOLO algorithm is an algorithm based on regression, instead of selecting the interesting part of an Image, it predicts classes and bounding boxes for the whole image in one run of the Algorithm. To understand the YOLO algorithm, first we need to understand what is actually being predicted.

The biggest advantage of using YOLO is its superb speed – it's incredibly fast and can process 45 frames per second. YOLO also understands generalized object representation. This is one of the best algorithms for object detection and has shown a comparatively similar performance to the R-CNN algorithms.

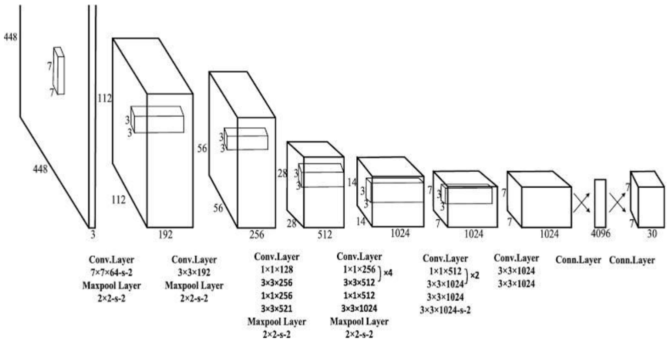


Fig. 2. Structure of YOLO.

V. Conclusion

In this paper, first place traffic cameras in the streets and at the junctions for capturing the person who doesn't wear helmet. We know that people wearing different kinds of helmet which are not safe and hence should be considered as violation of traffic rules and the riders wearing different kind of caps which should also be considered as violation.

The proposed method utilizes YOLO algorithm and this algorithm helps to detect the person who have not helmet. If the person is not wearing helmet, we have to identify the number plate of that vehicle. For this, OCR innovation helps for that process.it will change the picture containing composed content into machine clear content information. Finally, challan is created for that person who disobeying the law.

The main contribution of this paper is to implement the cameras to detect the person who isn't wearing helmet. So, the proposed method is scalable for detection. It is completely suitable and ready for commercial use and it would be one of the biggest achievements in the field of automation.

References

[1] K. Dahiya, D. Singh, and C. K. Mohan, "Automatic detection of bikeriders without helmet using surveillance videos in real-time," in Proc.Int. Joint Conf. Neural Networks (IJCNN), Vancouver, Canada, 24–29July 2016, pp. 3046–3051.

[2] D. Singh, C. Vishnu, and C. K. Mohan, "Visual big data analytics for traffic monitoring in smart city," in Proc. IEEE Conf. Machine Learning and Application (ICMLA), Anaheim, California, 18–20 Decemer 2016.

[3] Quadri, Tofiq Patel, Mayank. (2015). "Face Detection and Counting Algorithms Evaluation using OpenCV and JJIL".

[4] C. Vishnu, Dinesh Singh, C. Krishna Mohan, Sobhan Babu, 2017, 'Detection of motorcyclists without helmet in videos using convolutional neural network', 2017 International Joint Conference on Neural Networks (IJCNN).

[5] J. Chiverton, "Helmet presence classification with motorcycle detection and tracking," IET Intelligent Transport Systems (ITS), vol. 6, no. 3, pp. 259–269, 2012

[6] R. Silva, K. Aires, T. Santos, K. Abdala, R. Veras, and A. Soares,"Automatic detection of motorcyclists without helmet," in Proc. Latin American Computing Conf. (CLEI), Puerto Azul, Venezuela, 4–6 October2013, pp. 1–7.

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

Emotional State Detection for Parental Control Using Facial Emotion Detection

1st Akhilesh A
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

2nd Anandu D
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

3rd Jaike M Jayan
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

4th S Adithyan
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India

5th Supriya L P
Assistant professor
Dept. of CSE
Sree Buddha College of Engineering
Alappuzha, India

***Abstract*—Mobile usage among young adults has multiplied in big numbers withinside the latest years, which will increase withinside the coming years as proven via way of means of the research achieved by experts. As the utilization and customers of mobile phones multiplied the problems the teenagers face from them additionally growing with the growth in the wide variety of crimes in opposition to young adults are skyrocketing in the latest years. The troubles confronted through today's parents that they're not able to or now no longer getting time to have a communication with their children. And this trouble began out to create an opening among them, which makes the children experience a remoteness from their mother and father. So, the mission that we're doing right here is the improvement of a mobile application that can assist parents to connect to their children. The principal purpose entails the improvement of a facial emotion recognition code that can discover facial feelings like sad, angry on a child's face at some point of using their mobile phones, and then integrating this code to a mobile application that sends a notification to the parent with the information approximately their child's emotional state, about the application that they're using, etc. The output that we're seeking to obtain is to make a connection among the emotionally disturbed child and their parent so that they can communicate it out and get help before something much worse will happen.**

***Index Terms*—facial emotion detection, android application, parental control**

I. Introduction

The development of mobile phones had changed the world around us in various ways. Now mobile phones are a must-have among everybody irrespective of their age or the work they do. And the number of users keep on increasing and will keep doing so in the coming years with the majority users being youngsters, which includes teenagers. The one thing that kept on increasing with the numbers of mobile users was the number of problems that were created by this increasing usage, examples being cyberbullying, online frauds, various mental illnesses. An estimated 10-20% of teenagers globally experience mental health conditions, yet these remain underdiagnosed and undertreated [1]. Even when different ways were introduced as a means to put an end to the problems that are being caused online, none of it seemed to be effective.

Childhood mental health problems can have lasting effects on a child's life chances. Behaviour problems are the most common mental health problem in early childhood, affecting 5–10% of young children [2,3]. Established problems confer risk for a wide range of negative outcomes including school failure, delinquent behaviour, relationship difficulties, mental illness and physical ill health [4–7]. As such the lifelong cost of behaviour problems to children, families, and society is both substantial and far-reaching [8]. Parenting is considered a key risk factor in the development of early psychopathology [9].

So, the idea here is that, instead of trying to find a temporary way to stop the causer of these problems we intend to focus on the ones who are being affected by these problems. If it cannot affect their lives or their stable state of mind then we don't need to fight the problems. And by doing this we intend to help many lives of both teens and bring peace to the minds of their parents.

To do this, the focus will be on the facial emotions of a child. By using their emotions, we will be able to guess their emotional state and help them. There are 7 universal facial emotions like happy, sad, anger, surprise, disgust, fear, and neutral. The main focus is to create a facial emotion recognition code that will help to find these 7 universal facial emotions and help to find the state of the child during the usage of their devices. To train the code FER2013 dataset will be used here. The code will be integrated with an android application that will help the parent by notifying them with the help of emails about information of the emotions and the certain application that the child has been using.

With the information that they get, parents can get in touch with their children and allow them to open up their minds. Studies have shown that when a mentally disturbed child interacts with people in their peer groups, it helps them in taking a great deal of pressure from their mind and help them recover from their problems or fight against their problems.

II. Related Works

Ul Haque [10] in his paper explores the continued work of a research project that accomplished the end goal of the project which was to build a mobile device application that can teach children with Autism Spectrum Disorder (ASD) to recognize human facial expressions. The DCNN model was developed in the paper which can recognize 7 facial expression. The DCNN used here was inspired by VGGnet network especially by the VGG16 architecture. The DCNN model in this paper takes in a greyscale image of size 48*48 from the famous Kaggle's FER2013 dataset and got a final accuracy of 67.11%. The initial DCNN which was trained using the FER2013 dataset takes in a 48*48-pixel image and processes it through various convolution, pooling and fully connected layers. All the Convolution layers have a filter size of 3×3, and all the Pooling layers have a pool size of 2×2.To increase the accuracy more, the DCNN was trained with KDEF dataset and the hyperparameters were changed and tries different values to find which values gave the best accuracy. First, the input image resolution size was changed and increased to different pixel values such as 90×90,100×100, 128×128, 150×150, 400×400, and 512×512. Among all of these input resolutions, the model performed with the highest accuracies using the 100×100-pixel size. For the minibatch size, the values 32, 64, and 128 were tested among, and 64 gave the best accuracy. The final DCNN model was trained for 200 epochs, and the best result obtained was with a test accuracy of 86.44%.

The DCNN was then integrated with an iOS application which can open the camera and take an image then detect the face in the image and send the image to the DCNN which can identify the emotion that is in the image. The application can be used by the teachers, parents and doctors to teach children with ASD to understand different facial emotion of people.

Vijay Banerje [11] in his paper proposes a novel cyberbullying detection method dependent on deep neural network. Convolution Neural Network is utilized for the better outcomes when contrasted with the current systems. Here it uses convolution neural network to create a model that detect bully related tweets and predict the behaviour of the new data introduced. The proposed approach uses word vectors that are feed to the CNN for classification of tweets. The dataset of chats and tweets form various social media platforms is collected for the evaluation. The proposed system is implemented in Python and TensorFlow. TensorFlow is a high-performance computing framework which is widely used in research, development and analysis in the fields of data science and deep learning. The Twitter dataset used consists of 69874 tweets, which are converted to vectors using open-source word embedding Glove. These messages were sorted and labels were generated. Neural Network model revealed here were implemented utilizing Keras on top of TensorFlow. We preprocess the data, exposing it to standard tasks of expulsion of stop words, accentuation marks and lowercasing, before clarifying it to allocating individual labels to each remark. This model achieved a testing accuracy of 93.97%. This result is much better than various existing cyberbullying detection systems based on data mining, machine learning and RNN based deep learning system.

Yuta Kihara [12] in his paper, presents a newly developed dynamic facial expression database, which includes not only the facial expressions of healthy volunteers but also the facial expressions of the patients with facial paralysis. A quantitative analysis method was also proposed to investigate the application of the database. The new database can be easily extended to a 3D facial expression database for facial paralysis analysis, and is valuable for facial paralysis research and facial paralysis treatment. In this paper what they did is, they took 5 datasets containing images of faces of 3 people with facial paralysis and 2 normal people. The images contain the people showing 10 different expressions usually asked by doctors to evaluate facial paralysis. And they took 14 feature points from these images and these feature points was then used to calculate the facial symmetry and difference of facial shape between the normal side and paralysed side. These calculated values were then compared with the facial symmetry and difference of facial shape calculated of the normal people. This can be used to find whether a person is at the starting stages of facial paralysis and begin their early treatments. The disadvantages of this paper were that, they have only taken 5 datasets and alignment of facial outline between all frames is required for higher accuracy.

III. Proposed System

The proposed system for this project consists of two sections. The first one is an android application that helps the parent to monitor their child by providing them with information's like screen recording, incoming messages and calls. The second one is a facial emotion code that can help the parent by providing the information's about child's mental state.

The main idea of this paper is to provide the parent with the viable information about the child to help them understand the mental state of the child and the issues that the child is going through at certain time. The application can be downloaded on both the parent and child device and the parent can use their side of application to help them retrieve information regarding their child. The parent can use the second section of the idea i.e., the facial emotion recognition to identify their child's emotional state at any time that they want and if they find out that the emotion is a negative emotion like sadness or angry then they can make use of the first section of the project to retrieve information's like screen recording to get a glimpse of what their child's problem are and try to solve it.

The main purpose behind the application is to provide some information to a parent about their child and their mental state, thus providing a way for the parent to take necessary action before things get out-of-hand. Parent can understand that their child is going through some emotional trauma and use the information that they get from the application to find an immediate solution for the child's issues.

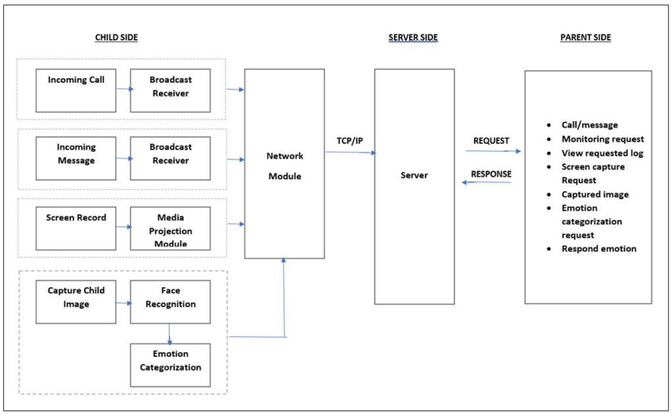


Fig. 1. Proposed Method.

A. Android Application

The proposed android application can be used by the parent to retrieve sensitive information's like screen recording, incoming messages and calls from the child's phone whenever the parent wants. Retrieving these informations can help the parent to understand what their child is going through.

1) Software and Hardware Specification: For developing this application, we have used JDK version 1.7, Eclipse version 3.3.2, Android SDK version 2.1-2.3, MySQL version 6.0 and Apache Tomcat version 7.0. Here the Application is built in Android and since the Android SDK and the emulator takes more resources to run, it will take more time if we are going for a system having less than 1GB RAM. To utilize the maximum with the 1GB RAM, we need a high-performance processor. JAVA IDE, Android SDK, Java SDK, Android Development Toolkit, Android plug-ins etc need to be stored in the system on which we are working, so 20GB or above RAM will be better for providing a decent environment to work with.

2) Module Descriptions:

- Child Module: This module will run in child's phone and helps to retrieve necessary information from the child side and send to the server whenever the parent request for certain information.
- Parent Module: Runs on the parent side application and helps the parent to collect child's data from the server.
- Server module: This module helps to collect data from the child's device and send that retrieved data to the parent's device using TCP/IP protocol whenever the parent module request for information.
- Network Module: This module is implemented in child, parent and server modules, and the main purpose of this module is to enable communication between the three modules.
- Database Manager Module: This module is used to retrieve data from database based upon the request from parent module.

B. Facial Emotion Detection

The second section of the project involves the development of a facial emotion recognition code. The main purpose behind adding this feature to the application is to help the parents to retrieve the emotional state of their child whenever they are using the device. This feature helps the parent to get an idea about their child's mental state.

1) Proposed Model: The facial emotion recognition that we are proposing is trained using an dataset that contains around 12000 color images of different people .The data set contains images corresponding to 5 facial emotions happy,anger,sad,neutral,surprise. We have used python with numpy and matplotlab for the facial emotion recognition and for detecting face in an given image haar cascade algorithm will be employed.

From the above mentioned dataset we created another dataset of grayscale images with faces identified using haarcascade and then with the dataset then formed we trained to code to identfy faces and their corresponding images by providing the input and its output. The trained recognizer will be able to differntiate between 5 different emotions. When an image is given ,that image will be converted to grayscale and then face will be recognised using haarcascade. From that image the recognizer will compare with the already trained dataset and provide us with the id corresponding to the emotion and the output will be an umage with the identified face ,the corresponding emotion and the perentage to which the emotion corresponds to that in the image.

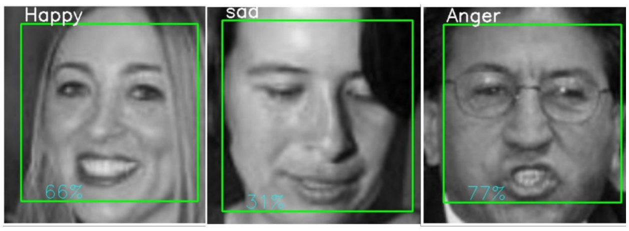


Fig. 2. Output of Facial Emotion.

Conclusion and Future Works

In this paper we proposed a method to improve the emotional state of a child by using facial emotion detection. Here we developed an application with facial emotion recognition feature, screen record and accessing incoming messages and calls. We developed and trained a facial emotion detection code and the code was implemented into an android application, so that the app can be used as a by-product of the model to be used by the parents to monitor their child. Using these features the parent can monitor their child's mental state and take necessary precaution to maintain the wellbeing of their child.

The future scope of this project is to develop a text emotion recognition to go hand-in-hand with the facial emotion recognition. A dataset can be developed which contain code mix language that can be used to train text emotion recognition. For the maximum utilisation of this application, it should come as an inbuilt application in devices so that parent can tag certain applications and get detail about their usage.

References

[1] Kessler RC, Angermeyer M, Anthony JC, et al. Lifetime prevalence and age-of-onset distributions of mental disorders in the World Health Organization's World Mental Health Survey Initiative. World Psychiatry 2007; 6: 168–76.

[2] Angold A, Costello EJ. The epidemiology of disorders of conduct: nosological issues and comorbidity In: Hill J, Maughan B, editors. Conduct disorders in childhood and adolescence. Cambridge: Cambridge University Press; 2001. p. 126–168

[3] Moffitt TE, Scott S. Conduct disorders of childhood and adolescence In: Rutter M, Bishop DVM, Pine DS, et al., editors. Rutter's child and adolescent psychiatry. 5th ed Oxford: Blackwell Publishing Ltd; 2008. p. 543–564

[4] Caspi A, Begg D, Dickson N, et al. . Personality differences predict health-risk behaviors in young adulthood: evidence from a longitudinal study. J Pers Social Psychol. 1997;73(5):1052–1063.10.1037/0022-3514.73.5.1052

[5] Petitclerc A, Tremblay RE. Childhood disruptive behaviour disorders: review of their origin, development, and prevention. Can J Psychiat. 2009;54(4):222–231.10.1177/070674370905400403

[6] Moffitt TE. Life-course-persistent and adolescence-limited antisocial behavior: a 10-year research review and a research agenda In: Lahey B, Moffitt T, Caspi A, editors. Causes of conduct disorder and juvenile delinquency. New York (NY): Guildford Press; 2003. p. 49–75

[7] Shaw DS, Gilliom M, Ingoldsby EM, et al. . Trajectories leading to school-age conduct problems. Dev Psychol. 2003;39(2):189–200.10.1037/0012-1649.39.2.189

[8] Romeo R, Knapp M, Scott S. Economic cost of severe antisocial behaviour in children – and who pays it. Br J Psychiatry. 2006;188(6):547–553.10.1192/bjp.bp.104.007625

[9] Gardner F, Shaw DS. Behavioral problems of infancy and preschool children (0–5) In: Rutter M, Bishop D, Pine DS, et al., editors. Rutter's child and adolescent psychiatry. Oxford: Blackwell Publishing Ltd.; 2009. p. 882–893.

[10]M. I. Ul Haque and D. Valles, "Facial Expression Recognition Using DCNN and Development of an iOS App for Children with ASD to Enhance Communication Abilities," 2019 IEEE 10th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON), 2019, pp. 0476-0482, doi: 10.1109/UEMCON47517.2019.8993051.

[11]V. Banerjee, J. Telavane, P. Gaikwad and P. Vartak, "Detection of Cyberbullying Using Deep Neural Network," 2019 5th International Conference on Advanced Computing Communication Systems (ICACCS), 2019, pp. 604-607, doi: 10.1109/ICACCS.2019.8728378.

[12]Y. Kihara, G. Duan, T. Nishida, N. Matsushiro and Y. Chen, "A dynamic facial expression database for quantitative analysis of facial paralysis," 2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), 2011, pp. 949-952.

THREAT IDENTIFICATION AND CLASSIFICATION IN IoT BASED NETWORK

1st Archana Radhakrishnan S
Computer Science and Engineering
Sree Buddha Colege of Engineering
Alappuzha , India
achu.archanakylm@gmail.com

2rd Dr.S V Annlin Jeba
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
email address

***Abstract*—Internet of things is defined as the resource constrained device via the internet of computing devices embedded in objects which have able to send and receive data.The huge number of devices and large network complexity lead to a chance of security issues.Existing monitoring technologies perform traffic analysis but which are very complex,expensive,inflexible and unscalable.So need an efficient system for identifying threats/vulnerabilities in IoT devices.In this system considering fives attacks ie, commonly occured in IoT devices.Distributed denial of service,Encrypted attacks,Flooding,Spoofing,Scanning these are the attacks under consideration .Aim of the system is to classify IoT devices and identifying threats in IoT.Machine learning play an important role in detecting threats in IoT.The proposed system uses convolutional neural network(CNN)for identifying the threats in each instance.KDD dataset is for traffic features.Changes in traffic value is passed to threat identification .It shows high accuray and precision than other algorithms.**

***Keywords*—Security,Machine learning,Internet of Things.**

I. Introduction

Internet of things (IOT) is an ecosystem of internet connected devices that are connected to the internet through wired or wireless connections.The huge number of devices and large network complexity lead to a chance of security issues.Lack of security in IoT faces number of challenges.Therefore,to maximize the visibility of IoT infrastructure and it is better manage security risks of these vulnerable devices .[2] The network operators want to know which IoT devices are connected to the network and their expected operations on the network,and monitor their activity for ensuring which devices behave normally or not. The aim of the system is to monitor behavior of IoT devices on the network using a combination of Software Defined Networking (SDN) telemetry and machine learning methods. SDN provides flow-level isolation and visibility in a low-cost and scalable manner. For accurate detection of devices and tracking of their dynamic behaviors, using machine learning algorithms to learn key patterns of traffic flows.

Primary focus in this work is to establish a machine learning framework based on various network traffic characteristics to identify and classify the default behavior of IoT devices on a network. The devices include cameras, lights, plugs, motion sensors, appliances and health-monitors.[4] Collect and synthesize data from this environment . A subset of our data is made available for the research community to use. Identify key statistical attributes such as activity cycles, port numbers, signaling patterns and cipher suites, and use them to give insights into the underlying network traffic characteristics. Develop a multi stage machine learning based classification algorithm and represent its capability to identify specific IoT devices with over ninety nine percentage accuracy based on their network behaviour.Evaluate the deployment of the classification framework in real-time, by examining the trade-offs between costs, speed, and accuracy of the classifier.

First contribution is to identify a set of TCP and UDP flows and highlight characteristics attributes, computed from timeseries of flows at multiple time-scales, distinguishing various IoT device types and their operating states on the network. Second contribution develops a multi-stage architecture consisting of a set of inferencing models that use flow-level attributes to automatically recognize traffic of IoT devices from non-IoTs, classify types of IoT devices, and identify operating states of each IoT during normal operation. Train the models and validate their performance to obtain high accuracy using real traffic traces. Finally, demonstrate the efficacy of scheme in detecting network behavioral changes due to firmware upgrade.

A. Scope

Rapid growth of IoT creates an operational challenge.Identifying what IoT devices are connected and whether they are functioning normally can become difficult for the administrator.[3][5] Lack of visibility into IoT devices can make it very complex for the administrator to trouble shoot problems in network, and can become particularly disastrous when cybersecurity attacks have breached this infrastructure. Most IoT devices send short bursts of data at irregular intervals. However, there has been no quantitative study in the literature to profile how much traffic they send in a burst, how long they idle between bursts, and whether these patterns are periodic or not. Also lack in understanding on how much signalling they perform in comparison to the data traffic they generate, or how much multicast/broadcast traffic they generate, needed for service discovery. No study has identified how these aspects vary from one IoT device to another,performing different functions.

B. Methodology

Internet of things is defined as the interconnection via the internet of computing devices embedded in objects which have able to send and receive data.It is regarded as a virtual network that interacts with real world taking internet as the core technology.As internet users continues to connect more IoT network devices,intruders try to gain greater surfaces to launch new types of attack.The deployment of IoT devices in both managed and unmanaged environment increases the complexity of systems,which in turn increases the vulnerability of IoT.The existence of such a large network of interconnected entities will definitely pose new security, privacy, and trust threats that put all those devices at a high risk, thus harming the affiliated users. Internet of things being the blend of so many technologies, all of these technologies have their own security and privacy flaws, which are to be addressed in IoT .It introduces the idea of categorising the attacks under four distinct types ,to cover the diversity of challenges and threats for all layers in IoT.The danger exposed by these internet connected things not only affect the security of IoT systems ,but also complete ecosystem.More attention should be paid to the analysis of these attacks,their detection as well as the prevention and recovery of attacks.

For example, in a local council, lighting sensors may be installed by the facilities team, sewage and garbage sensors by the sanitation department and surveillance cameras by the local police division. Coordinating across various departments to obtain an inventory of IoT assets is time consuming, and error-prone, making it nearly impossible to know precisely what IoT devices are operating on the network at any point in time. Gaining visibility into IoT devices in a timely manner is of paramount importance to the operator, tasked with ensuring that devices are in appropriate network security segments, are provisioned for requisite quality of service, and can be quarantined rapidly when breached. Network segmentation could have potentially prevented the attack and better visibility would have allowed rapid quarantining to limit the damage of the cyber attack on the enterprise network.[6]

Primary focus in this work is to establish a machine learning framework based on various network traffic characteristics to identify and classify the default behavior of IoT devices on a network. The devices include cameras, lights, plugs, motion sensors, appliances and health-monitors. Collect and synthesize data from this environment . A subset of our data is made available for the research community to use. Identify key statistical attributes such as activity cycles, port numbers, signaling patterns and cipher suites, and use them to give insights into the underlying network traffic characteristics. Develop a multi stage machine learning based classification algorithm and represent its capability to identify specific IoT devices with over ninety nine percentage accuracy based on their network behaviour.Evaluate the deployment of the classification framework in real-time, by examining the trade-offs between costs, speed, and accuracy of the classifier. First contribution is to identify a set of TCP and UDP flows and highlight characteristics attributes, computed from timeseries of flows at multiple time-scales, distinguishing various IoT device types and their operating states on the network. Second contribution develops a multi-stage architecture consisting of a set of inferencing models that use flow-level attributes to automatically recognize traffic of IoT devices from non-IoTs, classify types of IoT devices, and identify operating states of each IoT during normal operation. Train the models and validate their performance to obtain high accuracy using real traffic traces. Finally, demonstrate the efficacy of scheme in detecting network behavioral changes due to firmware upgrade. Also, quantify the trade-off between performance and cost of monitoring solution for real-time deployment. The solution builds upon preliminary work by identifying cost-effective attributes, and enhancing the architecture of inferencing that can detect changes in IoT devices. Believe that real-time monitoring solution empowers network operators to better manage cyber-security risks of their IoT infrastructure.

II. Related Works

Internet of things is defined as the resource constrained device via the internet of computing devices embedded in objects which have able to send and receive data.It is a virtual network that interacts with real world taking internet as the technology.The IoT objects have become smarter and is more intelligent and communications have turned informative. That is why , IoT is used in almost all domains like domestic, education, entertainment, energy distribution, finances, healthcare, smart-cities, tourism and even transportation.As a result, it is mandatory to supply high security modules that can determine the attacks very fast, so that the use cases can overcome from the effects of the attack and resume the normal operation at the earliest. But the lack of resources in IoT make it back breaking to provide security modules in IoT. The diverse IoT brands and user requirements also make it difficult to implement cross-device security solutions .Providing transparent services with security is the main challenge in establishing IoT.The distribution of IoT devices in both managed and unmanaged environment rises the complexity of systems,which in turn increases the risk of IoT.The existence of such a large network of interconnected entities will definitely constitute new security, privacy, and trust threats that put all those devices at a high risk, thus harming the associated with users.[3][4]

The instability displayed by these internet connected things not only affect the security of IoT systems ,but also complete eco system.Hence,for identifying various threats in IoT by using machine learning methods. In security ,machine learning simultaneously learns by examine the data to determine patterns so it is better to distinguish malware in encrypted traffic, find insider threats, foresee where dangerous neighborhoods are online to keep people safe when browsing, or protect data in the cloud by unwrapped apprehensive user behavior.Nevertheless, the evolution of the IoT security is far behind the footstep of the innovations . The uninterrupted enhancement of existing Internet security threats and bare a number of wireless network flaws that can be make use of active attackers. If essential precautions are not taken, the communication performance of authorised user will largely reduced, the accuracy of IoT systems will not be guaranteed, and even the personal safety and industrial production will be damaged.

So in this discussing about various mechanism for finding threats via machine learning.Approach that can learn the pigeonhole and corners of the threats and determine small malicious alternation in traffic. So, an efficient ML model with low threat identification time and better levels of accuracy is needed for IoT networks. IoT is a huge network and is connected with billions of IoT devices so, it generates a massive volume of data.The result is degraded when there is attacks in IoT , it is not easy to provide security in IoT. This system focus on developing a methodology that will have better attack detection time and better accuracy levels.[5]

The Internet of Things (IoT) explains the network of physical objects that are embedded with sensors and software the purpose of connecting and interchanging data with other devices and systems over the internet which means there is no human intervention. Considering the previous years, IoT has become the most important technologies of the 21st century. IoT can connect everyday objects like kitchen appliances, cars, thermostats, baby monitors—to the internet via embedded devices, seamless communication is possible between people and things.

By means of low-cost computing, the cloud, big data, analytics, and mobile technologies, physical things can share and collect data with minimal human intervention. The authenticity and security of IoT products depend on robust, end-to-end security approaches to protect consumers and their data. Many IoT network intrusion have been evolved using attacks indication or normal behavior specification.[2] But, these attacks or threats have; i) high false alarms; ii) inability to detect zero day attacks. So,investigators explored artificial intelligence (AI) and machine learning (ML) with an prominance on deep learning (DL) algorithms to build on systems security. Actually, learning techniques have a remarkable impact in fraud detection, image recognition and text classification. The efficacy of machine learning has encouraged the researchers to deploy learning algorithms among intrusion to enhance detection of cyber attacks, anomaly detection and determine abnormal behaviors among the IoTs. Therefore, this paper surveys and evaluates notable machine learning contributions for IoT network threats.

III. Research Methodology

In this section, first describe about dataset, its content, and the approach to preparing it for the learning task . Then, approach to extract data for the learning task , and explaining evaluation approach to evaluate the competency of the learning task .

A. Dataset

To have a clear view of the used dataset in this research, provides a description of traffic features, and gives the information about the characteristics of the dataset.

1) Dataset Over IoT Traffic Feature : KDD dataset is used throughout our project.The KDD data set is a well known benchmark in the research of Intrusion Detection techniques.It's evaluation is done by false alarm rate and detection rate.The KDD cup was an International Knowledge Discovery and Data Mining Tools Competition. In 1999, this competition was held with the goal of collecting traffic records Within the data set exists 4 different classes of attacks: Denial of Service (DoS), Probe, User to Root(U2R), and Remote to Local (R2L).[1]

The traffic features of IoT is collected from PCAP files in real time.Considering some IoT and non IoT devices for a particular time period and creating a network, passing data between them.Collected informations are traffic generated by the devices and traffic generated when user interacting with devices. Dataset which consisting of three states active,boot and idle state.Booting state is trying to connect with network.Active state is user interacting state and idle state is not active and idle.

2) Dataset Description: The dataset used is IoT traffic feature .KDD dataset is used for networking.IoT devices exhibit identifiable patterns in their traffic flows such as DNS/NTP/SSDP signaling profiles, activity cycles, and volume patterns.The dataset includes five categories of network traffic namely denial of service (DDoS),Spoofing,Flooding,encrypted,and Scan.

B. Correlation Based Feature Selection

Correlation based feature selection means,dataset contain many traffic features.In machine learning ,the system which learns the traffic features and according to that ,it takes decision for new instance.But no need all the features in the dataset to take decision .So need to reduce the feature in dataset.Attribute which is similar in their properties is reduced and only considering the important and dissimilar features which also take decision perfectly .And also it reduces the time complexity.

C. Evaluation Metrices

The following criteria are used to evaluate the utility of machine learning aided techniques in intrusion detection:

1) True Positive (TP): indicates that an intrusion is correctly identified.
2) True Negative (TN): indicates that a benign activity is detected as a non-malicious activity correctly.
3) False Positive (FP): indicates that a benign activity is falsely detected as a malicious activity.
4) False Negative (FN): indicates that an intrusion is not detected and labeled as a non-malicious activity.[3]

$$precision = \frac{TP}{TP + FP}.$$

$$Recall = \frac{TP}{TP + FN}.$$

$$F_1 = \frac{2 * Precision * recall}{precision + recall}.$$

IV. PROPOSED METHOD

The proposed method includes Convolutional Neural Network(CNN) that are trained with the prepared dataset and a decision that aggregates the output of CNNs. Figure illustrates the conceptual view of our proposed method. Using SDN ,considering set of flow rules that collectively characterize traffic signatures of iot devices .Flow rules are actively inserted into SDN swtiches to which IoT devices are connected.MAC address as identifier of device and then applying correlation based feature selection for reducing features .After that classifying IoT devices from Non IoT.Threat is identified using CNN algorithm of classified IoT devices.

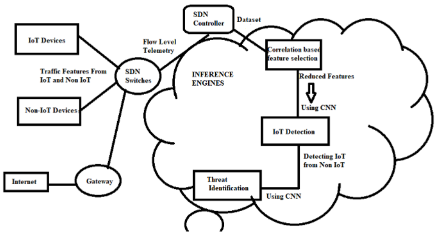


Fig. 1. System Architechture

A. IoT Verses Non IoT

Traffic features considered in dataset differentiate IoT device from non IoT .For finding IoT,determine the probability density of two attributes namely remote traffic and DNS query.In case of IoT devices it transfer only few amount of traffic data from remote network and the remote volume is very small.As compared with IoT ,Non IoT devices transfer more volume of data .In terms of DNS,IoT shows identifiable patterns of query but non IoT have a wider range of query.

B. IoT Device Types

Concentrating on IoT devices,considering three traffic attributes namely NTP responses,Upload volume of remote traffic and volume of SSDP responses .For identifying device type ,calculating above mentioned features of same IoT devices with different manufactures .From variation in responses determining the device type.[1]

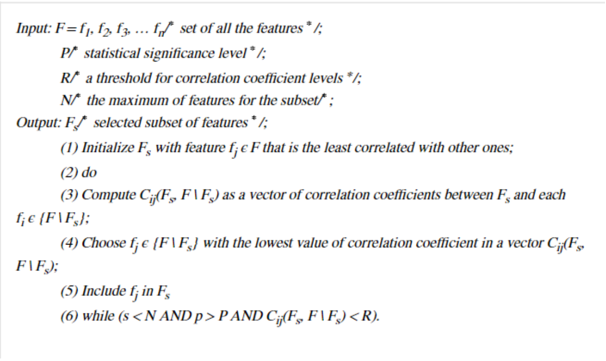
C. Threat Identification

In case of threat identification ,only examining IoT device type .In this system reviewing five types of threats namely DDoS,encrypted attacks,scanning ,spoofing and flooding are the attacks that considering for the threat identification.These attacks are caused when there is small variation in any of the traffic attributes.Change in values of traffic shows various threats. **DDoS attack** is a malicious attempt to interrupt the normal traffic of a targeted server which means it send flood of request which slowdown the system.Changes occur in flow ID,source IP,source port,destination port,timestamp and protocol can be considered as DDoS.According to vendors and devices,the value of the features may change. **Spoofing** is occured when security is breached through a lower level system on a shared IoT network.Identify spoofing attacks are very easy to get going in an IoT network.By the use of fake identity such as MAC and IP address of legitimate user ,spoofing attack can claim to another IoT device.**Flooding**,in this attack , the entire network is flooded by sending data packets .The attacker send huge amount of data then the flooded packet fail the network because it is very hard to identify this flooded node which corrupt the execution RREQ packet which causes MAC layer impacts and protocols like TCP is delicate to round trek.**scanning** attacks scan devices in HIS to gather network information of these devices before launching attacks to the HIS security.Scanning is commonly occured in IP address scanning ,port scanning and version scanning.So changes occurs in the features show scan attack in the instance.**Encrypted** attcks and IoT malware attack occurs over http ie,TSL and SSL encryption standards.So variation in values show the attack.These are the different attacks considered in the system for identifying threats in IoT over the KDD dataset.

D. Implementation

Correlation-based feature selection (CFS) figure shows ranks attributes according to a evaluation function based on correlations . The function evaluates subsets made of attribute vectors, which are correlated with the class label, but independent of each other. The CFS method assumes that irrelevant features show a low correlation with the class and therefore should be ignored by the algorithm.

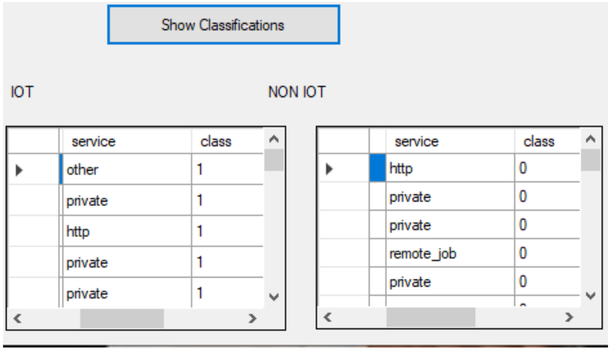
Algorithm



```
Input: $F = f_1, f_2, f_3, \dots f_n$/* set of all the features */;
        P/* statistical significance level */;
        R/* a threshold for correlation coefficient levels */;
        N/* the maximum of features for the subset/* ;
Output: $F_s$/* selected subset of features */;
        (1) Initialize $F_s$ with feature $f_j \in F$ that is the least correlated with other ones;
        (2) do
        (3) Compute $C_{ij}(F_s, F \setminus F_s)$ as a vector of correlation coefficients between $F_s$ and each
$f_i \in \{F \setminus F_s\}$;
        (4) Choose $f_j \in \{F \setminus F_s\}$ with the lowest value of correlation coefficient in a vector $C_{ij}(F_s,$
$F \setminus F_s)$;
        (5) Include $f_j$ in $F_s$
        (6) while ($s < N$ AND $p > P$ AND $C_{ij}(F_s, F \setminus F_s) < R$).
```

Fig. 2. CFS Algorithm

When IoT traffic features is passed through CFS,then it evaluated the traffic features and then it reduces the traffic features.Fig 3 explains the classification of IoT and Non IoT.The IoT classification I propose is based on the potential impact on living things in the event that the confidentiality, availability, or integrity of the IoT device’s information, internal operations, or components is compromised.After that applying CNN for threat identification. There exist a number of techniques such as Support Vector Machines (SVMs), and Decision Trees that can be used to train models to infer predefined classes. Performance of SVMs is very sensitive to selection of hyper-parameters, and hence it becomes difficult to train an accurate model. On the other hand, decision tree-based techniques are widely used since it is easier to generate (reasonably) accurate models with relatively small amount of data. Importantly they generate trees which can be readily interpreted but due to small amount of data decision take by the algorithms may be wrong. Neural networks



IOT

	service	class
▶	other	1
	private	1
	http	1
	private	1
	private	1

NON IOT

	service	class
▶	http	0
	private	0
	private	0
	remote_job	0
	private	0

Fig. 3. Classification of IoT and Non IoT

have proven to be very effective in classifying input data with high dimensions, and they demand a large amount of training data. It is best known for its performance in various classification tasks CNN algorithm is implemented in this system for classification of IoT devices and the threat identification.Threat identification follows four layers in CNN ,input layer ,max pool layer,dense layer and output layer. After applying correlation based feature selection ,the ouput is reduced features ,that can take decision by using reduced features.These reduced attributes are the input of CNN algorithm.Applying CNN algorithm firstly it enhance the attribute values of each instance.After maximizing the values it tends to dense layer ,there setting a threshold value for each attribute which take the decision .ie,any of the instance in the test data has threats .So in dense layer the threat is determined and it is passed to output layer.figure 2 shows all the layers. And when the threats occured or the values which the threats occuring is mentioned in above section threat identification.According to the operating state of the devices ,which type of alerts are given to the devices.

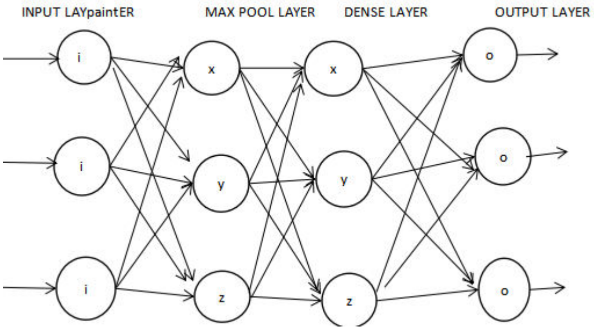


Fig. 4. CNN Layer

A network consist of various devices which flows continuously,but the features of IoT and non IoT are separated with the packet feature.After detecting the feature ,identifying if there is any fault occurs or not .If there is no threat then it is send to the intended recipient.If any fault occurs then different alerts are given to the corresponding device.And most of the IoT devices send short burst to destination continuously.minor traffic variations in different operating states can only be well learned with device-specialist models training a model of states classifier with instances from various devices will lead to an inaccurate prediction.

V. Performance Evaluation

Evaluate their performance using test instances. For both training and testing the traffic classifiers use Weka tool.Here considering KDD dataset which consist of more than thousand records and each of the instance carry fifty plus attributes.So each of the instance having values for attributes.Training system by using this dataset.Test data is given, the decision is taken based on learned data .Weka is a collection of machine learning algorithms for data mining tasks. The algorithms can either be applied directly to a dataset or called from Java code. Weka contains tools for data pre-processing, classification, regression, clustering, association rules, and visualization.[1]

Focusing on the safety and performance issues of enormous IoT data, blockchain is contemplated as a hopeful solution to store, process, and share data securely and efficiently. To meet the high power need,a deep reinforcement learning (DRL) performance-based optimization framework for blockchain-enabled IoT systems, whose objectives are triple:1) Providing a way to evaluate the system in terms of scalability, decentralization, security, and delay .2) Improving the scalability of the infrastructure blockchain without affecting the decentralization, delay, and security of the system; And 3) sketching a customizable blockchain for IoT systems, where block manufacturers, Integration algorithms, block sizes, and block spacing can be selected and adjusted using the DRL method. The simulation consequences show that their suggested framework can Better returns of blockchain-enabled IoT systems and be well reconcile to IoT dynamics. The modern development in data impelled technology has significantly standardized software-defined networking (SDN) features for different cloud-enabled streamlined applications. SDN also leverages the operational price of IoT sponsored the diverse and dynamic user necessary cases by on-line services. Though, the collaboration of various wireless networking components has created IoT unsafe for many natures of security attacks while worked with SDN. A robust security framework namely abbreviated as RF-IoT to address security loopholes has been Provided in the IoT networking environment .

To examine the impact and to describe relevant study challenges in the RFID area, this work produces the idea of the needed measurements by applying SDR technology, while arguing that PHY and MAC layers should be observed at integrally. To develop DFSA throughput (the number of reading tags in the unit of time) and so race up tag identification, easy calculations show that the number of tags should match the frame size. In changing RFID scenarios, such as intelligent shops or mechanical surroundings, it is important to know every good, with a used RFID tag, before it moves the examination space. Currently, mercantile reader solutions choose DFSA protocol as a mild MAC that controls the connection between a reader and various tags. Though, the literature presenting RFID performance explains that tag responsiveness is stochastic, while this has been usually neglected when considering the throughput. In the evaluation crusades, the metric of TRP is applied, provided as tag reply chance distribution, which can be applied for displaying the MAC layer as detailed . How to give uncomfortable bounds reported on the performance of the best-unbiased algorithms requiring a parameter from the attacked data and communications following an expected statistical model reading whence the sensor data depends on the parameter ere the attack. These attacks provide a certified attack performance in terms of the bounds careless of the algorithms the unbiased opinion system employs. IoT developed pervasive sensing and inspection abilities by the support of new digital relationships, signal processing, and large propagation of sensors without present difficult security challenges. The decisions exist notwithstanding the unbiased estimation algorithm selected, which could operate deep learning, machine learning, statistical signal processing, or any other way. Attackers can change the data registering or communicate of the IoT sensors, which can become a serious impression on each algorithm applying these data for reasoning

Precision	Recall	F1	ML Algorithms
0.979	0.987	0.983	RF
0.981	0.990	0.987	SVM
0.875	0.833	0.853	KNN
0.881	0.911	0.896	MLP
0.987	0.990	0.992	CNN

In terms of time complexity, an ideal cyber-attack detection should have reasonable and short training and inference times while having acceptable detection performance. During the training time, proposed method achieves acceptable performance in training .

VI. Conclusion

Operators of smart environments face mounting pressure to enhance their visibility into their IoT infrastructure with many vulnerable devices. This paper developed for solution of IoT devices using SDN-based flowlevel telemetry combined with machine learning.Identified traffic flows that can collectively characterize the network behavior of IoT devices and their states such as booting, user interaction or idle. Then trained a set of classification models for a inference architecture using traffic traces of IoT devices collected over KDD dataset. After validate their efficacy in detecting IoT devices from non IoTs, classifying their type, and identifying their operating state for detecting threats. Lastly, demonstrated how operators can use it to detect IoT behavioral changes .Machine learning algorithm is used for better performance .CNN shows high accuracy than other ML algorithms.

References

[1] Managing IoT Cyber-Security Using Programmable Telemetry and Machine Learning Arunan Sivanathan , Hassan Habibi Gharakheili , and Vijay Sivaraman

[2] Identification of Active Attacks in Internet of Things: Joint Model- and Data-driven Automatic Modulation Classification Approach Sai Huang, Member, IEEE, Chunsheng Lin, Wenjun Xu, Senior Member, IEEE, Yue Gao, Senior Member, IEEE, Zhiyong Feng, Senior Member, IEEE, Fusheng Zhu

[3] Semi-Supervised Learning based Security to Detect and Mitigate Intrusions in IoT Network Nagarathna Ravi, Student Member, IEEE, and S. Mercy Shalinie, Senior Member, IEEE

[4] An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic Mahdis Saharkhizan, Amin Azmoodeh, Ali Dehghantanha, Senior Member, IEEE, Kim-Kwang Raymond Choo, Senior Member, IEEE, Reza M. Parizi, Senior Member, IEEE

[5] A Machine Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT Mariam M. N. Aboelwafa, Karim G. Seddik, Senior Member, IEEE, Mohamed H. Eldefrawy, Yasser Gadallah, Senior Member, IEEE, and Mikael Gidlund, Senior Member, IEEE

[6] Active Machine Learning Adversarial Attack Detection in the User Feedback Process VICTOR R. KEBANDE 1,2,3, SADI ALAWADI 4 , FERAS M. AWAYSHEH 5, AND JAN A. PERSSON 1,2

Head Motion Controlled Smart Wheelchair

1st Ashif Safeer
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
ashifsafeer72@gmail.com

2nd Pavithra Thampi
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
pavithrathampib@gmail.com

3rdPrajeesh
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
prajeeshprasanna@gmail.com

4th Sreelekshmi P L
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha, India
sreelekshmipresanna99@gmail.com

5th Arya Raj S
Assistant professor
Dept. of CSE
Sree Buddha College of Engineering
Alappuzha, India
aryarajs89@gmail.com

***Abstract*—Loss of mobility to an injury is typically amid a loss of self-confidence. Designing a system with independent mobility for such disabled people is our aim in this paper. This wheelchair could be operated in any direction using head tilt movements by the handicapped person.The system also provides an emergency voice alert to a smartphone using gesture sensors and also allows a simple automation for one or two home appliances.**

***Index Terms*—accelerometer, dc motor, arduino microcontroller**

I. Introduction

The advancement and development of technology has always influenced a couple of parts of our lives since quite while and can keep it up doing such things with additional capacity and more unexpected development. In our project we have attempted our greatest to correlate between the advancement of technology and therefore the human requirement for the easiness of human life.

Unfortunately, day by day the amount of handicapped people is increasing because of road accidents as well as the disease which leading paralysis. As an assistive means of transportation, both elderly and disabled people need wheelchairs urgently. Normal and electrical wheelchairs with simple functions became gradually unable to the requirements of users. To supply elderly and disabled people with means of transportation with superior performance, and to assist them improve their freedom of mobility and reintegration, wheelchair now tend to be more intelligent.

The main aim of this project is to manage wheelchair through head movements. This project is especially designed for physically challenged people that are hooked in to wheelchairs and particularly those people that cannot utilize their hand to tug their wheelchair on account of some incapacity. Use of electrical wheelchair prompts a great deal of freedom for people with a physical handicap who can neither walk nor operate a mechanical wheelchair alone.

II. Background

Wheel chair is a gadget used by crippled and elderly persons for their transportation.A few sorts of smart wheel chairs are already available in the market,but a paralyzed or patients who cannot operate manual wheelchairs need a smart wheel chair for their purpose.So based on the patient requirements smart wheelchairs are developed based on motion,voice,eye,brain controlled etc.

III. Related Works

The proposed idea of the paper ‘development of the control system of voice operated wheelchair with multi posture charecteristics’ by Duojin wang [1] presents the control system of a voice-operated wheelchair. The implementation structure of the multifunction wheelchair is a mechanical structure, and the core part is the Control system. The system bears all the transformations of the wheelchair, including driving and posture change. The control system acquires a signal from the control terminal. The master controller of the control system processes the signal, and transmits a control signal to the control circuit of the corresponding execution module in order to control the execution module. As we can see, there are two driving motors and three linear actuators that are controlled by the system. Driving motors drive of the wheelchair. The actuators for lying and for standing can achieve posture change from sitting to lying and standing respectively. This not only simplifies the structure, but is also beneficial for the planning of the system . In addition, when considering safety in posture change, two anti-sway wheels are added under the footrest to make sure the center of gravity will not shift too much. The anti-sway wheels will not touch the ground in the sitting posture and will not affect obstacles encountered by the

Identify applicable funding agency here. If none, delete this.

wheelchair. Front driving wheels and universal wheels at the rear also improve stability and safety within the lying posture. An actuator is added to expand leg support making patients comfortable when lying on chair.

The proposed idea of the paper ‘control system of powered wheelchair based on tongue motion detection’ by Lu Liao [2] is to implement a smart wheel chair using tongue motion. The system is especially composed of the tongue motion sensors and embedded controller. The sensors detect the movement of the tongue in the mouth and sensor data is transmitted to an external controller via wireless communication device. The controllers receive the sensor data and processes the information received from the headset generating square wave signal to operate the wheelchair. The state of motion of wheelchair includes forward, left, right and stop. The system mainly rely on the wearable headset which detect tongue motion, to control the chair the tester first need to wear the headset and sit in the chair. When the tongue gore left side once the forward switch is connected, when tongue gore left side twice in predetermined time ,it moves left, when tongue gore right side twice it turns right. The tongue sensor in this system is the piezoelectric film sheets placing in the headset. There are two pieces of piezoelectric film sheets which placed on the right side and left side. The task of piezoelectric film sheets is to detect the motion of tongue then deliver the signal causing by tongue motion to microcontroller through the circuit.The control system is integrated into headset and has some advantages such as low cost, universal interference, which can be used in many different configuration and application. The system also use wireless receiver modules. When receive the radio signal, this module will process it by its internal circuit and then it send to the microcontroller via interface. Wireless receiver module is placed in the bottom of the wheel chair. The control system of wheelchair based on tongue motion is a new intelligent technology which is helpful for individuals with tetraplegia and similar impairments to improve life quality.

The proposed idea of the paper ‘A brain controlled wheel chair based on common spatial pattern’ by Yanyan xic [3] is to develop a brain controlled wheelchair. A Brain Computer Interface (BCI) system is an Electroencephalograph (EEG) -based system that can establish an information communication channel between human and environment. The BCI system uses only brain activity to drive and control external devices without the participation of peripheral nerves and muscles. The realization of EEG based BCI systems mainly involves three processes: signal collection, feature extraction, feature classification. . The BCI system is aimed at providing the disabled a way to communicate with the outside world at first goal, such as mind-control wheelchairs, prosthesis. As a substitute of walking tool, the wheelchair can assist the disabled individuals. The individuals who suffer from motor disorder with the cognitive ability can employ EEG signals to realize their purpose by the wheelchair. Therefore, the flexibility and convenience of BCI is the foundation of the wheelchair application.

IV. Proposed System

The main aim of the proposed system is to control wheel chair through human direction. In this system we use head motion module to recognize the motion of the user for controlling the direction of wheelchair. The wheel chair move towards left, right, forward and backward direction with respect to the motion of head. An Accelerometer is used to track these motions. The sensor is fitted to cap on head. A micro-controller is used to fetch the input signals, based on these signals micro-controller is programmed to take decisions which in turn control the movement of wheelchair. The system also provides a voice alert to a smart phone based on the patient’s finger movements. Gesture sensors are used for detecting the finger movements. On detecting the movement an alert will send to a smart phone. Also it provides a small home automation for one or two objects using the finger movement, the user can turn on or off his home appliances. For voice alert voice generation, when finger is moved the sensor sense the input and gives to the micro-controller, then it sends the input to Bluetooth module to activate voice alert on the smart phone. For Automation, the finger movements are sensed by the gesture sensors and the input is transmitted to the micro-controller, wireless connectivity is used for this mechanism.

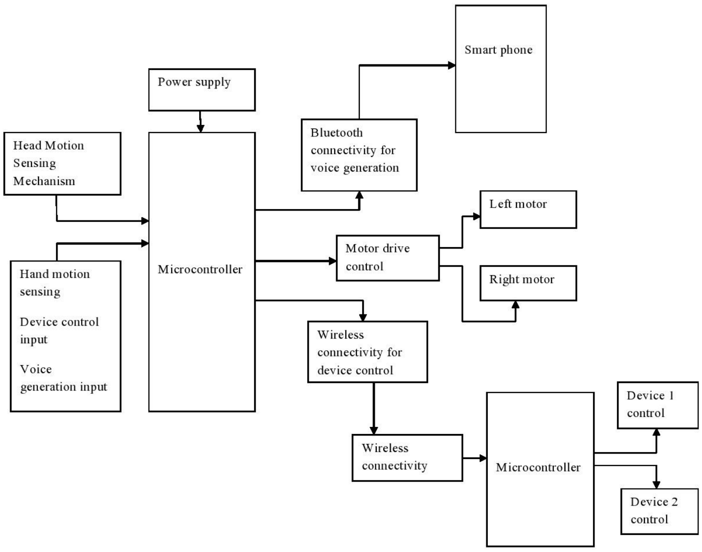


Fig. 1. System Architecture.

A. Accelerometer

An accelerometer is an electronic sensor that measures the acceleration forces working on an object, so as to see the object’s position in space and monitor the object’s movement. It is capable of measuring how fast the speed of object is changing. It generates analog voltage as the output which is used as an input to the control system. The accelerometer used in this system is ADXL345-1.

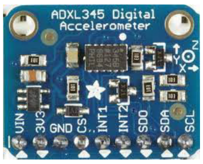


Fig. 2. Accelerometer Sensor.

B. Arduino

The Micro Controller which we are using is ATMEGA328. The Arduino Uno is microcontroller board dependent on ATmega328. It has 14 input/output pins, 6 analog input sources, a 16 MHz oscillator ,a USB association, power jack, ICSP header and a reset catch.

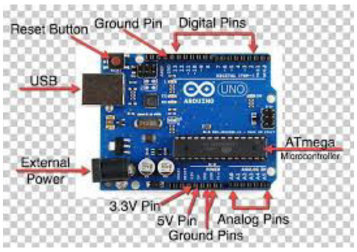


Fig. 3. ATmega 328.

C. Gesture Sensor

We use APDS9960 gesture sensor in this system. It has advanced gesture detection. Gesture detection utilizes four directional photodiodes to sense reflected IR energy to convert physical motion information to a digital information.

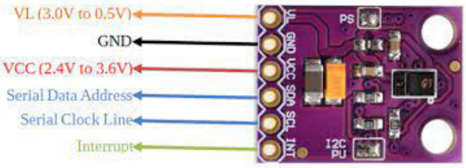


Fig. 4. Gesture Sensor.

D. Bluetooth Module

We use HC-05 Bluetooth module in this system. It is used for the automation and voice alert system. HC-05 Bluetooth Module is an easy to use Bluetooth SPP (Serial Port Protocol) module,designed for transparent wireless serial connection setup. Its communication is via serial communication which makes a simple path to interface with controller or PC. HC-05 Bluetooth module provides switching mode between master and slave mode which implies it to use neither receiving nor transmitting data.

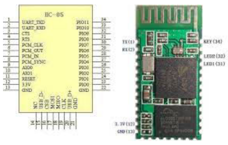


Fig. 5. HV-05 Bluetooth Module.

E. Motor

Motor receives power from the Motor driver IC. This power is used to move the wheelchair. DC motor orientation, speed and operation can be controlled by the microcontroller. We can start, stop and make it go in clockwise and anti clockwise direction.

F. Motor Driver

L293D is a dual H-Bridge driver, so with one IC we can interface two DC motors which can be controlled in both clockwise and anti clockwise direction and a motor with fixed direction of motion.

G. Power Supply

A device or a system that provides electrical or other forms of energy to associate output load.

V. Working

The head motion controlled wheel chair is work on the accelerometer sensor. The accelerometer sensor is connected with pin A1 and and gesture sensor is interfaced with with pin A0. These sensors sense the signals from the patient and convert it into the suitable signal which is given to ATmega328 microcontroller. The initiating movement is taken by toggle switch. The direction of the wheelchair is perpendicular to each axis forward,right and left. The relay is used to interface the microcontroller and dc motor wheel. The relay for motor R1 is connected at pin 12. for motor R2 at pin 13. The gesture sensor on the hand senses the signals according to finger movement, according to the finger movement it give input for the voice alert and automation. The voice alert is done by using a bluetooth module. An application is built for this purpose. The application installed in the smart phone will raise a voice alert. For automation, when input signal comes, it turn on the device. Wireless connectivity is used for this purpose. Based on the movement the device will turn on or off.

VI. Analysis

A. Motion Recogonition

This wheelchair allows the patient to have a control over four directions, left, right, forward and backward. Here shows the sample images of head motion for the movement of wheelchair.

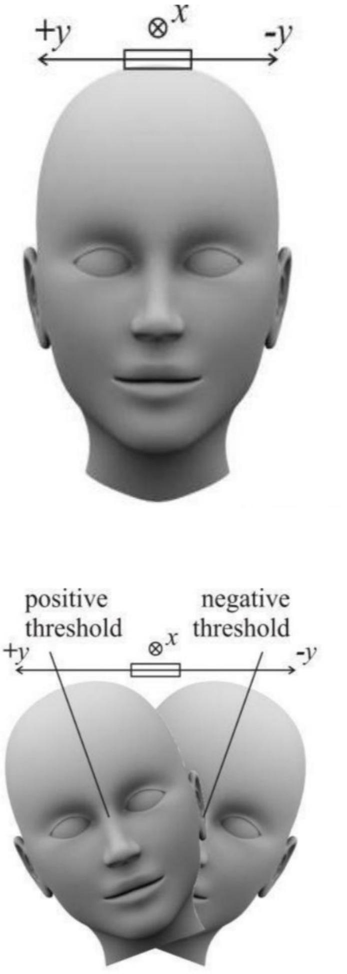


Fig. 6. The position of the accelerometer relative to head motion in right and left side.

VII. Result

The wheel chair controlled by Accelerometer is successfully designed. These wheel chair is created for the disable patient those who lost their or being paralyzed. The aim of this project is to use chair without the help of a companion.

VIII. Future Scope

We can use newest technologies for the movement of wheelchair. Numerous technologies are developed nowadays to improve the quality of human life. Researchers are going on for the improvement of smart wheelchair using nervous system of human.

IX. Conclusion

This paper presents the model of a wheel chair that is controlled by using accelerometer. The accelerometer is controlled by the tilt movement of head and it steer the wheelchair. Along with that it provides a voice alert to a smart phone using the hand gesture and also enable to power on/off one or two home appliances using hand gesture. By this we try to give more independence to the handicapped peoples.

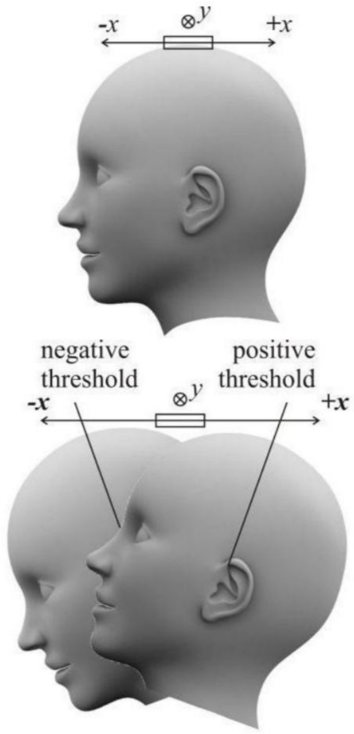


Fig. 7. The position of accelerometer relative to head motion in forward and backward direction.

References

[1] "Development of the Control System of Voice-Operated Wheelchair with Multi-posture Characteristics", Duojin Wang, Hongliu Yu - Shanghai Engineering Research Center of Assistive Devices Institute of Rehabilitation Engineering and technology, University of Shanghai for Science and Technology Shanghai, China.2017 2nd Asia-Pacific Conference on Intelligent Robot Systems.

[2] Lu liao, Ying Wu, yi xang, "Control System of Powered Wheel Chair based on Tongue Motion Detection"-2016 IEEE 15 international conference on cognitive informatics and cognitive computing.

[3] Yanyan xie, xiaow yi, "A Brain Controlled Wheelchair based on Common Spatial Pattern"- 2015 international symposium on Bio electronics and Bio Informatics.

E-GOVERNMENT SERVICES WITH ARTIFICIAL INTELLIGENCE

Gayathri Gireesh

Department of CSE, SBCE, Pattoor, Alappuzha, Kerala

e-mail: gayathrigireeshan@gmail.com

***Abstract*-The e-government's ultimate objective is offering enhanced portfolio of public services in an efficient and cost-effective way to citizens. The e-government also could give more transparency for the government because it enables the public to be informed about what government is working on and the policies which are enforced. The primary benefit would be replacing and optimizing the Paper Based System while implementing electronic government. That could save lots of time, money and also environment in return due to reducing paper consumption and the implementation of e-government could also promote better communication with government and business sectors. Although, it still faces several challenges. A framework that uses AI technologies to automate and facilitate the e- government services is proposed and tackle the challenges of E-Government. In this paper first, a framework for the management of e-government information resources is configured and then a set of deep learning models that aims to automate several e-government services is developed. Finally, a smart e-government platform to integrate recent advances in AI techniques in the e-government systems and services is proposed to improve the overall trust, transparency, and efficiency of e-government.**

***Keywords*-- Artificial Intelligence, Deep learning, Web services, E- Government, Convolutional Neural Network.**

Lakshmi S

Assistant Professor, Department of CSE, SBCE, Pattoor, Alappuzha, Kerala

e-mail: lakshmi.rnath@gmail.com

I. INTRODUCTION

Artificial Intelligence (AI) can be defined as the ability of a computer to simulate the intelligence of human behavior. AI is a field that falls at the intersections of several other domains. E-government is the use of technological communication devices, such as computers and the internet to provide public services to citizens and other persons in a country and the application of employing advanced electronic techniques and web services to present, exchange, and advance the government's services for citizens. E-government plays a critical role in advancing the economy of the government, citizens, and industry.

The advantages of implementing E-Government applications are;

- Transparency: It can be enhanced by providing easier access to up-to-date news and notifications.
- Trust: It can be enhanced by providing services and government information through transparent and easy-to-use technologies.
- Citizen Participation: By involving citizens in decision making and conducting survey processes, citizen participation can be improved.
- Environment Support: The large amount of paper applications can be reduced by E- Government services. This will support environment support. This framework uses recent advances in AI to improve the E-government systems and their interactions with the citizens. Develop

deep learning models that aim at automating E-government services. The system includes automating recognition of hand-written digits, recognition of hand-written letters and sentimental analysis. Integrating AI and deep learning applications in E-government services requires strong policy measures on data security and privacy. Several studies conducted for enhancing e-government services. Only few of them address utilizing recent advances in AI and deep learning. Utilizing deep learning algorithms can significantly improve the current state of e-government services and systems to become more efficient and economic. Automation is the technology in which a process or procedure is performed with minimal human assistance. The term AI and automation are often used interchangeably. Automation is basically making a hardware or software that is capable of doing things automatically without human supervision. They are associated with software or a physical robots and other machines that allow us to handle more effectively and efficiently.

Deep learning is an AI function that mimics the working of the human brain processing data and creating patterns for use of decision making. Learning can be supervised, semi-supervised or unsupervised. That is, deep learning AI can be able to learn without human intervention, drawing from data that is both unlabeled and unstructured. Different deep learning models developed for the systems are; Hand-Written Letters Recognition, Hand-Written Digits Recognition and Sentiment Analysis.

Hand-writing recognition is the capability of a computer to receive and interpret hand-written input from sources such as paper document, photographs, touch-screens and other devices.

Sentiment analysis is a Natural Language Processing technique applied to the data to determine whether data is positive, negative or neutral. Sentiment analysis is often performed on textual data to help various IEEE papers are described. Section two gives the literature survey where various IEEE papers are described. Section three gives an Overview of the Proposed System, section four presents Conclusion of the system. The future work comes in section five.

II. LITERATURE SURVEY

In the paper (A survey on Sentiment Analysis Challenges), the evolution of the internet as websites, social networks, blogs, online portals, reviews, opinions, recommendations, ratings, and feedback are created by writers. This writer generated sentiment content can be about books, people, hotels, products, research, events, and so on. These sentiments become very beneficial for businesses, governments, industries, and individuals. While this content is meant to be useful, a bulk of this writer produced content require using the text mining techniques and sentiment analysis. The research in a sentiment challenge and the average of accuracy rates are inversely proportional.

The work (Service Composition Applied to E-government) is concerned with the requirements on Web Service dynamic composition, it present a framework to discovery and compose Web Services and to invoke and execute the new composite service. This emphasizes the coexistence and seamless interoperation on varieties of software components, which have been distributed based on legacy applications or on emerging service standards. Here a Framework for Web Services composition that is part of an e-government platform Prototype is proposed. The system uses a metamodeling infrastructure and the Model Driven Architecture (MDA) concepts in order to be independent of composition technologies as conversation, choreography, orchestration and transaction.

The study (The Public Value of E-Government) organizes existing research on the public value of e-government in order to investigate the current state and what value e-government is supposed to yield. This literature study theorizes a descriptive and multidimensional framework that can improve our understanding of the public value of e-government from different viewpoints, and the overlap between them in actual e-government designs and implementations. Also, the performance of e-government is expected to help governments deliver services and transform relations with citizens, businesses and other arms of government. This research aim is to examine the existing research on the public value of e-government in order to understand the existing knowledge about the public value of E-government.

The paper (Sentiment Analysis using CNN) proposed a framework called Word2vec+Convolutional Neural Network (CNN). This service will show people the sentiment analysis of the product by using the data of people reviews in some online shopping sites. If the error and complexity of sentiment analysis can be reduced, this service will be more helpful. The objective of using word2vec is to gain the vector representation of word and reflect the distance of words. Three pairs of convolutional layers and pooling layers are used in this architecture. This is the first time that a 7-layers architecture model is applied using word2vec and CNN to analyze sentences' sentiment. Word2vec is a neural net that processes text before that text is handled by deep learning algorithms. In this problem, the aim is to classify the sentences with CNN, but CNN can't understand the sentences directly as a human. To overcome this, word2vec translates text into the vector that CNN can understand.

The existing system improves the E-government systems and their interactions with the citizens. The system includes 3 phases to automate E-government;

- Hand-Written Letters Recognition
- Hand-Written Digits Recognition
- Sentimental Analysis

Deep learning models are developed, that aims at automating E-government services. Utilizing deep learning algorithms can significantly improve the current state of E- government services and systems to become more efficient and economic.

A. Hand-Written Letters Recognition

Automating the process of converting hand-written text to digital text can play significant roles. It is used to archive and digitize files and written applications. Handwriting recognition system utilize basic computer vision and image processing algorithms to segment characters from an input image. The ResNet18 model is retained for this classification problem using the transfer learning technique.

B. Hand-Written Digits Recognition using NLP

It is used to facilitate detecting digits from paper applications, cars license plates, home addresses, street numbers and other products. A handwritten digit's recognition system was executed with the famous MNIST data set. Given the fact that the problem on hand (digits recognition) is similar in nature to letters recognition, the same steps in Hand-Written Letter Recognition is used here i.e., ResNet18 architecture is used.

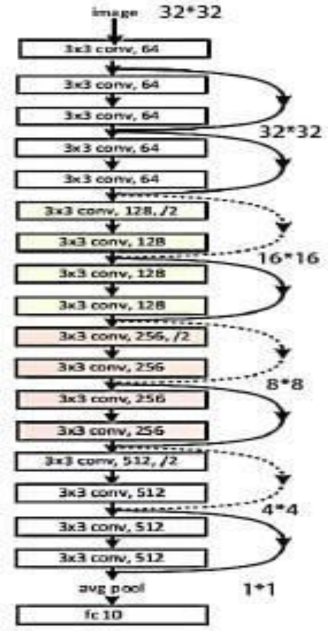


FIG 1: ResNet18 Architecture Overview

Steps to implement the CNN handwritten digit recognition using the NLP:

1. Import the libraries and load the MNIST dataset:
   The MNIST dataset is one of the most common

datasets used for image classification and accessible from many different sources. The MNIST database contains 60,000 training images and 10,000 testing images.

2. Data Preprocess and Normalize: To be able to use the dataset in Keras API, need 4- dims NumPy arrays. In addition, must normalize the data as it is always required in neural network models. This can be achieved by dividing the RGB codes to 255.
3. Building the Convolutional Neural Network: Build the model by using high-level Keras API which uses either TensorFlow or Theano on the backend. There are several high-level TensorFlow APIs such as Layers, Keras, and Estimators which helps us generate neural networks with high-level knowledge.
4. Compiling and Fitting the Model: With the above code, a non-optimized empty CNN is created.
5. Evaluating the Model: Finally, evaluate the trained model.

C. Sentiment Analysis

Sentiment analysis is used to identify and classify opinions of users in order to quantify and study their attitude towards a particular topic, service or a product. In order to help automating sentiment analysis services, deep neural network is presented. For the classification task, a unique architecture is implemented based on the Recurrent Neural Network (RNN). RNN employs feedback loops where the output from each step is fed back to the RNN to affect the outcome of current step, this process is repeated for each subsequent step.

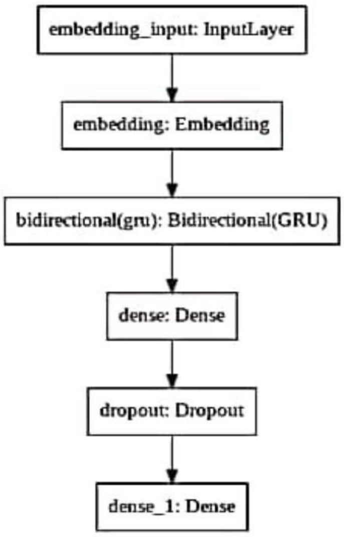

embedding_input: InputLayer
embedding: Embedding
bidirectional(gru): Bidirectional(GRU)
dense: Dense
dropout: Dropout
dense_1: Dense

FIG 2: Architecture of Sentiment Analysis Classification Model

Some disadvantages of the existing system are:

- If the dataset is too big, the work of labeling data will be huge
- Due to intrinsic sequential nature of RNN, the networks are hard to train on a parallel system.
- Sentiment Analysis still faces problems such as textual order, changeable sequence length, and complicated logic.
- Inaccessibility: Significant issues on accessing the internet and its services.

III. PROPOSED SYSTEM

The proposed system will improve the sentiment analysis phase by combining Convolutional Neural Network (CNN) and Long Short-Term Memory(LSTM). Emotion detection methods are classified into three, based on how detection are made to improve the outcome of sentiment analysis;

- Keyword-based detection: Emotions are detected based on the related sets of keywords found in the input text.
- Learning-based detection: Emotions are detected based on previous training result with respect to specific statistic learning methods

- Hybrid detection: Emotions are detected based on the combination of detected keyword, learned patterns, and other supplementary information. Semantic analysis utilizes techniques of natural language processing.

D. . Sentiment Analysis using CNN-LSTM

The current standard of keyword and attribute extractions is rule-based and ad-hoc, semantic analysis is proposed to extract keywords based on the linguistic information of sentences. LSTM channel is skilled at processing sequential information, while the CNN channel is capable of extracting abstract features from different horizons. CNN and LSTM layers were organized in an ordinal manner. The experiments are conducted on the Tensor Flow framework running on Python. The LSTM model take textual order and sequence length into consideration, the CNN is aimed at exploiting local features within the text. A regional CNN–LSTM model takes both local information within sentences and long-distance dependency across sentences into consideration for classification. The performances of LSTM and CNN rely on the amount and quality of labeled data. The quality of word embedding significantly influences the classification results since it measures the relationship among word vectors in vector space. The word2vec is used to gain the vectors for the words as the input. Word2vec is a neural net that processes text before that text is handled by deep- learning algorithms. This problem classifies the sentences with CNN, but CNN can't understand the sentences directly as a human. To deal with it, word2vec converts text into the vector that CNN can understand. At the same time, the vector produced by the word2vec can represent.

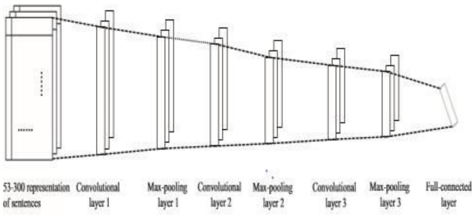


FIG 3: Architecture of Convolutional Neural Network

Here, convolutional layers, pooling layers, Parametric Rectified Linear Unit (PReLU) layers and dropout layers in CNN are used. In the architecture of CNN, the most time of training the neural network is spent in the convolution. The main aim of convolution is to extract the input feature, and pooling is to sample the convolution matrix. When training a neural network model, the dropout will be an important trick. It solves the main problem in machine learning, that is over-fitting. The dropout consists of setting to zero and output of each hidden neuron with probability of 0.5. Among all emotion models, the OCC model, which includes 22 emotion categories. By the use CNN, the test accuracy of the system can be increased up to 5%. Incorporating emotion models into semantic analysis would yield a more systematic way to analyze various textual inputs.

After representing each word by its corresponding vector trained by Word2Vec model, the sequence of words $\{T_1, \ldots, T_n\}$ are input to LSTM one by one in a sequence.

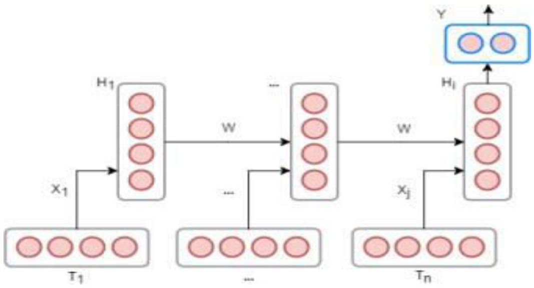


FIG 4: The idea of LSTM

Each term T_j is first converted to the corresponding input vector x_j using Word2Vec model and input into LSTM one by one. At each time j, the output W of the hidden layer H_j will be propagated back to the hidden layer together with the next input x_j+1 at the next point of time j+1. Finally, the last output W_1 will be fed to the output layer. To conform with the sequential input of LSTM, first convert posts into three-dimensional matrix M(X, Y, Z), where X is the dimension of Word2Vec word embedding model, Y and Z are the number of words in the post and the number of posts respectively. To avoid the very long training time, here a single hidden-layer neural network is adapted. The number of neurons in input layer is the same as the dimension of Word2Vec model, and the number of neurons in output layer is the number of classes, which is 2 in this case. By gradient-based back propagation through time, we can alter the weight of edges in hidden layer at each point of time. After several epochs of training, we can obtain the sentiment classification model.

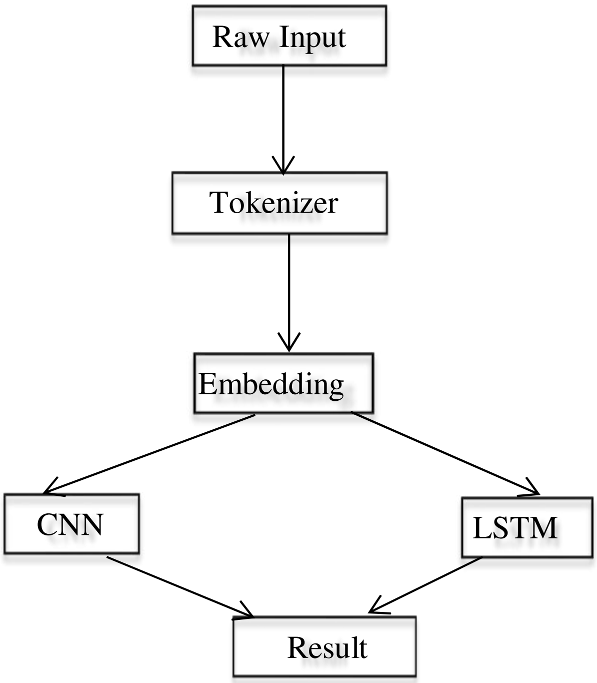


FIG 5: Simple Architecture of Sentiment Analysis using CNN-LSTM

IV. CONCLUSION

More government agencies are starting E-government services to improve their systems and services with the recent advances in AI and deep learning technologies. Surveyed existing research of emotion detection and reviewed the limitations to improve detection capabilities. The proposed system only focusing on the Sentiment Analysis phase, because in the existing system the test accuracy is low. By the implementation of the improved sentiment analysis phase, the overall performance of the system can be improved. The goal of this system is to improve the overall trust, transparency, and efficiency of e- government.

V. FUTURE WORK

For the future research, it is worth investigating that the application of deep learning architectures in the user’s interests discovery, and recommendation and to improve the quality of the word embedding by integrating WordNet lexical database with the input layer.

REFERENCES

[1] K. He, X. Zhang, S. Ren and J. Sun, "Deep residual learning for image recognition", Proc. IEEE Conf. Comput. Vis. Pattern Recognit., pp. 770-778.

[2] Y. LeCun, Y. Bengio and G. Hinton, "Deep learning", Nature, vol. 521, no. 7553, pp. 436-444.

[3] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith and P. Steggles, "Towards a better understanding of context and context-awareness", Proc. Int. Symp. Handheld Ubiquitous Comput, pp. 304-307.

[4] Yequan Wang, Minlie Huang, Li Zhao and Xiaoyan Zhu, “Attention-based LSTM for Aspect-level Sentiment Classification”, State Key Laboratory on Intelligent Technology and Systems Tsinghua National Laboratory for Information Science and Technology Department of Computer Science and Technology, Tsinghua University, Beijing 100084

[5] D. M. El-Din Mohamed Hussein, "A survey on sentiment analysis challenges", J. King Saud Univ.-Eng. Sci., vol. 30, no. 4, pp. 330-338.

[6] Xi Ouyang, Pan Zhou, Cheng Hua Li and Lijun Liu, “Sentiment Analysis Using Convolutional Neural Network”, IEEE International Conference on Computer and Information Technology.

[7] Al-Smadi M, Talafha B, Al-Ayyoub M, Jararweh Y , “Using long short-term memory deep neural networks for aspect-based sentiment analysis of Arabic reviews”. Int J Mach Learn Cybern. https ://doi.org/10.1007/s13042-018-0799-4.

[8] Kim Y, “Convolutional neural networks for sentence classification”, pp 1746–1751. https ://doi.org/10.3115/v1/D14-1181. arXiv :1408.5882.

[9] Savita Ahlawat, Amit Choudhary, Anand Nayyar, Saurabh Singh, Byungun Yoon, “Improved Handwritten Digit Recognition Using Convolutional Neural Networks (CNN)”, https://www.mdpi.com/1424-8220/20/12/3344.

[10] Kartik Dutta, Praveen Krishnan, Minesh Mathew, C.V. Jawahar, “Improving CNN- RNN Hybrid Networks for Handwriting Recognition”.

[11] WeiLia, Luyao Zhua,Yong Shib, KunGuob, Erik Cambriaa, “Sentiment analysis using lexicon integrated two-channel CNN–LSTM family models”, Nanyang Technological University, 639798, Singapore b School of Economics and Management, University of Chinese Academy of Sciences.

CryptLoc: Location Based Crypto-Locking System

Akhil H
Department of Computer Science and Engineering
Sree Buddha College of Engineering, Pattoor
Kerala, India
akhilbkv@gmail.com

Niji Anna Saji
Department of Computer Science and Engineering
Sree Buddha College of Engineering, Pattoor
Kerala, India
nijiannasaji007@gmail.com

Sayan T Mathew
Department of Computer Science and Engineering
Sree Buddha College of Engineering, Pattoor
Kerala, India
sayantmathew9895@gmail.com

Shyno S Koshy
Department of Computer Science and Engineering
Sree Buddha College of Engineering, Pattoor
Kerala, India
shynokoshy909@gmail.com

Dr. S.V Annlin Jeba
Head of the Department
Department of Computer Science and Engineering
Sree Buddha College of Engineering, Pattoor
sureshannlin@gmail.com

***Abstract*—- Cybersecurity is very important because of some security threats and cyber-attacks. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.Nowadays, theft of goods, important things and valuable properties from a vehicle is increasing. The security of such things while transporting from one place to another is a major concern. Eventhough many precautions and safety measures are adopted in order to ensure the security of valuables inside a vehicle, theft activities are happening. There are many existing methods to prevent the attacks against a vehicle.Locking systems can ensure security to an extent. But, physical locks can be attacked easily. So smart lock system ensures the security by increasing connectivity among the devices.In recent days GSM and GPS module used in theft detection and vehicle tracking system. These technologies play a major rolein vehicle security, but they can be affected by cyber attacks. The proposed method describes a cryptographically shielded highly secure lock system to resolve the valuables security and information security issues. Here, a secure smart hybrid lock (CryptLoc) with location and cryptography is designed that will provide end-to-end security for various applications in the real world. This CryptLoc protects the valuables that are carried in a vehicle from one place to another.**

***Index Terms*—Cybersecurity, vehicle security, Cryptography, Location, Locks**

I. Introduction

Cybersecurity affects each one of us in a multitude of levels. Our professional work, our personal lives, evens our vehicles that depend on connectivity and technology which runs in complex software. As information technology becomes increasingly integral to our daily life. Our dependency on subsequent information systems grows. In turn, we experience an increase in potential attacks and vulnerabilities against those systems[1]. Cybersecurity loom out of necessity to protect these systems and the information contained within them. Applied to vehicles, cybersecurity takes on an even more important role: systems and components that govern safety must be protected from harmful attacks, unauthorized access, damage, or anything else that might interfere with safety functions. Currently, the transportation of rare and expensive materials is very prone to theft and tampering[2]. Especially, in India there are many such cases which have been reporting thefts of products from the vehicle. In the transportation of valuable materials, theft is very common in transit. Petroleum products are stolen from tankers by whom they were authorized to transport.

Question papers of examinations are stealed away in transit before the examinations and leaked to the public. Milk, oil and other such products are diluted and degraded while they are being transported. All these thefts happens due to the design of locking mechanism in such a way to provide the authority of entry to the person who has the key. Recently vehicle tracking system is getting vast popularity due to the rising number of stolen vehicles. Vehicle theft is happening on parking and sometimes driving in unsecured places[3].

To solve this unpleasant scenario, an advanced security system is implanted in the vehicle which is used for transportation of products. This security system consists of a mobile application, a server and hardware. Cryptographical lock is introduced to open and close the lock which will be opened and closed at a particular location which is predefined.

The proposed method contributes to the security of the valuables inside a vehicle, eliminates the human intervention while transportation and is capable of being accessed only at the source or the destination.

II. LITERATURE REVIEW

IoT is revolutionizing the world. One of its renowned applications is a smart door lock system to protect the valuables and secrets behind the door. [4] Presents a secure door lock system named as cryptoLock which is using three emerging fields of the modern era. A complete cryptoLock system consists of hardware, a server, and an Android application. Hardware is highly secure and sends updates to the server through a secure channel. In case of unauthorized access, it generates an alarm to alert the local security and also informs the user through the app[5]. The users can interact with cryptoLock using both keypad and android app. The user login to the Android application using a unique username and password and authenticated by the server. After authentication the user exchange information over the network using AES-128 and SHA-512 algorithms[6]. The user can now lock the door, unlock the door, reset the password also in case of unauthorized access, the user will receive an emergency notification from our cryptoLock. A cryptoLock has two security steps while transmitting data over the network[7]. The first is data hashing in order to maintain the integrity of data and to avoid reply attack and the second step is data encryption in order to maintain data confidentiality. The main issues faced here is the CIA principle is partially fulfilled i.e, attacker can reproduce the parameters so Integrity is not satisfied, Key management issues can be occurred due to Symmetric key.

Fuel is one of the most valuable commodities worldwide, and this has led to a manifold increase in fuel theft globally. [8] Proposes a system that monitors the real time fuel level inside the storage tank of the tanker using a level sensor placed at the ceiling of the tank. If the averaged reading falls below a certain threshold, an SMS indicating low fuel level is sent to the appropriate authorities. A GPS module fitted on the tanker will continuously send the location of the vehicle to a mobile application[9]. A security system comprising of an electronic lock protects the compartment which houses the fuel valve and the lock uses password protection. Two separate OTPs, one for the tanker guard/driver and another for the agency which is taking the fuel delivery are randomly generated using an algorithm and get delivered on separate mobile applications[10]. The security system uses a keypad which is used to enter the received OTPs to the micro-controller. The micro-controller program is written in such a way that only if both the entered OTPs are matched correctly with the ones which were generated and sent to the mobile application, then only the user will have the access to the fuel in the tanker. For this, a solenoid lock is used which activates only when the correct OTP is entered and allows the user to access the fuel, otherwise it is closed preventing the unauthorized access of the fuel[11]. Although the fuel level drops below a certain level, which is a result of the fuel theft, it is sensed by the level sensors and is informed to the microcontroller. The micro-controller then sends commands to the GSM module to inform the fuel agency by sending them an SMS message. The SMS is sent using the SIM card with the help of a cellular network[12]. The message to be sent is conveyed to the GSM module by the micro-controller by serial communication. The main issue faced in this paper is that there is no cyber-security provided and so the attacker can access GPS parameter.

Vehicular ad-hoc network(VANET) is a part of mobile adhoc networks where data communication happens among the vehicles over a wireless network. [13] Explains vehicle security in VANET and data origin authentication using ECDSA. VANET needs to satisfy before its deployment onto the network is: vehicle authentication, message non-repudiation, vehicle anonymity and availability, message, confidentiality and integrity[14]. These requirements protect the message transfer from tampering. To stop the attackers to build any new fake profile of the user, these privacy requirements ensure that the information of the user is hidden and anonymous. A number of attacks can happen in the network due to its wireless, decentralised and dynamic nature[15]. They can be either be insider, i.e., internal vehicles that are unauthorised or from outside by the external vehicles. Different types of attacks which can harm the smooth functioning of the communication among the vehicles: DoS attack, Sybil attack, wormhole attack. In this paper, the Sybil attack and its removal by ECDSA is discussed in order to secure the authenticity of packets containing crucial messages[16]. The elliptical curve digital signature algorithm has been used to check the authenticity of the message and to strengthen the privacy of the vehicle[17]. The main issue faced in this paper is that the Replay attack can be occurred and timestamp is not included.

Authentication of the communication peers and encryption of the secret messages are often used as countermeasures to the attacks. [18] Uses location-based encryption method that not only ensures message confidentiality, but also authenticates the identity and location of communicating peers. This method is an extension of geo-encryption which limits the area inside which the intended recipient can decrypt messages. The main contributions include: (i) a detailed design of the key composition and recovery mechanism, including techniques to map the location coordinates to a unique value in order to authenticate the communicating peer's location; (ii) the prediction of the decryption region in a dynamic vehicular environment (iii) the modification of geo-encryption. The population of vehicle is huge and vehicles move from place to place[19]. Geo-encryption scheme uses symmetric cryptographic algorithms. The GeoLock mapping function converts geographic location, time and mobility parameters into a unique value as a lock. This unique lock value validates that the recipients satisfy certain restriction, for example the decryption region at a certain time interval[20]. The main issue faced in this paper is the overhead of packet size increase and the decryption time by varying the updated pause time. The updating pause time is the time interval to update locations of senders and receivers.

The use case of door lock, connected to the Internet and with ability to enter or exit room based on rights, is used for design and analysis of custom made systems regarding security. [21] Describes Internet of Things Cyber Security: Smart Door Lock System which is designed to offer some features like

Flexibility, Evaluation and prediction and Energy savings. The hardware module i.e, the lock is deployed to listen for commands directed from the central unit. Every lock client only corresponds with one central unit at the time, following the “separation of concerns” principle[22]. When registered, clients are granted access to certain restricted areas by system administrator, i.e. they are assigned security roles which enable them access to secured resources. End users interact with the system through mobile and web applications which are implemented for that purpose[23]. Web application which is used for resource management and security administration handling, providing detailed insight into resource usage over the time, as well as the current state of occupied resources[24]. Firstly, User logs in the system via mobile app. Provided credentials are validated on the server (central unit) and the authentication response is returned to the client. Successfully logged in user is offered various resources available to occupy (unlock). After the resource is selected by the client, the request is sent to the central unit to be validated. If authorized, user will be given right to use the resource, and the request will be forwarded to the corresponding lock client, eventually unlocking the resource. Server is the core element of the system, representing the mediator in every communication between end clients and physical locks[25]. The main issues faced in this paper is that the False impersonating attack can be occured as a lock to the authentication server might be possible if the attackers had access to credentials stored within the lock and the other attack that can be occurred is man-in-the middle (MITM) attack. It implies that the attacker managed to put a malicious node between authentication server and a lock, using one of the several methods for MITM[26]. This would allow the attacker to eavesdrop and change the packets that are transferred.

When researching related works and existing commercial solutions, one can also notice that most solutions doesn’t offer Cyber-security for their locks, which may also lead to a significant security attacks. However, some papers focus on the security issues but they cannot fulfill the basic principles of cyber-security i.e, Confidentiality, Integrity, Authentication (CIA Triad). So in this paper we propose and describe the smart lock system with similar functionality as existing solutions but put a focus on security of the proposed lock. This is necessary in order to anticipate vulnerabilities that were observed throughout the related work and to highlight potential issues in existing lock solutions.

III. BRIEF DESCRIPTION OF CRYPTLOC

First of all, the server is updated by entering the VehicleId, ExpectedLocation, ExpiryTime through the mobile application. The vehicle contains a Hardware Module which consists of servo motor to open and close the lock, an accelerometer sensor to detect the motion of the vehicle, a GPS sensor to fetch the location of the vehicle and a Raspberry pi based Microcomputer Whenever the vehicle is stopped, the accelerometer sensor detects that the vehicle has stopped and the hardware module triggers a request to the containing current location with some parameters such as Encrypted Random Nonce, VehicleId, CurrentTime, CurrentLocation and Signature. The server checks whether the current location is the same as the expected location. If the location and the parameters are matching, then an access token is generated from the server and it is be sent to the vehicle. The lock is opened and a success message is sent back to the server. The server updates the unlock status and send a push notification to the user. This is the case when the user selects Auto Unlocking in the mobile application.

If the user selects manual unlocking, the server pushes a notification to the mobile application. When the user accepts the notification then only the lock gets opened and if the user rejects then the lock will not open. The manual unlocking method is thereby used to give control to the user of the mobile application to open the lock or not.

IV. PROPOSED METHODOLOGY

This Section gives an overview about the working of each module of the CryptLoc which includes (i) Cryptloc Application (ii) Hardware Module (iii) Server

A. *CryptLoc Application Design*

The App has been developed to enter the details to the database. The mobile application has two main Activity: Login Activity and Main Activity .The user login to the App using Username and password. In the server side, server checks whether the Username and password are correct. If both are correct, the user gets access to the Main Activity. In the Main Activity, update the server by entering the data such as VehicleId, ExpectedLocation, ExpiryTime of the vehicle. There are two options in the mobile application, one is Auto Unlocking and the other is Manual Unlocking. If the user selects Auto Unlocking, then the lock is automatically opened when the vehicle reaches the expected location. But if the user selects Manual Unlocking, a notification is send to the user’s mobile application when the vehicle reaches the expected location. The lock is opened only if the user accepts the notification.

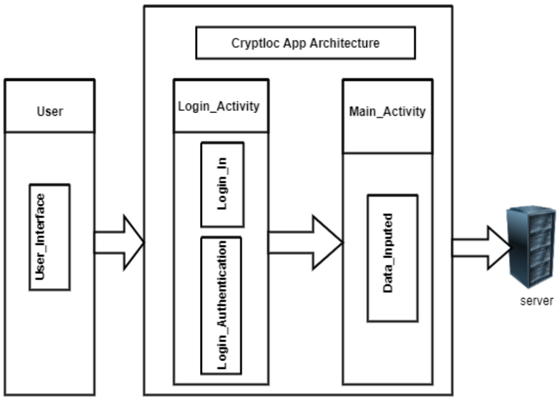


Fig. 1. CryptLoc Application Architecture.

Fig.1. shows the architecture of the CryptLoc application. CryptLoc Application receives input User.It updates the information into the Server.

B. Hardware Module

The CryptLoc hardware consists of the following components:

- Servo Motor
- ADXL345 Digital Accelerometer
- Raspberry PI
- UBLOX NEO6M GPS Module

The hardware module is fitted to the vehicle. Whenever the vehicle is stopped, the accelerometer sensor detects that the vehicle has stopped. Now, the Hardware Module will trigger a request to the server which contains the CurrentLocation of the vehicle, Current Time, Encrypted Random Nonce, Signature and ExpiryTime. The Server sends back a response to the module containing an Access Token. The Hardware Module verifies the Access Token and if it is valid, then the lock gets opened.

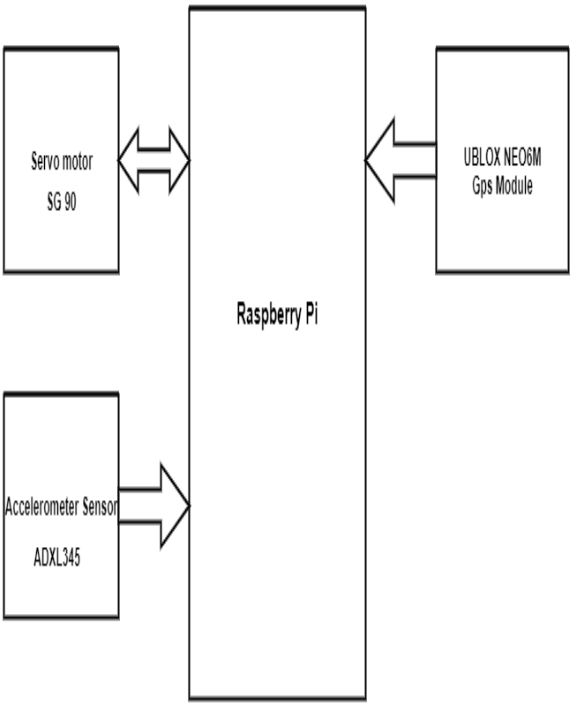


Fig. 2. Hardware Architecture

Fig.2. shows the architecture of the hardware.Raspberry Pi is a minicomputer which processess the information received from Servomotor, Accelerometer Sensor, GPS.

C. Server Design

The server contains the database and it also works as a handler. The server receives data from the mobile application and the data is verified. Then it processes the data and adds it to the database. Server waits for the request from the vehicle. When it receives the Access Token request, it verifies whether the ExpectedLocation from the mobile application and CurrentLocation from the vehicle are same, also verifies VehicleId, ExpectedLocation, ExpiryTime and other parameters. If all are correct, the Access token is sent to the vehicle.

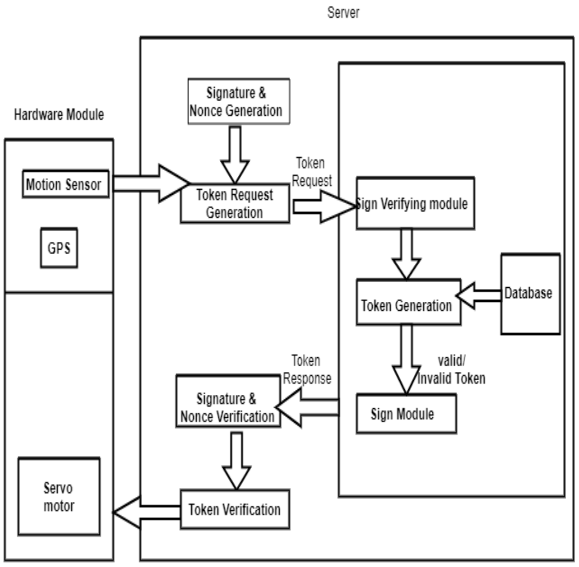


Fig. 3. Hardware to Server Architecture

Fig.3. shows the communication path between the Hardware Module and The Server.Server receives the information from the Hardware Module and performs the operations such as Token generation ,Signature verification etc.

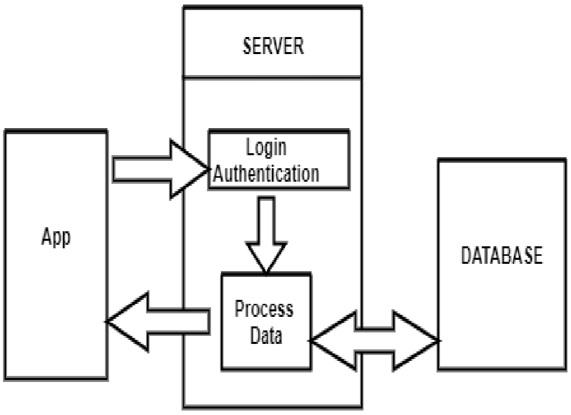


Fig. 4. App to Server Architecture

Fig.4. shows the communication path from Mobile application to the Server.The username and password given in the Mobile Application is authenticated by the Server and the data is also processed.

D. Operational Security

The CyptLoc has security steps to address all the known security issues.Signature is used in order to maintain the integrity of data , Random Nonce is used to avoid reply attack. Assymetric data encryption is used to maintain data confidentiality.

First of all, we update the server by entering the VehicleId, ExpectedLocation, ExpiryTime through the mobile application.

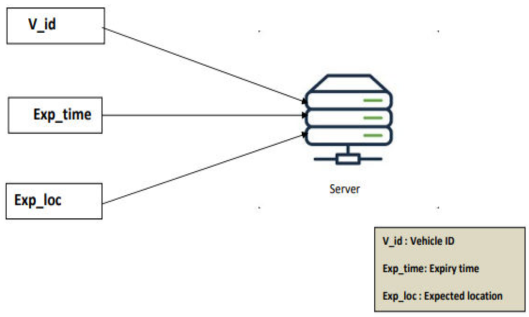


Fig. 5. Sending information to server from Mobile Application

The vehicle contains a Hardware Module which consists of servo motor to open and close the lock, an accelerometer sensor to detect the motion of the vehicle, a GPS sensor to fetch the location of the vehicle and a Raspberry pi based Microcomputer. Whenever the vehicle is stopped, the accelerometer sensor detects that the vehicle has stopped and the Hardware Module triggers a request to the server containing CurrentLocation, Encrypted Random Nonce, VehicleId, CurrentTime, CurrentLocation and Signature.

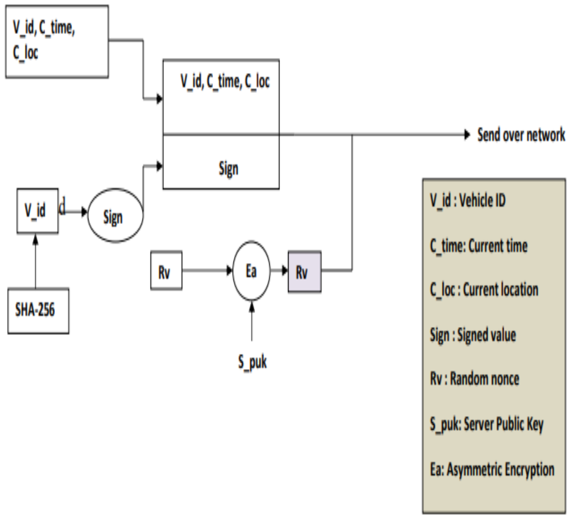
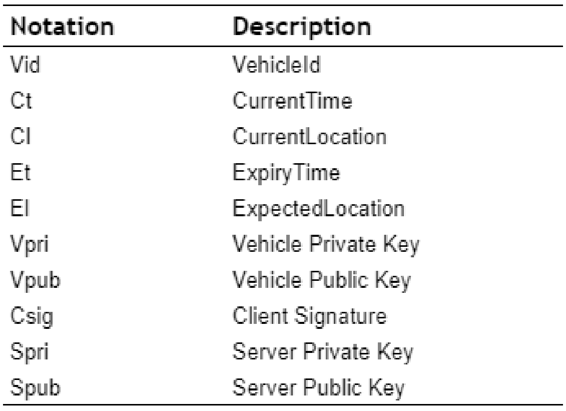


Fig. 6. Sending information from Hardware module



Notation	Description
Vid	VehicleId
Ct	CurrentTime
Cl	CurrentLocation
Et	ExpiryTime
El	ExpectedLocation
Vpri	Vehicle Private Key
Vpub	Vehicle Public Key
Csig	Client Signature
Spri	Server Private Key
Spub	Server Public Key

Table 1: List of various notations used in Algorithms

Algorithm 1: Token Request generation at vehicle side

```
1.After a given time t (assume 30 sec) the CryptLoc
  vehicle module checks the vehicle is moving or not
  by checking Accelerometer current value and
  previous value.
if Acurrent == Aprev then
        Go to Step 2;
else
        Acurrent = Aprev;
end
2.Sign Vehicle id(Vid) using vehicle private key (Vpri)
      Csig = SignVid Vpri
3.Create a random nonce Rv. Encrypt Rv using server
  public key Spub.
      Erv = EncRv Spub
4.Generate the token generation request using -
  VehicleId, CurrentLocation, Signature, Encrypted
  Random Nonce and send to server.
      Treq= Csig+ Vid + Cl + Erv
```

The Random Nonce is encrypted using the server's public key. It is decrypted by the server's private key. VehicleId is signed using Vehicle's private key. The corresponding public key is available in the server so that the signature can be verified in the server side.

At the server side, signature is verified using vehicle public key. The Random Nonce is decrypted using server's private key. Then the conditions are checked whether the current location and expected location are equal.If the current time is less than the expiry time, then access token is generated and the Random Nonce Rv' is stored into another variable.

Algorithm 2: Token Request verification at Server

```
1. Verify vehicle signature Csig using vehicle public
  key Vpub.
  if Csig == Valid then
  |  Go to Step 2;
else
  |  Discard the request;
end
2. Decrypt encrypted random nonce Erv using server
  private key (Spri)
       Rv = DecErv Spri

3. if Current time(Ct) ¡= Expiry time(Et) and Current
  Location(Cl) == Expected Location(El) then
  |  Go to step 4;
else
  |  Go to Step 6;
end
4. Generate access token (Atoken) copy the value of
  Rv to Rv'

5. Sign Vehicle id(Vid) using server private key (Spri).
  Encrypt Rv' , Access Token and Expiry time Et using
  vehicle public key Vpub

       Ssig = Sign[Vid]Spri

       Ereply = Enc[Atoken + Rv'+ Et] Vpub

6. Generate Error token Etoken Sign Vehicle id(Vid)
  using server private key [Spri]. Encrypt Rv' , Error
  Token and Expiry time Et using vehicle public key
  Vpub.

       Ssig = Sign[Vid] Spri
       Ereply = Enc[Etoken + Rv'+ Et] Vpub

7. Create the TrespusingSsigandEreply. Send Tresp to
  vehicle.

       Tresp= Ssig+ Ereply
```

Then the server sends response to the hardware module. The response contains a Signature and Encrypted Access token with ExpiryTime and the Encrypted Random nonce Rv'.

In the vehicle side, the vehicle verifies the signature using the server's public key. Decrypt the access token and Random nonce Rv' using vehicle's private key and check whether Rv' is equal to Rv. If they are equal then it is considered as a fresh response and verifies the Access token and expiry time.Then the hardware module generates 5V to the Servo motor.

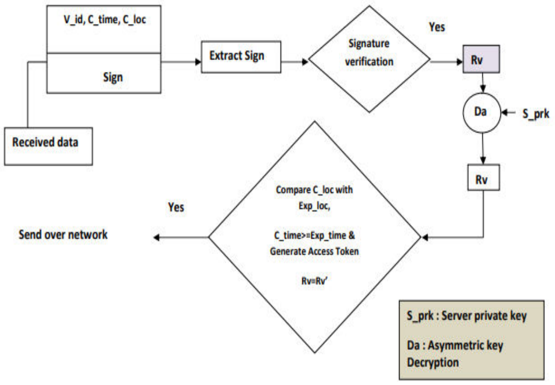


Fig. 7. Receiving information at Server

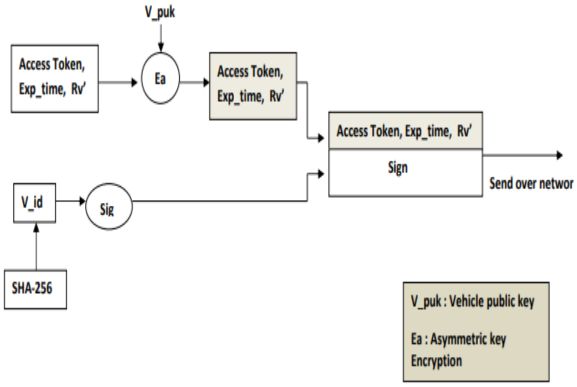

V_puk
Access Token, Exp_time, Rv'
Ea
Access Token, Exp_time, Rv'
Access Token, Exp_time, Rv'
Sign
Send over networ
V_id
Sig
SHA-256
V_puk : Vehicle public key
Ea : Asymmetric key Encryption

Fig. 8. Sending information from Server

Algorithm 3: Token Verification at vehicle side

```
1. Verify server signature Ssig using server public key
  Spub. if Ssig == Valid then
  |  Go to Step 2;
else
  |  Discard the request;
end
2. Decrypt encrypted Ereplyusing vehicle private key
  (Vpri) if Rv' == Rv then
  |  Go to Step 4;
else
  |  Discard the packet;
end
4.if contains Access Token then
  |  Verify the access token and open the lock;
else
  |  Log the error message;
end
```

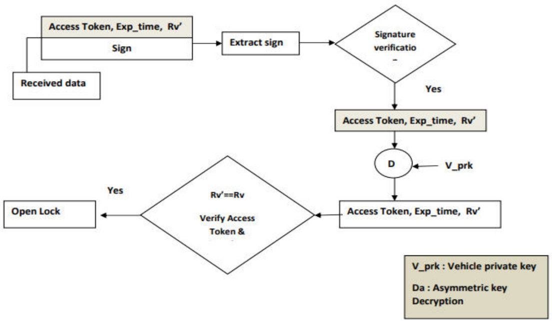
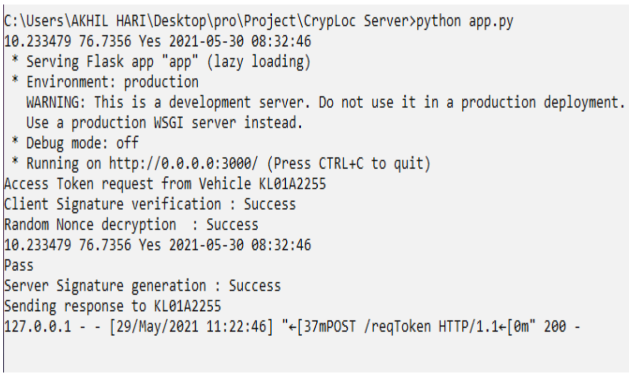

Access Token, Exp_time, Rv'
Sign
Received data
Extract sign
Signature verificatio
-
Yes
Access Token, Exp_time, Rv'
D
V_prk
Yes
Open Lock
Rv'==Rv
Verify Access Token &
Access Token, Exp_time, Rv'
V_prk : Vehicle private key
Da : Asymmetric key Decryption

Fig. 9. Receiving information at Hardware module

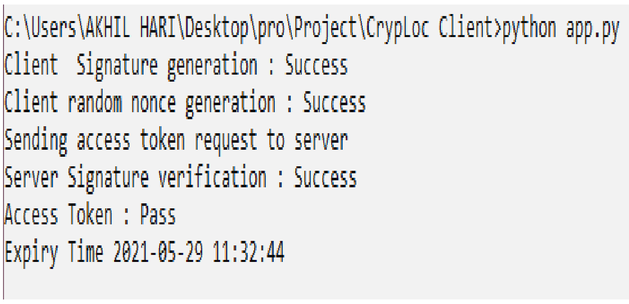
V. Implementation Result

Fig.10 and Fig.11 shows the communication between Client and Server. Server runs on http://0.0.0.0:3000/ Client vehicle (for eg. KL01A2255) generates access Token, Signature and Encrypted Random Nonce. Now the client sends these informations to the Server. Server receives the request from the Client. Server verifies the signature and decrypt the Random nonce. Now the Server sends a success message to the Client and Server generates a Signature.This generated signature is send to the client and the client verifies the signature and sends a success message to the Server.



```
C:\Users\AKHIL HARI\Desktop\pro\Project\CrypLoc Server>python app.py
10.233479 76.7356 Yes 2021-05-30 08:32:46
 * Serving Flask app "app" (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on http://0.0.0.0:3000/ (Press CTRL+C to quit)
Access Token request from Vehicle KL01A2255
Client Signature verification : Success
Random Nonce decryption  : Success
10.233479 76.7356 Yes 2021-05-30 08:32:46
Pass
Server Signature generation : Success
Sending response to KL01A2255
127.0.0.1 - - [29/May/2021 11:22:46] "←[37mPOST /reqToken HTTP/1.1←[0m" 200 -
```

Fig. 10. Server Side Operation



```
C:\Users\AKHIL HARI\Desktop\pro\Project\CrypLoc Client>python app.py
Client  Signature generation : Success
Client random nonce generation : Success
Sending access token request to server
Server Signature verification : Success
Access Token : Pass
Expiry Time 2021-05-29 11:32:44
```

Fig. 11. Client Side Operation

VI. Performance Evaluation

The performance of the proposed model can be evaluated by the factors such as Confidentiality, Integrity, Availability, Replay Attack and Round Trip Time (RTT).

A. *Confidentiality*

Confidentiality ensures the protection of data by preventing the unauthorised disclosure of information. A failure to maintain confidentiality can lead to the access to private information. The proposed model ensures confidentiality by Encryption. The request from the Client contains Random nonce which is encrypted by using Server Public Key. This Random nonce is decrypted by the server using Server Private Key. The Random Nonce is used inorder to prevent replay attack. If the Random Nonce is leaked then there is a possibility of replay attack.

B. *Integrity*

Integrity involves maintaining the consistency and trustworthiness of data over its entire life cycle. In existing model, integrity is achieved by authentication. But in the proposed model, integrity is achieved by Mutual authentication. Digital Signature is used to mutually authenticate both client and server. Here, the client signs the VehicleId using Vehicle Private Key which is verified by the server using Vehicle Public Key.

C. *Availability*

Mutual Authentication is implemented in our proposed system so it communicate with proper Client-Server only. If the signature is mismatching then the System will ignore the request. The Server side blocks a particular IP if there arises consecutive Signature mismatching.In the Client side no ports of the hardware module are open so only Client-Server-Client communication can be established.

D. *Replay Attack*

Replay Attack is that the client would receive the message twice. In this paper, inorder to avoid replay attack, the server responses to the client only if the request from the client contains Random nonce.

E. *Round Trip Time(RTT)*

RTT is the time taken by the client to receive back the response from the server after the client's request. The performance is analysed on an Ubuntu 18.04.1 LTS,Intel® Core™ i7-6820HQ CPU@2.70GHz×2Processor, 8GB RAM machine. It is analysed that there is only a slight change in RTT with signature and nonce of the proposed model as compared with the existing model. This provides cyber-security for the entire CryptLoc system and doesn't affect the performance.

VII. CONCLUSION

In this article ,it is presented a comprehensive review of Vehicle cyber security that recently arouse society concerns have more complicated vulnerabilities, compared to ordinary computer and internet cyber security. In addition, more frequent connection between vehicle and smart phone with limited security mechanism is considered to raise security risks. In response to the increasing concern about vehicle cyber risks, a new system is introduced here. This system is hybrid model of location and cryptography. It is a defense in depth against cyber security threats. It has fully automatic workflow. To the best of our knowledge, this survey provides a comprehensive overview of Location Based Crypto-Locking System.

REFERENCES

[1] G. Burzio, G. F. Cordella, M. Colajanni, M. Marchetti and D. Stabili, ”Cybersecurity of Connected Autonomous Vehicles : A ranking based approach,” 2018 International Conference of Electrical and Electronic Technologies for Automotive, 2018, pp. 1-6, doi: 10.23919/EETA.2018.8493180.

[2] M. R. Parmar, M. U. Kumari and R. S. N, ”CYBER SECURITY IN VEHICLE COMMUNICATION,” 2020 IEEE International Conference for Innovation in Technology (INOCON), 2020, pp. 1-5, doi: 10.1109/INOCON50539.2020.9298286.

[3] R. E. Haas and D. P. F. Möller, ”Automotive connectivity, cyber attack scenarios and automotive cyber security,” 2017 IEEE International Conference on Electro Information Technology (EIT), 2017, pp. 635-639, doi: 10.1109/EIT.2017.8053441.

[4] Muhammad Ahtsham,Huang Yan Yan and Usman Ali“IoT Based Door Lock Surveillance System Using Cryptographic Algorithms”.

[5] R. Divya and M. Mathew, ”Survey on various door lock access control mechanisms,” in Circuit, Power and Computing Technologies (ICCPCT), 2017 International Conference on, 2017, pp. 1-3

[6] P. R. Nehete, J. Chaudhari, S. Pachpande, and K. Rane, ”Literature survey on door lock security systems,” Int. J. Comput. Appl, vol. 153, pp. 13-18, 2016

[7] M. K. Shafin, K. L. Kabir, N. Hasan, I. J. Mouri, S. T. Islam, L. Ansari, et al., ”Development of an RFID based access control system in the context of Bangladesh,” in Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on, 2015, pp. 1-5

[8] PushkarBhilegaonkar,RupeshPatil,AnamayBelekar,MohnishGujarathi and ShilpaSondkar “Fuel Theft Prevention System”2020 International Conference on Industry 4.0 Technology (I4Tech) Vishwakarma Institute of Technology, Pune, India. Feb 13-15, 202.

[9] Sachin S. Aher, Kokate R.D. (2012), “Fuel Monitoring and Vehicle Tracking”, International Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, Issue 3, 166-169.

[10] Naomi SomerLepcha, TsheringSangmo Sherpa, Jitendra Singh Tamang (2015), “GSM Based Fuel Theft Detector Using Microcontroller”, International Journal of Advance Electrical and Electronics Engineering (IJEIT), Vol. 4, Issue 3, 7-12

[11] Jinfeng Sun, Zhiyue Zhang, Xiaoli Sun (2016), “The intelligent crude oil anti-theft system based on IoT under different scenarios”, International Conference on Knowledge Based and Intelligent Information and Engineering Systems, 1581-1588.

[12]] SanghoonLeea , Byeongkwan Kanga , KeonheeChoa, Dongjun Kanga , KyuheeJanga , Leewon Parka, and Sehyun Park (2017), “Design and Implementation for Data Protection of Energy IoT utilizing OTP in the Wireless Mesh Network”, 4th International Conference on Power and Energy Systems Engineering, CPESE 2017.

[13] RashmiKushwah, AyushiKulshreshtha, Krishnapal Singh andShivanshu Sharma “ECDSA for Data Origin Authentication and Vehicle Security in VANET”.

[14] R. S. Raw, M. Kumar, and N. Singh, “Security Challenges, Issues and Their Solutions ForVanet,” International Journal of Network Security and Its Applications, vol. 5, no. 5, pp. 95-105, 2013.

[15] B. Mokhtar and M. Azab, “Survey on Security Issues in Vehicular Ad Hoc Networks,” Alexandria Engineering Journal, vol. 54, no. 4, pp. 1115-1126, 2015.

[16] D. Kushner, ”The real story of stuxnet”, IEEE Spectrum, vol. 50, no. 3, pp. 48-53, March 2013.

[17] Y. Seralathan et al., ”IoT security vulnerability: A case study of a Web camera,” 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-siGangwon-do, Korea (South), 2018, pp. 172-177.

[18] Gongjun Yan and Stephan Olariu “An Efficient Geographic Location-based Security Mechanism for Vehicular Adhoc Networks”.

[19] OhsungDoh, Ilkyu Ha. A Digital Door Lock System for the Internet of Things with Improved Security and Usability; Advanced Science and Technology Letters, Vol.109 (Security, Reliability and Safety 2015), pp.33-38, doi://10.14257/astl.2015.109.08

[20] JayantDabhade et al: Smart Door Lock System: Improving Home Security using Bluetooth Technology, International Journal of Computer Applications (0975 – 8887), Volume 160 – No 8, February 2017

[21] Marko Pavelić ,ZvonimirLončarić , Marin Vuković and Mario Kušek “Internet of Things Cyber Security: Smart Door Lock System” [22] K. P. Laberteaux, 1. J. Haas, and Y.-C. Hu, ”Security certificate revocation list distribution for vanet,” in VANET ’08: Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking, 2008, pp. 88-89.

[22] K. P. Laberteaux, 1. J. Haas, and Y.-C. Hu, ”Security certificate revocation list distribution for vanet,” in VANET ’08: Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking, 2008, pp. 88-89.

[23] G. Yan, S. Olariu, and M. C. Weigle, ”Providing VANET security through active position detection.” Computer Communications: Special Issue on Mobility Protocols for ITSIVANET, vol. 31, no. 12, p. 2883C2897, 2008 .

[24] R. Ramesh and S. Kumar, ”Secure position routing using ad hoc network,” Dec. 2006, pp. 200-201.

[25] M. Raya, A. Aziz, and 1.-P. Hubaux , ”Efficient Secure Aggregation in VANETs,” in Proceedings of the ACM Workshop on Vehicular Ad Hoc Networks (VANET), Los Angeles, CA, Sep. 2006, pp. 67-75.

[26] A. AI-Fuqaha and O. Al-Ibrahim, ”Geo-encryption protocol for mobile networks,” Comput. Commun., vol. 30, no. 11-12, pp. 2510-2517, 2007.

MULTIMODAL IMAGING APPROACH TO COVID-19 DETECTION

1st Vrinda Vijayakumar
PG Scholar
Dept of CSE
Sree Buddha College of Engineering, Pattoor
vrindavijayakumar123@gmail.com

2nd Prof. Anil A.R
Associate Professor
Dept of CSE
Sree Buddha College of Engineering, Pattoor
anilar123@gmail.com

***Abstract*—On March 11, 2020, the World Health Organization declared that COVID-19 was a global pandemic, indicating significant global spread of an infectious disease (World Health Organization , 2020).The virus was extremely contagious and led to death in the most vulnerable, particularly those older than 60 and those with underlying conditions. Common signs of infection include respiratory symptoms, fever, cough, shortness of breath and breathing difficulties. In more severe cases, infection can cause pneumonia, severe acute respiratory syndrome, kidney failure and even death .Standard recommendations to prevent infection spread include regular hand washing, covering mouth and nose when coughing and sneezing, thoroughly cooking meat and eggs. Avoid close contact with anyone showing symptoms of respiratory illness such as coughing and sneezing. Detecting COVID19 early may help in devising an appropriate treatment plan and disease containment decisions. In this study, we demonstrate how machine learning can be used to perform COVID-19 detection using images from three most commonly used medical imaging modes X-Ray, Ultrasound, and CT scan.We identify a suitable Convolutional Neural Network (CNN) model through initial comparative study of several popular CNN models. We then optimize the selected VGG19 model for the image modalities to show how the models can be used for the highly scarce and challenging COVID-19 datasets. The new approach is aimed to reduce unwanted noise from the images so that deep learning models can focus on detecting diseases with specific features from them**

***Index Terms*—COVID-19 detection, imaging models, CNN models - VGG19, X-ray, Ultrasound and CT based detection**

I. INTRODUCTION

The current COVID-19 pandemic has impacted the world with over millions of infections and deaths so far. So Early identifying, isolation and care for patients is a key strategy for a better management of this pandemic. Our study aims to provide a conceptual transfer learning framework to support COVID-19 detection with use of image classification using deep learning models for multiple imaging modes including X-Ray, Ultrasound, and CT scan. The acquisition of a sufficiently large, publicly available corpus of medical image sample data for fully training deep learning models is a challenging task for novel medical conditions such as COVID-19 since collection and labelling of images requires significant time and resources to compile.

An alternative method of training deep learning models is "transfer learning" whereby a deep learning network is pre-weighted with results of a previous training cycle from a different domain. This technique was commonly used as a basis for initializing deep learning models which are then fine-tuned using the limited available medical sample data set with results that have been documented to outperform fully trained networks under certain circumstances[1]. This will demonstrate how transfer learning can be used for COVID-19 detection for three commonly used imaging modes X- Ray, Ultrasound, and CT scan. This study could assist practitioners and researchers in developing a supporting tool for highly constrained health professionals in determining the course of treatment. The study further establishes a pre-processing pipeline for improving the image quality, for deep learning based predictions. An initial testing is also directed to understand the suitability of various popular deep learning models for the limited available dataset in order to select a model for the proposed image classification demonstrations on multiple image modes.

Computer vision diagnostic apparatuses for COVID-19 from multiple imaging modes such as X-Ray, Ultrasound, and CT would provide an automated "second reading" to clinicians, assisting in the diagnosis and criticality assessment of COVID-19 patients to assist in better decision making in the global fight against the disease. COVID-19 often results in pneumonia, and for radiologists and practitioners differentiating between the COVID-19 pneumonia and other forms of pneumonia (viral and bacterial) solely based on diagnostic images could be challenging[2]. Deep learning artificial neural networks, and the Convolutional Neural Networks (CNNs) have proven to be highly active in a vast range of medical image classification applications[3].

II. LITERATURE SURVEY

A. A fully integrated computer-aided diagnosis system for digital X-ray mammograms via deep learning detection, segmentation and classification.

A journal paper "A fully integrated computer-aided diagnosis system for digital X-ray mammograms via deep learning detection, segmentation and classification" was published by Elsevier on June 2018. This paper was authored by Mugahed A.Al-antari, Mohammed A.Almasui, Mun-Tack Choi, Seung-Moo Han, Jae-seong Kim. It uses the concept of Multimodal imaging. Here X-ray is the medium. A completely integrated CAD system is proposed to screen digital X-ray mammograms. It involves detection, segmentation and classification of breast masses via deep learning methodologies. To detect breast mass from entire mammograms, You-Only-Look-Once (YOLO), a regional deep learning approach is used. To segment them mass full resolution convolutional network model is proposed and utilized. A deep CNN is used to recognize the mass and classify it as either benign or malignant. To evaluate the proposed integrated CAD system, the publicly available and annotated INbreast database was utilized. The experimental results demonstrate that the proposed CAD system, outperforms the latest conventional deep learning methodologies.

B. Lung cancer detection based on CT-Scan images using transfer learning

A journal paper "Lung cancer detection based on CT Scan images by using transfer learning" published on October 2019, was authored by TulasiKrishna Sajja, Retz Mahima Devarapalli and HemanthaKumar Kalluri. In this paper, a deep neural network is designed based on GoogleNet, a pre-trained CNN. To reduce the computing cost and avod overfitting in network learning, the densely connected architecture of proposed network was sparsified, with 60network was verified through a simulation on a preprocessed CT-Scan image dataset: The Lung Image Database Consortium (LIDC) dataset, and compared with that of several pretrained CNNs. The result shows that this network achieved better classification accuracy than the contrastive networks. In future, this proposed network performance is test on different dropout ratios and without dropout and also need to verify the importance of inception layers added to the network and how many inception layers are sufficient for achieving better performance

C. Rational use of CT- Scan for the diagnosis of Pneumonia: comparative accuracy of different strategies

The paper "Rational use of CT Scan for the diagnosis of Pneumonia: comparative accuracy of different strategies" was published on April 2019. It gives a clinical prediction score based on four easily available variables allows for more superior accuracy for the diagnosis of pneumonia than standard assessment. When targeting patients at low or intermediate predicted risk, Low-dose CT is indicated for 54is obtained for all patients, the accuracy of the clinical diagnosis of Pneumonia is only moderate when comparing with a reference diagnosis. However, obtaining a CT-Scan in all cases of suspected pneumonia has significant drawbacks.

D. Feature enhancement in medical ultrasound videos using contrastlimited adaptive histogram equalization.

A paper "Feature Enhancement in Medical Ultrasound Videos using Contrast-Limited Adaptive Histogram Equalization" published in 2019 by the authors Prerna Singh, Ramakrish Mukundan, Rex De Ryke, proposed a novel framework for both multiplicative noise suppression and robust contrast enhancement and demonstrate its effectiveness using a wide range of clinical ultrasound scans. This approach to noise suppression uses a novel algorithm based on CNN that is first trained on synthetically modeled ultrasound images and then applied on real ultrasound videos. The feature improvement stage uses an improved contrastlimited adaptive histogram equalization method for enhancing texture features, contrast, resolvable details and image structures to which the human visual system is sensitive in ultrasound video frames. Subjective assessments by four radiologists and experimental validation using three quality metrics clearly indicate that this proposed framework generates superior performance compared with other well established methods. Its future work is directed towards development of a feature enhancement process within a filtering method to reduce computational complexity and improve overall efficiency. The proposed system could also be extended to an ultrasound video classification framework. For the classification of ultrasound videos, deep neural architecture will be considered and comparative study will be performed with other supervised learning techniques.

E. A deep step pattern representation for multimodal retinal image registration

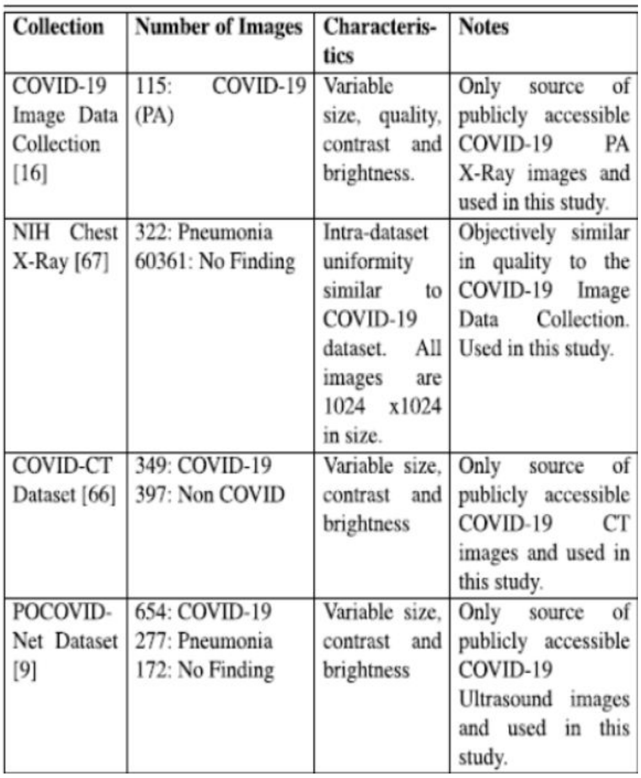
IEEE published a paper " A deep step pattern representation for multimodal retinal image registration" on November 2019, which was authored by Jimmy Lee, Peng Liu, Jun Cheng and Huazhu Fu. This paper presents a novel feature based method that is built-upon a convolutional neural network(CNN) to learn the deep representation for multimodal retinal image registration.

Most existing deep learning based methods require a set of manually labeled training data with known corresponding spatial transformations, which limits the size of training datasets. By contrast, this method is fully automatic and scale well to different image modalities with no human intervention. They generate, feature classes from simple step patterns within patches of connecting edges formed by vascular junctions in multiple retinal imaging modalities. They used CNN to learn and optimize the input patches to be used for image registration. Spatial transformations are estimated based on the output possibility of the fully connected layer of CNN for a pair of images. One of the key advantages of this proposed algorithm was its robustness to non-linear intensity changes, which widely exist on retinal images due to the difference of acquisition modalities. The experimental results demonstrate the robustness and accuracy over state-ofthe-art multimodal image registration algorithms. The disadvantage was that, CNN are not actually invariant to large transformations of the input data.

III. EXISTING SYSTEM

A. Dataset Development

1) Dataset Development : Large numbers of X-Ray, CT and Ultrasound images are available from some publicly accessible datasets. With the arrival of COVID-19 being very recent none of these large repositories contain any COVID-19 labelled data, thereby requiring that we rely upon multiple datasets for Normal, Pneumonia, COVID-19 and other non COVID-19 source images. COVID-19 chest X-Rays were acquired from the publicly accessible COVID-19 Image Data Collection. This collection has been sourced from websites and various pdf format publications. Naturally, the images from this collection are of variable size and quality. Image contrast levels, brightness and subject positioning are highly variable within this dataset. The analysis in this article is based on a download of this dataset made on 11 May 2020.



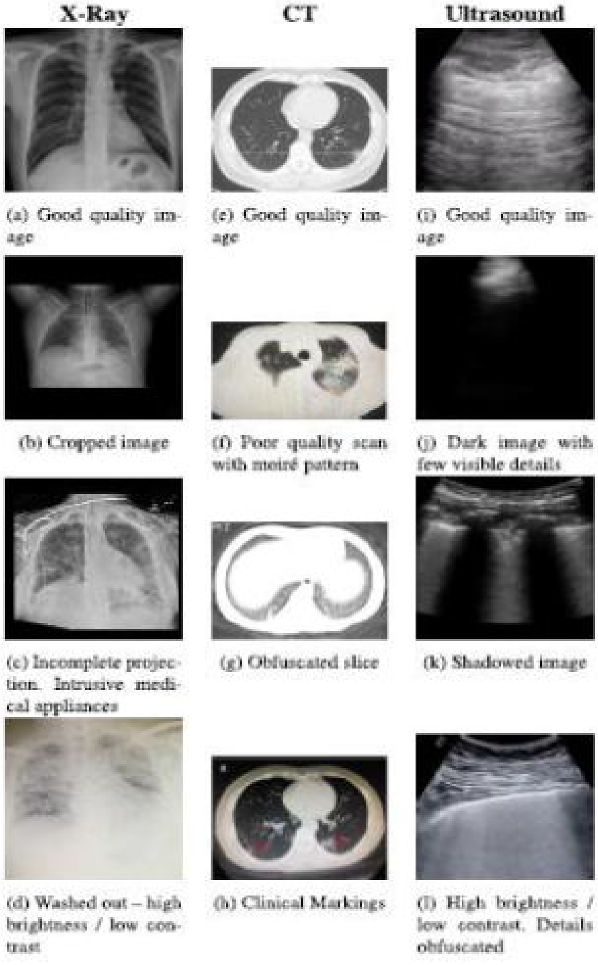
Collection	Number of Images	Characteristics	Notes
COVID-19 Image Data Collection [16]	115: COVID-19 (PA)	Variable size, quality, contrast and brightness.	Only source of publicly accessible COVID-19 PA X-Ray images and used in this study.
NIH Chest X-Ray [67]	322: Pneumonia 60361: No Finding	Intra-dataset uniformity similar to COVID-19 dataset. All images are 1024 x1024 in size.	Objectively similar in quality to the COVID-19 Image Data Collection. Used in this study.
COVID-CT Dataset [66]	349: COVID-19 397: Non COVID	Variable size, contrast and brightness	Only source of publicly accessible COVID-19 CT images and used in this study.
POCOVID-Net Dataset [9]	654: COVID-19 277: Pneumonia 172: No Finding	Variable size, contrast and brightness	Only source of publicly accessible COVID-19 Ultrasound images and used in this study.

Fig. 1. Summary of data sources used.

CT scans for COVID-19 and non COVID-19 were obtained from the publicly available COVID-CT Dataset. This dataset has been sourced by extracting CT slice images viewing the COVID-19 pathology from preprint papers. Once again, images from this collection are of variable size and quality. Moreover, the process of CT scanning is dynamic, with a full scan consisting of many discrete slices taken in a helical pattern along the thoracic cavity. The images in this collection only present a single, or small number of slices per patient. Ultrasound images for COVID-19, Pneumonia and Normal conditions were obtained from the publicly accessible POCOVID-Net data set. These images have been sampled from video sourced from various online sources. Ideally ultrasound video would be taken in a systematic way to allow for greater comparability of the condition datasets with every frame in the video subject to analysis. The number of images of each dataset along with a description of characteristics of the datasets is described in Table 3.1. We believe the major quality variations between data from different classes need to be balanced for deep learning models to learn actual disease related variations. So, our study stresses the importance of sampling bias/signal noise removal from the image datasets prior to using them for model development and classification inorder to obtain meaningful and trustworthy classification results. Certain illustrative examples of this variability of these datasets is shown in Figure.

Of these examples images (b), (c) seem to have been cropped from journal articles and in the case of (f) scanned. These images are of poor quality and lacking detail that would specify a pathology to our machine learning models. Images (g), (j) and (k) also lack detail as a result of device positioning.

Images (d) and (l) show high brightness and low contrast, hence hiding pathological details. Despite the variability of the datasets we chose to only very lightly curate data as described in Data Pre-processing section and shown in figure.



(a) Good quality image (e) Good quality image (i) Good quality image

(b) Cropped image (f) Poor quality scan with moiré pattern (j) Dark image with few visible details

(c) Incomplete projection. Intrusive medical appliances (g) Obfuscated slice (k) Shadowed image

(d) Washed out – high brightness / low contrast (h) Clinical Markings (l) High brightness / low contrast. Details obfuscated

Fig. 2. Different variations observed in the COVID-19 datasets.

2) Data Sampling : In this study, we aim to use real X-Ray, Ultrasound and CT scan data only, and not considering creation and use of artificial data at this stage. And we also used a relatively balanced dataset size for our model experiments, with imbalance addressed using calculated class training weights.

The X-Ray COVID-19 dataset was lightly curated to remove a single image that was an wrongly labeled projection. All other COVID-19 images were involved for the various modes. The non-COVID-19 images were also lightly curated to eradicate images that were mislabelled projections or dominated by intrusive medical devices. This left us with some usable image samples for X-Ray, Ultrasound and CT scan to work with. Since the resulting sample corpus was still comparatively small for deep learning application, we applied several data augmentation transformations including horizontal fiip, horizontal and vertical shift or rotation to increase the volume and variety of the sample set.

Since the machine learning classifiers, use a pixel array as a data source, any systematic difference in pixel intensity between the datasets would present sampling bias in the results. This would have the significance of training the machine learning classifiers on systematic image histogram differences rather than the actual clinical image content of interest. To reduce the effect of sampling bias, we applied histogram equalization to images using the N-CLAHE method. This method both normalizes images and enhances small details, textures and local contrast by first globally normalizing the image histogram followed by application of Contrast Limited Adaptive Histogram Equalization (CLAHE). This was executed using the OpenCV equalizeHist and createCLAHE functions.

B. Model Development

1) Classification Pipeline : Unprocessed images are read with directory names that was used as class labels. N-CLAHE is then applied to normalize images and highlight the smaller details for the attention of the machine learning classifiers. Images are then resized to the classifier default size, for example 224*224 pixels for VGG16/VGG19 and 299*299 pixels for InceptionV3. Following image resizing, data augmentation is applied to increase the number and variation of images delivered to the classifier. Augmentations applied consist of horizontal flip, rotation, width shift, and height shift. Vertical flip was not applied as X-Ray images are not vertically symmetrical, and the resulting flipped image would not resemble a real chest X-Ray. Finally, the augmented images are utilized by the machine learning classifier using an 80:20 Train or Test split.

2) Model Consideration : One of the key goals of this study was to achieve reliable classification results using publicly accessible data and “out-of- the-box” models with transfer learning to both compensate for the limited size of the sample data sets, and to accelerate the training process so that this could be reasonably performed on modest hardware. CNN based models are well used for image classification purposes and we want to initially select a suitable CNN based deep learning model for our multimodal image classification study.

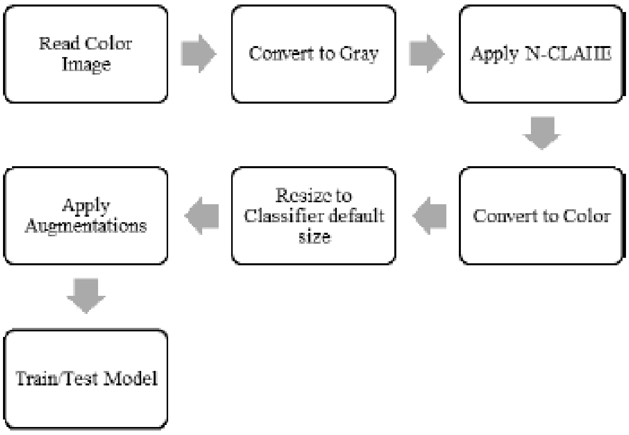


Fig. 3. Experiment pipeline for preprocessing and classification.

Our main aim is not to perform exhaustive performance evaluation among all available models, rather we aim to show the generic applicability of popular model genres for the challenging and limited time critical dataset for COVID-19 chest images in multiple modes including X-Ray, CT and Ultrasound to provide reasonable precision. In order to catch the most suitable model for our study, we focused on widely popular models, suitable for transfer learning, and readily available in packaged form through trusted public libraries such as Keras. Hence, we only measured representatives of the base models in this domain as discussed below. Suitably, these models are all available as part of the Keras API and each support transfer learning in the form of supporting the pre-application to the model of the ImageNet weights.

1. VGG16 AND VGG19

VGG16 and VGG19 are convolutional neural network (CNN) architectures with very small convolution filters (3 *3) and a stride of 1 designed to achieve high accuracy in large-scale image recognition applications. The two implementations differ in depth of convolution/max-pooling and fully connected layers, with VGG16 having 16 layers in the base model and VGG19 having 19 layers.

2. RESNET50 V2

The ResNet CNN was developed as a means of avoiding the vanishing gradient problem inherent in deep neural networks by implementing a system of skip connections between layers known as residual learning. This architecture results in a network that is more efficient to train, allowing for deeper networks to be designed that positively impact the model accuracy. ResNet50 is such a network with 50 layers of implementing residual learning.

3. INCEPTION V3

The Inception V3 CNN aimed to improve utilization of computing resources inside the network by increasing the depth and width of the network whilst keeping computation operations constant. The designers of this network coined the term “inception modules” to describe an optimized network structure with skipped connections that is used as a building block. This inception module is repeated spatially by stacking with occasional max-pooling layers to reduce dimensionality to a manageable level for computation.

4. XCEPTION

The Xception CNN was developed by Google Inc. as an "extreme" version of the Inception model. The Inception modules described above are replaced with depth wise separable convolutions. This Xception was shown to outperform Inception on a large-scale image classification dataset (comprising 350 million images of 17,000 classes).

5. INCEPTIONRESNET V2

The InceptionResNetV2 CNN combines the Inception and Resnet architecture with the objective of achieving high classification performance using a ResNet architecture with the low computation cost of the Inception architecture.

6. NASNETLARGE

The NASNet (Large) CNN has been developed by Google Brain as a data driven dynamic network that uses reinforcement learning to determine an optimal network structure for the image classification task at hand.

7. DENSENET121

The DenseNet 121 CNN [27] uses shorter connections between layers in order to allow more accurate and efficient training on very deep networks.

3) Model Selection : The Models discussed in the earlier section was firstly tuned using Keras-tuner to determine an optimum range of learning rate, hidden network size and dropout rate. From this process, optimal hyperparameter ranges were determined to be:

Learning Rate = 10^-3 - 10^-5

Hidden Layer Size = 8 - 96 neurons

Dropout = 0.1 - 0.2

Each model was then trained 5 times over 100 epochs with precision, recall, training/testing accuracy and loss metrics captured along with training curves and confusion matrices for further analysis. The test was repeated for learning rates between 10^-3 and 10^-5 with order-of-magnitude increments.

The hidden layer size was also varied between 8 and 96. The batch size was varied between 2 and 16. Each classifier was trained on the ImageNet weights for transfer learning. Finally, where models converged well, the best training hyperparameters were selected by inspection of training curves. The number of training epochs was then adjusted to prevent overfitting. The training and testing were then repeated with selected epochs and optimized hyperparameters to obtain performance scores.

The testing results as shown in Table 3.3 that the simpler VGGclassifiers were more trainable on all three image modes and provided more consistent results across all three image modes. We also noted that ultrasound provided best classification results across all deep learning models compared to the CT and X-Ray image modes. The more complex models tended to either overfit in early epochs (¡10) or failed to converge at all. Where reasonable results were obtained from the more complex models training curves typically showed overfitting and somewhat erratic training behavior in several cases.We also found that the more complex model trainability was highly dependent upon initial model hyperparameter choice, whereas the VGG classifiers produce good results for a wider range of hyperparameter choices.

Finally, we noticed that the more complex models exhibited a higher training metrics deviation between epochs with randomly selected train/test splits. We believe the smaller data size and high fine-grained variability within the datasets were detected by the sensitive complex models, thus resulting in poorer performances. We expect complex model performance to improve with larger and better-quality data. Based on our initial testing results, we have chosen the VGG19 model for our multimodal image classification testing in this study. We anticipate that future novel pandemics can also be expected to initially produce small, low quality medical image datasets and suggest that our findings are likely to extend to similar future applications with such challenging datasets.

IV. PROPOSED SYSTEM

Data fusion concept allows us to combine multiple modes of data to improve model classification performance. Although data fusion comes with its own set of challenges , it has been used successfully in other application areas such as remote sensing, action detection, and medical diagnosis and imaging. I plan to extend this study with multimodal data fusion when sufficient data is available. Motivations for data fusion are numerous. They include obtaining a more unified picture and global view of the system at hand; improving decision making; exploratory research; answering specific questions about the system, such as identifying common versus distinctive elements across modalities or time; and in general, extracting knowledge from data for various purposes. However, despite the evident potential benefit, and massive work that has already been done in the field for the knowledge of how to actually exploit the additional diversity that multiple data sets offer is still at its very preliminary stages.

V. RESULTS AND DISCUSSIONS

With the selected VGG19 model for each experiment listed in Table we first conducted the extensive performance tuning by adjusting multiple parameters including learning rate, batch size, node size and drop rate. We noted that dropout rate had only a minimal effect on the model accuracy except at the highest learning rate of 10^-3 and lowest learning rate of 10^{-6} where a dropout rate of 0.2 proved to be more stable than a dropout rate of 0.1. For learning rates for 10^-3 and 10^{-4} the dropout rate selection has no discernable effect on model accuracy. The results of the five experiments are listed in Table .

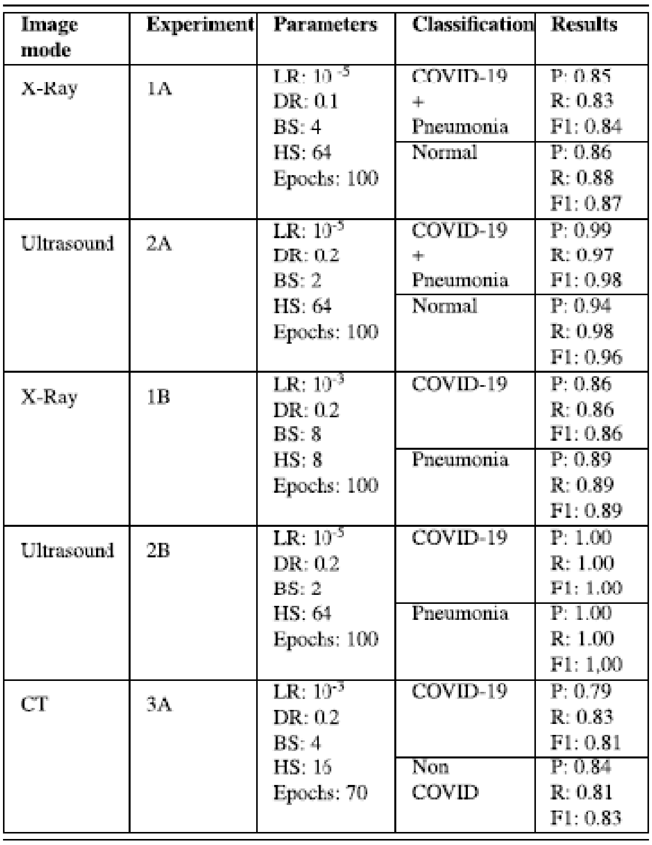


Image mode	Experiment	Parameters	Classification	Results
X-Ray	1A	LR: 10^{-5} DR: 0.1 BS: 4 HS: 64 Epochs: 100	COVID-19 + Pneumonia	P: 0.85 R: 0.83 F1: 0.84
			Normal	P: 0.86 R: 0.88 F1: 0.87
Ultrasound	2A	LR: 10^{-5} DR: 0.2 BS: 2 HS: 64 Epochs: 100	COVID-19 + Pneumonia	P: 0.99 R: 0.97 F1: 0.98
			Normal	P: 0.94 R: 0.98 F1: 0.96
X-Ray	1B	LR: 10^{-3} DR: 0.2 BS: 8 HS: 8 Epochs: 100	COVID-19	P: 0.86 R: 0.86 F1: 0.86
			Pneumonia	P: 0.89 R: 0.89 F1: 0.89
Ultrasound	2B	LR: 10^{-5} DR: 0.2 BS: 2 HS: 64 Epochs: 100	COVID-19	P: 1.00 R: 1.00 F1: 1.00
			Pneumonia	P: 1.00 R: 1.00 F1: 1,00
CT	3A	LR: 10^{-3} DR: 0.2 BS: 4 HS: 16 Epochs: 70	COVID-19	P: 0.79 R: 0.83 F1: 0.81
			Non COVID	P: 0.84 R: 0.81 F1: 0.83

Fig. 4. Experiment results for three image modes.

VI. CONCLUSIONS

We have demonstrated that with current limited and challenging COVID-19 datasets, VGG19 model could be used to develop suitable deep learning-based tools for COVID-19 detection. The model is capable of classifying both Pneumonia vs Normal and COVID-19 vs Pneumonia conditions for multiple imaging modes including X-Ray, Ultrasound, and CT scan. With very little data curation, we achieved considerable classification results using VGG19 from all imaging modes. Perhaps the most interesting observation is that the pretrained models tuned very effectively for the Ultrasound image samples, which to the untrained eye appeared noisy and difficult to interpret.

VGG19 also trained well against the X-Ray image corpus however, without modified thresholding we found that the proportion of false negatives was concerning but not unexpected given data quality challenges. Our finding that experiment 1A/2A yielded lower F1 scores and higher false negatives than experiments 1B/2B was unexpected since the manifestation of COVID-19 is itself a form of viral pneumonia. This may indicate that despite our attempts to remove sampling bias using N-CLAHE pre-processing there may still be systematic differences in the COVID-19 image datasets that leads the VGG19 classifier to more easily distinguish the COVID-19 images from the pneumonia images.As a higher quality corpus of COVID-19 diagnostic image data becomes available, it may be possible to produce clinically trusted deep learning-based models for the fast diagnosis of COVID-19 as distinguished from similar conditions such as pneumonia. Such a tool would prove invaluable in practice, where other diagnostic tests for COVID-19 are either unavailable or unreliable. As the COVID-19 spread progresses throughout remote and economically challenged locations, an ability to diagnose COVID-19 from a readily available and portable medical imaging equipment such as X-Ray and Ultrasound machines would help slow the spread of the disease and result in a better medical outcome for the population.

REFERENCES

[1] H. Ravishankar, P. Sudhakar, R. Venkataramani, S. Thiruvenkadam, P. Annangi, N. Babu, and V. Vaidya, “Understanding the mechanisms of deep transfer learning for medical images,”Springer, 2016.

[2] G. Carneiro, Ed. Cham,”Recommendations-for -Chest-Radiography-and-CT-for-Suspected- COVID19-Infection,”2016.

[3] R. Yamashita, M. Nishio, R. K. G. Do, and K. Togashi, “Convolutional neural networks: An overview and application in radiology,” 2018.

[4] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition, ”2014.

[5] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, USA, Jun. 2016.

[6] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z.Wojna, “Rethinking the inception architecture for computer vision,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, USA, Jun. 2016.

DiabApp – " Hybrid Transfer Learning Neural Network using Multiple Image Recognition Pretrained Models."

Christine Mariam Joseph, Arunima TA, Aleena Acca Benny, Aparna S

Department of Computer Science and Engineering
Saintgits College of Engineering
Pathamuttom, Kottayam, Kerala
christine.mj1721@saintgits.org
arunima.ta1721@saintgits.org
aleena.ab1721@saintgits.org
aparna.s1721@saintgits.org

***Abstract* - Diabetics has escalated in almost every part of the globe. Healthy eating is one of the main strategies for controlling diabetics. It is a common opinion that appropriate modifications and monitoring of food intake can assist in proper management of diabetes coupled with weight management as well as the control of both blood glucose and plasma lipid levels. Intake of fruits and vegetables at an adequate amount can lead to many health benefits. But in some cases, like that of diabetic patients, before consumption we have to make sure if he/she can have that vegetable or fruit. So here the problem is to clarify and quantify how the intake of a particular fruit/vegetable affects the patient's health, blood glucose level in this scenario. As a solution, we are proposing "DiabApp", that will assist diabetics patients to decide whether to consume this unpacked food (fruits or vegetables) and give valid reasoning to this suggestion. Even though there are numerous applications that help diabetics patients in maintaining diet and exercise, an app that suggests to us which food is good and which is bad for our health and why are extremely rare. This can be made possible by creating a hybrid transfer learning neural network using multiple image recognition pretrained models.**

Keywords: Deep learning, Convolutional neural network, Hybrid model, Diabetics, Lifestyle diseases.

I. Introduction

Diabetes is a chronic, metabolic and non-communicable disease characterized by elevated levels of blood glucose (or blood sugar), which leads over time to serious damage to multiple important organs of the body like the heart, kidneys, eyes, blood vessels and nerves. Usually in adults, the most common is type 2 diabetes, which occurs when the body becomes impervious to insulin or doesn't produce enough insulin. In the past few decades, the commonness of type 2 diabetes has ascended dramatically in countries of all income levels. Type 1 diabetes, also known as juvenile diabetes or insulin independent diabetes, is an acute condition in which the pancreas produces little to no insulin. Access to affordable diabetes care, such as insulin, is vital for people with the condition to survive. A global agreement was made to halt the increase of diabetes and obesity by 2025

Diabetes affects approximately 422 million people worldwide, the majority of whom live in low- and middle-income countries, and diabetes is directly responsible for 1.6 million deaths per year. Over the last few decades, both the number of cases and the incidence of diabetes have gradually increased.

A healthy lifestyle characterized by proper diet control and exercise is essential to control the disease. The aim of diabetes management is to keep blood sugar levels as close to normal as possible without causing low blood sugar. Dietary modifications, exercise, weight loss, and the use of effective drugs are normally enough to achieve this (insulin, oral medications). The above-mentioned information itself shows it is high time to develop an assistive technology for diabetic patients. Diabapp is such an assistive technology to patients dealing with diabetes. It will be effective if developed as a mobile/desktop app. This helps patients to realize the sugar level content of an unpacked food thus he can decide if he/she should consume it or not. DiabApp will be a good addition to the medical sector in order to control many lifestyle diseases, not just diabetes. Diabapp is a friendly recommender app, which helps people to know about the valid assessment of each food item. We are hoping to use datasets available from Kaggle and for implementation python and html are preferred

II. Related Works

As deep learning is one of the most emerging fields,each and everyday new innovations are made which help the day to day life of a common man much easier in various aspects of life.Different studies are done earlier to incorporate technologies into one's life. Let us see such concise studies done earlier.

Wilma Mary Thomson, Aswathy T,Venkateswaramurthy.N[1]presented a study focused on developing an Android-based cell phone application for diabetics with various features for disease management. Methodologies included comprehensive analysis of all currently available diabetes applications for Android operating systems was conducted to identify the functionalities needed in the app, and a questionnaire was used to assess the app's usability.

Mohammed Asif[2] mentioned Diabetes mellitus, also known as type-2 diabetes, is one of the world's most serious non-communicable diseases and one of the fastest-growing public health issues. It is a difficult to treat and costly disease to handle. According to estimates, the number of diabetics in the world would double from its current level. It is shown here that proper testing, care, and lifestyle changes are necessary.

Myeungee Han and Eunjoo Lee[3] conducted a research. The aim of this study was to see whether mobile health apps could help people change their health-related habits and clinical health outcomes. Despite the high risk of bias, such as selection, performance, and identification, this systematic review found that using mobile health apps improves health-related behaviors and clinical health outcomes.Vidya Kudva, Keerthana Prasad and Shyamala Guruvare[4] conducted an in depth analysis of Transfer learning with deep pre-trained convolutional neural networks which is rapidly being used in the medical sector to solve a wide range of problems. Despite having been trained on images from a completely different domain, these networks are adaptable enough to solve a problem in a different domain.They looked at identifying appropriate filters using pre-trained networks including AlexNet and VGG-16 net to detect cervical cancer from cervix images in this research.Horea Muresan and Mihai Oltean [5]specified in their research paper that their aim was to propose a new dataset of common fruit images. Fruits-360 was the name of the dataset.Inkyu Sa,Zongyuan Ge, Feras Dayoub, Ben Upcroft, Tristan Perez, and Chris McCool[6]This paper's aim is to propose a new dataset of common fruit images. The dataset's name was Fruits-360. Faster Region-based CNN is a state-of-the-art object detector developed as a result of recent work in deep neural networks (Faster R-CNN). They use transfer learning to adapt this model for the task of fruit detection using imagery from two modalities: a color (RGB) and NIR information.This method is not only more accurate, but it is also much faster to implement for new fruits.

Er-Yang H and Gui-Hua[7] Wen specified that many image classification models have been successfully developed using convolutional neural networks, but this requires a large amount of training data. There is a scarcity of clinical data in the field of Traditional Chinese Medicine. To address this problem, they proposed a transfer learning-based method for constitution classification. The DenseNet-169 model, which was trained in and ImageNet is applied. Namgyu Ho and Yoon-Chul Kim[8] stated that since transfer learning is well suited to medical image data where labeled data is scarce and costly to acquire, the feasibility of using deep convolutional neural networks (CNNs) to automatically identify the short axis slice range was needed to be investigated.Natalie Best, Jordan Ott &Erik J. Linstead[9]They looked at how transfer learning could be used to classify software unified modeling language (UML) diagrams using models that were pre-trained on non-software engineering data. Even though the pre-trained model was not exposed to training instances from the program, our experimental findings indicate that training responds positively to transfer learning as a function of sample size.Sakshi Indolia,Anil Kumar Goswami,S.P.Mishra and Pooja Asopa[10] in their research paper said that that the Convolutional Neural Network (CNN) is a deep learning technique for solving complex problems. It gets around the drawbacks of conventional machine learning methods. The aim of this research is to provide information and knowledge about different aspects of CNN. This research presents a conceptual interpretation of CNN, as well as the three most popular architectures.Mingyuan Xin and Yong Wang[9] said for maximum interval minimum classification error, a groundbreaking depth neural network training criterion was suggested. To get better results, the cross entropy and M3CE are measured and combined at the same time. Finally, they put their proposed M3 CE-CEc to the test on MNIST and CIFAR-10, two deep learning standard databases.

III. Proposed Innovation

Traditional classification algorithms cannot learn the complicated non linear relationships in image data. Deep neural network methods for extracting features in images are not very efficient and accurate. In convolutional neural network methods, only the training samples provided by us yields knowledge from scratch to the neural network. So when it comes to real time application, images may show complex behaviour which will show a huge difference from those trained image sets of a model, in such cases, there is a need of using pretrained models. Big companies like Google and Facebook have trained image recognition models for their large scale general requirements. Pretrained models are actually big data models. Thus these models contain the shapes and features of a huge variety of items within it. If we try to use these shapes and features learned within pretrained models, from input later to intermediate layers, we can connect it to our particular task for classes. Each pretrained model performs different tasks. Traditional methods like CNN and deep learning play a substantial role in building up hybrid models. Hidden or custom layers introduced in between each layer helps in combining various features and fine tune these layers to create the shapes in our training data. Thus only knowledge can be extracted from these models and can be trained for our purpose. This will provide us a model mimicking a hugely trained model in the same task.

IV. Units

In the proposed methodology, the system is divided into six different modules. In the first module a dataset with a considerable amount of fruits and vegetable images will be generated. It is then partitioned into training, testing and validation data. From which training and validation data will undergo data augmentation in the second module. A hybrid model is designed in module three, where the model is trained and optimized. In the next module, the testing data is used for evaluating the model to obtain results as well as performance of the proposed model. Model deployment is what comes in the next module followed by the creation of a real time prediction webapp

Unit 1: Dataset Generation and Partitioning

First of all, a dataset with a considerable amount of fruits and vegetable images will be generated.Here the dataset used is Fruit 360. The dataset can be extended to contain double the number of subjects. For the purpose of matching images, these data will be stored into the database. Generated dataset will be partitioned into training data, testing data and validation data.

The training data is a compilation of data used to teach a programme how to learn and generate sophisticated results using technologies such as neural networks. Data testing is used to assess the model's success using a performance metric. A validation dataset is a sample of data from your model's training that is used to estimate model ability when tuning the model's hyperparameters.

Unit 2: Data Preprocessing

Synthetic images can be generated by augmenting data. Applying random, but practical transformations to the training images, such as rotation and horizontal flipping, to artificially introduce sample diversity.. This helps to expose the model to different aspects of the training data and reduce overfitting. For our model to pass through all of our training data one time in each epoch, steps per epoch equal to a number of batches is provided.

Unit 3: Designing Model Architecture

A hybrid model of architectures like VGG, GoogLeNet and ResNet50 will be used for fruit/vegetable image classification and recognition. Pretrained models from the Keras Applications have the benefit of allowing you to make predictions with weights that have already been measured. We use Imagenet weights in this case, and the network is a ResNet50. GlobalAveragePooling2D is used to apply average pooling on the spatial dimensions until each spatial dimension is one, and leaves other dimensions unchanged. One of the most used image-recognition architectures, VGG is a cutting-edge object-recognition model of up to 19 layers. VGG, which was built as a deep CNN, outperforms baselines on a variety of tasks. Loss of a model is the deviation of expected performance from the desired outcome. It can be minimised and the model made more effective using optimization techniques. During compilation of the model,since there are two classes, a binary cross-entropy loss is used given that the model provides a linear output. Optimizer used is Adam, which is the deep learning model training algorithm that replaces stochastic gradient descent. Weights in various layers of the neural network are modified during optimization, and the model will be trained again for better performance. The model's hyperparameters and trained parameters are obtained after training is completed.

Unit 4: Model Training and Performance Evaluation

In this unit, model training is done by saving the model in each epoch. Here the best weights are taken up for training the model after the entire set of epochs have completed.This helps in increasing the accuracy of the current model.After each epoch the accuracy is being calculated and if the accuray have not increased, the learning rate should be reduced. The validation loss is being calculated to know if there is any betterment after each epoch. After this, the performance evaluation is carried out by checking the training and validation loss and making sure that the model is not overfitted.

Unit 5: Model Deployment

In this unit, the created model that is the trained model is saved as a file since otherwise it would be time taking as we have to train this model each time when it comes to use and also helps in easier predictions. So this trained knowledge is saved as an .h file where .h file is commonly used to save codes and import them whenever needed.

Unit 6: WebApp Creation

Finally, In this module, Webapp creation is done which is a real time prediction. In order for the users to access its usage, a webapp is built which helps customers to know how the fruit or vegetable they intend to buy/eat will affect their blood glucose level and if the customer is willing to input their latest data of blood glucose level, the app will provide with a suggestion about the intake of that particular fruit/vegetable.

V. Results and Discussion

The trained network for generation of realistic images from datasets was tested on a number of times. By using hybrid models we perform both classification and prediction. The model was also viewed to perform reasonably well on images with varying stance, illumination, etc. These captured images undergo image recognition using a transfer learning approach from a pre-trained convolutional neural network which is already trained with a large number of images for recognition. The model could recognize the image from the captured realistic photo and it has a better performance then the existing methods.

The major application of this system is the help provided to the users who are diabetic. The system can be integrated into a desktop with camera connectivity in grocery stores or supermarkets systems to identify fruits/vegetables from real time visuals. Or in a more convenient way, it can be developed as a mobile/web app. It can be used for knowing more about the fruit/vegetable the user does not know about. In future, this system can be implemented in real time scenarios integrated with IoT devices, to manage diets of many people with non communicable diseases.

VI. Conclusion

An efficient system for fruit recognition and recommendation is proposed here. Existing methods do not provide satisfactory results in such classification and recommendation tasks. Current practices include health benefits information of each fruit and vegetable which help users to get tips about controlling their diet and tips that help in maintaining a healthy lifestyle. But there are only a few sites which provide sugar level contents. Thus, a new system is essential to ease the task and which will be helpful for all diabetics patients, young as well as older generations. With help of various pretrained models and with the usage of transfer learning and fine tuning, images are easily classified and results are provided with the hybrid model we proposed. The future scope of this system is that it can be implemented not only for diabetics but for almost all non-communicable lifestyle diseases such as cholesterol, increase in sodium level and so on. The introduction of such apps will help many in the medical field as well helping patients to know better about the unpacked food items that they should consume. Most people think in such a way that consuming fruits and vegetables at a high rate does not have any effects on their body, but with the development of this app people can be made aware about what quantity of such food should be consumed and how it may affect them.

References

[1] Thomson, Wilma & T, Aswathi & .N, Venkateswaramurthy & Kumar, R. (2018), “DEVELOPMENT OF ANDROID BASED HEALTHCARE APPLICATION FOR DIABETES PATIENTS”, International Research Journal Of Pharmacy. 9. 198-206. 10.7897/2230-8407.099213

[2] Asif, Mohammad. (2014), “The prevention and control the type-2 diabetes by changing lifestyle and dietary pattern”, Journal of education and health promotion. 3. 1. 10.4103/2277-9531.127541.

[3] Han, Myeunghee & Lee, Eunjoo. (2018,.” Effectiveness of Mobile Health Application Use to Improve Health Behavior Changes: A Systematic Review of Randomized Controlled Trials. Healthcare Informatics Research”, 24. 207. 10.4258/hir.2018.24.3.207

[4] Kudva, V., Prasad, K. & Guruvare, S,” Hybrid Transfer Learning for Classification of Uterine Cervix Images for Cervical Cancer Screening”,J Digit Imaging 33, 619–631 (2020). https://doi.org/10.1007/s10278-019-00269-1

[5] Mureșan, Horea & Oltean, Mihai. (2018),”Fruit recognition from images using deep learning”,Acta Universitatis Sapientiae, Informatica. 10. 26-42. 10.2478/ausi-2018-0002.

[6] Sa I, Ge Z, Dayoub F, Upcroft B, Perez T, McCool C,” DeepFruits: A Fruit Detection System Using Deep Neural Networks”, Sensors (Basel). 2016;16(8):1222. Published 2016 Aug 3. doi:10.3390/s16081222

[7] Huan, EY., Wen, GH,” Transfer learning with deep convolutional neural network for constitution classification with face image”, Multimed Tools Appl 79, 11905–11919 (2020). https://doi.org/10.1007/s11042-019-08376-5

[8] Ho, N., Kim, YC,” Evaluation of transfer learning in deep convolutional neural network models for cardiac short axis slice classification".,Sci Rep 11, 1839 (2021). https://doi.org/10.1038/s41598-021-81525-9

[9] Best, N., Ott, J. & Linstead, E.J,”Exploring the efficacy of transfer learning in mining image-based software artifacts”,J Big Data 7, 59 (2020). https://doi.org/10.1186/s40537-020-00335-4

[10]Xin, M., Wang, Y,”Research on image classification model based on deep convolutional neural network” J Image Video Proc. 2019, 40 (2019). https://doi.org/10.1186/s13640-019-0417-8

PROTAKER: A SYSTEM TO SECURE PATIENT CREDENTIALS

1st Devika Krishnan
Dept.of CSE
Sree Buddha College of Engineering
Alappuzha,India
devujk736@gmail.com

2nd Gokul G Nair
Dept.of CSE
Sree Buddha College of Engineering
Alappuzha,India
gokulg41@gmail.com

3rd Kevin Jacob
Dept.of CSE
Sree Buddha College of Engineering
Alappuzha,India
kevinjacob@gmail.com

4th Niksa Wilson
Dept.of CSE
Sree Buddha College of Engineering
Alappuzha,India
niksajewel@gmail.com

5th Dr. S.V Annlin Jeba
Head of the Department
Dept.of CSE
Sree Buddha College of Engineering
Alappuzha,India
sureshannlin@gmail.com

***Abstract*—In recent times the personal and protected health information of patients and other sensitive data are being exposed online without the knowledge of covered entities which is nearly intolerable for them. Here the goal of this design is to provide a low cost, portable and efficient mechanism to provide security to the patient's credentials along with a well potent health monitoring system. It provides privacy and secure transmissions through AES algorithm and access control mechanism algorithms. IoT sensors are used here in-order to collect various data and transmit it to the network. The transmitted data is then stored in the cloud and this data can be monitored by the doctor at any time to provide remarks or even medical attention to the patient's in real time. This idea mainly focuses on those who are elderly and have disabilities and are not able to look after themselves. A GSM module is provided over this mechanism to provide an alert message in case of emergency situations.**

***Index Terms*—IoT, AES algorithm, Access Control Mechanism algorithm, Sensors.**

I. Introduction

The Internet of Things (IoT) has been established over the past few years. These technologies lead our life to interact with the sensors/devices of the world and help to collect smart data from them to make our life so easy and convenient. They are widely used in various areas like smart home monitoring, smart cities, smart healthcare systems etc.

In healthcare applications, IoT devices are introduced to patients. Their health information is collected from devices and these data are stored for future references. IoT in E-medicine uses the emerging technologies to provide immediate treatment to the patient. It also monitors and keeps track of the health record of a person [1]. IoT performs various computations on the collected data and provides health related advice.

Various diseases like Lung failures and heart related diseases are increasing day by day. It is necessary to check the health of elderly people as well people with disabilities at home or at hospitals. But it requires constant observation of Doctors and caretakers[7]. Cyber security and healthcare providers have been struggling hard to secure each and every sensor/device in the IoT network with the integrity of its data because safety and comfort of patients' everyday health relies on this data collection; this data is greatly affected by cyber threats/attacks. Thus, patients' privacy sensitive data can also be affected. various solutions offer security to patients' health monitoring data but they often fail to deal with complicated attacks. Thus, IoT devices are made for remote health monitoring in the healthcare sector in order to keep patients safe and healthy, and it also helps the medical practitioner to deliver sudden care to the patients[8]. As a result, it increased patient satisfaction, as interactions with doctors have become easier and more efficient. Also, remote health monitoring of patients helps to reduce the visit to the hospital and keeps track of patient health records. It also reduced healthcare costs and improved treatment outcomes[9][10]. However, the IoT paradigm still requires various efficient solutions to protect patient credentials against cyber threats/attacks

Identify applicable funding agency here. If none, delete this.

throughout the way from the IoT sensors toward the healthcare provider. Thus, in this paper we contribute to the protection of IoT-based healthcare data as well as a health monitoring system is provided in order to collect data from the patients and transfer it to the doctors in an ease.

II. RELATED WORK

In this section we shall discuss some cyber threats and their related solutions. We mainly focus on IoT based hardware modules implemented over some sophisticated mechanisms of cyber security. We have included some in this section.

A wireless device which was developed by Kovuru Chandu Chowdary [1] is used for calculating oxygen saturation, pulse rate, temperature and blood pressure. The fingerprint sensor is attached to the microcontroller to allow access only to the concerned physician. The goal of this paper was to design a low cost, portable monitoring system consisting of different sensors incorporated for measuring physical parameters of patients as well as wireless transmission of data.

Ashwini Gutte and Ramkrishna Vadali[2] states that with the help of IoT's it has certain features and it helps to keep the necessary details and reports of a patient organized and available to all actors in the system. IoT devices like power sensors are used to gather data from patients and these data are displayed using LCD and are stored on any of the personal computers. It is also stored on the cloud thus, any actor in the system can refer to it.

Taniya Shirely Stalin1, Abey Abraham suggested a system where its goal is to design and implement a low cost, portable effective patient health monitoring system [3]. It can transmit the vital signs of a patient in case of emergency situation continuously through a wireless communication network system. IoT networks have various potentialities which can be used to monitor the health of a patient by examining the collected data regularly. It ensures privacy and also offers secure communication using Data security Algorithm. There are enormous security concerns with patient health monitoring sensors in IoT. These concerns are realized by advanced security and privacy attacks which includes data breaching, data integrity etc.

Hai Tao, Md Zakirul Alam Bhuiyan, Ahmed N. Abdalla, Mohammad Mehedi Hassan, Jasni Mohamad Zain, and Thaier Hayajneh[4] proposed a secure data collection scheme for IoT-based healthcare system named Secure Data which aims to tackle security concerns. The performance of Secure Data is substantiated through simulations with FPGA in terms of hardware frequency rate, energy cost, and computation time and the results show that Secure Data can be efficient when put in application with protecting security risks in IoT-based healthcare.

Entao Luo; Md Zakirul Alam Bhuiyan[5] proposed a system for patient privacy protected data collection, with the objective of preventing various types of attacks. Privacy Protector includes the plan of secret sharing and share repairing for patients' data privacy. In this chassis, a distributed database consisting of multiple cloud servers ensures the privacy of patients' personal data can remain protected as long as one of the servers remains determined. It also presents a patient access control scheme in which multiple cloud servers cooperate in shared construction to offer patients' data to healthcare providers without disclosing the content of the data. The privacy performance analysis has shown that the Privacy Protector framework is secure and privacy-protected against various types of attacks.

H. Al-Hamadi and I. Chen[6], here work is concerned with a health IoT system consisting of different IoT devices carried by members of an environmental health community. It proposes a novel trust-based decision making protocol that uses trust-based information sharing among the health IoT devices, so that a collective knowledge base can be built to rate the environment at a particular location and time. This knowledge would enable an IoT device acting in favor of its user to decide whether or not it should visit this place/environment for health reasons. This trust-based health IoT protocol considers risk classification, reliability trust, and loss of health probability as three design dimensions for decision making, resulting in a protocol suitable for decision making in health IoT systems.

III. PROPOSED SYSTEM

The system consists of a hardware section and a software section. The health parameters are obtained through the wearable sensors provided at the hardware section and the required data is pushed to the cloud using a gateway system. The pushed data can be accessed by the healthcare provider like doctors using the interface provided and take the necessary actions through analysing and prescribing the requirements for the patients. The block diagram of the proposed architecture is shown in fig 1.

A. Hardware Section

The patient is monitored wirelessly using sensors. Health data of patient's are collected using various health

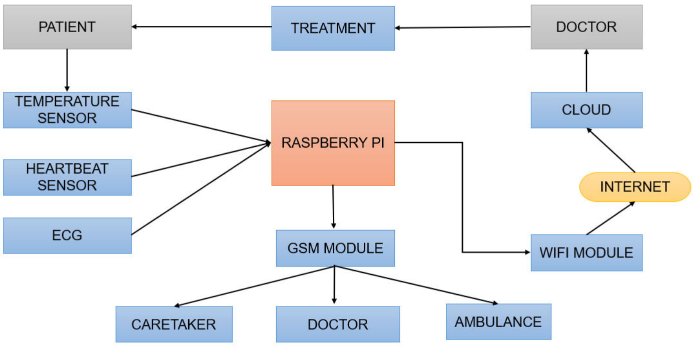
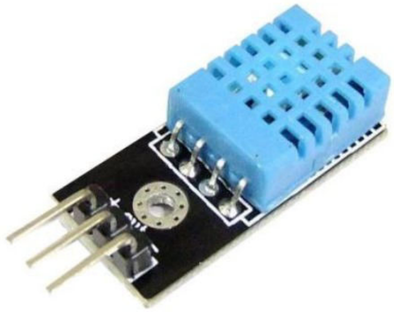


Fig. 1. Block diagram of the proposed health monitoring system

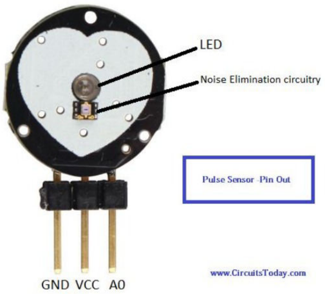
parameters like temperature, Heart rate, ECG parameters using wearable sensors[12]. Here we use three different types of sensors.

- Temperature Sensor



The temperature sensor is used to measure the body temperature of a person. The sensing element is composed of multiple thermocouples on a silicon chip to measure an object’s infrared energy. TE packages and customizes thermopiles in various package sizes and with different wire lengths to accommodate customer needs[11].

- Heart rate Sensor
Heart rate sensor is an electronic device that is used to measure the heart rate i.e., speed of the heartbeat.The heartbeat is measured in beats per minute or bpm, which indicates the number of times the heart is contracting or expanding in a minute.The principle behind the working of the Heartbeat Sensor is Photoplethysmograph[13]. According to this principle, the changes in the volume of blood in an organ is measured by the changes in the intensity of the light passing through that organ.



- ECG Sensor

Electrocardiogram (ECG) is a used to detects cardiac (heart) abnormalities by measuring the electrical activity generated by the heart as it contracts[15].This allows us to understand the level of physiological arousal that someone is experiencing, but it can also be used to better understand someone’s psychological state.

The collected data from various sensors are interfaced to Raspberry PI4. The data collected by sensors are in the form of analog signals which should be converted into digital signals using an Analog to Digital Converter (ADC)[14]. The data collected are transferred to the Doctor via the Wi-Fi module. A GSM module is attached with the raspberry PI.

- GSM Module
GSM detects the critical condition and provide an alert message to the receiver unit. The receiver can

view data and the message regarding the patient's health status through internet connectivity in the system or mobile. The objective of GSM module is to provide mobile healthcare for patients. This system will reduce the time and it is easy to use. It is also used for self-monitoring the patients anywhere at any time. If it exceeds the condition, immediately send the information to the doctor's mobile phone or relatives via SMS using GSM modem and the doctor sends back the precaution notification to them. For emergency situations, the alert messages are sent to the ambulance with the help of a GSM module. So that user will be aware of their health and can take care accordingly. GSM works on UART protocol and it passes AT commands when the threshold value from the sensor increases or decreases. When the AT commands are passed, GSM will get activated.

B. Software Section

In this section we will discuss about the cloud server and User Interface. The data from the Raspberry PI are pushed towards the cloud using an API gateway. The working of Raspberry PI is shown in fig 2. Cloud server serves two functions, Database storage and hosting. The data collected from the sensors are encrypted using AES algorithm and data hashing for providing the patient's credential security when they are passed to the cloud and decrypted when they are retrieved from it. For pushing to the cloud server we use MQTT protocol and the users have to log into the webpage for accessing the site.

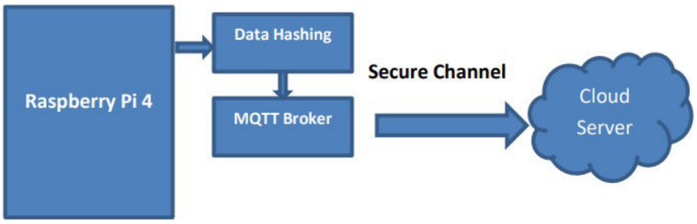


Fig. 2. Block diagram for working of Raspberry PI

Through Role Based Access Control (RBAC) mechanism the data stored in the cloud can be retrieved by the user. The roles are already described accordingly and are checked with the user and privileges according to them are provided. A user can enter the website through user credentials already created and the provided access control mechanism checks the permissions to provide. Here the main roles provided are the Doctors, hospital management and patient. A doctor can add read and write assessments about the patient's health along with the prescriptions. The Hospital Management is able to add and remove the user accordingly and the patient or the patient's caretaker can access the information that is provided by the doctors.

Doctors can access the data stored in the cloud through a provided webpage. By analyzing the data obtained the doctors can provide prescriptions and required information to the caretakers of the patient thus a mutual communication and monitoring of the healthcare providers get involved without frequent visits to the hospital.

C. RBAC Algorithm

Algorithm 1 **Access decision for Role Based Access Control(RBAC) mechanism**

Input: A UA context in RBAC (K$_{U,R}$).
A PA context in RBAC (K$_{R,DXP}$)).
User (Usr) in U, the role (Rle) in R and permission (Perm) to access the data object (Obj) in (D×P).
Output: Access decision(access): permit or deny.

```
For each $U_{t_1} \in K_{U,R}$
    If($U_{t_1} == Usr$)$then$
        For each $R_{t2} \in K_{U,R}$ $do$
            If ($R_{t_2} == Rle$)$then$
                $UA_{t1t2} \Leftarrow K_{U,R}(U_{t1}, R_{t2})$.
            EndIf
            If($UA_{t1t2} == 1$)$then$
                $R_{active} \Leftarrow R_{t_2}$
            Else
                $access \Leftarrow deny$
            EndIf
        EndFor
    EndIf
```

```
EndFor
For (each $(D \times P)_{t3} \in K_{R,(D \times P)}(R_{active},(D \times P))do$
    If $((D \times P)_{t3} == (Obj \times Perm) then$
        $st \Leftarrow K_{R,(D \times P)}(R_{active},(D \times P)_{t3})$
    EndIf
EndFor
If$((st == 1)$
        $access \Leftarrow permit$
    Else
        $access \Leftarrow deny$
    EndIf
Return $access$
```

The above algorithm defines the Role based access control mechanism. Here UA context refers to the role of the user and it checks what is the role of the user. PA context checks that what permission does the user has. When a user enters, it checks whether the user is in the database or not. If it exists it checks the role of the user. Roles are assigned as per fig 3. For example, if the user is a doctor then the role of the user will be doctor. After this is checked, it checks what permissions are given to the user and this particular user can access only certain fields in the database. The output of the algorithm is an access decision i.e., permit or deny.

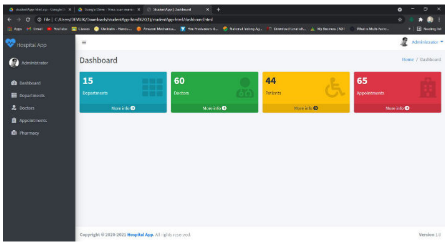
USER	*ROLE*	*PERMISSION*
U1	Doctor	Read/Write Patient Details
U2	Hospital Management	Add/Remove User
U3	Patient	Read his Information

Fig. 3. Role Based Access Control

Theoretical Analysis

In this section we evaluate the proposed e-health monitoring system to the existing SecureData model. We use a more sophisticated mechanism in our system to make it more secure and thus leading to low percentage of data leakage. The traditional models use the DES algorithm for data encryption and here we implement the AES algorithm which is far more secure and provides better encryption for the data. The data that is pushed to the server is actually passed through a secure channel which is provided by the use of data hashing and MQTT protocol. This also enhances the data security. Thus we are able to prevent data breach at any level and the patient's credentials are safe within the system. On top of that we have implemented a well established access control mechanism in our system to provide priorities to the users who are interacting with the system. A Role based access control mechanism is used here with specific instructions which are set by default so that no manipulation is done from within the system and the Admin has the authority to remove if found any. These modifications provide a greater upper hand to our proposed system over the traditional ones.

Implementation Result



Dashboard

15 Departments

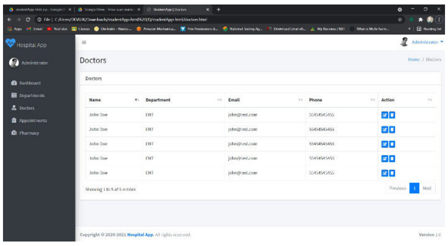
60 Doctors

44 Patients

65 Appointments

Copyright © 2020-2021 Hospital App. All rights reserved. Version 1.0

Here is the UI of the home page that the user gets when he/she logs into the system. This particular one consists of several features like Department Doctor patient and appointments. Each dashboard is suitably assigned for specific actions that could help the user to have a much interactive yet simple experience with the developed system



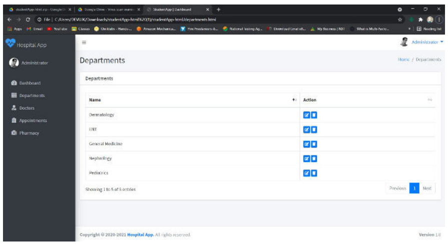
Doctors

Name	Department	Email	Phone	Action
John Doe	ENT	john@test.com	5545454545	
John Doe	ENT	john@test.com	5545454545	
John Doe	ENT	john@test.com	5545454545	
John Doe	ENT	john@test.com	5545454545	
John Doe	ENT	john@test.com	5545454545	

Showing 1 to 5 of 5 entries

Copyright © 2020-2021 Hospital App. All rights reserved. Version 1.0

Here we have the Doctors tab. We have the list of available doctors listed one by one along with their corresponding department and contact information for selecting them and making an appointment with them. And actions are taken accordingly



Departments

Name	Action
Dermatology	
ENT	
General Medicine	
Nephrology	
Pediatrics	

Showing 1 to 5 of 5 entries

Copyright © 2020-2021 Hospital App. All rights reserved. Version 1.0

This right here is the department tab where various departments that are enlisted in the site are listed down and the user can easily check through them with ease

CONCLUSION

Here we provide a new architecture of IoT based Health monitoring system along with secure channel, data security for the patient's credentials and access control mechanism. This system will be more useful for bedridden and aged patients. This system sensed data through the sensors and is pushed to the cloud where the doctors are able to access them for further analysis. Alerts are provided to the caretakers and other provided contacts though the GSM module when the monitored health data become fatal for the patient. The channel for carrying the information is secured using the AES and further data security is provided using Role Based Access Control (RBAC) mechanism. This system is self-monitoring and efficient and provides a secure frequent checking on a patient's health by the communication between the caretaker and the doctor.

REFERENCES

[1] Kovuru ChanduChowdary, K.Lokesh Krishna, K Lalu Prasad,K.Thejesh "An Efficient Wireless Health Monitoring System " Proceedings of the IEEE second International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)

[2] Ashwini Gutte and Ramkrishna Vadali "IoT Based Health Monitoring System using Raspberry Pi" IEEE Fourth International Conference on Computing communication Control and Automation (ICCUBEA), 2018

[3] Taniya Shirely Stalin1, Abey Abraham "Iot Based Health Monitoring System And Telemedicine" International Research Journal of Engineering and Technology (IRJET)

[4] Hai Tao, Md Zakirul Alam Bhuiyan , Ahmed N. Abdalla, Mohammad Mehedi Hassan , Jasni Mohamad Zain, and Thaier Hayajneh "Secured Data Collection With Hardware-Based Ciphers for IoT-Based Healthcare" ieee internet of things journal, vol. 6, no. 1, february 2019

[5] Entao Luo; Md Zakirul Alam Bhuiyan; Guojun Wang; Md Arafatur Rahman; Jie Wu; Mohammed Atiquzzaman "PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems" ure and privacy-protected against various attacks. IEEE Communications Magazine (Volume: 56, Issue: 2, Feb. 2018)

[6] H. Al-Hamadi and I. Chen, "trust-based decision making for health iot systems"," IEEE Internet of Things Journal, no. 99, 2017,Volume: 4, Issue: 5, Oct. 2017.

[7] Muhammad Irmansyah, Anggara Na sution, Era Madona, Roni Putra " Low cost Heart Rate Portable Device for Risk Patients with loT and Warning system "International Conference on Applied Information Technology and Innovation (ICAITI),2018.

[8] X. Yi, A. Bouguettaya, D. Georgakopoulos, A. Song, and J. Willemson, "Privacy protection for wireless medical sensor data," IEEE Trans. Depend. Secure Comput., vol. 13, no. 3, pp. 369–380, May/Jun. 2016.

[9] N. Cai and R. W. Raymond, "Secure network coding," in Proc. IEEE Int. Symp. Inf. Theory, 2002, pp. 1–8

[10] Adamkó Attila, Ábel Garai, István Péntek "Common Open Telemedicine Hub and Infrastructure with Interface Recommendation" 11th IEEE International Symposium on Applied Computational Intelligence and Informatics • May 12-14, 2016

[11] Adamkó Attila, Ábel Garai, István Péntek "Common Open Telemedicine Hub and Infrastructure with Interface Recommendation" 11th IEEE International Symposium on Applied Computational Intelligence and Informatics • May 12-14, 2016

[12] Umar Albalawi and Shital Joshi "Secure and Trusted Telemedicine in Internet of Things IoT" in proceedings of 2018 IEEE 4th World Forum on Iot, 2018

[13] C. Cannière, O. Dunkelman, and M. Kneževic, "KATAN and ´ KTANTAN—A family of small and efficient hardware-oriented block ciphers," in Cryptographic Hardware and Embedded Systems-CHES 2009. Berlin, Germany: Springer, 2009, pp. 272–288

[14] J. Shen et al., "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," J. Netw. Comput. Appl., vol. 106, pp. 117–123, Mar. 2018, doi: 10.1016/j.jnca.2018.01.003.

[15] J. Li et al., "L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing," Knowl. Based Syst., vol. 79, pp. 18–26, May 2015.

SURVEY ON AYURVEDIC PLANT DETECTION

Pooja V A[1], Sreelekshmi A N [2]

Sree Ayyappa College Eramallikkara Alappuzha, Kerala

Poojava6@gmail.com, sreelekshmiajithanasim@gmail.com

Abstract: Plants are an indispensable part of our ecosystem and globally it has a long history of using plants as a source of medicines. In ancient year people known about their plant's species and their usages. But now a day's people have no knowledge about the plant species and their harmful and usages. So, detection of ayurvedic plant is major benefits in this world. Different kind of medicinal plant species are available on earth, but it is very difficult to identify the plant. This paper explores survey of various ayurvedic leaves recognition using different classification methods. In this first leaf image is captured and uploaded to the system where this image is compared with another image which is stored in the database. Comparison is taken place with the help of algorithms. This paper presents not only survey of various techniques but also concisely discusses important concepts of image processing and classification algorithms for the detection of ayurvedic plant. The main objective of the survey is to identify the various classification techniques and recognition of leaf by various feature extraction methods.

Keywords: Classification, Feature Extraction, Medicinal plants

1. INTRODUCTION

Plants are the key factor for the survival of life on earth. One of the most important tasks of scientists, identify the correct plant species. Because plants have important have an important role in the nature of life. Oxygen in the air is major role in life. Almost all oxygen in the air that breathe by the humans and animals is produced by plants. Without the plants is difficult to existence of life in the world.

All the traditional Indian medical systems namely Ayurvedic, siddha etc are use medicinal plants. Most types of plants have unique leaves that are different from each other based on the number of characters, such as colour, shape, texture and vein [6]. In the world there are lot of plant species, some of them are medicinal plants, others are existents and others are harmful to use. Leaves are most commonly used for the plant identification, the stem, flowers, petals, seeds and even the whole plant can be used in an automated process [6]. Medicinal plants are the backbone of system of medicines called Ayurveda and it is useful for treatment of certain chronic diseases.

Ayurveda is considered as a form of alternative to allopathic medicines in the world and this Indian system of medicine has rich history. The ethnic groups of people in India classify plants according to their medicinal values. Identification of medicinal plants is considered as an important activity in the preparation of herbal medicines. The identification of ayurvedic plants based on the leaf images. It is very useful to many areas such as forestry, physicians, pharmaceutical laboratories and even used in the medicinal areas. Now a days the ayurvedic plants have important role in the medicines field.

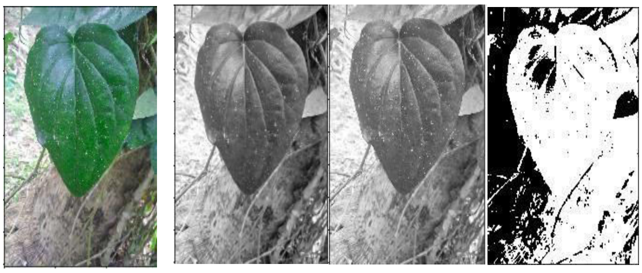
The main aim of this paper is to survey on various feature extraction methods and classification of the leaf Images and their accuracy. The paper detection of ayurvedic plants based on the leaf images. Mainly four stages or phases are used for detection, they are acquisition, pre-processing, feature extraction and classification. Image acquisition are collection of datasets based on the species and pre-processing is used to remove the noise from the images and enhanced the image quality. Feature extraction is to extract the features from the leaf images

11. RELATED WORK

Researchers have tried many methodologies to extract the features and identify the plant species automatically. Most of these methods make use of combination of many parameters. Figure 1 illustrates the general framework of the Ayurvedic leaf identification system. Identify the ayurvedic plant from the given leaf images are described below:

1. Foremost step in the plant classification is acquisition. Image acquisition is the collection of plant species from different areas. Leaf image is captured in a digital camera or phone and it is termed as an input Image. Different categories of images are used for detection, they are real image.

2. Then the input images are pre-processed to enhanced the important features. Pre-processing the images is an important step as it increases the probability of getting desired output in the future steps of image processing [3]. The pre-processing removes the noise or unwanted things from the image and enhance the images for better accuracy. Enhancing process includes the image is converted into Gray scale, image segmentation, smoothing, thresholding, boundary extraction. The objective of image pre-processing is to improvement in getting image information so that it can suppress unwanted information and enhancing the relevant image features for further processing.
   Figure 1 illustrate the pre-processing stages of leaf image.



3. The Image processing techniques are used for extracting the features from the images. The values of the extracted features represent the information of the image. The features that are extracted from the images are Shape, colour, vein and texture, margin. Each leaf has unique features that makes it different from each other.

4. In the next process, the significant attributes are drawn and mapped by the image in the database. The input image is classified to the plant whose leaf image comprises most extreme match score using some matching algorithm from which the information about the input image is obtained.

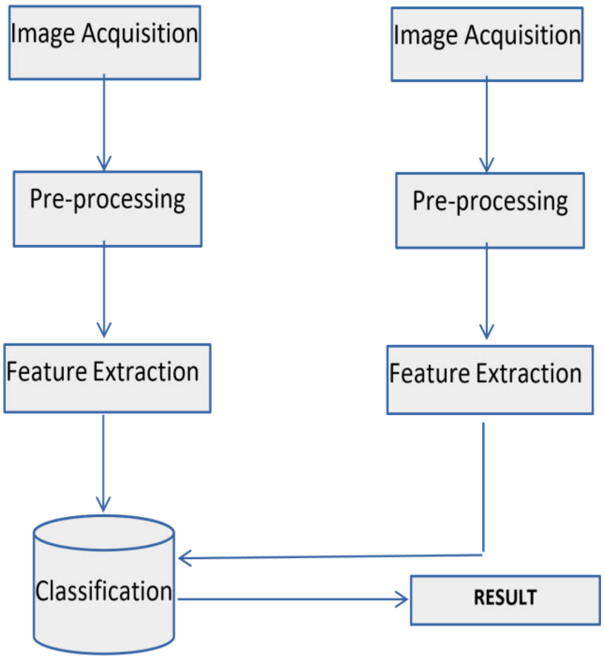


Fig 2: Block Diagram of Ayurvedic plant Prediction

111. SURVEY ON EXISTING METHODOLOGIES

Abdul Kadir, Adhi Susanto [1] "Leaf Classification Using Shape, Colour, and Texture Features". The system proposed the classification of leaves. The classification can do through the feature extraction. Several features are extracted from the leaves. The shape and vein, colour, and texture features were incorporated to classify a leaf. In shape feature, there are two kinds of shape features used in the identification system are geometric features and Fourier descriptors of PFT such as slimness and roundness. Colour moments represent colour features to characterize a colour image.

The features extracted are mean, standard deviation, skewness, and kurtosis. For RGB colour space, the three features are extracted from each plane R, G, and B. Vein features can be extracted by using morphological opening. That operation is performed on the Gray scale image with flat, disk-shaped structuring element of radius and subtracted remained image by the margin. At last is texture feature and feature normalization method are used. Twelve textures features are extracted from lacunarity.

After the feature extraction, apply classification method. The neural network called Probabilistic Neural network (PNN) was used as a classifier. The 40 kinds of plant leaves used to classify. The dataset used as Flavia dataset. Based on the dataset, 40 plants per species were used to train the network, and 10 plants per species were used to test performance of the system. The result gives 94% of accuracy.

Esraa Elhariri, Nashwa El-Bendary [2] "Plant Classification System based on Leaf Features". The method to classification approach based on Random Forests (RF) and Linear Discriminant Analysis (LDA) algorithms for classifying the different types of plant. The proposed approach consists of three phases that are pre-processing, feature extraction, and classification phases.

The colour features extracted from the leaves are mean, standard deviation, skewness and kurtosis. Then the vein feature, Leaf vein is one of the most basic features for leaf characterization and classification. This is because, different types of plants have different leaf vein patterns. So, it can be considered as a differentiating factor between different plant type. The shape feature is extracted based on geometric features, they are eccentricity, solidity, aspect ratio, isoperimetric factor, elongation, stochastic convexity, maximal indentation depth, lobedness. Texture features refer to the information describes the arrangement of pixels in any pattern. The first order texture features are average intensity, average contrast, smoothness, uniformity, entropy. Then also used second order texture features are angular moment, contrast, correlation, entropy, variance, homogeneity, cluster shape, prominence.

After the feature extraction, classification processes are occurred. Two approaches are used for classification, first one is Random Forests (RF). The Random Forests (RF) is one of the best-known classifications and regression techniques, which has the ability to classify large dataset with excellent accuracy. Random Forests algorithm generates an ensemble of decision trees. The input is entered at the top and as it traverses down the tree, the original data is sampled in random, but with replacement into smaller and smaller sets.

The next method is Linear Discriminant Analysis (LDA) algorithms. The is a commonly used technique for data classification and dimensionality reduction. Linear Discriminant Analysis easily handles the case where the within class frequencies are unequal and their performances has been examined on randomly generated test data. Its basic idea is to find a linear transformation that best discriminate among classes, then classification can be performed in transformed space based on some metrics such as Euclidean distance.

The dataset of total 340 images for leaves of different plants for both training and testing datasets with l0-fold cross-validation. Experimental results showed that LDA achieved classification accuracy of (92.65 %) against the RF that achieved accuracy of (88.82 %) with combination of shape, first order texture, Gray Level Co-occurrence Matrix (GLCM), HSV colour moments, and vein features.

Pushpa BR, Anand C and Mithum Nambiar P [3] “Ayurvedic Plant species Recognition using statistical parameters on leaf images”. This paper proposes a simple and efficient methodology for Ayurvedic plant classification using digital image processing and machine vision technology. The three major phases in proposed methodology are pre-processing, feature extraction and classification. Pre-processing is done in order to highlight the relevant features and reduced the unwanted noise from the images. The first set is image acquisition, in this paper defined clearly about the acquisition section. Image acquisition means collection dataset from different areas. It contains 208 leaf images of 26 different species and that are different angles and orientation images.

Then the next is pre-processing, it contains rgb to gray scale conversion, gray to binary, then apply smoothing and filtering. After that feature extraction processes is used. Arithmetic mean, standard deviation, convex hull ratio, isoperimetric quotient, eccentricity, entropy features are extracted. Then the classification is applied. The algorithm yields 92.7% of accuracy to get.

Adams Begue, Venitha Kowlessur [5] “Automatic Recognition of Medicinal Plants using Machine Learning Techniques”. A fully automated method for the recognition of medicinal plants using computer vision and machine learning techniques has been presented. Leaves from 24 different medicinal plant species were collected and photographed using a smartphone in a laboratory setting. A large number of features were extracted from each leaf such as its length, width, perimeter, area, number of vertices, colour, perimeter and area of hull. Several derived features were then computed from these attributes.

In this work the dataset is collected using the smart phones. The 30 images of different leaves were taken from 24 different plant species. The petiole of each leaf was removed and then placed one by one on a sheet of white paper before being photographed. The size of each image was 1024x600 pixels. The images are stored in the jpeg format.

Then used automatic pre-processing steps. They are converts rgb to gray scale, gray to binary, apply thresholding, erosion and dilation operation are used. There are number of features where extracted: length, width, area of the bounding box, area of leaf, perimeter of leaf, hull area, hull perimeter, number of vertices, horizontal & vertical distance maps, 45o radial map and the original RGB values of each pixel. There are 12 features were extracted from the dataset. The random Forest algorithm are used for classification. The accuracy of 90.1% was obtained from the random forest classifier.

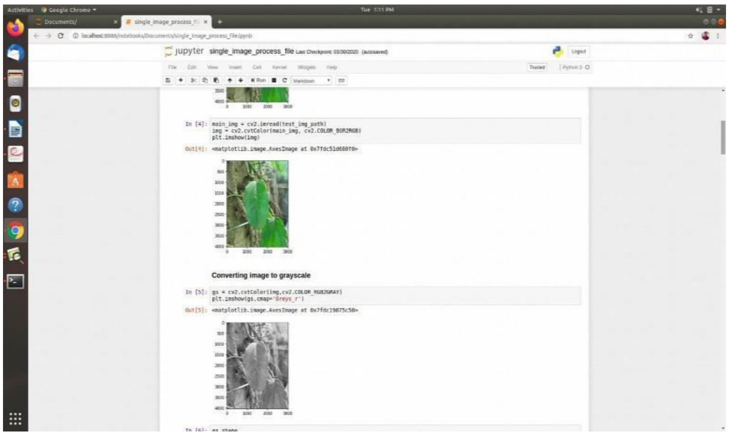
1V. OBSERVATION

From this survey, I recommended a Probabilistic neural network classifier, to get more accuracy when compare to other classifiers. This help to identify the exact name of medical leaf and reduce searching delay. In the feature Extraction phase, more feature is extracted from dataset, we get more accuracy. And also, the dataset is important think in the accuracy detection. The dataset number is increased or the leaf images are high, we get the accurate and high accuracy.

Figure 3 show the comparison table of different algorithm corresponding to their accuracy

CLASSIFICATION	ACURRACY
Neural Network	94%
LDA	88%
Machine Vision	92.7%
Support Vector machine	93%
Random Forest	90%

Figure 4 illustrate the simple image processing



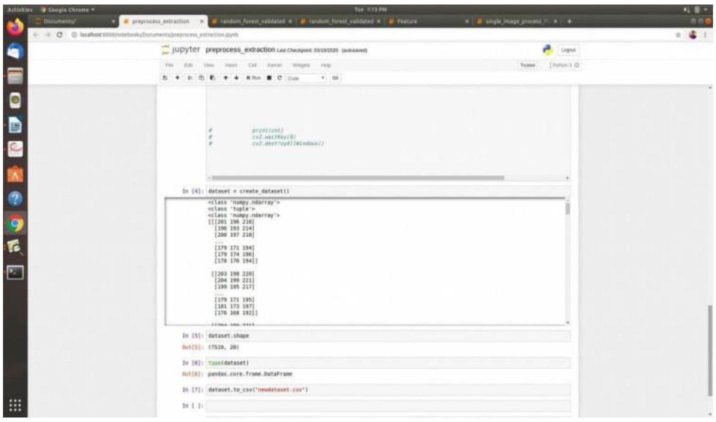
```
In [4]: main_img = cv2.imread(test_img_path)
        img = cv2.cvtColor(main_img, cv2.COLOR_BGR2RGB)
        plt.imshow(img)
Out[4]: <matplotlib.image.AxesImage at 0x7fdc51d680f0>
```

Converting image to grayscale

```
In [5]: gs = cv2.cvtColor(img,cv2.COLOR_RGB2GRAY)
        plt.imshow(gs,cmap='Greys_r')
Out[5]: <matplotlib.image.AxesImage at 0x7fdc19875c50>
```

jupyter
single_image_process_file Last Checkpoint: 03/30/2020 (autosaved)
Logout
Trusted
Python 3

Figure 5 illustrate the classification of leave image



```
#           print(cnt)
#           cv2.waitKey(0)
#           cv2.destroyAllWindows()

In [4]: dataset = create_dataset()
        <class 'numpy.ndarray'>
        <class 'tuple'>
        <class 'numpy.ndarray'>
        [[[201 198 218]
          [196 193 214]
          [200 197 218]
          ...
          [179 171 194]
          [179 174 196]
          [178 170 194]]

         [[203 198 220]
          [204 199 221]
          [199 195 217]
          ...
          [179 171 195]
          [181 173 197]
          [176 168 192]]

In [5]: dataset.shape
Out[5]: (7519, 20)

In [6]: type(dataset)
Out[6]: pandas.core.frame.DataFrame

In [7]: dataset.to_csv("newdataset.csv")

In [ ]:
```

jupyter
preprocess_extraction Last Checkpoint: 03/19/2020 (autosaved)
Logout
Trusted
Python 3

V. CONCLUSION

In this survey, we have discussed a brief overview of different medicinal leaf classification methods and recognition of plant species. We have also analysed in many ways, for the classification and recognition dataset. In this paper various techniques for leaf identification have studied and explained. The study shows that the research for identification of Ayurvedic plant. Among all the five papers, Abdul Kadir, Adhi Susanto [1] gives the maximum accuracy in identifying the ayurvedic plant. Our future work with be focused on more efficient algorithm and collection of more dataset.

REFERENCES

[1] Abdul Kadir, Lukito Edi Nugroho, Adhi Susanto, Paulus Insap Santosa”Leaf Classification Using Shape, Color, and TextureFeatures”

[2] Esraa Elhariri *, Nashwa El-Bendary ,*, Aboul Ella Hassanien ,* “ Plant Classification System based on Leaf Features”.

[3] Pushpa BR, Anand C and Mithum Nambiar P, “Ayurvedic Plant species Recognition using statistical parameters on leaf images”ISSN 0973-4562 Volume 11, Number 7 (2016) .

[4] P. Manoj Kumar,C. M. Surya,Varun P. Gopi ”Identification of ayurvedic medicinal plants by image processing of leaf samples”

[5] Adams Begue, Venitha Kowlessur, “Automatic Recognition of Medicinal Plants using Machine Learning Techniques” Vol. 8, No. 4, 2017

[6] Thibaut Beghin, James S Cope, Paolo Remagnino and Sarah Barman, "Shape and Texture Based Plant Leaf Classification", In International Conference on Advanced Concepts for Intel ligent Vision Systems (ACVIS), Sydney, Australia, December 13-16, pp. 345-353, 20 I 0, S pringer

[7] T. Sathwik, R. Yasaswini, Roshini Venkatesh and A. Gopal,”Classification of Selected Medicinal Plant Leaves Using Texture Analysis”, 4th ICCCNT, July 4 -6, 2013.

[8] Shitala Prasad, Krishna Mohan Kudiri, and R.C. Tripathi ,” Relative Sub-Image Based Features for Leaf Recognition using Support Vector Machine ”, in Proceeding International Conference on Communication, Computing & security ,Pages 343-346 , 2013.

[9] Vijayashree, T. and Gopal, A., 2015. Classification of Tulsi Leaves Based on Texture Analysis

[10] Stephen Gang Wu, Forrest Sheng Bao, Eric You Xu, Yu Xuan Wang, Yi-Fan Chang and QiaoLiang Xiang, "A leaf Recognition Algorithm for Plant Classification Using Probabilistic Neural Network", In The 7th International Symposiumon Signal Processing and Information Technology,Cairo, Egypt,pp. 11-16, 2007, IEEE.

[11] R.Janani, A.Gopal,” Identification of selected medicinal plants leaf using Image Features and ANN", in proceedings International Conference on Electronic Systems, 2013.

[12] Pedro F. B. Silva, Andre R.S. Marcal and Rubim M. Almeidada S ilva,"Evaluation of Features for Leaf Discrimination", InImage Analysis and Recognition, Springer Lecture Notes in Computer Science, vol.Berlin Heidelberg.

[13] Vinita Tajane, Prof. N.J. Janwe, “Medicinal Plants Disease Identification Using Canny Edge Detection Algorithm, Histogram Analysis and CBIR” Volume 4, Issue 6, June 2014

[14] Abdul Kadir, Lukito Edi Nugroho, Adhi Susanto, Paulus Insap Santosa”Leaf Classification Using Shape, Color, and TextureFeatures” July to Aug Issue 2011

[15] Manojkumar P, Surya C. M, Varun P. Gopi ”Identification of Ayurvedic Medicinal Plants byImage Processing of Leaf Samples” November 2017

[16] https://www.youtube.com/watch?v=t3yHNZhSXLE

[17] https://www.kaggle.com/arshid/support-vector-machine-on-iris-flower-dataset

[18] https://archive.ics.uci.edu/ml/datasets.php

[19] http://programiz.com/

[20] https://www.kdnuggets.com/2017/12/robust-algorithms-machine-learning.html

Automatic Guided Vehicle for Hospital Application

Anaswara Raj
Department of Computer Science and Engineering,
Sree Buddha College of Engineering, Pattoor
Alappuzha, Kerala, India - 690529
Email: anaswararaj9898@gmail.com

Rinchu T S
Department of Computer Science and Engineering,
Sree Buddha College of Engineering, Pattoor,
Alappuzha, Kerala, India - 690529
Email: rinchurinchu05@gmail.com

Reshma A S
Department of Computer Science and Engineering,
Sree Buddha College of Engineering, Pattoor
Alappuzha, Kerala, India - 690529
Email: reshmarptpm@gmail.com

Sidharth S Nair
Department of Computer Science and Engineering,
Sree Buddha College of Engineering, Pattoor
Alappuzha, Kerala, India - 690529
Email: sidharthmidas07@gmail.com

Arun P S
Assistant Professor
Department of Computer Science and Engineering,
Sree Buddha College of Engineering, Pattoor
Alappuzha, Kerala, India - 690529
Email: arunpstec@gmail.com

***Abstract*——The IoT and robotics communities are coming together to create The Internet of Robotic Things (IoRT). The IoT is a network of things that are connected to the internet, including IoT devices and IoT-enabled physical assets ranging from consumer devices to sensor-equipped connected technology. With the advancements of robotic technologies, the medical environments are adopting more and more aspects of automation to enhance the services in hospitals. In pandemic conditions such as COVID 19, direct contact with patients may result in the spreading of disease. Hence the health community finds difficulty in distributing medicines. Here we are going to specify the design and development of an automatic guided vehicle for hospital applications, which can be controlled remotely.It has infrared sensors at the bottom for path identification and an ultrasonic sensor held in front of the vehicle for obstacle detection. It collects medicines from the nurse's station and follows the path provided to reach the supply point, which is the patient's bed. The sensors provided will detect the bed and opens the corresponding box of medicine. In addition to this, it helps in real-time monitoring of patient's parameters such as temperature, pulse rate, etc. and sends information to the doctor through the internet.**

***Keywords*—Arduino Microcontroller, robotics, sensors**

I. Introduction

Technology is evolving day by day. As the population increases, the need for automation in the health care sector is essential. Hence hospitals adopt novel ways to increase productivity and efficiency without investing more in human resources. On handling pandemic conditions such as COVID 19, the lives of health workers are in grave danger. Nurses and associated workers in the hospital are in fear of getting diseases while working in isolation wards. Therefore the development of an automatic guided vehicle (AGV) is important for doing hospital functions like the supply of medicines, patient monitoring, and waste management. The noticeable development in the field of power electronic converters and electric drives enhances the growth of AGV. With the advancements of robotic technologies, the medical environments are adopting more and more aspects of automation to enhance the services in hospitals. In pandemic conditions such as COVID 19, direct contact with patients may result in the spreading of disease. Hence the health community finds difficulty in distributing medicines and disposal of waste. Many hospitals already adopted some methods for automation, such as conveyors for moving medicines from one place to another. But the automatic guided vehicle is a more reliable system that can be adopted over other automation systems. By using advanced technologies in locomotion and interfaces which ease the handling of the vehicle leads to transplant AGV, which is familiar in the manufacturing sector to hospital environments. This prototype includes an automatic guided vehicle for carrying medicines, real-time monitoring of patient's parameters such as temperature, pulse rate, etc. and sends information to the doctor through the internet, automatic sanitizer, mask disposal and waste management. It helps in cost reduction, better efficiency, proper waste disposal, and reduction of time. Now the hospital is becoming a 4.0 facility, hence the automatic guided vehicle will performing a frequently important part to guarantee excellent performance

II. RELATED WORKS

The research paper ”Automated Guided Vehicle Design Methodology - A Review” is focused on design method in the AGV. Material handling is a key task and a non-value added an activity for the growth of a company. In order to make material handling smoother and stable, use a fully automated guided vehicle (AGV) as it reduces the human efforts, improve the customer services as well as increase the efficiency and the productivity along with the reduction in time. AGV design methods, monitoring, Controlling along with focus on the different design methodology used for AGV designing. Material handling is nothing but moving materials within short distances in a storage area. AGV is the effective and the best option for material handling. AGV automated guided vehicle is a smart vehicle designed and built with lots of features used in industrial application for transportation purpose, delivering the raw material, it is also known as a system without driver. Because of their user friendly nature and affordable price AGV are becoming more popular. Industries currently using AGVs are manufacturing, automotive, warehouses, hospitals, chemical industries, and assembly line for different applica- tions. AGV consists of lots of subsystems such as navigation system, drive system, control system, safety system, hooking system, traffic management system, communication system. Most important and part of AGV is the navigation method which shows movement of AGV around provided place and it also shows the exact position of the automated vehicle. There is lots of navigation system available, previously navigation was done on the magnetic tape, color, spot, and wire but now days with development in technology using optical, laser or natural navigation is increased. AGV are said to be intelligent transportation as it deliver the material at right place within right time. It does not have any adverse effect on environment and safe to use. Natural navigation focus on using a laser navigation sensor to in deep lanes, etc. It is mainly used for trailers loading and unloading. This way, the trailers need not to be changed to allow the vehicles to navigate within them.

The article ”Implementation of Automated Guided Vehicle System in Healthcare Facility” deals with the use of automated guided vehicle (AGV) system in the hospital. Automatic Guided Vehicles (AGV) or self-guided vehicles (SGV), have been widely used in material handling for decades. In these days, the demand for mobile robots and their use in hospitals has increased due to changes in demographic trends and medical cost control. For healthcare facilities, these automated systems are designed specifically for handling bulk material, pharmacy medicines, laboratories samples, central supply and transportation of food, dirty dishes, bed laundry, waste (biological, recyclable), biomedical instruments etc. Operating efficiency is gained by automating these supplies, which allows the transfer of human resources to other departments or activities. Automated systems are working 24 hours a day, 7 days a week. Automated solution can streamline traffic flow of material in the hospital, control costs, reduce workload. Hospital operating installation have to fulfil some important requirements, such as Safety and clinical quality, Effective technology utilization, information and patient management etc. These requirements and the use of modern logistics systems significantly affects the operation of the entire facility and its economy, improves the quality of patient care and increases their safety. In the case study, they designed AGV cart and transport methods for inpatient ward of healthcare facility. The economic assessment then pointed out that the AGV technology is currently not cheap and is affordable only for bigger facilities managing in profit. Proper and effective implementation for a given type of healthcare facility depends on many factors and requires a detailed assessment and analysis. AGV is also a technology, which potential is high but its specific application must be analysed through several methods of industrial engineering (e.g. simulation). Since many healthcare facilities are deterred particularly by high acquisition costs of this technology, healthcare managers need to realize that the purpose of the new, modern technology is mainly to help healthcare professionals to work more efficiently and improve the quality of healthcare services. If our healthcare facilities want to respond to technology- driven environment of care and be prepared for the future development, the designers must not only design healthcare facilities as a buildings. They need to meet the requirements of patients and staff, and must predict the future.

The paper ”Automated Guided Vehicle using Robot Operating System” focuses on proof of concept prototype modelling and development of fully autonomous guided robot using embedded controller integrated with GUI Robotic operating systems, which can be used to carry goods and materials at industry, hotels and so many environment. Most of the industries as small, medium, and large scale accepted automated guided vehicle (AGV) to shift raw material and finished goods from one place to another. But still most of the AGVs are not fully automatic. It needs operators to operate AGV for specific task like guiding it by using various wireless protocols like Bluetooth, wireless network, RFID. Some of the AGVs are line follower which take feedback from line as a path using various sensors like magnetic sensor, IR sensor, color sensor or laser sensor sometimes AGVs path is predefined in software, fixed line path. Disadvantage of earlier work in AGVs have cannot work in poor light and without user. So to overcome these both problem this paper presenting proof of concept proptype modelling of an design the fully automated control system for AGV. System consist of Arduino Mega board, mic, speaker and Kinect sensor is interfaced with PC. The PC has operating system Ubuntu 16.04.04 and Robot Operating System(ROS) running on it. It receives the data from Kinect and converts it into the equivalent laser sensor data. This 3D data capture from Kinect is used to map the environment using SLAM. Voice command is used for communication purpose with user and robot. The speed commands generated in ROS nodes are sends to Arduino. Arduino Mega process on it and send appropriate PWM values to the motor driver. This project proposed voice command system using audio format work command and implemented in real environments. Vision based sensor to map the total environment and for path planning purpose advanced IMU sensor Oblu is used. Oblu gives the 98percent accurate reading of velocity, distance and angle by which the path planning accuracy gets high. ROS is middleware which collects software frameworks for robot software development. It is not an operating system, it just provide computer cluster like hardware abstraction, device control, convey message between the process and packet management. It creates note which multiplex sensors, actuators, controls and other messages. ROS is under open source licensed. There are many ROS are available but we used Kinetic Kame ROS. In this study model for navigation purpose Kinect sensor is used and for accurate path Oblu sensor is used. Oblu gives 98percent accurate speed so the maximum accuracy is achieved. The average location error is 2.85 cm. We adopted hybrid algorithm. AGV works smoothly in indoor and obstacles are avoided successfully

III. PROPOSED METHOD

The primary aim of the vehicle is to supply medicines to the patients and monitor their body parameters such as temperature. A control app that is used to communicate between vehicle and nurse. The nurse has to select the mode of travel after placing medicines on the box. Once the control signal is given, robot checks for an obstacle in front of the vehicle. If no obstacle is found robot starts its navigation through the black path which is directed by the IR transmitter and receiver signals. When the vehicle reaches near the patient's bed a proximity sensor gets activated sending signals to stop the vehicle. The patient can take the medicine from the box with the help of bystanders. LED display indicates the directions to tie the temperature sensor band. It has an LM35 sensor. The measured temperature will be displayed on the led screen and it also gets sent to the concerned doctor through the internet.

A. Hardware Module

The Hardware modules used here are : (1) Arduino Mega: The Board used here is Arduino Mega which contains Atmega 2560 as it's Micro controller. (2)Ultrasonic Sensor for Automatic Sanitizer Dispenser: Whenever the hand is shown to ultrasonic sensor a servo motor interfaced to it will rotate and sanitizer dispenses. (3) Pulse Rate Sensor for Pulse Rate Monitoring: The pulse rate sensor is used to measure the pulse rate of human and it is given to Android App using ESP8266 Module. (4) MLX90614 Temperature Sensor for Temperature Monitoring: Non Contact temperature measurement using MLX90614 Sensor.

B. Navigation Module

An ultrasonic sensor is placed in front of the vehicle to avoid collision with other objects. L293d is used as the motor driver it can drive the dc motor used for navigation in either direction. Left data in pins will control the motor attached at the left-hand side and, pins on the right-hand side are employed for the motor on the right. The motors are operated based on the information rendered through the input pins such as LOGIC LOW or LOGIC HIGH. The line follower mechanism is employed using Infrared sensors. It has an Emitter, which is an Infrared light-emitting diode and, the detector is an Infrared photodiode placed in the vehicle. Based on the received infrared light, resistance of photodiode and output voltage changes. The light from the infrared LED hits the non-transparent facade, gets collected by the sensors , which recognize the tint of the facade beneath it. It transmits a signal to the microcontroller or the central circuit, which then makes a judgment according to the algorithm established in programming. The infrared beam gets reflected and received from the dark path surrounded by the light tint surface. Black color will absorb the beam falling on it completely. The crucial element of our work was programming. The initial part of the code is to control the movement of the vehicle to the front, back, left, and right. The microcontroller drives high or low to motor driver according to data inputs from sensors. The motor driver IC controls the motors according to the information from the controller. There are three cases of movement:

- Case 1: AGV will start its movement in forward direction when both motors are turned on at the same time.
- Case 2: The AGV will move to the left when the right motor is turned on, and the left motor is turned off.
- Case 3: The AGV will move to the right when the left motor is turned on, and the right motor is turned off.

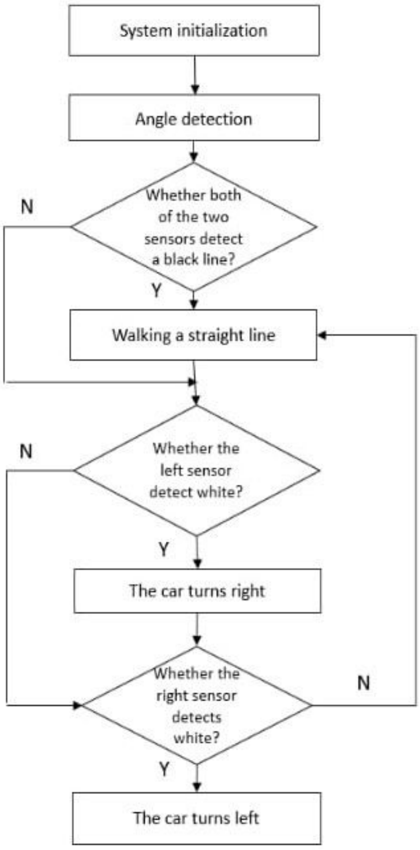

System initialization
Angle detection
Whether both of the two sensors detect a black line?
N
Y
Walking a straight line
Whether the left sensor detect white?
N
Y
The car turns right
Whether the right sensor detects white?
N
Y
The car turns left

Fig. 1. Flow chart for Navigation.

C. Communication Module

An Android app was developed for monitoring patient data and controlling the movement of the vehicle. The communication between AGV and android app is via Bluetooth. The Bluetooth module used in AGV is HC05. It consist of various sensors such as ultrasonic sensors and infrared sensors for obstacle detection and path finding. According to the response from the sensors provided, command is generated and is given to the motor driver, here represented by vehicle controller and motor controller block. According to the input received by motor driver, the motor is powered. It also consist of battery, a display which gives various instructions like those given to patients while temperature sensing and also displays the measured temperature. It has two modes of operation, medicine supply mode and waste collection mode. All are connected to the micro controller.

It consist of various sensors such as ultrasonic sensors and infrared sensors for obstacle detection and path finding. According to the response from the sensors provided, command is generated and is given to the motor driver, here represented by vehicle controller and motor controller block. According to the input received by motor driver, the motor is powered. It also consist of battery, a display which gives various instructions like those given to patients while temperature sensing and also displays the measured temperature. It has two modes of operation, medicine supply mode and waste collection mode. All are connected to the microcontroller. Once the control signal is given, robot checks for an obstacle in front of the vehicle. If no obstacle is found robot starts its navigation through the black path which is directed by the IR transmitter and receiver signals. When the vehicle reaches near the patient's bed a proximity sensor gets activated sending signals to stop the vehicle. The patient can take the medicine from the box with the help of bystanders.

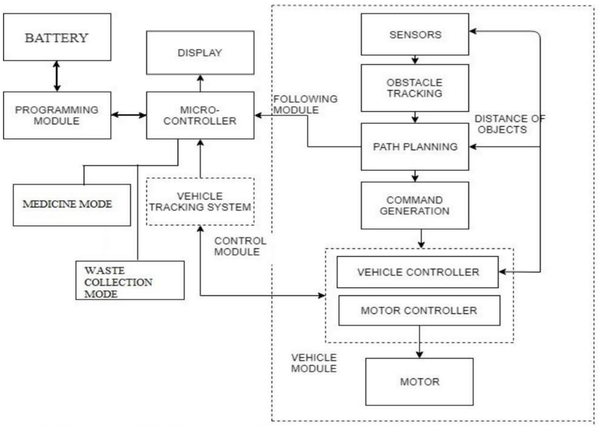


Fig. 2. Block Diagram of Prototype of AGV for Hospitals.

Conclusion

This thesis has outlined the construction of an AGV designed for the distribution of medicines and disposal of waste in hospital environments. The AGV mainly does main five functions, medicine distribution, sensing of body temperature,pulse rate checking, automatic hand sanitizer dispenser and waste collection and disposal. It collects the medicines for different patients and follows the path provided. On reaching the supply point it supplies the medicine for that particular patient. By the use of a band provided, the body temperature of the patient is measured. Automatic Sanitizer Dispenser works as whenever the hand is shown to ultrasonic sensor a servo motor interfaced to it will rotate and sanitizer dispenses.It also collects waste from specially designed baskets kept at the passages and properly dumps the waste at a predefined place. This prototype can be used in pandemic conditions for the treatment of affected people. Therefore AGV reduces spread of COVID 19 by avoid direct contact with the people. The prototype built is lightweight and designed for a single bed. In the future, a step climbing facility can be employed to the bots to improve the application range of the product.

References

[1] X. Cheng and R. Tao, ”Design of Automatic Guided Vehicles and Dunking Robot System,” 2011 Third International Conference on Intelligent Human-Machine Systems and Cybernetics, Zhejiang, 2011, pp. 3-6

[2] T. Said, S. ”Real-time multi-object detection and tracking for autonomous robots in uncontrolled environments,” in 2012 Seventh International Conference on Computer Engineering Systems (ICCES), 2012, pp. 67-72.v

[3] F. Rios, R. A. Flores and V. Soloiu, ”Design of an Intelligent Vehicle for Industrial, Office and Home Environments Applications,” SoutheastCon 2018, St. Petersburg, FL, 2018, pp. 1-3

[4] D. Plinta, M. Krajčovič, Production system designing with the use of digital factory and augmented reality technologies, in: Advances in Intelligent Systems and Computing, vol. 350 (2016), ISSN 2194-5357, pp. 187-196.

[5] J. Evans, B. Krishnamurthy, B. Barrows, T. Skewis, and V. Lumelsky, “Handling real-world motion planning: A hospital transport robot,” IEEE Control Syst., vol. 12, no. 1, pp. 15–19, Feb. 1992.

[6] Risang Gatot Yudanto, Frederik Petré, Flanders Make ”Sensor Fusion for Indoor Navigation and Tracking of Automated Guided Vehicles” 2015 International Conference on Indoor Positioning and Indoor Navigation (IPIN), 13-16 October 2015, Banff, Alberta, Canada

Social Distance Monitoring

Swathi R
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha,Kerala,India
swathirajeev19@gmail.com

Milan Varghese George
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha,Kerala,India
m4mamba@gmail.com

Reenu Rachel Thomas
Computer Science and Engineering
Sree Buddha College of Engineering
Alappuzha,Kerala,India
reenurachelthomas@gmail.com

Abstract—**The year 2020 witnessed the outbreak of Covid 19 pandemic and the world is still battling with it. Social distancing is one of the effective measures to prevent the transmission of virus from person to person. This work provides a method to detect any social distancing violation among people by making use of deep learning and image processing techniques. YoloV4 object recognition model is used to detect humans in video sequences. Coordinates of each person's point of contact with the ground are obtained in terms of pixels. These are converted to ground coordinates. Then the Euclidean distance from the point of contact of a person with the ground to another person's point of contact with the ground is calculated. If this distance turns out to be less than the threshold distance, then alerts or warnings can be issued to authorities.**

I. Introduction

The COVID-19 pandemic is an ongoing global pandemic of coronavirus disease 2019 (COVID-19) caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). The first case was reported in Wuhan, China in December 2019. The World Health Organization declared it as a pandemic on 11 March 2020. As of 1 June 2021, more than 170 million cases have been confirmed, and more than 3.55 million Covid 19 related deaths have been reported[1]. Though vaccines have been invented, it might take a long time to vaccinate the entire world population. In such a situation it is necessary to control the spread of the virus. When an infected person coughs, sneezes, or talks, droplets or tiny particles called aerosols carry the virus into the air from their nose or mouth[2]. Anyone who is within 6 feet of that person can breathe it into their lungs. One best practice known in stopping the spread of Covid-19 is by implementing social distancing between people with at least one metre away. But to monitor each and every public place in person is a difficult task for authorities and in their absence people may violate the social distance criteria. To ease the work of authorities, this work proposes a method in which the video footage from surveillance cameras in public places can be processed to detect humans in the field of view of camera and calculate the distance between them. If this distance is less than 1 metre, then authorities can be alerted about the violation.

II. BACKGROUND STUDY

YOLO stands for You Only Look Once. YOLOv4 is an upgraded version from YOLOv3. It is the very famous real-time Object Recognition technology that is capable of recognizing multiple objects in a single frame. YOLOv4 is found to be much efficient that it can achieve 43.5% Average Precision(AP)/ 65.7% AP50 accuracy in accordance with the Microsoft COCO test and is at the fastest speed of 62 Frames Per Second (FPS) Titan V or 34 FPS RTX 2070. YoloV4 is faster than other existing competing object recognition models [3]. Its Average Precision(AP) is 10% more than the available models and Frames Per Second(FPS) is 12% than the YOLOv3 [3].

III. PROPOSED SYSTEM

To find the distance between people in terms of metres, any four points on the ground in the field of view of the camera are taken, say A, B, C, D. One of these four points, say A, is taken as origin on the ground and with respect to this origin the coordinates of the other three points are calculated by measuring their actual distance from the origin i.e., A. Also the coordinates of these four points in the image plane are obtained in terms of pixel. Now using the pixel coordinates and their corresponding ground coordinates, homography matrix H is obtained. Video sequence is read frame by frame. Each frame is then given as input to YoloV4 object detection model. If the label of detection is 'person' then the bounding box around that detection is obtained and the lowermost point of the bounding box is found out in terms of pixels say (x', y'). Now these coordinates can be converted to ground coordinates (x, y) by using the following mapping.

$$\begin{bmatrix} x \\ y \\ 1 \end{bmatrix} \sim H \begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix}$$

where (x,y) represent ground coordinates, (x', y') represent pixel coordinates and H is the homography matrix[4]. Once each person's ground coordinates are obtained, we can calculate the Euclidean distance between them by using following equation.

$$\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}$$

where (x_{1},y_1) are ground coordinates of person 1 and (x_{2},y_2) are ground coordinates of person 2. If this distance turns out to be less than 1 metre then authorities can be alerted.

IV. RESULT

Following are the results obtained by processing a self-taken images.

TABLE I RESULTS OBTAINED FROM SELF TAKEN VIDEO

Test	Actual Distance (metre)	Calculated Distance (metre)
Test1	1	0.96410197
Test2	1.5	1.3974082
Test3	2	2.1104538
Test4	2.5	2.5578268
Test5	3	3.0040722
Test6	3.5	3.6036472

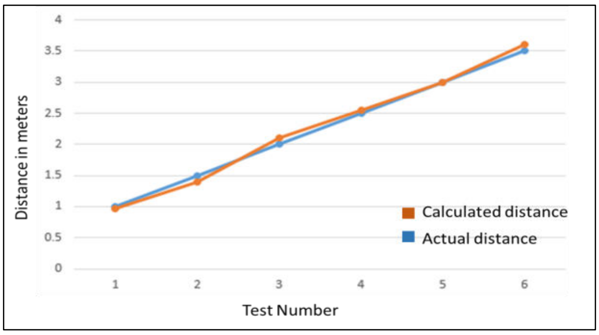


Fig. 1. Calculated distance and measured distance

The images were captured in a controlled atmosphere with two people standing at some distance from each other. Six such images were taken with different distance between the two people. Table 1 shows the result obtained in each test. Fig.1 is a graph indicating the comparison between the actual distance between the two people and the distance calculated by the proposed model.

V. CONCLUSION

The proposed work can assist authorities in monitoring and ensuring social distancing among people in public places. Further improvements can be made in this work like detecting and tracking the people who have violated social distance using face recognition methods.

REFERENCES

[1] https://en.wikipedia.org/wiki/COVID-19

[2] https://www.webmd.com/lung/coronavirus-transmission-overview#1

[3] https://www.techleer.com/articles/625-yolov4-optimal-speed-and-accuracy-of-object-detection/

[4] https://zbigatron.com/mapping-camera-coordinates-to-a-2d-floor-plan/

R-NAS-Unet Architecture for Semantic Image Segmentation

Neethu John, *Department of Computer Science, Sree Buddha College of Engineering, Kerala, India*
Prof. Gopu Darsan*, Asst. Professor, Department of Computer Science, Sree Buddha College of Engineering, Kerala, India*

***ABSTRACT* - Medical image analysis is the first step in analyzing medical images, which helps to make images more in-built and expands diagnostic competence. Medical image segmentation is a serious step in the field of medical image analysis. In order to deliver a reliable basis for clinical diagnosis and pathology research, and support doctor to make a more accurate diagnosis, it need to segment the parts of medical images, we focus and extract relevant features. Neural architecture search (NAS) has substantial progress in improving the accuracy of image classification. To outspread NAS to image segmentation which shows initial viability. The U-net architecture successfully applied to various medical image segmentation. In this paper we propose a lesion segmentation by enhancing the tradition UNET by adding the recurrency to it merge layers. So, a deeply connected convolutional UNet takes full advantage of Bi directional LSTM, which can improve model performance on sequence classification problems and deep convolution layers of UNet. The proposed system combines features of the corresponding encoding path and previous up convolutional layer in a nonlinear way. To get a strong feature extraction system we use a densely connected convolutions in final layers. We accelerate the convergence speed of the system by adding batch normalization into it.**

Keywords – Medical image segmentation, convolutional neural architecture search, deep learning

I. Introduction

Medical image segmentation has an essential role in computer-aided diagnosis systems in different applications. The huge investment and development of medical imaging modes such as X-ray, ultrasound, computed tomography (CT) and magnetic resonance imaging (MRI), attract researchers to implement new medical image-processing algorithms. MRI is the most commonly used technique in the field of radio imaging. An MRI may produce different statistics compared with CT. In deep learning, image segmentation generally denotes semantic segmentation, which refers to the recognition of images at the pixel level. The most successful type of deep learning models for image analysis to date are convolutional neural networks (CNN). It is the most commonly used neural network in the field of computer vision which is proposed to solve image classification problem. CNN can be used to classify each pixel in the image individually, by presenting it with patches extracted around the particular pixel and produce a multichannel likelihood map of the same size as input image.

Fully Convolutional Networks (FCNs) is one of several methods proposed to prevent this decrease in resolution. FCNs can accept any size of input. U-net consists of convolutional layers, down-sampling layers and up-sampling layers. The convolutional neural network, U-Net was established for biomedical image segmentation. It can able to do image localization by predicting the image pixel by pixel. U-net practices the skip connection operation to attach each couple of down-sampling layer and the up-sampling layer, which makes the spatial evidence directly applied to much deeper layers and a more precise segmentation result. The focus of current convolutional neural network has moved to NAS. It's a subfield of AutoML (Auto Machine Learning) and has significant overlap with hyper-parameter optimization and meta learning. The present research on NAS focuses on three aspects: search space, search strategy and performance estimation strategy. The search space outlines which architectures can be signified in principle. The search strategy specifics how to discover the search space. The objective of NAS is to bargain architectures that have high appraised performance on unseen data. Even though NAS has countless potential in the field of computer vision, the real potential depends on that can be stretched to deal with visual errands other than image classification. Encouraged by the accomplishment of U-net and its variants in medical image segmentation, we use a U-like architecture as our backbone network. We get our architecture denoted as R-NAS-Unet. This reveals that NasUnets are more efficient in the parameters usage and get a much better performance than U-Net in all types of medical image dataset. This is the primary shot to apply NAS to medical image segmentation. We propose different primitive operation sets on U-Like backbone network for searching. The performance of NAS-Unet outperforms U-Net in all types of medical image segmentation datasets we evaluated.

NAS has mostly solved image classification responsibilities since it was proposed. The depth wise-separable convolution operation will be introduced since it will dramatically reduce network parameters without sacrificing network performance. In CNN architecture, the features we generate for all channels are directly combined evenly. The squeeze-and-excitation process overpowers some superfluous structures and improves useful features by assigning weights to feature channels. To solve the problem of image segmentation, different from image classification tasks, the architecture with image segmentation needs high-resolution input. To evaluate the performance of NAS-Unet, we use three types of medical image datasets MRI, CT, and ultrasound.

II. LITERATURE REVIEW

A neural network that has one or more convolutional layers and are used mainly for image processing, classification, segmentation is a CNN. It is mostly sliding a filter over the effort. Relatively looking at a complete image at once to find certain features, it can be more effective to look at smaller portions of the image. There are quite typical tasks such as image segmentation and signal processing, for which CNNs fit at. CNN can also be executed as a U-Net architecture, which are fundamentally two almost mirrored CNNs resulting in a CNN whose architecture can be offered in a U shape. U-nets are used where the production needs to be of alike to the input such as segmentation and image improvement.

A. Neural networks have hastily grown popularity over the last few years due to their triumph in variety of tasks, such as image recognition and machine translation. These neural networks are designed by hand, which is an exhausting, time-consuming process. The vast number of possible configurations requires expert knowledge to restrict the search. A preliminary process that randomly constructs networks and trains them with SGDR. This simple baseline achieves 6%-7% test error on CIFAR-10[1], which already rivals several existing methods for NAS. Due to its easiness, the baseline offers a valuable starting point for the progress of more sophisticated methods in the future. NAS by Hill climbing (NASH), a simple iterative approach that, applies a set of alternative network morphisms to the current network. NASH inventions and trains viable architectures at a computational rate of the equivalent demand of magnitude as training a single network. After one day the error is reduced to almost 5%. Replicas from different phases of the algorithm can be united to attain an error of 4.7 % within two days on a solo GPU. On CIFAR-100,to achieve an error below 24% in one day and get close to 20% after two days. This method is easy to use and easy to extend, so it hopefully can serve as a basis for future work Experiments on CIFAR-10 and CIFAR-100 showed that this method yields competitive results while requiring considerably less computational resources than most alternative approaches. The algorithm is easily extendable, evolutionary approaches for generating new models, other methods for cheap performance evaluation. In this sense, this approach can serve as a basis for the development of more sophisticated methods that yield further improvements of performance.

B. Computed tomography (CT)[2] is an effective approach to diagnose disease, by which the doctor can intuitively examine a patient's body structure and efficiently analyze the possibility of illness. It is tough to recognize the images holding nodules, which should be analyzed for supporting early lung cancer diagnosis, from a large number of pulmonary CT images. CT is widely used to assist computer aided diagnosis (CAD) based on artificial intelligence (AI). A convolutional autoencoder for deep learning framework to support unsupervised image features learning for lung nodule through unlabeled data can be used, which only needs a small amount of labeled data for efficient feature learning. By the comprehensive experiments, the planned scheme is superior to other methods, which efficiently solves the intrinsic labor-intensive problem during artificial image labeling. The proposed convolutional autoencoder method can be stretched for similarity dimension of lung nodules images. The training in CANN is based on the work including unsupervised training and supervised fine-tunning. The two datasets that is included are the unlabeled and the labeled dataset. An autoencoder technique for unsupervised learning, can abstract output data to rebuild input data and compare it with original input data. After frequent iterations, the value of cost function ranges its optimality, which means that the renovated input data is able to approximate the original input data to a supreme extent. The approach based on segmentation and hand-craft-features is time consuming and labor-intensive, while the data driven approach is available to avoid the loss of important information in nodule segmentation. CANN-based method for data-driven feature knowledge, is functional for lung nodule recognition, classification and similarity check, which suggestively resolves the issues of time consuming for ROI labeling and inadequate labeled data. Compared with other data-driven approaches, it verifies that this method is superior through comprehensive experiments. Moreover, it proves that the system performance and feasibility may be affected by the quality of data, because the role of expert is ignored.

C. The network extends u-net architecture by replacing all 2D processes with 3D counterparts. The implementation performs on-the-fly elastic deformations for efficient data augmentation during training. It is trained end-to-end from scratch. The standard u-net[3], it has an analysis and a synthesis path each with four resolution steps. In the analysis path, each layer contains two 3×3×3 convolutions each followed by a rectified linear unit, and then a 2×2×2 max pooling with strides of two in each dimension. In the synthesis path, each layer consists of an up convolution of 2×2×2 by strides of two in each dimension, followed by two 3×3×3 convolutions each followed by a rectified linear unit. Shortcut connections from layers of equal resolution in the analysis path provide the essential high-resolution features to the synthesis path. To avoid bottlenecks by doubling the number of channels before max pooling and also adopt this scheme in the synthesis path. The input to the network is a 132×132×116 voxel tile of the image with 3 channels. The output in the final layer is 44×44×28 voxels in x, y, and z directions respectively. We also introduce batch normalization. Each batch is normalized during training with its mean and standard deviation and global statistics are updated using these values. This is followed by a layer to learn scale and bias explicitly. At test time, normalization is done via these computed global statistics and the learned scale and bias. The important part of the architecture, which allows us to train on sparse annotations, is the weighted SoftMax loss function. Setting the weights of unlabeled pixels to zero makes it possible to learn from only the labelled ones and, to generalize to the whole volume. An end-to-end learning method that semi-automatically and fully-automatically segments a 3D volume from a sparse annotation. It offers an accurate segmentation for the highly variable structures of the Xenopus kidney. We achieve an average IoU of 0.863 in 3-fold cross validation experiments for the semi-automated setup. In a fully-automated setup we demonstrate the performance gain of the 3D architecture to an equivalent 2D implementation. It is not optimized in any way for this application. We expect that it will be applicable to many other biomedical volumetric segmentation tasks.

D. Semantic segmentation is an active area of research in medical image analysis. With the introduction of CNN, significant improvements in performance have been achieved in many standard datasets. While CNNs are typically realized by a contracting path built from convolutional, pooling and fully connected layers, FCN[4] adds an expanding path built with deconvolutional or un-pooling layers. The expanding path recovers spatial information by merging features skipped from the various resolution levels on the contracting path. In standard FCNs, only long skip connections are used to skip features from the contracting path to the expanding path in order to recover spatial information lost during down sampling. Extend FCNs by adding short skip connections, that are similar to the ones introduced in residual networks, in order to build very deep FCNs. A review of the gradient flow confirms that for a very deep FCN it is beneficial to have both long and short skip connections. Consider three types of blocks, each containing at least one convolution and activation function: bottleneck, basic block and simple block. Each block is capable of performing batch normalization on its inputs as well as spatial down sampling at the input (marked blue; used for the contracting path) and spatial up-sampling at the output (marked yellow; for the expanding path). The bottleneck and basic block are based on those introduced in which include short skip connections to skip the block input to its output with minimal modification, encouraging the path through the non-linearities to learn a residual representation of the input data. To minimize the modification of the input, apply no transformations along the short skip connections, except when the number of filters needs to be adjusted to match the block output. Use 1x1 convolutions to adjust the number of filters but for spatial adjustment rely on simple decimation of the input so as not to increase the number of parameters. The influence of skip connections on FCN for biomedical image segmentation showed that a very deep network can achieve results near the state of the art on the EM dataset without any further post-processing and confirmed that although long skip connections provide a shortcut for gradient flow in shallow layers, they do not alleviate the vanishing gradient problem in deep networks. Consequently, apply short skip connections to FCNs and confirm that this increases convergence speed and allows training of very deep networks.

III. PROPOSED SYSTEM

By taking inspiration from Nas UNet LSTM (recurrent neural network) we propose a R-NAS-UNet are shown in the figure(fig 1 and fig 2).

A convolution layer is abbreviated as \Conv". Its explanation contains three portions: number of channels; kernel spatial extent (kernel size); padding (`p') and stride (`st') size. A pooling layer is abbreviated as \Pool". Only max pooling is used here. The pooling kernel size is permanently 2 × 2 and the stride is permanently 2. A fully connected layer is abbreviated as \FC". Fully connected layers are implemented using convolution. Its size is in the format n1× n2, where n1 is the size of the input, and n2 is the size of the output. The convolution layers among the two pooling layers have the identical number of channels, kernel size and stride. In fact, stacking two 3×3 convolution layers are equivalent to one 5×5 convolution layer; and stacking three 3×3 convolution kernels replace a 7 × 7 convolution layer. Stacking a few (2 or 3) smaller convolution kernels, however, computes faster than a large convolution kernel. In addition, the number of parameters is also condensed.

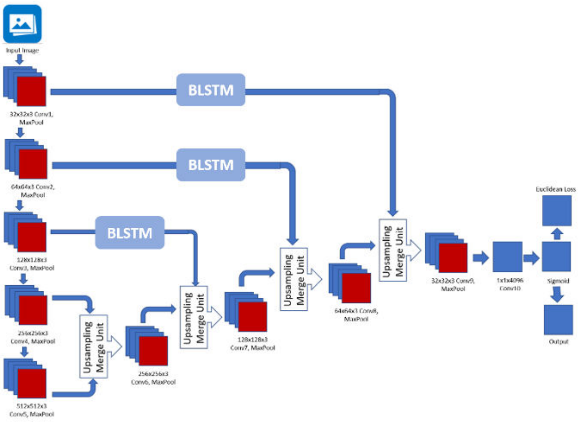


Fig 1 R-Nas-UNet

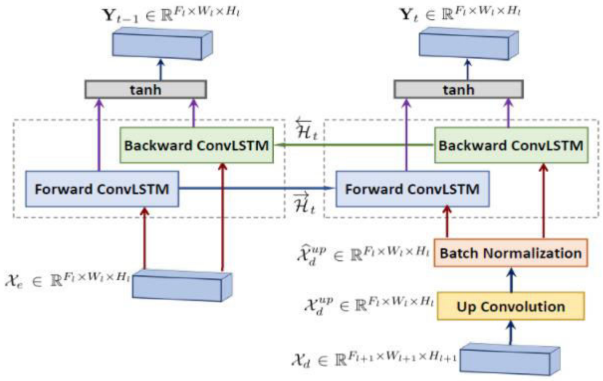

$\mathbf{Y}_{t-1} \in \mathbb{R}^{F_l \times W_l \times H_l}$
$\mathbf{Y}_t \in \mathbb{R}^{F_l \times W_l \times H_l}$
tanh
tanh
$\overleftarrow{\mathcal{H}}_t$
Backward ConvLSTM
Backward ConvLSTM
Forward ConvLSTM
Forward ConvLSTM
$\overrightarrow{\mathcal{H}}_t$
$\widehat{\mathcal{X}}_d^{up} \in \mathbb{R}^{F_l \times W_l \times H_l}$
Batch Normalization
$\mathcal{X}_e \in \mathbb{R}^{F_l \times W_l \times H_l}$
$\mathcal{X}_d^{up} \in \mathbb{R}^{F_l \times W_l \times H_l}$
Up Convolution
$\mathcal{X}_d \in \mathbb{R}^{F_{l+1} \times W_{l+1} \times H_{l+1}}$

Fig 2 Recurrent Neural Network

Proposes a lesion segmentation by enhancing the tradition UNET by adding the recurrency to it merge layers. So, a deeply connected convolutional UNet takes full advantage of Bi directional LSTM and deep convolution layers of UNet. The proposed system combines features of the corresponding encoding path and previous up convolutional layer in a nonlinear way. To get a strong feature extraction system we use a densely connected convolutions in final layers. We accelerate the convergence speed of the system by adding batch normalization into it.

In a convolution layer, numerous convolution kernels are generally used. Assuming D kernels are used and individually kernel is of spatial span H × W, we represent all the kernels as f. f is an order 4 tensor in $\mathbb{R}^{H\times w\times D^{l}\times D}$. Similarly, we use index variables $0 \leq i < H$, $0 \leq j < W$, $0 \leq d^{l} < D^{l}$ and $0 \leq d < D$ to pinpoint a specific element in the kernels. Likewise, the set of kernels f denotes to the same object as the notation w^{l}. It is also clear that even if the mini-batch approach is used, the kernels continue unchanged. One more benefit of the convolution layer is that all spatial locations share the same convolution kernel, which greatly reduces the number of parameters needed for a convolution layer. In a deep neural network setup, convolution also encourages parameter sharing. The combination of convolution kernels and deep and hierarchical structures are very effective in learning good representations (features) from images for visual recognition tasks.

A. ENCODING PATH

The contracting path of R-Nas-Unet includes 4 steps. Each pace contains two convolutional 3×3 filters followed by a 2×2 max pooling function and ReLU. The amount of feature maps is doubled at each stage. The contracting path abstracts increasingly image representations and rises the dimension of these representations layer by layer. Ultimately the final layer in the encoding path produces a high dimensional image representations with high semantic information. The original Unet contains a sequence of convolutional layers in the last step of encoding path. Taking an order of convolutional layers in a network produces the method learn different kinds of features. However, the network might acquire redundant features in the succeeding convolutions. To moderate this problem, densely linked convolutions are proposed. This supports the network to progress its performance by the impression of "collective knowledge" in which the feature maps are reclaimed through the network. It means feature maps learned from all previous convolutional layers are concatenated with the feature map learned from the current layer and they are forwarded to use as the input to the next convolution.

The knowledge of densely connected convolutions has some advantages over the consistent convolutions. First of all, it helps the network to learn a diverse set of feature maps instead of redundant features. Moreover, this idea improves the networks representational power by allowing information flow through the network and reusing features. Furthermore, dense connected convolutions can benefit from all the produced features before it, which prompt the network to avoid the risk of exploding por vanishing gradients. In addition, the gradients are directed to their particular places in the network more rapidly in the backward path. We employ the knowledge of densely connected convolutions in the future network. To do that, we familiarize one block as two successive convolutions. There is a sequence of N blocks in the last convolutional layer of the encoding path. These blocks are densely connected. We consider x_e^i as the output of the i^th convolutional block. The input of the i^th (i∈ {1,….,N}) convolutional block receives the concatenation of the feature maps of all preceding convolutional block as its input, ie, $[x_e^1, x_e^2, \cdots, x_e^{i-1}] \epsilon \mathbb{R}^{(i-1)F_l\times w_l\times H_l}$, and the output of the i^th block is $x_e^i \epsilon \mathbb{R}^{F_l\times w_l\times H_l}$. In the remaining part of the paper, we use simply X_e instead of X_e^N .

B. DECODING

Each step in the decoding path starts with performing an up-sampling function over the output of the previous layer. In the standard Unet, the corresponding feature maps in the contracting path are cropped and copied to the decoding path. These feature maps are then concatenated with the output of the up-sampling function. In RNAS Unet, we employ RNN to process these two kinds of feature maps in more complex way. Let $X_e \epsilon \mathbb{R}^{f_l\times w_l\times H_l}$ be the set of feature maps copied from the encoding path , and t $X_d \epsilon \mathbb{R}^{F_{l+1}\times w_{l+1}\times H_{l+1}}$be the set of feature maps from the previous convolutional layer, where F_i is number of feature maps at layer l, and $W_l \times H_l$ is the size of each feature map at layer l. It is worth mentioning that $F_{l+2} = 2*F_l$, $W_{l+1} =½ *W_l$, and $H_{l+1} = ½*H_l$. X_d is first passwd to an up-convolutional layer in which an up-sampling function followed by a 2 × 2 convolution are applied, doubling the size of each feature map and halving the number of feature channels, ie, producing $x_d^{up} \in \mathbb{R}^{f_l\times w_l\times H_l}$. In other words, the expanding path increases the size of the feature maps layer by layer to reach the original size of the input image after the final layer.

C. BATCH NORMALIZATION

After up-sampling, x_d^{up} goes through a BN function and produces $\hat{x}_d^{up}$. A problem in the intermediate layers in training steps is that the distribution of the activations varies. This problem makes the training procedure very slow since each layer in every training stage has to learn to familiarize themselves to a new distribution. BN is utilized to increase the stability of a neural network, which standardizes the inputs to a layer in the network by subtracting the batch mean and dividing by the batch standard deviation.

IV. CONCLUSION

The given deep recurrent conv net captures, more discriminative information which interns gives more accurate segmentation results. We were able to execute the system faster by utilizing batch normalization after every merging layer.

V. FUTURE WORK

We can improvise the precision of the segmentation result by refining the convolutional layers of the proposed system.

REFERENCES

[1] Ö. Çiçek, A. Abdulkadir, S. S. Lienkamp, T. Brox, and O. Ronneberger, ``3D U-net: Learning dense volumetric segmentation from sparse annotation,'' in Proc. Int. Conf. Med. Image Comput. Comput.-Assist. Intervent.(MICCAI), Oct. 2016, pp. 424432.

[2] M. Drozdzal, E. Vorontsov, G. Chartrand, S. Kadoury, and C. Pal, ``The importance of skip connections in biomedical image segmentation,'' in Deep Learning and

[3] Data Labeling for Medical Applications, G. Carneiro et al., Eds. Cham, Switzerland: Springer, 2016, pp. 179187.

[4] T. Elsken, J. H. Metzen, and F. Hutter ``Simple and efcient architecture search for convolutional neural networks," in Proc. Int. Conf. Learn. Represent. (ICLR), Jan. 2018, pp. 114.

[5] Chen, X. Shi, Y. Zhang, D. Wu, and M. Guizani, ``Deep features learning for medical image analysis with convolutional autoencoder neural network," IEEE Trans. Big Data, to be published.Science, 1989.

[6] G. Huang, Z. Liu, I.. Van Der Maaten, and K. Q. Weinberger. Densely connected Convolutional networks. In Proceedings of the IEEE conference on computer vision and patern recognition, pages 4700-4708,2017.

[7] S. Ioffe and C. Szegedy. Batch normalization: Accelerating deep network training by reducing internal covariate shift. pages 448-456.2015.

HaleHaven : An Advanced AI Phishing URL Detection System

Lekshmi Mohan
Dept. of CSE
Sree Buddha College of Engineering, Pattoor
Alappuzha, India
lekshmimohan1998@gmail.com

Amal P
Dept. of CSE
Sree Buddha College of Engineering, Pattoor
Alappuzha, India
worldofamal11@gmail.com

Arun P S
Assistant professor
Dept. of CSE
Sree Buddha College of Engineering, Pattoor
Alappuzha, India
arunpstec@gmail.com

***Abstract*—Different machine learning and deep learning-based approaches have been proposed for designing defensive mechanisms against various phishing attacks. Recently, researchers showed that phishing attacks can be performed by employing a deep neural network-based phishing URL generating system called DeepPhish. To prevent this kind of attack there is a detection system called Phish Haven to identify AI-generated as well as human-crafted phishing URLs. But the drawback of phish haven is that it is a voting-based system. Hence the accuracy of the output is very low. To overcome this, we have proposed an advanced AI phishing URL detection system called HaleHaven. It is based on Ensemble learning technique that uses 10 ML models. The primary objective of this is to build a fast and more efficient AI generated Phishing URL detection system along with human crafted phishing URLs, tiny URLs and Zero-Day Attacks. Analysis of our solution shows that it can always detect tiny URLs, and it can detect future AI-generated Phishing URLs based on our selected lexical features with very high accuracy.**

***Index Terms*—AI-generated phishing URLs, ensemble machine learning, human-crafted phishing URLs, lexical features, multi-threading, tiny URLs, URL HTML encoding**

I. Introduction

The distinctive characteristics of machine learning, ranging from detecting and extrapolating patterns to adapting a new environment, enable it to be a crucial part of technological systems like nuclear power plants monitoring, cyber and homeland security, computer vision, IoT etc. With the increasing demand of security, machine learning-based systems usually outperform traditional humans-based security monitoring systems[1]. Among a wide range of online threats and cyber-attacks, phishing is the most common one. Phishing attack is any fraudulent attempt that involves an activity of disguising oneself as a trustworthy party to obtain sensitive information. Phishing attacks can be of different types which include E-mail spoofing, website forging, social engineering, etc. One of the subtle yet deceiving methods to perform phishing attacks is phishing URLs[1]. Phishing URLs are types of URLs which are especially crafted by phishing attackers. Several researches have been conducted to prevent, mitigate and even to correct phishing attacks[2]. Majority of the researches are focused on using different machine learning models, deep learning models and/or the combinations of the models. There is a model named “DeepPhish” which is specially designed to generate AI phishing URLs. DeepPhish takes Simple Phishing URLs, i.e., human-crafted phishing URLs as its input and generates new phishing URLs. Majority of these newly generated phishing URLs, i.e., AI-generated Phishing URLs are capable enough to easily bypass existing prevalent phishing detection systems[3]. With this, the near future of cyber-attacks can be easily forecasted where AI will be used to carry out highly sophisticated malicious attacks, known as “Offensive AI”. PhishHaven is the only existing system that detects AI phishing URLs created by DeepPhish[4]. But the accuracy of PhishHaven is very low and there is a chance for false detection since it is based on unbiased voting. So, we are proposing an advanced AI phishing URL detection system called HaleHaven that has all the features of PhishHaven and additional features like detection of Zero-day attacks with very high accuracy.

II. Literature Survey

A. Phishing Detection from URLs Using Deep Learning Approach

Rapid developments of global networking and advanced technologies have made changes to our daily works. Social networking, cyber banking, cyber commerce, etc. are shifted to the information space. Although the Internet has various advantages some consequences present a serious security weakness. Consequently, the identification of a phishing or legitimate web page is a challenging issue due to its semantic structure. In this paper, a phishing detection system is implemented using deep learning techniques to prevent such attacks. The system works on URLs by applying a convolutional neural

ISBN: 978-93-5473-994-1

network (CNN) to detect the phishing webpage. In paper the proposed model has achieved 97.98 Percent accuracy whereas our proposed system achieved accuracy of 98.00 percent. This system doesn't require any feature engineering as the CNN extract features from the URLs automatically through its hidden layers.

B. An Automated Framework for Real-time Phishing URL Detection

An increasing number of services, including banking and social networking, are being integrated with world wide web in recent years. The crux of this increasing dependence on the internet is the rise of different kinds of cyberattacks on unsuspecting users. One such attack is phishing, which aims at stealing user information via deceptive websites. The primary defence against phishing consists of maintaining a black list of the phishing URLs. However, a black list approach is reactive and cannot defend against new phishing websites. For this reason, a number of researches have been done on using machine learning techniques to detect previously unseen phishing URLs. While they show promising results, any such implementation is yet to be seen. This is because 1) little work has been done on developing a complete end-to-end framework for phishing URL detection 2) it is prohibitively slow to detect phishing URLs using machine learning algorithms. In this work we address these two issues by formulating a robust framework for fast and automated detection of phishing URLs. We have validated our framework with a real dataset achieving 87 percent accuracy in a real-time setup.

C. Phish Haven- An Efficient Real-Time AI Phishing URLs Detection System

Among a wide range of online threats and cyber-attacks, phishing is the most common one. Phishing attack is any fraudulent attempt that involves an activity of disguising oneself as a trustworthy party to obtain sensitive information. Phishing attacks can be of different types which include E-mail spoofing, website forging, social engineering, etc. One of the subtle yet deceiving methods to perform phishing attacks is phishing URLs. The proposed system uses lexical features-based extraction and analysis techniques. To proactively detect and classify a URL on-the-fly, we additionally introduce URL HTML Encoding as a lexical feature. Phish Haven employs unbiased voting concept in decision-making process to assign final labels (i.e., either phishing or normal) to the URL(s). Although Phish Haven has achieved a significant accuracy in classifying both AI-generated and human-crafted phishing URLs, it has a limitation that it can detect only those AI-generated Phishing URLs which consist of lexical features and patterns similar to that of DeepPhish.

III. Proposed Solution: HaleHaven

We are proposing HaleHaven, an advanced AI phishing URL detection system. The primary objective of this system is detect AI generated Phishing URL along with human crafted phishing URLs, tiny URLs and Zero-Day Attacks fastly and efficiently with very high accuracy.

A. Preliminaries

To understand our proposed system we have to familiar with some preliminaries that explained below.

1) URL Hit: URL shortening is an approach that helps in shortening the expanded or lengthy URLs, which results in the formation of tiny URLs. With the motive of obtaining sensitive information such as passwords, personal credentials etc., phish attackers are now using tiny URL approach. Therefore, to detect tiny URLs efficiently, it is very important to understand how these tiny URLs work. The tiny URL works because of browser's redirect functionality. When a user clicks on a tiny URL or types a tiny (shortened) URL in the browser, the browser sends a HTTP request to the server directing it to fetch the requested page. After this the server sends a redirect requests. Following are some of them:
1) 301: Moved Permanently
2) 302: Found
3) 303: See Other
4) 304: Not Modified
5) 305: Use Proxy
6) 307: Temporary Redirect
Tiny URL is also one of the main characteristics of phishing URLs. Through these tiny URLs, attackers can easily hide paths of malicious pages or deploy a malicious piece of code. Therefore, detection of tiny URLs is also very essential. But the characteristics of tiny URLs make it difficult for the detection systems to detect those tiny URLs. It is incorporated into our detection system in a way that whenever a user types or paste a tiny URL in our Graphical user interface the URL is then hit by our system. Then we fetch the response of the respective hit URL of tiny URL in terms of an extended URL, i.e., it returns an actual URL.Then the Features Extractor component extracts features from actual URL.

2) Feature Extraction: There are two main categories of special characters used to create a full-fledged URL:
i) Reserved Characters: These include dollar sign, ampersand , plus (+), common (,), virgule (/), colon (:), semi-colon (;), equals sign (=), question mark (?), and at (@) symbol. All of them have various purposes and significant meanings when used in URLs.
ii) Unreserved Characters: These include space ( ), quotation marks (' '), less than(¡), greater than (¿), hash , percent, left curly brace (), right curly brace (), pipe (—), backslash, caret , tilde, left square bracket ([), right square bracket (]), and grave accent ('). They are also known as "Unsafe Characters". If these characters are not encoded properly within the URLs it can be easily misunderstood for various reasons.
Using URL HTML encoding we extract non-ASCII charcters also.

B. Methodology

For designing an advanced AI phishing URL detection system, we designed HaleHaven and classifies a URL using five subcomponents.First subcomponent, URL Hit which extracts extended URLs from tiny URLs. The second subcomponent is Features Extractor which extracts selected lexical features from the extended URLs. Then the third subcomponent, Modelics, which executes ten machine learning models in parallel and collects the classification results. The fourth subcomponent is second layer SVM that classifies the results that comes from the previous models more accurately. And lastly, Decision Maker subcomponent. It assigns a final class, i.e., phishing URL or normal URL

1) URL HIT: When a user enters a URL in the Graphical User Interface of our detection system HaleHaven, it is hit with the request response in terms of the entered URL. The respective Requested response may be a expanded URL if the entered URL is a tiny URL or the entered URL itself if it is a expanded URL. Then this response is passed to the next subcomponent.

2) Feature Extraction: The Feature Extractor divides the expanded URLs into their respective five parts, i.e., segment, netloc, path, query and fragment. This is followed by all the process of feautre extraction. Regular Expressions are used to extract all the different types of features and then these extracted features are passed to next subcomponent.

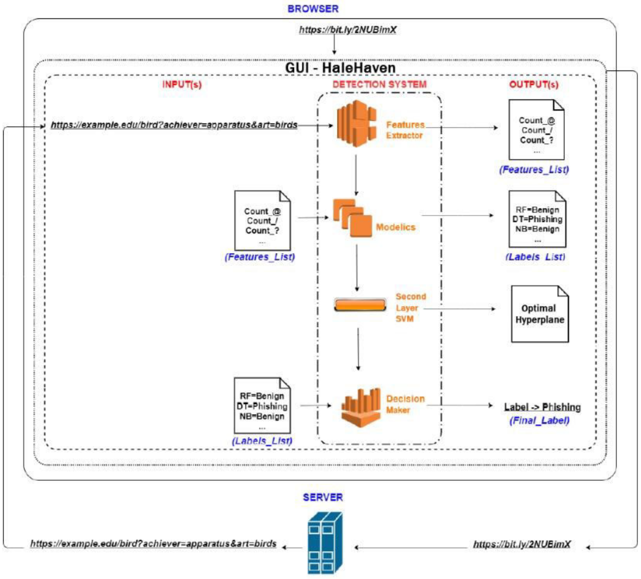
3) Modelics: In this subcomponent, different machine learning models are set in parallel as individual and independent threads.A set of extracted features from the previous subcomponent, Features Extractor, becomes an input to this subcomponent. This subcomponent, Modelics, consists of ten machine learning models. We categorize machine learning models according to our case into three categories, i.e., boosting based approach, non-learning-based approach and learning based approach because we want to introduce variance in decision making and feature selection processes.

4) Second layer SVM: There are ten ouputs from the previous subcomponent. These rtesults are passed to the second layer SVM for the final classification. The SVM draws decision boundaries based on the results from the machine learning models in a hyperplane. The objective of the support vector machine algorithm is to find a hyperplane in an N-dimensional space that distinctly classifies the data points. To separate the two classes of data points i.e, Phishing and Normal, there are many possible hyperplanes that could be chosen. Our objective is to find a plane that has the maximum margin, i.e the maximum distance between data points of both classes. The Class with Maximum margin is passed to the last subcomponent decision maker.

5) Decision Maker: In this subcomponent the class with maximum margin will be labelled as the result and will be displyed on the graphical user interface. i.e, Phishing or Normal.

IV. System Architecture

The architecture of HaleHaven. HaleHaven, an advanced AI phishing URL detection system, takes a URL and employs URL Hit approach to extract an extended URL from the server. Then using the Features Extractor subcomponent, HaleHaven extracts selected lexical features from an extended URL. Next HaleHaven executes the Modelics subcomponent to generate a list of labels. Then these labels are passed to second layer SVM to draw bounadries and find a class with maximum margin,i.e, Phishing or Normal. Finally, HaleHaven uses Decision Maker subcomponent to assign the final label using the Class from previous subcomponent to the initial entered URL.



Related Works

A. Content-based Techniques

This approach analyzes the content of the webpage to classify the respective page either as phishing or normal. A main limitation which makes this approach not only computationally inefficient but also not a viable technique for most of the scenarios is that it requires either source code or the entire content of the website, i.e., images or text for performing features extraction and analysis process.

B. Lists and Heuristics based Techniques

In these techniques, detection mechanisms employ whitelists or blacklists and a set of rules to compare and classify a URL either as phishing or normal. A major drawback of these approaches is that they completely fail in detecting newly generated phishing sites called zero-day phishing sites. Furthermore, they require continuous update of lists and rules. Also, websites which are similar in terms of URL contents to those in blacklists or whitelists, and websites which are similar in terms of appearance to those set heuristics can be easily misclassified.

C. Third party based Techniques

Some detection mechanisms use third-party-based features and services. The main drawback of this approach is high error rate in terms of misclassification. The main reason for misclassification is that they heavily rely on either the age of a domain or the number of occurrences in search results. There are likely chances in this approach that newly setup legitimate sites can be misclassified as phishing sites.

CONCLUSION

In this paper we proposed HaleHaven. HaleHaven is an advanced AI phishing URL detection system. The main novelty of HaleHaven lies in its detection, i.e., it is especially crafted to detect AI-generated Phishing URLs. Furthermore, HaleHaven is capable to deal with tiny URLs with our URL Hit approach. In addition to this, it is unique in terms of its parallel execution of ensemble machine learning models. There are 10 models used for ensemble learning. A second layer SVM model for final classification which will use the output of first layers is implemented for training. The system will be able to detect tiny URLs, Zero-day as well as future AI-generated Phishing URLs based on our selected lexical features with 100 percent accuracy. Experimental analyses will be conducted for two cases, i.e., AI-generated and Simple Phishing URLs. The dataset in the first case consists of AI-generated Phishing URLs and Normal URLs. The dataset in the second case consists of Simple Phishing URLs and Normal URLs. The proposed solution will efficiently address the detection of AI-generated Phishing URLs in the forthcoming future as well as Simple Phishing URLs prevalent these days.

REFERENCES

[1] A.-C. Bahnsen, I. Torroledo, D. Camacho, and S. Villegas, “DeepPhish: Simulating malicious AI,” APWG Symp. Electron. Crime Res. (eCrime), 2018, pp. 1–8.

[2] MARIA SAMEEN 1 , KYUNGHYUN HAN 2 , AND SEONG OUN HWANG , PhishHaven—An Efficient Real-Time AI Phishing URLs Detection System, supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea Government (MSIT) under Grant 2020R1A2B5B01002145, VOLUME 8, 2020 Approach, 3rd ed., vol. 2. 978-1-7281-9180-5/20/ ©2020 IEEE

[3] Swetha Singh,Ramprakash Pandey and M.P Singh, Phishing Detection from URLs Using Deep Learning Approach, 3rd ed., vol. 2. 978-1-7281-9180-5/20/ ©2020 IEEE

[4] Farhan Sadhique,Raghav Kaul, Shahriar Badsha, and Shamik Sengupta, An Automated Framework for Real-time Phishing URL Detection,supported by the National Science Foundation (NSF), USA, Award, 978-1-7281-3783-4/20/ ©2020 IEEE

MALICIOUS CODE DETECTION USING K MEANS CLUSTERING ANALYSIS

Akhila L
Dept. of CSE
Sree Budddha College of Engineering Pattoor
Alappuzha, India
goshakhila342@gmail.com

Melba Mariam John
Dept. of CSE
Sree Budddha College of Engineering Pattoor
Alappuzha, India
melbamariamjohn@gmail.com

Praveena K P
Dept. of CSE
Sree Budddha College of Engineering Pattoor
Alappuzha, India
vpraveena792@gmail.com

Soumya Murali
Dept. of CSE
Sree Budddha College of Engineering Pattoor
Alappuzha, India
soumya4687@gmail.com

Abstract- The security of the network is posing major challenges to the system of devices due to interruption of the process through malicious code. Hence, the need for extracting the features has been approached for detection methods which are not sufficient to detect the malware. On the other hand, the malicious codes have the power to changes their behaviour and content as per the system and its configurations, which cause more inefficiency in detection techniques. The proposed process thus can be handled with the help of K-means clustering analysis which used the concept of Adaptive weights (AW-MMKM). The features of page behaviour, fault behaviour, active behaviour and network scanning behaviour can be used for the process of identification of malicious code with the help of the proposed algorithm. It can also result in providing higher accuracy in the experimental results and is also compatible to work on multiple devices and platforms.

I. INTRODUCTION

A. Overview

Malicious code is considered as harmful code which can prove harmful to a system by causing undesired impacts as well as creating certain damages to the system. This threat of malicious code is not efficient to be handled by any software of antivirus. It can include the various system of security threat which may consist of Trojan Horse, virus and scripts that can enter into the network can easily propagate. It is responsible for creating overloading in server and network through the various process like reformatting hard disk, deleting document files, stealing password and data, send malicious emails and so on. Thus, detection of malicious code is done through the technology of interconnection of the networks and predicting the behaviour data transmission among the various hosts in the LAN.

B. Methodology

The malicious code can be detected by the possible four behaviour features of the network with the analysation of the behaviour of the network. These features are page behaviour, fault behaviour, active behaviour and network scanning behaviour. These features can be extracted using the malicious code detection framework [2-3]. Moreover, the detection of the method which is proposed in this paper is conducted by the AW-MMKM clustering algorithm. The conference paper is going to establish the knowledge regarding the detection of the malicious through analysis by clustering process. K- means algorithm is a clustering algorithm that can be used for detection of malicious code of the proposed system based on the adaptive weights.

II. PROPOSED SYSTEM

A. Analysis of Malicious Code and Detection Technology

(1) Static Analysis technology

In this case, the static analysis for the detection of malicious code refers to the process which involves the analysis of the data holding malicious code directly without executing as a real program using any static analysis tool. For analysing the malicious code, the division map for the code is required to understand the functional module. Basically, the methods in this process are dependent on the properties of the malicious code, and the methods are dependent on abstract algorithms. The specific analysis that is involved in the process includes feature analysis, feature extraction, modelling and abstraction.

(2) Dynamic Analysis technology

In this case, the method of dynamic analysis denotes the process of analysing a program that is executable in order to obtain the characteristics of the behaviour related to the malicious code. This is done by the execution of the malicious code in an environment that is protected. Dynamics analysis utilises the malicious code in the form of deformation and packers' behaviour. The technology is divided into virtual machine technology and sandbox technology, and so on. Moreover, it usually contains the access of the network, the call sequence of API and the file system.

B. K-Means Algorithm [1]

Commonly used initialization methods for k means cluster analysis are Forgy and Random Partition. The Forgy method randomly chooses k observations from the dataset and uses these as the initial means. The Random Partition method first randomly assigns a cluster to each observation and then proceeds to the update step, thus computing the initial mean to be the centroid of the cluster's randomly assigned points. The Forgy method tends to spread the initial means out, while Random Partition places all of them close to the center of the data set. The idea behind using this algorithm is to select various points of feature, which is determined into k clusters. This means the entire dataset is divided into the k different sets; these instances are divided on the basis of the cluster centre in order to compute the smallest distance of the points from the cluster centre. The sum of the square errors is obtained on the basis of k cluster centres which can be computed through continuous computations through iterations. The iteration halts when the maximum limit of the iterations is completed or any of the cluster points are calculated for the second time.

$$W_n = \sum_{j=1}^{k} V_j = \sum_{j=1}^{K} \sum_{i=1}^{N} \delta_{ij} \, || \, x_i - m_j \, ||^2$$

Some of the advantages of k means algorithm for clustering is easy implementation, convergence speed is faster, and simplicity makes it the first method that is usually preferred for the cluster analysis that can be performed using the various field. The algorithm also possesses some disadvantages as the algorithm can get affected by any of the isolated points, and the number of selected points in the cluster can be randomly selected, which outcomes different results of clustering depending on the clustering centre selected. The selecting of cluster centers keeps on repeating till the value of cluster centers remains same for more than one time. Each cluster center selected keeps on comparing with the features and each time a cluster center is selected a new set of clusters are formed. It also some complexities in the efficieny of processing in order to handle a big volume of data set features.

C. MinMax k-Means Algorithm [4]

The purpose of this algorithm is to reduce the errors that are obtained from the sum of the maximum square instead of reducing the errors of squares. It also starts from a chosen set of cluster centres that are randomly selected. The objectives of the normal k- means algorithm are to find the square errors and add them by the clustering process in the set of features. In the next iteration, it generally changes the distance between the cluster centre and the points. This results in dividing the closest of the clusters. If the data objects that are involved is larger and the density of the clusters are similar, then the resultant value can be larger. So, in order to reduce the cluster value, the clusters can be split in order to change the impacts of quality by the process of clustering. Thus the algorithm is obtained by the square of some of the errors that are resulted from each cluster which is constructed by a formula consisting of weights.

$$W_\omega = \sum_{j=1}^{K} \omega_k^q D_j = \sum_{j=1}^{K} \omega_k^q \sum_{i=1}^{N} \delta_{ij} \, || \, x_i - m_j \, ||^2$$

where, $\omega_j \geq 0$, $0 \leq q \leq 1$.

This algorithm helps to provide a result of clustering, which is compact and also will prevent producing a large sum while performing the errors of squares. If a higher sum is obtained for square errors, it will directly increase the weight, which is possible to be achieved by increasing the value of weight. The MinMax k means algorithm is used to obtain alternative options of optimisation to find a solution that is optimal. The optimisation value that is obtained as a result denotes the largest and the smallest problem of the objective function. This algorithm generally offers the benefits of improving the accuracy of the results of the clustering. However, it has some problems. The exponent q, which is already pre-defined in the equations as a constant, works as the key constraint of the algorithm since it limits the specific indicator that can be provided for the selection. For this case, it is therefore required to select an appropriate value for q, which can be used for the repeated clustering process. If the value of the q is quite large, then it can result in the high sum of the errors of squares in clustering, which will be generated from the points that are already far away from the cluster centre. At the same time, the low error squared sum that results from the clustering may outcome that the instance does not belong to the cluster or possible not to the nearby location of the cluster centre.

III. ALGORITHM FOR DETECTING MALICIOUS CODE BASED ON K-MEANS CLUSTER ANALYSIS WITH ADAPTIVE WEIGHTS [3]

A. Malicious Code Feature Extraction

(1) Analysis of Botnet network behaviour

Botnets are considered a malicious attack that can be discovered in the system network and is becoming widespread these days. Botnets are used by the attackers of the network in order to begin the service of DDOS for achieving malicious activities in the system. In order to understand the features of the behaviour of the botnets, three aspects are required to be considered [5].

i) Original data layer

The traffic from the switch of the network is required to exchange in the form of offline packets in the original Dara layer. Thus, it required to consider five attributes of character which includes the fault signals, destination port, destination IP address, source IP address and time.

ii) Data processing layer

In this case, the main purpose of the data processing layer is the classification of the IP address. The network is inspected for the LAN IP address. All the suspicious IP address are also recovered based on the signal of connection for the determination of the type of IP. If any kind of signal failure is obtained, then it can be stated that the IP address has an inactive external network. Otherwise, the IP address possesses an active external network.

iii) IP layer

In this case, the layer characteristics are determined for each IP based on the parameter of the connections obtained in the data processing layer. The specified value of the attribute is used to calculate each in order to get the largest eigenvalue. This value represents the key characteristics of IP.

(2) Analysis of Trojan network behaviour

In this paper, the behaviour of the web Trojans is also examined in the network, which is stated in two different layers.

i) Original data layer

A flow of the trojan can be detected while crawling through the traffic of data in the device of the network by the help of destination port, destination IP and source IP.

ii) Data Processing layer

It gives the definition of any particular connection based on the flow of connection detected in the original data layer.

B. Malicious Code Detection Process

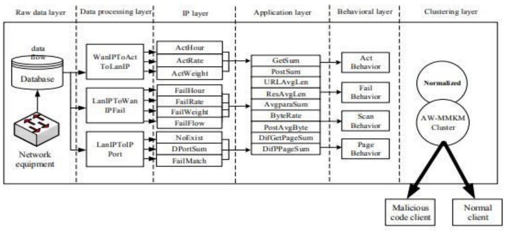


Figure 1: Malicious code detection framework

Similar behaviour can be obtained from the features with the help of analysis of clustering in order to detect malicious network and their technology. The AW-MMKM algorithm serves the purpose to reduce the sum of the weights of the errors of the squares. The AW-MMKM algorithm chooses a small random quantity of points from the data set to perform the calculation of the squared error within the classes [2]. It then puts the adaptive weights for each of the clusters that are selected on the basis of the size of the sum of the errors of squares. Similarly, the reallocation of the objects is possible on the basis of objects of the distance consisting of weights. In order to maximise the difference among the classes, the parameters that consist of weights distances are utilised. The proposed algorithm is beneficial in enhancing the efficiency of the execution of the algorithm and also helps in the optimisation of the objective function [4].

Step1: Normalisation of feature

Step 2: Initialising a cluster centre randomly using the AW-MMKM algorithm.

Step 3: The size of the feature subset is initialised using the AW-MMKM algorithm.

Step 4: The cases are then selected without clustering on a random basis.

Step 5: The distance is calculated from the cluster

$$\omega_j^t = \gamma\omega_j^{t-1} + (1-\gamma)\left(D_j^{1/(1-q)} / \sum_{j'=1}^{K} D_{j'}^{1/(1-q)} \right), \qquad 0 \le \gamma \le 1$$

centre to each of the feature instances in the subset of the feature. Then these instances are divided in the having the least distance of weights. The calculation of these weights is done using series of maximisation and minimisation steps.

Step 6: The cluster centre is recalculated.

Step 7: Go to Step 4. The iterative calculation is repeated until the maximum number of iterations is achieved or any of the cluster centres are calculated for the second time.

Step 8: The difference between the squared difference is used to represent the new k classes.

Step 9: Suppose it is found that Dq ≥ Dmax, then the value for Dq and Dmax is updated, and the new clusters that regenerated are saved.

Step 10: The normal data set and the abnormal data set is classified based on the results of clustering. The obtained group of results for abnormal data set helps to achieve the goal for the detection of malicious code.

IV. CONCLUSION

The AW-MMKM algorithm works to provide the conclusion of detecting the various analysis regarding the behaviour of the contents and features of the detection of malicious codes. With the help of this algorithm, the weighted method can be used to measure the distance, which can address the issues through the algorithm of K-means in the processing of the data in real-time. This algorithm comes with a special advantage that it provides high accuracy in the analysis as well as the detection analysis is low. For improving the performance through this algorithm, the adaptive weighted methods are used in order to process the large-scale data in real-time, which helps to solve the issues of malicious code in the system by measurement of weighted distance using the K- means clustering.

REFERENCES

[1] D. H. Shin, K. K. An, S. C. Choi, and H.-K. Choi, "Malicious Traffic Detection Using K-means," *J.Korean Inst. Commun. Inf. Sci.*, 2016, doi: 10.7840/kics.2016.41.2.277.

[2] J. Singh and S. Singla, "Enhanced intrusion network system using Fuzzy –K-Mediod clustering method," *Int. J. Innov. Technol. Explore. Eng.*, 2019, doi: 10.35940/ijitee.L2583.1081219.

[3] Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, "K-Means Clustering and Naive Bayes Classification for Intrusion Detection," *J. IT Asia*, 2016, doi: 10.33736/jita.45.2014.

[4] W. Yang, "Security detection of network intrusion: Application of cluster analysis method," *Comput. Opt.*, 2020, doi: 10.18287/2412-6179-CO-657.

[5] M. Zhou, L. Han, H. Lu, C. Fu, and D. An, "Cooperative malicious network behavior recognition algorithm in E-commerce," *Comput. Secure.*, 2020, doi: 10.1016/j.cose.2020.101868.

[6] R. Agarwal, S. Barve, and S. K. Shukla, "Detecting malicious accounts in permissionless blockchains using temporal graph properties," *Appl. Netw. Sci.*, 2021, doi: 10.1007/s41109-020-00338-3.

[7] H. Zare and S. Emadi, "Determination of Customer Satisfaction using Improved K-means algorithm," *Soft Comput.*, 2020, doi: 10.1007/s00500-020-04988-4.

[8] W. Yassin, S. Rahayu, F. Abdollah, and H. Zin, "An Improved Malicious Behaviour Detection Via k-Means and Decision Tree," *Int. J. Adv. Comput. Sci. Appl.*, 2016, doi: 10.14569/ijacsa.2016.071227.

[9] S. Zhang, Y. Wang, P. Wan, J. Zhuang, Y. Zhang, and Y. Li, "Clustering Algorithm-Based Data Fusion Scheme for Robust Cooperative Spectrum Sensing," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2019.2963512.

[10] O. I. Al-Sanjary, M. A. Bin Roslan, R. A. A. Helmi, and A. A. Ahmed, "Comparison and Detection Analysis of Network Traffic Datasets Using K-Means Clustering Algorithm," *J. Inf. Knowl. Manag.*, 2020, doi: 10.1142/S0219649220500264.

[11] S. Bayhan, A. Zubov, P. Gawlowicz, and A. Wolisz, "Smart contracts for spectrum sensing as a service," *IEEE Trans. Cogn. Commun. Netw.*, 2019, doi: 10.1109/TCCN.2019.2936190.

DETECTION OF COVID-19 FROM CHEST CT-SCAN

Saran soni
Computer Science and Engineering
Sree Buddha College of Engineering,
Pattoor Alappuzha, India
Email:saransoni00256@gmail.com

Richa Anna ribu
Computer Science and Engineering
Sree Buddha College of Engineering,
Pattoor Alappuzha, India
Email:richaribu@gmail.com

Sandra sauji
Computer Science and Engineering
Sree Buddha College of Engineering,
Pattoor
email:sausandra.ji@gmail.com

***Abstract*—COVID-19 has spread rapidly across the world bring a global pandemic with no feasible cure. COVID-19 detection has been a major task for physicians. The laboratory tests cause erroneous results and delays which led researchers to concentrate on another options. Computed Tomography (CT) and radiological images provides important information for clinical diagnosis. Deep learning is a method that uses the concept of human brain to solve complex problems through artificial neural network that learns from data. The prevailing deep learning approaches heavily rely on large labelled data sets, which are hard to acquire in this situation. In our paper, we use an end-to-end Semi-Supervised architecture (Inception v3) for the classification of Covid Chest CT Scan Images. Besides, Long Short-Term Memory (LSTM) is employed to get the axial dependency and to apply in time series data. We have normal and Covid based chest CT Scan images that will be passed to the architecture for the classification of the data. This method can reduce the need of large labelled CT images, but still be skilled to get an exact infection detection also to distinguish between COVID-19 from non-COVID-19 cases.**

Keywords: COVID-19, Computed-Tomography, Detection,Semi Supervised Learning

I. INTRODUCTION

The COVID-19 pandemic has spread over 214 countries and areas in the world . The aggressive human-to-human spread of the virus induce worldwide comprehension which consequently forced the nations to take uttermost measures in search of effective solutions. Out of the current diagnosis solutions, the real-time Reverse Transcription Polymerase Chain Reaction (rRT-PCR) test is the principal standard for COVID-19 confirmation. This test is mainly done on respiratory samples obtained from people who have shown clinical symptoms. However, the pre vailing rRT-PCR solutions have very high false-positive rates, which leads the presume patients to be tested several times for achieving conclusive diagnosis. To efficiently utilize the scarce rRT-PCR resources as well as finer accuracy in COVID- 19 diagnosis, doctors are also depending on additional medical imaging technologies.

Analysis of chest CT based on AI for probable COVID-19 diagnosis involves multiple steps from image acquisition, image pre-processing, segmentation, and final diagnosis. Although, the recent deep learning-based approaches require labelled datasets to train models. Since this labelling process of CT scans requires expert knowledge and a significant amount of time, most of the supervised learning-based models are trained on a limited amount of data. Fully supervised methods that are trained on insufficient which affect in their performance. Therefore, a semi-supervised approach or method is sufficient for COVID-19 detection from the old So we propose a new and modern approach to detect COVID-19 in the individual slices of CT scan with volume level data labels. Convolutional Neural Network named Inception V3 is proposed that integrates a lung segmentation mask with the corresponding CT volume and extract spatial features from the CT volume. Furthermore, as a pre-processing, two enhancement approaches are exploited for improving the accuracy of the model

II. RELATED WORKS

The outburst of COVID-19 in numerous parts of the world has shocked the whole world and caused several deaths. The scarcity of RT-PCR testing resources may retard the successive clinical decision and treatment [1]. Under this condition, chest CT imaging has becoming a vital tool for the detection of COVID-19 patients [2]. Various Imaging techniques including X-ray [3],[4], CT [5],[1],[6], and ultrasound [7],[8] have been applied for diagnosis of COVID-19. These imaging techniques can be used with the growing number of deep learning based COVID-19 detection methods. Commonly, a preprocessing step like enhancement [9], noise removal [10] etc. are preceded by deep learning algorithms. The prevailing deep learning-based diagnosis on CT Scan images is mainly focused on lung nodules detection for COVID diagnosis. Setio et al. [11], proposed a nodule detection technique where 2D patches of the contender nodules in lung CT are pull out from collective planes. The network consists of various 2D Convolution Network for each patch and finally the output is fused to get the final classification. Likewise, Xie et al. [12] put forward a nodule detection technique enhancing the fast region-based Convolution neural network [13] with establishment of two region proposal network. The introduced network concatenates applicable information from the lower layer and their deconvolution layer to get candidate nodules [14]. For feature extraction they used VGG16[15]. Also, they integrate the 3D input data related information that is caused by training three distinct models on three types of slices and then fused the results. To bring down the amount of fast positive, ZNET (novel architecture) is established that uses two convolution neural network's: one for getting candidate nodules and the other to bring down false positive rates [15]. The success of such techniques leads to the deployment of several AI-based approaches for COVID-19 detection [16]. However, the major part of these techniques relies on fully supervised learning, both on slice level and volume level. Such methods require time and resources of experts for data labelling purpose. To resolve such issues, our proposed framework is relying on a semi-supervised attention-based network that requires only volume level data labels.

III. Proposed method

Initially the CT images undergo preprocessing, it involves stochastic enhancement, tone mapping and masking. An accurate image-based disease detection requires high quality images.To enhance the quality of input image we use two enhancement techniques, stochastic enhancement and tone mapping. Stochastic sampling based image enhancement algorithm helps in highlighting the lung tissues and bronchioles in the CT image. This algorithm analyzes the intensity similarity between the target pixel and neighboring pixels, which are categorized by gradient between the neighboring pixel, target pixel, and their intensity difference. The second technique we consider for CT image enhancement is through tone mapping. In certain imaging condition, the linear transformation of CT images, usually of high dynamic range format to low dynamic range image formats leads to loss of image details. A combination of gamma and sigmoidal corrections are used for the preservation and enhancement of contrast of CT scans, during image format conversion. Chest CT images contain lung and non-lung tissues such as bones and fat. Since COVID-19 effects can only be viewed in the lung region, therefore we use a circular mask to enhance the lung region. The CT scan images are then fed to the proposed Inception-V3 network for extracting the spatial features. Inception-v3 is a pre-trained convolutional neural network .The Architecture creation is done by adding layers. After extracting the spatial features from the image, the feature maps are given to the LSTM.It exploits the axial dependency in the image and convert the spatial features to spatio-axial features. The resulted spatio-axial features are fed to the attention layer. Slice attention is a method that enables the network to focus on the semantic slices to help in modeling the axial dependencies in the input image. In addition to LSTM and attention layer, time distributed layer and dense layer are also added to the architecture .This architecture will be trained with the vectors obtained along with the labels and the obtained classifier after training will be saved as model. This model will be used to classify the Covid-19 Chest CT scan or Normal Chest CT Scan.

IV. Conclusion and Future Works

A. Conclusion

In this paper, a semi supervised deep learning-based network for the detection of COVID-19 has been proposed. The number of Covid-19 patients are increasing day after day.So we must need a system which automatically and without any lag predicts the diseased CT scan hence it makes the process easier for the Doctors and nurses We use an Inception V3 architecture for the classification of the Chest CT Scans. The images in the dataset are preprocessed and features are extracted. The extracted features are classified on the basis of Architecture

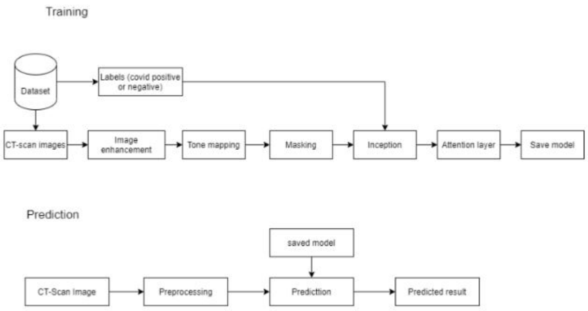


Fig. 1. Proposed Method.

B. Future Works

More COVID-19 cases will be labeled and added to the dataset, to demonstrate the strength of our model and to improve the attention. Larger dataset also helps in improving the data imbalance issue. The stochastic enhancements are applied to gray scale images, which may result in loss of information in quantization step. So, further investigation should be done regarding the application of enhancement on original image.

References

[1] Yicheng Fang, Huangqi Zhang, Jicheng Xie, Minjie Lin, Lingjun Ying, Peipei Pang, and Wenbin Ji, "Sensitivity of chest CT for COVID-19: comparison to RT-PCR," Radiology, p. 200432, 2020.

[2] Feng Pan, Tianhe Ye, Peng Sun, Shan Gui, Bo Liang, Lingli Li, Dandan Zheng, Jiazheng Wang, Richard L Hesketh, Lian Yang, et al., "Time course of lung changes on chest CT during recovery from 2019 novel coronavirus (COVID-19) pneumonia," Radiology, p. 200370, 2020.

[3] United Imaging, "United imaging sends out more than 100 CT scanners and X-ray machines to aid diagnosis of the coronavirus," https://www.itnonline.com/content, 2020, Online. Visited April 8, 2020.

[4] Ioannis D Apostolopoulos and Tzani A Mpesiana, "Covid-19: automatic detection from x-ray images utilizing transfer learning with convolutional neural networks," Physical and Engineering Sciences in Medicine, p. 1, 2020

[5] Ying-Hui Jin, Lin Cai, Zhen-Shun Cheng, Hong Cheng, Tong Deng, YiPin Fan, Cheng Fang, Di Huang, Lu-Qi Huang, Qiao Huang, et al., "A rapid advice guideline for the diagnosis and treatment of 2019 novel coronavirus (2019-nCoV) infected pneumonia (standard version)," Military Medical Research, vol. 7, no. 1, pp. 4, 2020.

[6] Deng-Ping Fan, Tao Zhou, Ge-Peng Ji, Yi Zhou, Geng Chen, Huazhu Fu, Jianbing Shen, and Ling Shao, "Inf-net: Automatic covid-19 lung infection segmentation from ct scans," arXiv preprint arXiv:2004.14133, 2020.

[7] Buonsenso, A Piano, F Raffaelli, N Bonadia, K De Gaetano Donati, and F Franceschi, "Novel coronavirus disease-19 pnemoniae: a case report and potential applications during covid-19 outbreak," European Review for Medical and Pharmacological Sciences, vol. 24, pp. 2776–2780, 2020.

[8] Subhankar Roy, Willi Menapace, Sebastiaan Oei, Ben Luijten, Enrico Fini, Cristiano Saltori, Iris Huijben, Nishith Chennakeshava, Federico Mento, Alessandro Sentelli, et al., "Deep learning for classification and localization of covid-19 markers in point-of-care lung ultrasound," IEEE Transactions on Medical Imaging, 2020

[9] Ahmed Mohammed, Ivar Farup, Marius Pedersen, Øistein Hovde, and Sule Yildirim Yayilgan, "Stochastic capsule endoscopy image enhancement," Journal of Imaging, vol. 4, no. 6, pp. 75, 2018.

[10] Shiba Kuanar, KR Rao, Dwarikanath Mahapatra, and Monalisa Bilas, "Night time haze and glow removal using deep dilated convolutional network," arXiv preprint arXiv:1902.00855, 2019.

[11] Arnaud Arindra Adiyoso Setio, Francesco Ciompi, Geert Litjens, Paul Gerke, Colin Jacobs, Sarah J Van Riel, Mathilde Marie Winkler Wille, Matiullah Naqibullah, Clara I Sánchez, and Bram van Ginneken, "Pulmonary nodule detection in ct images: false positive reduction using multiview convolutional networks," IEEE transactions on medical imaging, vol.35, no. 5, pp. 1160–1169, 2016.

[12] Hongtao Xie, Dongbao Yang, Nannan Sun, Zhineng Chen, and Yongdong Zhang, "Automated pulmonary nodule detection in CT images using deep convolutional neural networks," Pattern Recognition, vol. 85, pp. 109–119, 2019.

[13] Ross Girshick, "Fast R-CNN," in Proceedings of the IEEE international conference on computer vision, 2015, pp. 1440–1448.

[14] Sarah E Gerard, Taylor J Patton, Gary E Christensen, John E Bayouth, and Joseph M Reinhardt, "FissureNet: A deep learning approach for pulmonary fissure detection in CT images," IEEE transactions on medical imaging, vol. 38, no. 1, pp. 156–166, 2018

[15] Karen Simonyan and Andrew Zisserman, "Very deep convolutional networks for large-scale image recognition," arXiv preprint arXiv:1409.1556, 2014.

[16] Arnaud Arindra Adiyoso Setio, Alberto Traverso, Thomas De Bel, Moira SN Berens, Cas van den Bogaard, Piergiorgio Cerello, Hao Chen, Qi Dou, Maria Evelina Fantacci, Bram Geurts, et al., "Validation, comparison, and combination of algorithms for automatic detection of pulmonary nodules in computed tomography images: the luna16 challenge," Medical image analysis, vol. 42, pp. 1–13, 2017.

AUTHOR INDEX

RTACT'21

Online National Conference on

Recent Trends in Advanced Computing Technologies

ISBN 978-93-5473-994-1

RTACT'21

SREE BUDDHA COLLEGE OF ENGINEERING

PATTOOR ALAPPUZHA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING