FREE HAND INTERACTION THERAPY FOR PARKINSON'S DISEASE USING LEAP MOTION

Akilani Wijethunga

Professor, University of Moratuwa, Srilanka.

E-mail: akilaniw@gmail.com

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Abstract- Occupational Therapy is used to help people with Parkinson's disease to continue with their daily tasks as the disease progress. This paper is based on a system for Parkinson's disease patients to give them freehand interaction therapies using the leap motion controller. Leap Motion is an optical sensor specially designed for acquisition of 3D positions and orientations of hands and fingers. The Leap Motion Controller can detect and tracking hands, fingers, and tools in its field of view. In this project, the Leap Motion sensor is used to give hand and finger therapies for Parkinson's patients using serious game application developed using three js. The aim of this project is to track the motion of the fingers of the hand and to exercise the fingers of the hand. Further to track the progress of the patient by giving an analysis of the output. Each patient should use a separate login and it will help to keep the records and analyze to monitor the progression of the Parkinson's patient.

Keywords—Parkinson's Disease, Leap Motion Controller,Interaction Therapy.

1. INTRODUCTION

Parkinson's disease is a progressive disorder of the nervous system that affects movement. It affects the nerve cells in the brain. A brain chemical called dopamine acts as a messenger between two brain areas; the substantia nigra and the corpus striatum to produce controlled and smooth movements. Most of the movement related symptoms of Parkinson's disease are caused by a lack of dopamine due to the loss of dopamine producing cells in the brain. When the amount of dopamine is too low, communication between the substantia nigra and corpus striatum becomes ineffective, and movement becomes impaired. The cause of this disease is unknown, but it may involve both genetic and environmental factors a small proportion of cases can be attributed to known genetic factors. Other factors have been associated with the risk of developing Parkinson's disease, but no causal relationships have been proven. There is an increased risk in people exposed to certain pesticides and among those who have had prior head injuries while the risk is reduced in tobacco smokers and those who drink coffee or tea. Around 15% of individuals with Parkinson's disease have a first-degree relative who has the disease and 5-10% of people[1] with Parkinson's disease are known to have forms of the disease that occur because of a mutation in one of several specific genes.

Parkinson's disease develops gradually, sometimes starting with a barely noticeable tremor in just one hand. But while a tremor may be the most well-known sign of Parkinson's disease, the disorder also commonly causes muscle rigidity, stiffness, slowing of movement or Poor balance and coordination. Primary signs of Parkinson's disease include tremor of hands, arms, legs, jaw, and face. As symptoms get worse, people with the disease may have trouble walking, talking, or doing simple tasks. They may also have problems such as depression, sleep problems, or trouble chewing, swallowing, or speaking. The hand therapies and rehabilitation methods using serious game without any device attached to the body is proposed for Parkinson's patients with limited mobility in order to restore their ability to independently perform the basic activities of daily living or to recover a lost or diminished function by performing exercises on a regular basis. To cover these specific objectives, several finger therapies have been created to exercise different purposes proposed by healthcare professionals.

2. LITERATURE SURVEY

The research article, "The Effectiveness of Exercise Interventions for People with Parkinson's disease: A Systematic Review and Meta-Analysis" is describing how to systematically review

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

randomized controlled trials (RCTs) reporting on the effectiveness of exercise interventions on outcomes (physical, psychological or social functioning, or quality of life) for people with Parkinson's disease. RCTs meeting the inclusion criteria were identified by systematic searching of electronic databases. Key data were extracted by two independent researchers [2]. Among the research articles discussing the analysis of tremor of Parkinson's patients, "Detection of Parkinson Disease Rest Tremor" is measuring the rest tremor of 30 human subjects, consisting of 10 Parkinson's subjects, 10 Essential Tremor subjects, and 10 healthy control subjects to classify test subjects as either Parkinson or non-Parkinson[3]. The rest tremor was measured by recording the three-dimensional position and acceleration of their index finger while at rest over a set period of time using two devices. The first device, the Tremorometer TM, has 510k clearance to measure and quantify tremor by measuring acceleration in human patients. The second device, the Leap MotionTM Controller, is a three-dimensional camera that uses two CCD (Charged Coupled Device) cameras, three infrared Light Emitting Diodes (LEDs), and preprocessing in order to obtain position data. Research article "Free-Hand Interaction with Leap Motion Controller for Stroke Rehabilitation" describes how to use leap motion technology in rehabilitating stroke patients[4]. In this paper, it leveraged the technology of free-hand interaction to rehabilitate patients with stroke. It modified the game of Fruit Ninja to use Leap Motion controller's hand tracking data for stroke patients with arm and hand weakness to practice their finger individuation. In a pilot study, it recruited 14 patients with chronic stroke to play the game using natural interaction. This finding suggests that our freehand Fruit Ninja's score is a good indicator of the patient's hand function and therefore will be informative if used in their rehabilitation.

In the research paper "A virtual ball task driven by forearm movements for neuro-rehabilitation", the prefrontal cortex hemodynamic responses during the executions of demanding manual tasks performed in a semi-immersive virtual reality environment is studied [5]. The leap motion controller is used to track the hand movements and to enable subjects to transpose their hand movements within a virtual 3D task. In a research paper "Digitizing the hand rehabilitation using serious games methodology with user-centered design approach", the user-centered methodology for the design of serious game based on leap motion controller is presented[6]. The implemented exercise game accomplishes with both the users and the therapists considerations for the hand rehabilitation. In the research paper "Gesture-based interactions in video games with the leap motion controller", the leap motion controller as a gesture controlled input device for computer games was studied[7]. The experience with the leap motion controller into two different game setups was evaluated, investigating differences between gamers and non- gamers with 15 participants. Results indicated the potential in terms of user engagement and training efforts for short time experiences.

A tool for doctor on which they can prescribe patient to imitate standard exercise hand motion and get automatic feedback, such as score, is proposed in "Leap motion based online interactive system for hand rehabilitation"[8]. According to similarity in the scoring, the rehabilitation effect is enhanced. Other similar study, but focused on the cerebral palsy treatment is shown in "Real-time static gesture recognition for upper extremity rehabilitation using the leap motion"[9]. Because the purpose of these systems is to measure the similarity between the standard gestures and those performed by the patient, an immersive virtual environment is not necessary. A study for the treatment of motor and cognitive impairments in children with cerebral palsy is addressed in "Novel virtual environment for alternative treatment of children with cerebral palsy"[10]. Integration between patient and virtual environment occurs through the leap motion controller plus the electroencephalographic sensor Mind Wave, responsible for measuring attention levels during task execution. Based on results, the level of attention can be correlated with the evolution of the clinical condition

3. METHODOLOGY

After a discussion with medical experts, several physiotherapy treatments/exercises given to the Parkinson's patients were captured. According to the information gathered from the them, there is a wide range of exercises that is applicable to whole body that has been practicing to the patients for their rehabilitation. In order to narrow down the scope of the project and to focus on one specific area, some finger therapies were chosen to

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

implement in this system that will be very useful to improve their coordination.

We combined the physical therapies for fingers of the hand with the Leap sensor. Since our focus is finger individuation, we customized the therapy so that patients can do their own hand therapies without a physiotherapist. Using the hand tracking information of the Leap sensor, we monitor the patient's finger movement. The setup includes a PC/notebook and a Leap sensor that is plugged in via its USB. The physical therapies run on a browser (e.g., Google Chrome) while the hand is monitored using our java API code which is writtenon top of the Leap sensor's SDK.

Conducted a pilot study with Parkinson's patients, to determine the feasibility of free-hand interaction using Leap Motion controller for Parkinson's exercises. The participants should ask to play our free-hand finger therapy. We also wish to simplify the exercises so that patients with Parkinson's with different levels of hand deficits can do the finger therapy.

To avoid turning the rehabilitation exercises into boring and repetitive tasks, exercises are often interesting. The patients who are engaging in the proposed system can be keep a record of their improvement after doing these finger therapies regularly, which makes it appropriate for hand rehabilitation.

To track the finger motions of the patient, a stand-alone Java program was written in order to access and record the positions detected by the Leap Motion Controller. The Eclipse platform used to write the code necessary to access and record the data obtained from the device for thirty seconds. The stand-alone Java program that was written, recorded the position of each fingertip on the hand that exhibited the most tremor. The code was run twice for each patient and each time it was run, it saved a separate comma delimited CSV file and keeps the records. Then that data is used to analyze, compare and monitor the progression of the Parkinson's patients.

Design Process

Main objective of the proposed research is to develop a system to give hand therapies like tapping fingers and squeezing and stretching the fingers of the hand. Such activities will overcome the broadness of doing exercises and make the hand therapies more interesting and fun. We are using the leap motion to track the finger movements, and then we record and analyze data of the patient to monitor the progression of the patient. This system will contain another option if the patient is willing to do a regular exercise session, then it will guide through the sequence of steps from warming up to cooling down. It will monitor the time and give instructions to the patient. All the exercises and physical therapies include in this system are recommended for the Parkinson's patients to improve their flexibility and body control.

To conduct rehabilitation for hand/finger motion disabilities is an adequate hardware for virtual reality environment needs to be set up. Here, we are presenting LeapMotion + 2D display.

This combines 2D display and Leap Motion as input device, as shown in the following figure. 2D display is a standard part of every computer, and any kind of 2D display can be empowered for this task. However, limitations are obvious, as the conversion of real 3D hand/ finger motions to a 2D virtual world renders one dimension unavailable for preview. Losing this insight into the third (depth) dimension limits the set of applications.

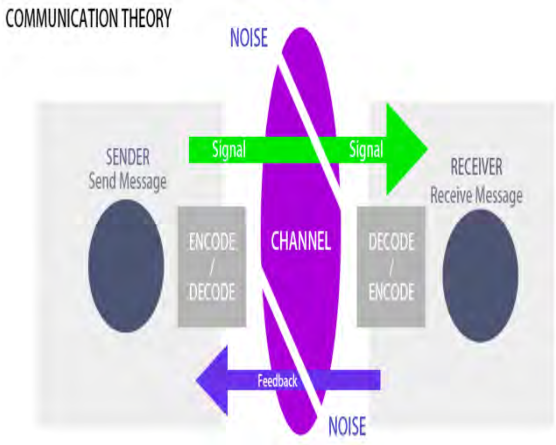


Fig.1. Interaction of Patient/User with proposed virtual environment

The present concept for the system software is designed by utilizing a database and activities which imitates physical therapies which developed using serious gaming concept. The database is a well-defined collection of data specific fora user.

Personal information of the user should include sex, age, hereditary disease risk, and all other personal data which could influence the

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

rehabilitation progress. Specialist medical reports and prescription data are the most valuable data for creating future exercise plans and prognosis of expected results. Rehabilitation progress data should contain all important data collected during exercises performance sortedby date.

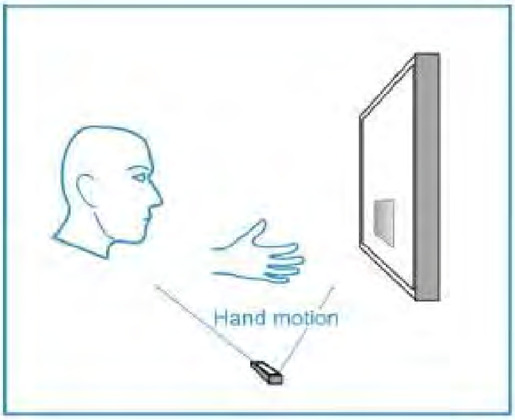


Fig. 2. System Hardware Setup: Configuration with 2D Display

The serious game developed in the virtual reality software part is responsible for all feedback from system to user and should be implemented on the game software already supported by Leap Motion SDK and three js. Finally, it will show guidance and results depending on the chosen analysis and monitor the progression of the disease.

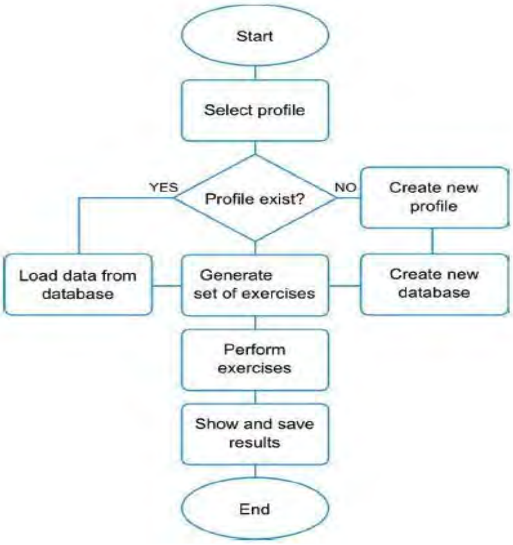


Fig. 3. General Workflow of the Application

4. RESULTS AND PERFORMANCE ANALYSIS

The hand therapies for the patients created using three js and it is combined with the inputs of Leap Motion controller. After completing the implementation part of the system, it was tested for a set of Parkinson's patients. The potential risks that were determined for the participants were mild and considered unlikely. The predetermined potential risks are discomfort from attempting to hold one hand still, boredom or frustration during the recordings and stress if the patient exhibits too severe of upper limb tremor to record the data. To reduce the potential risk to the subjects, a physician was present throughout all studies.

Since we are considering the patients who are at the early stages of Parkinson's disease, the implemented exercises willbe helpful to rehabilitate the Parkinson's patients according to the information provided by the medical experts.

Participants are planning to recruit in person during their clinic visits with their physician or nurse. If the potential participant expressed interest in the study and fit all inclusion/exclusion criteria, informed consent materials wereprovided. The document with the potential participant, which give the participant an opportunity to ask questions. Potentialparticipants will then give time to read the document in its entirety, ask questions, and speak with friends/family members if they desired. If the potential participants agreed to participate in the study, the user accounts will be created for each participant and keep the record of the results of each hand therapy. Each therapy is done twice or thrice a week and keep the record of data over the time.

This evaluation method is an experiment based evaluation since it is going test the system against a set of Parkinson's patients and record the relevant data over a period. There is no benchmark or a baseline to evaluate this approach. We aregoing to keep a track of the result values of each therapy and then monitor the progression over time. This application was tested using two Parkinson's patients and got the results as follows:

Table 1: Results of patient records

	Task 01	Task 02
Patient 01	Accuracy 9%	Time: 46.03Seconds
Patient 02	Accuracy 12%	Time: 32.09Seconds

To get the maximum benefit of this application, we should record the output data of each task of the patients for a period and then analyze it to monitor the progression of the patients.

5. CONCLUSION

This system is based on the Leap Motion controller, which is an optical sensor based on stereo vision. The system incorporates the controller with advanced software, enabling rehabilitation progress monitoring and customization of the exercise program. The Leap Motion controller is a promising device for enabling user-friendly gesture recognition services. Based on this project, the Leap Motion device can be accurately classified by representing its 3D gesture paths as set of 2D image projections, which can then be used to do physical therapies for the Parkinson's patients. The serious games implemented in this work, are a versatile tool in rehabilitation processes, since different functional problems can be treated according to the configuration defined by the therapist. Different treatment protocols can be created in an easy way. One of the applications is to use these gestures to navigations in the Virtual Reality Environment. In this research, we adopt four different gestures with hands to represent moving left/right, focusing a fingertip, tapping, and stretching fingers. Using these gestures, the patient could do the physical therapy that will be helpful to rehabilitate the patients. Based on the user experience, the use of the leap motion controller based serious game application in the treatment of Parkinson's has been favorably accepted. The utility of the games has been highlighted by the users, however there are certain exercises that have been difficult to perform and required the help of the therapist. The concept of the system can also be extended with a reminder, and a remote monitoring component. The reminder will ensure regular training, while the monitoring component will enable specialists to remotely check the progress of the rehabilitation.

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

REFERENCES

[1] Samii A, Nutt JG, Ransom BR : "Parkinson's disease". Lancet. Vol.363. (29 May 2004).

[2] Victoria A. Goodwin, Suzanne H. Richards, Rod S. Taylor,Adrian H. Taylor, and John L. Campbell, "The Effectiveness of Exercise Interventions for People with Parkinson's Disease: A Systematic Review and Meta-Analysis", Movement Disorders, Vol. 23, No. 5, 2008, pp. 631–640.

[3] Johnson, Matthew J., "Detection of Parkinson Disease Rest Tremor" (2014). Engineering and Applied Science Theses & Dissertations. 12.http://openscholarship.wustl.edu/eng_etds/12.

[4] Maryam Khademi, Lucy Dodakian, Hossein Mousavi Hondori, Cristina V. Lopes, Alison McKenzie, Steven C. Cramer, "Free-Hand Interaction with Leap MotionController for Stroke Rehabilitation", CHI 2014, Apr 26 - May 01, 2014, Toronto, ON, Canada.

[5] A. Petracca, M. Carrieri, D. Avola, S. B. Moro, S. Brigadoi, S. Lancia,M. Spezialetti, M. Ferrari, V. Quaresima, and G. Placidi, "A virtual ball task driven by forearm movements for neuro-rehabilitation," in Virtual Rehabilitation Proceedings (ICVR), 2015 International Conference on. IEEE, 2015, pp. 162–163.

[6] A. Elnaggar and D. Reichardt, "Digitizing the hand rehabilitation using serious games methodology with user-centered design approach," in Computational Science and Computational Intelligence (CSCI), 2016 International Conference on. IEEE, 2016, pp. 13–22.

[7] J. Pirker, M. Pojer, A. Holzinger, and C. G¨utl, "Gesture-based interactions in video games with the leap motion controller," in Human-Computer Interaction. User Interface Design, Development and Multimodality: 19th International Conference, HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings, Part I, M. Kurosu, Ed. Cham: Springer International Publishing, 2017, pp. 620– 633. [Online]. Available: https://doi.org/10.1007/978-3-319-58071-5 47.

[8] Z. Liu, Y. Zhang, P.-L. P. Rau, P. Choe, and T. Gulrez, "Leapmotion based online

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

interactive system for hand rehabilitation," in International Conference on Cross-Cultural Design. Springer, 2015, pp. 338–347.

[9] S. N. Gieser, A. Boisselle, and F. Makedon, "Real-time static gesture recognition for upper extremity rehabilitation using the leap motion," in International Conference on Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management. Springer, 2015, pp. 144–154.

[10] J. M. de Oliveira, R. C. G. Fernandes, C. S. Pinto, P. R. Pinheiro, S. Ribeiro, and V. H. C. de Albuquerque, "Novel virtual environment for alternative treatment of children with cerebral palsy," Computational Intelligence and Neuroscience, vol. 2016, (2016).

[11] N. Yu, C. Xu, H. Li, K. Wang, L. Wang, and J. Liu, "Fusion of haptic and gesture sensors for rehabilitation of bimanual coordination and dexterous manipulation," Sensors, vol. 16, no. 3, p. 395, (2016).

[12] V. H. Andaluz, C. Patricio, N. Jos´e, A. Jos´e, and L. Shirley, "Virtual environments for motor fine skills rehabilitation with force feedback," in International Conference on Augmented Reality, Virtual Reality and Computer Graphics. Springer, 2017, pp. 94–105.

[13] K. Nagamune, Y. Uozumi, and Y. Sakai, "Automation of the simple test for evaluating hand function using leap motion controller," in International Conference on Universal Access in Human-Computer Interaction. Springer, 2016, pp. 312–319.

[14] Y. Sano, A. Kandori, K. Shima, Y. Yamaguchi, T. Tsuji, M. Noda, F. Higashikawa, M. Yokoe, and S. Sakoda, "Quantifying parkinson's disease finger-tapping severity by extracting and synthesizing finger motion properties," Medical & biological engineering & computing, vol. 54, no. 6, pp. 953–965, (2016).

[15] J. G¨uttler, R. Shah, C. Georgoulas, and T. Bock, "Unobtrusive tremor detection and measurement via human-machine interaction," Procedia Computer Science, vol. 63, pp. 467–474, (2015).

[16] H. Kaji and M. Sugano, "A noncontact tremor measurement system using leap motion," in Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications. ACM, 2017, pp. 76–79.

[17] P. L. Kubben, M. L. Kuijf, L. P. Ackermans, A. F. Leentjes, and Y. Temel, "Tremor12: An open-source mobile app for tremor quantification," Stereotactic and functional neurosurgery, vol. 94, no. 3, pp. 182–186, (2016).

[18] A. H. Smeragliuolo, N. J. Hill, L. Disla, and D. Putrino, "Validation of the leap motion controller using markered motion capture technology," Journal of biomechanics, vol. 49, no. 9, pp. 1742–1750, (2016).

A CLOUD BASED ANDROID SYSTEM FOR REPORTING CRIMES AGAINST CHILD SEXUAL ABUSE

Jasmine J[1], Rajkumar Kalimuthu[2]

[1,2]Lecturer, School of Computer Science and Information Technology, DMI St. John the Baptist University, Malawi, East Africa.

E-mail: jasmichael1990@gmail.com[1], rajkumarengg2020@gmail.com[2]

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Abstract- A Cloud based Android System for reporting crimes against child sexual abuse is a real time cloud-based system to be used by the general public to report child sexual abuse crimes to relevant organizations. Usually, when crimes of this kind happen, the victims or witnesses go to the police, or call related organizations to report crimes. The crimes are then processed through a paper-based system where the cases are recorded and them handled accordingly. This approach is usually slow and in sometimes reads to dissatisfactions to the victims and relatives. With the wide spread of android phones, android system to report the crimes would make the crime management easier and faster as the crimes will be reported in real time using an android phone. Management of the cases will also be fast as the crimes will be directly reported to a cloud database which will make crime tracing and management faster. A global positioning system will also be implemented to send the location of the crime incident. Firebase real time database will be used to store the data reported. All the users of the system will be authenticated to make sure they are not eligible to use the application and for privacy of user information. Thus, a cloud based android system will be beneficial to both the public and the acting organizations and there by improve measures to reduce sex crimes against children.

Keywords— Cloud, Global Positioning System, Real Time Database, Firebase, Authentication

1. INTRODUCTION

In the recent years, there have been a rampant increase of abuse cases in terms of sex as far as minors are concerned. Mainly child sexual abuse, Child abuse, is a type of kid abuse that an adult or older youth employs to sexually stimulate a child [1]. Child sexual abuse includes the sexual activity of children, indecent (genital) exposures, child care [2] and child sexual exploitation including child pornography [3]. child pornography is a major part of sexual abuse. The legal definition of the kid usually refers to an individual less than the age of majority[4]. The legal definition of children is normally a minor. Different solutions have been brought forward by different concerned organisations and people in order to fight against these issues[5]. This project aims to propose a better solution in trying to combat child sexual abuse issues using an android application. Here, a cloud based android system will be developed where the victims or even anyone surrounding the crime incident place or who has knowledge of the developed situation will be able to report the case to the concerned organization which deals with issues of child sexual abuse cases directly through an android phone[6]. Two applications will be developed, one for the reporting side while one will be for the concerned organization side for them to retrieve the reported data[7]. The two applications will be connected through a cloud database and hence data will be reported and be retrieved in real time which will prompt the organization to act in time[8].

2. LITERATURE SURVEY

In this survey systematic literature review process is issued. First of all, we tried to search for recent relevant papers, presentations, research reports. Here, a survey on the already published related books and research papers is taken into account by going through the recent papers and discussing the methods that got to be used in such a paper. Shown in Table.1 Review report advantages and disadvantages

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Table.1 Summary of Crime System Report with Advantages and Disadvantages

No.	Paper Name and Techniques	Description	Advantage	Disadvantage
1.	**Godlin Jesil, Rajat Basant, Pratishvir** Crime Reporting System Using Android Application	Because readily accessible information is not available at any moment during an investigation, a new area where mobile combined with technology is effective for crime reporting. This is a major problem for police department communication. Therefore, with the help of cloud, we will strive to provide the Android police application with all information on criminals throughout their investigation, which will speed up the entire criminal tracking process.	It is more reliable when the internet is working and easy detect. high speed	It is expensive. It need more hardware and software management It need internet
2.	**Mark Phil B. Pacot** Mobile Based Crime Mapping and Event Geography Analysis for CARAGA	The Caraga region's Mobile Crime Mapping and Event Geography analysis is an important part of guaranteeing peace, safety and security of its citizens' lives and properties. To achieve this aim, the researcher devised a novel method for predicting future incident and criminal commissions using online and mobile technologies for analysis and prevention. It also features a participatory community in terms of crime reporting via mobile application for local government officials' rapid response.	It is fast and more reliable	It requires internet access. there is need to purchase some hardware
3.	**Junhua Chen, Theodoros Spyridopoulos, Panagiotis Andriotis, Robert Ludwiniak, Gordon Russell** Real-Time Monitoring of Privacy Abuses and Intrusion Detection in Android System	They examined the notion of privacy, privacy abuse behavior, and privacy abuse in Android systems in this study, which may be extremely beneficial for distinguishing malicious apps from 'regular' apps. They also studied the injection, service and service proxy technologies in Android systems, which is commonly exploited to steal confidentiality information through regular applications. An Android system is being developed to check potential privacy misuse via a real-time monitoring system (app). The app can monitor requests and assess potential misuse of privacy for all installed applications.	The issues of data privacy and security was analysed and implemented successfully	The need use of internet wasn't properly addressed
4.	**Mary Ann E. Ignaco September 2019** Development of Mobile Application for Incident Reporting	The research named "Developing the Mobile Incident Reporting Request" is a request to report and respond to crime events in the Philippine community. It consists of two major applications: Crime Reporting, Crime Responder, and the website. The Crime Reporting app is utilized by the victim or witness to submit an incident report with photographs, which is subsequently coordinated with the local barangay or police station.	Helped to reduce the crime rate in Philippines	Need internet connection Supports only up to version 6.0 android phones
5.	**Paul M. Wambugu** Application of Mobile Phone in Crime	The objective of the project was to develop application in central police department, Nairobi City Counter, of mobile phone apps by police personnel in crime prevention. Mobile telephone	It fasten the process of crime reporting and recording	The application need internet connection

	Prevention Within Central Division, Nairobi City County	use in the police is not being used to ensure that the organization does not profit completely from its use. The organization can help to prevent crime by understanding the use of mobile telephone applications by the police personnel. Due to its capacity to get consumers to work at cheap prices on a timely and direct basis, mobile apps are important to the police organisation.		
6.	**William P. Rey, et al.,** MELDEN: An Android Based Mobile Crime Reporting Application Using Crowdsourcing	Melden is a mobile criminal reporting Android-based application that leverages crowdsourcing to report different road crimes to Barangay officials.	Fast, easy and Reliable	It needs an internet connection
7.	**Pranjal Gupta , et al.,** Live Crime Reporting	This applies to the reporting of live crime as well as the e-logging of complaints from the application.	Support in the location of the closest hospitals to the sufferer.	Requires hardware and software management and purchase
8.	**R. Dhinakaran; et al.,** Android Based Crime Reporting System Using Firebase	Crime reporting system based on Android is a publicly available, online crime reporting system. In our company individuals generally go to the police station to complain about their reports, but here we create a system of public reporting online.	Both the public and the police may benefit. It promotes quick and formal communication	It requires an internet connection

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

5. METHODOLOGY

In order to achieve the outlined objectives, the project will be deployed through the following detailed models will be used.

1. The application will contain two main modules, one for the Admin and one for the users to report the crimes.
2. Registration for users: every user whether admin or general user has to be registered in the system to allow him/ her to access the application. A security code will be used to allow the user to register as an admin and the codes will be uploaded in the admin database and stored by the organization. Using firebase authentication each user has to be registered.
3. Storage service: since the crimes will be uploaded and the user information will also be uploaded to a cloud database, Firebase/ Microsoft azure storage service will be employed to offer storage for the crimes and the whole database of users.
4. Location: A Global Positioning System (GPS) module will also be implemented in order to keep track of where a user is reporting the crime from.

The Objective is to develop a user-friendly crime reporting application the general public will be able to report crimes concerning sexual abuse against children. Here anyone can register and report crimes to concerned organizations in real time and the admins at the organizations will access the reported crime and act on them accordingly. A centralized cloud database is utilized for the storing and processing of data throughout the system {user application and administration application}. For authenticity and integrity, the data of the user might be kept secret. The system's design comprises several diagrams, such as the architectural diagram which highlights the overall structure, behaviour, and performance analysis of system operations. In logical design the input and output of data in the system pertains an abstract representation of how data flows. It includes entity-relationship diagrams (E-R diagrams). While physical design dwells much on how input and output are explained relating to the data is feed to the system for verifications/authentication, and how it is processed and displayed. Divided into many parts systems design gives a glimpse of how the project will look like to the user's point of view. In this system, we use system architecture just to show how the system coordinates.

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

System Architecture

The process of defining the components, modules, interfaces, and data for a system to meet stated criteria is known as system architecture. The architecture of the system is as follows.

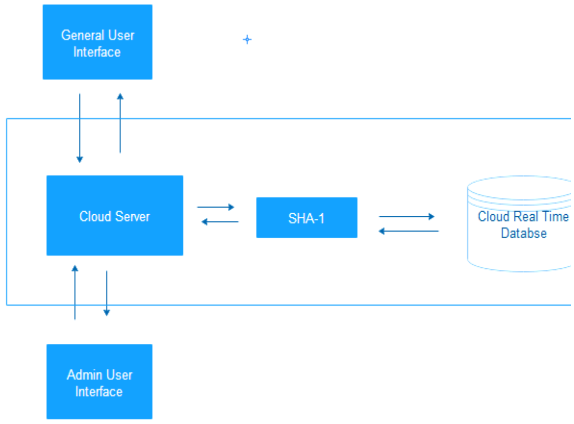


Fig. 1. Overall System Architecture

5. ALGORITHM AND TECHNIQUES

Model View Controller (MVC)

Model–view–controller is a software design pattern that organizes related program logic into three interrelated parts and is widely used for designing user interfaces. This is done to isolate internal information representations from how information is presented to and accepted by the user [4]. We utilized the MVC approach in gathering user details, criminal details, in which a custom java class Helper class was developed to function as the model to allow processing of details for multiple users.

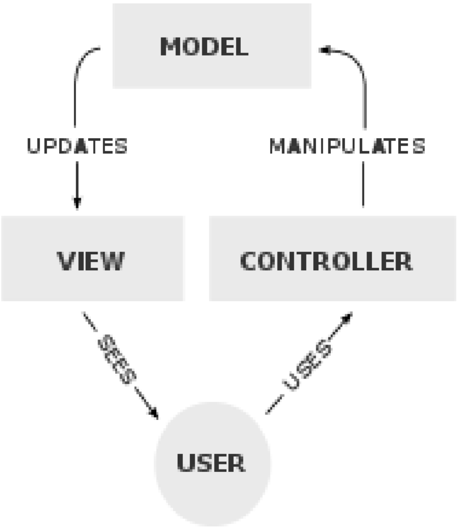


Fig. 2. MVC model

The XML files serve as the VIEW for the user interface, displaying the details. The Firebase real-time database is utilized for the application's backend processing and data storage

Multi Factor Authentication

Authentication by two factors (2FA) represents a way to improve your account's security. The first "factor" for every account is your ordinary password. The second "factor" is a verification code from an application on a mobile device or PC. 2FA is basically comparable to the security token device required for online banking by some organizations in certain regions. Other names for 2FA systems include OTP (One-time password) and TOTP (Dual-Factor Authentication) (Time-based One-time Password algorithm).

6. CONCLUSION

Based on the results of the application testing, we were able to enhance the timeliness of reporting and handling of offenses involving child sexual abuse. However, in the future, we must design the system so that it does not require internet connections every time a person attempts to report a crime, as this is the only issue that has arisen thus far.

REFERENCES

[1] U.S National Library of Medicine, “Child Sexual Abuse”, Medline Plus, 2008-04-02

[2] Williams, Mike, "The NSPCC's Protect & Respect child sexual exploitation programme: a discussion of the key findings from programme implementation and service use", NSPCC, 29-03-2019

[3] Williams, Mike, "Evaluation of the NSPCC's Protect & Respect Child Sexual Exploitation Group Work Service" NSPCC, March2019.

[4] Reenskaug, Trygve; Coplien, James O, "The DCI Architecture: A New Vision of Object-Oriented Programming", Artima Developer, 20 March 2009.

[5] William Akotam Agangiba, Millicent Akotam Agangiba, “Mobile solution for Metropolitan Crime Detection and Reporting”, Journal of Emerging Trends in Computing and Information sciences, Vol.4, No.12, 2013.

[6] Pragya Gupta, Sudha Gupta, "Mobile Cloud Computing: The Future of Cloud", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 1. September 2012.

[7] Manav Singhal, Anupam Shukla, *"Implementation of location based services in Android using GPS and Web Services",* International Journal of Computer Science Issues, Vol. 9, January 2012

[8] Godlin Jesil, Rajat Basant, Pratishvir, "Crime Reporting System Using Android Application", International Journal for Pure and Applied Mathematics, Volume 119, No. 7, 2018, 533- 538

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

BI-LSTM AND CNN HYBRID APPROACH FOR THE IMPROVEMENT OF TWITTER SENTIMENT ANALYSIS

Prafful Choudhary[1], Arun Solanki[2]

[1,2]Lecturer, Department of Computer Science and Engineering, Gautam Buddha University, Greater Noida, Uttar Pradesh, India.

E-mail:chaudhary.prafful@gmail.com[1], asolanki@gbu.ac.in[2]

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Abstract- Sentiment Analysis provides the sentiments of Textual data. It is used widely by multinational companies to know customer sentiment to gain information about market trends and product reviews. In this field, we see a constant development and are still being extensively researched in different areas by top organizations and universities all around the globe. One significant flaw in their technique is that it is unable to account for the overall dependencies of sentences in a document. We look at sentiment analysis approaches based on deep learning, which have already shown promise in a variety of difficult problems in domains such as vision, speech, and text analytics. We recommend using the Bi-LSTM combined with CNN model, which operate like this: the CNN model is used for extraction of features, and the Bi-LSTM model receives input from the CNN model's output and retains the previous data. In this proposed work, we studied Machine Learning techniques and Deep Learning approaches for their uses in Sentiment Analysis. Our Proposed work is using a Hybrid approach with Glove embeddings, Bi-LSTM, and CNN layer in the deep learning model. Results show that the model we planned beats existing Naive Bayes, Support Vector Machine (SVM), Linear Regression, and LSTM and gives an accuracy of 82.74. Our CNN-Bi-LSTM model does 2.69% better than a regular LSTM model. On the other side, the Bi-LSTM-CNN model does 3% better than a normal LSTM model and 7.05% better than a Bernoulli NB model.

Keywords— Sentiment, Convolution Neural Network (CNN), LSTM, Bi-LSTM, Support Vector Machine (SVM), Linear Regression, Naive Bayes (NB), Random Forest.

1. INTRODUCTION

Sentiment Analysis also called Opinion Mining is a part of Natural Language Processing (NLP) that tries to builds systems to identify and find the opinions within textual data. Usually, besides identifying the sentiment, these systems extract attributes of the expression e.g.

- **Polarity:** tweets give a positive or negative review.
- **Subject:** the product or issue for which the tweets are carried out
- **Opinion holder:** the Twitter ids that express the sentiment.

Nowadays, sentiment analysis is a subject of immense interest and improvement for the reason that it has many real-time applications. Since publicly and privately reachable facts over the Internet are continuously turning into big, a massive quantity of textual content data expressing sentiments are present in assessment sites, forums, blogs, and social media. With the help of sentiment analysis systems, this unstructured information could be automatically modified into structured information of public sentiments about products, services, brands, politics, or any different subject that people can express opinions about. Our proposed model on sentiment analysis can be categorized from different perspectives: the method used, rating level, view of the text, level of detail of text analysis, etc. From a technical point of view, we recognized machine learning, rule-based approaches, lexicon-based, and statistical.

- The machine learning approach makes use of several learning algorithms to get the sentiment through training on a known dataset.
- The lexicon-based technique includes finding sentiment polarity for a tweet by using the "Semantic orientation" of various sentences in the tweets. The “Semantic orientation" is known for its calculation of opinion and subjectivity in text data.
- The rule-based technique used for sentiment analysis in textual data and then identify them based on the variety of negative and positive words. It considers distinct rules for classification such as negation words, idioms, emoticons, booster words, mixed sentiments, etc.

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

2. PROPOSED WORK

Automatic Approaches

Automatic methods, unlike rule-based systems, are now primarily dependent on machine learning techniques rather than manually created rules. The sentiment analysis task is often characterized as a classification technique, in which textual material is given into a classifier, which returns a sentiment category, such as negative, neutral, or positive (in case of sentiment analysis is being asked). Although we have sentiment analysis techniques using machine learning algorithms like Naive Bayes, SVM, regression, random forest, etc. it cannot contextually understand the text data. A sentence is treated as a bag of words and each word is treated separately without any relation to the words in its neighborhood. Deep learning is advanced and preferred over the traditional ML approach as it can easily understand the context of the sentences and thus help give better sentiment analysis outcomes [1]. Our proposed work uses deep learning algorithms such as convolutional neural network (CNN), Long-Short Term Memory (LSTM), Bi-LSTM model, and two networks that integrate convolutional and LSTM layers.

Following contributions are made in our proposed work:

- Classifying user Tweets as negative or positive affiliations deep learning-based sentiment analysis algorithms.\
- To compare TF-IDF and bag-of-words (BoW) over word embedding learned with LSTM, Bi-LSTM, CNN-Bi-LSTM, and Bi-LSTM-CNN for tweet classification as positive and negative.
- Using various Machine Learning methods to compare the results of the suggested model.
- In terms of improved accuracy, our technique outperforms ML methods by a wide margin.

3. RELATED WORK

The author mainly focuses on finding the capability of multiple machine learning algorithms (SVM, NB) to classify sentiments using supervised learning methods. The author tries to find the opinions on Amazon with the help of Amazon API [2]. The author focuses to explain the key variations between RF, SVM, and hybrid Random Forest Support Vector Machine algorithms (RFSVM) which are efficient in giving guidelines for the classification models. The outcomes from this test concluded that the RFSVM algorithm is a great algorithm for the sentiment analysis on Amazon Product reviews [5].The author proposed an automated and improved way of Figuring out the sentiment of tweets with the help of Distant Supervision. The polarity of tweets is divided into negative or positive according to the query. The applied dataset is used for the classification of tweets consists of emoticons, which are termed noisy labels. This paper explains the pre-processing steps encouraged for getting high accuracy [9]. The Author proposed a hybrid system that offers satisfactory results and the best use of base classifiers and a hybrid approach. When compared with the other classifiers the hybrid NB-GA approach offers a higher percentage of accuracy and due to decreasing the dimension of the data, the testing time interval is improved[11].The author defined classifier lexicons and ensembles are used in the automatic classification of the polarity of tweets. The tweets are labeled as negative or positive. Sentiment analysis can be used by organizations that generally checking the public perceptions of their products, customers who search their products online, and more [13].

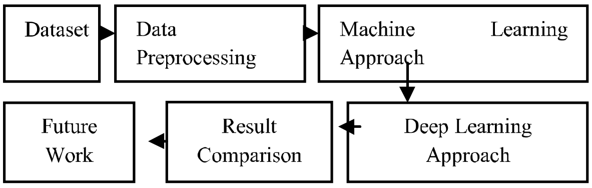


Fig.1. Process Flow

Dataset Used

This is the tweeter 1.6M dataset. It contains 1600000 tweets extracted using the Twitter API. The tweets have been distributed (0 = negative, 4 = positive) and they can be used to detect sentiment.

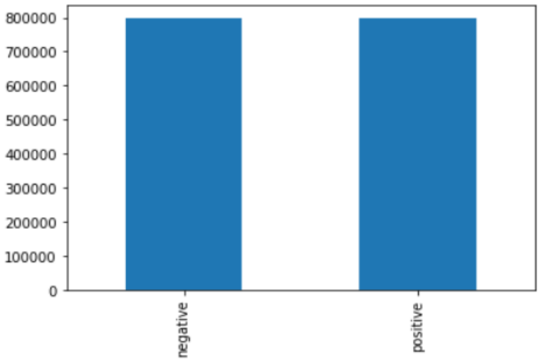


Fig.2. Dataset Distribution

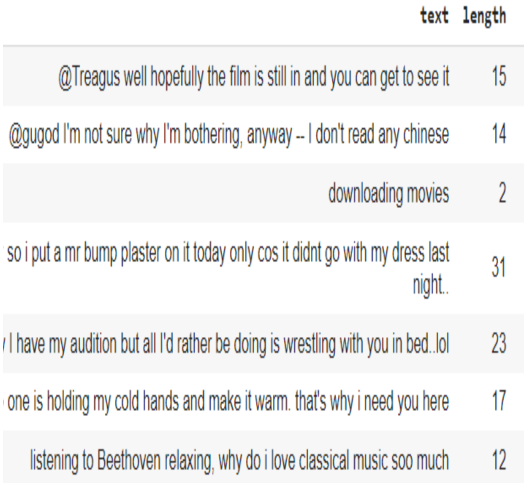
4. DATA PREPARATION

The Preprocessing steps:

• Exclude Unicode strings from the tweets
•Exclude URL address
•Exclude hash-tag before a word
•Exclude whole numbers
•Exclude HTML unique elements (for example &amp)

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

•Exclude tickers
•Exclude hyperlinks
•Exclude Punctuation and split ('s,'t, 've) with space for channel
•Exclude words with 2 or fewer letters
•Exclude whitespaces
•Exclude single space staying at the front of the tweet
•Exclude characters past the essential multilingual plane of tweets



text	length
@Treagus well hopefully the film is still in and you can get to see it	15
@gugod I'm not sure why I'm bothering, anyway -- I don't read any chinese	14
downloading movies	2
so i put a mr bump plaster on it today only cos it didnt go with my dress last night..	31
I have my audition but all I'd rather be doing is wrestling with you in bed..lol	23
one is holding my cold hands and make it warm. that's why i need you here	17
listening to Beethoven relaxing, why do i love classical music soo much	12

Fig.3. Cleaned Dataset

5. MACHINE LEARNING APPROACH

Bernoulli Naive Bayes

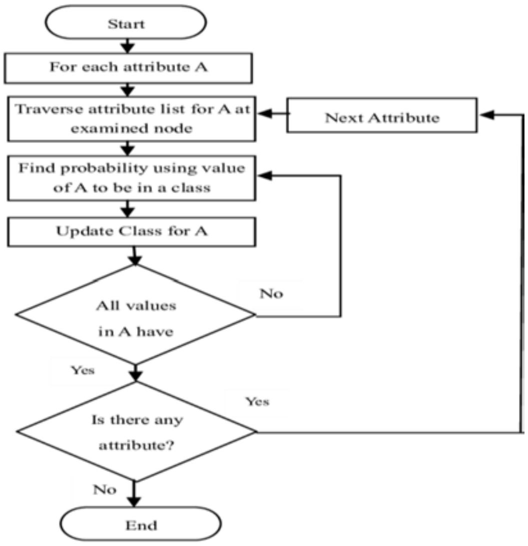


Fig.4. NB Flow chart

Naive Bayes is a Machine Learning-based classification algorithm based on statistics. The goal of this approach is to use conditional probability to forecast statistics of texts, phrases, and classes belonging to a class. The independent occurrence of words is the significant element of this strategy. The dependency of words with any class is not evaluated by Naive Bayes. Bernoulli Bayes, Nave: The predictors are Bovariables, generally referred as Boolean variables, which become identical to the multinomial NB.

Logistic Regression

Logistic regression is a famous machine learning approach that predicts the result of a categorical dependent variable. As a consequence, the output must be a discrete or categorical value. It can be 1 or 0, Yes or No, True or False, etc. However, instead of providing the actual value as 0 and 1, it provides the hypothetical values which lie between 1 and 0 [8]. In Logistic regression, we are not interested in fitting a regression line, instead of that, we try to draw an "S" shaped logistic function, which helps to give the predicted value between two maximum points (1 or 0).

Random Forest

Random forest is a supervised machine learning method. The "forest" refers to the ensemble or set of decision trees that it creates, which is normally pre-trained using the "bagging" method. The principle behind the bagging strategy is that combining a variety of learning models helps in improving outcome. While developing the trees, the random forest adds to the model's randomness. So rather than finding the most important feature when splitting a node, it searches for the best feature among a set of features at random. [12]. this produces a wide variety of results, which often leads to a better model.

Support Vector Machine

The Support Vector Machine is another well-known classification approach in Machine Learning. We also deployed an SVM Scikit-Learn tool with a linear kernel in our proposed model. This is a vector space system based on a classifier that requires feature vectors to be converted into numerical values before classification. In several cases, the text is converted into a multi-dimensional tf.idf vector.

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

6. DEEP LEARNING APPROACH

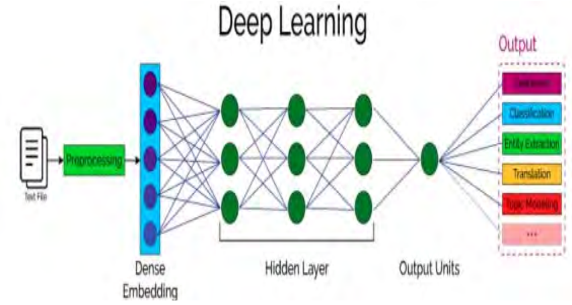


Fig.5. Artificial Intelligence Overview

Deep Learning is a very efficient method of learning. This helps to use neural networks to perform a given set of tasks. Neural Networks are known to be analogs that exhibit the working of biological neurons in the brain of a human. The artificial neural networks (ANN) having three layers: an input layer, an output layer, and a hidden layer. Neural networks are generally shown as fully attached graphs that associate each edge with some particular weight, each node with an input value which is usually random values, and a set value of bias is added. The working of a neural network is based on finding out the weighted sum [15].

Weighted sum = $\sum wi * xi + b$ (1)

The weighted sum is given as a special function to optimize the output. Such special functions are known as Activation Functions which can help to make the outcome non-linear and help in classification [16].
Relu is rectified linear unit which is used to get only zeros & positive values.

Relu = max (0, x) (2)

The sigmoid function is generally an S-shaped curve that limits the values to 0/1 [17].

Sigmoid = $\frac{1}{1+e^{-x}}$ (3)

In the Deep learning model ,the training data sets the group of examples that are helping to train the neural network. As the outcomes to the given input are known already, the neural network tries to learn from the set of examples because that it could provide the predicted results. The ratio of the number of accurately classified sets and the totally different number of sets that are used as training data and now it gives out the training accuracy. In Deep learning, the testing dataset is that set of models which are utilized to test the neural organization and check how well the neural organization Figured out how to arrange from the preparation dataset. As the answers for these sources of info are now known, the neural organization is tried on these guides to look at if it's giving the ideal forecasts while it has been tried on new information which is not quite the same as the preparation dataset.

Model 1: LSTM

Embedding Layer

It is one of the general layers in Keras. This is primarily used in Natural Language Processing (NLP) related areas such as modeling languages, and it can also be helpful in other processes that include neural networks. When we are facing NLP problems, we can use word embeddings that are pre-trained such as Glove. We can also train our embeddings with the help of the Keras embedding layer. [18].

LSTM layer

Long short-term memory (LSTM) is a different type of RNNs where the singular unit having the memory cell and three main gates called the input gate, output gate, and forget gate. The memory cell is generally used for holding the element dependencies of the input sequence while the main gates control the storage & transfer of data: input gates help to control the amount of data into the unit, forget gate controls the degree of data that should remain in the unit and the output gate controls the activation of the unit.

A dense layer

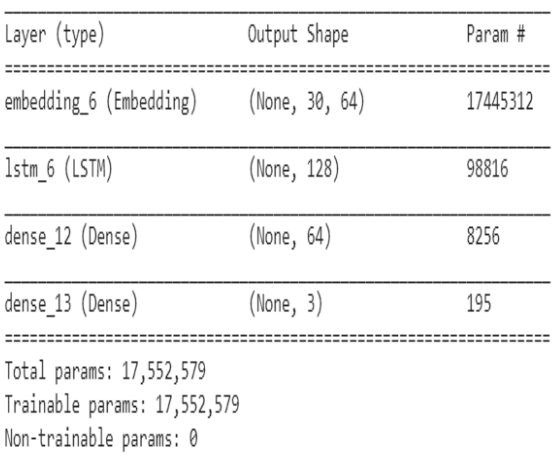
A dense layer is the general deeply connected neural network layer. It is the most common and frequently used layer. The output dimension of the dense layer will be changed by the number of neurons/units provided in the dense layer.

Dropout layer

The main function of the dropout layer is to avoid over fitting in a model. The dropout layer tries to randomly deletes or shut down the

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

activation of neurons in the embedding layer as the dropout is carried out on the embedding layer, whereas each neuron in the embedding layer depicts the dense representation of a word in a sentence [18].



```
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
embedding_6 (Embedding)      (None, 30, 64)            17445312
_________________________________________________________________
lstm_6 (LSTM)                (None, 128)               98816
_________________________________________________________________
dense_12 (Dense)             (None, 64)                8256
_________________________________________________________________
dense_13 (Dense)             (None, 3)                 195
=================================================================
Total params: 17,552,579
Trainable params: 17,552,579
Non-trainable params: 0
```

Fig.6. LSTM model layer

Model 2: Bi-LSTM & Additional Drop Out with Glove Embedding Bi-LSTM: (Bi-directional long short-term memory)

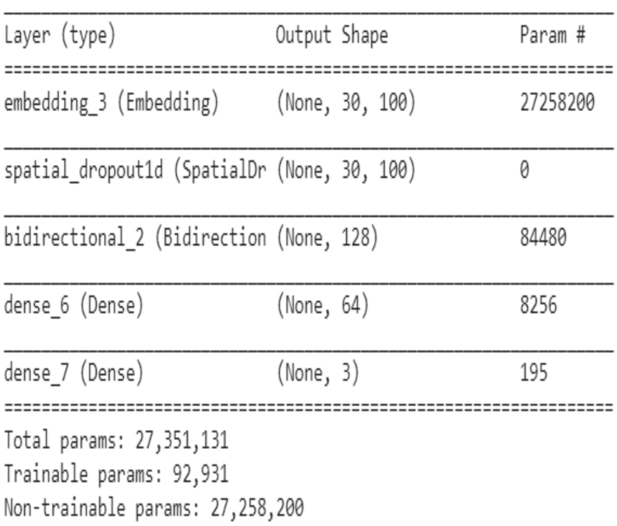
Bidirectional recurrent neural networks (RNN) are nothing new but just putting two independent RNNs together. This helps to allow the networks to have both forward and backward information of the sequence at every unit time step Using bidirectional will run our inputs in two different ways, one from future to past and other one is from past to future, and what is different in this approach from unidirectional is only that in the LSTM which runs backward we can store data from the future and using the two hidden states together we are capable in any interval of time to restore the data from future and past [18].

Spatial Dropout

It is having the same function as dropout, but it drops the entire 1-D feature map. Generally used when the particular elements are strongly co-related, as this would regularize it better and enhances independence between feature maps [19].

Word embeddings using Glove

Word embeddings help to provide a dense representation of words and their respective meanings. Embedding Matrix is a group of all words and their respective embeddings. Embedding matrix is used in embedding layer in model to fix a word into its vector representation form that contains all the information regarding that word. Embedding vocabulary is obtained from the tokenize and the corresponding vectors from the embedding model defined, which the Glove model is in this case. The Glove model is trained on values that are non-zero and having a global word-word co-occurrence matrix, which shows and calculates how frequently words co-occur with one another in a given corpus [19]. Generally, this matrix only requires a single pass through the entire corpus to get all the statistics.



```
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
embedding_3 (Embedding)      (None, 30, 100)           27258200
_________________________________________________________________
spatial_dropout1d (SpatialDr (None, 30, 100)           0
_________________________________________________________________
bidirectional_2 (Bidirection (None, 128)               84480
_________________________________________________________________
dense_6 (Dense)              (None, 64)                8256
_________________________________________________________________
dense_7 (Dense)              (None, 3)                 195
=================================================================
Total params: 27,351,131
Trainable params: 92,931
Non-trainable params: 27,258,200
```

Fig.7. Model 2 Layers

Model 3: Hybrid Model (CNN+Bi-LSTM with Glove Embedding)

A convolutional neural network is a type of layered neural network. The first layer represents the embedding layer which helps to embed the words into low-dimensional vectors. The second layer known as the layer of convolution, layer performs multiplication of the input vector, and weight vectoris obtained to find the weighted sum. The fourth is the Dropout layer; this helps avoid over fitting problems and is active only at training time [19].

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

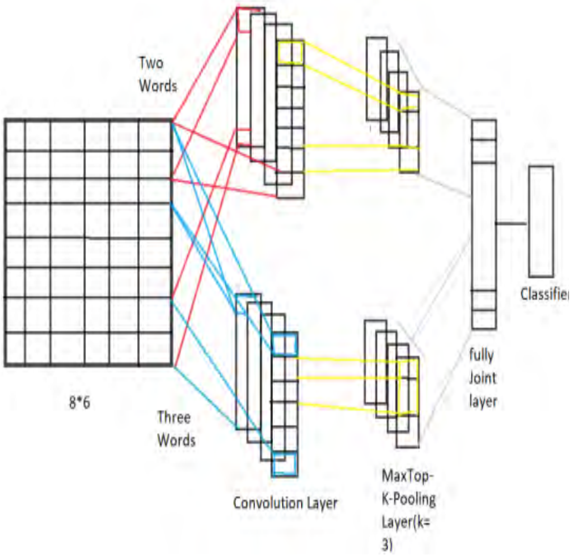
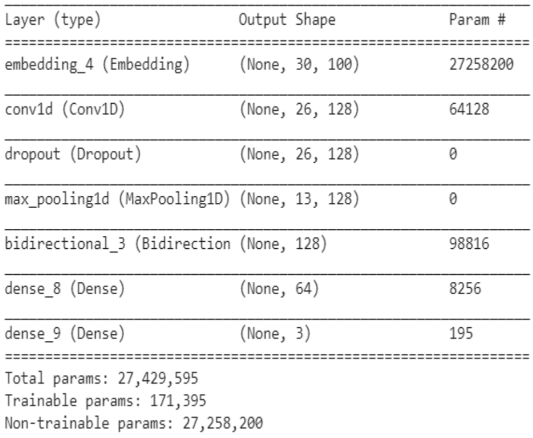


Fig.8. CNN implementation for text sentiment analysis

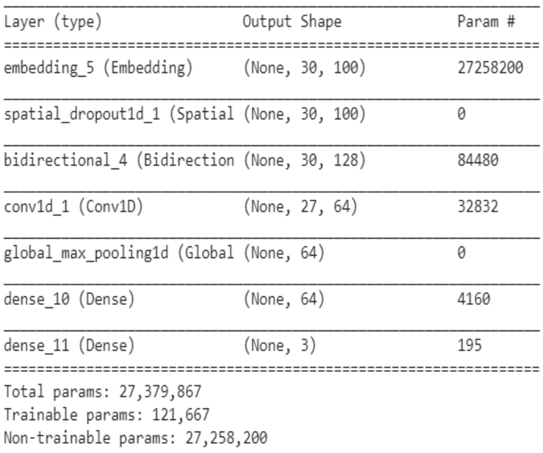


```
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
embedding_4 (Embedding)      (None, 30, 100)           27258200
_________________________________________________________________
conv1d (Conv1D)              (None, 26, 128)           64128
_________________________________________________________________
dropout (Dropout)            (None, 26, 128)           0
_________________________________________________________________
max_pooling1d (MaxPooling1D) (None, 13, 128)           0
_________________________________________________________________
bidirectional_3 (Bidirection (None, 128)               98816
_________________________________________________________________
dense_8 (Dense)              (None, 64)                8256
_________________________________________________________________
dense_9 (Dense)              (None, 3)                 195
=================================================================
Total params: 27,429,595
Trainable params: 171,395
Non-trainable params: 27,258,200
```

Fig. 9. Model 3 Layers

Model 4-Hybrid2 (Glove+Bi-LSTM+CNN)

In our proposed work, we provide a method that gives the performance of Bi-LSTM with the Convolutional Neural Network (CNN) model to find the tweets containing content with negative and positive sentiments. We train the neural classifier, for the classification of positive and negative content. The working steps of the network are comprised of the different steps: (i) Embedding, the layer in which every word in a sentence is allotted a distinct index to built a fixed-length vector, (ii) Dropout layer is used here to solve the problem of overfitting, (iii)Bi-LSTM layer is used to get the long-distance dependence across tweets, (iii) feature extraction is performed using a convolution layer, (iv) The layer of global_max_pooling1d aims at minimizing the dimension of feature map by accumulated the information.



```
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
embedding_5 (Embedding)      (None, 30, 100)           27258200
_________________________________________________________________
spatial_dropout1d_1 (Spatial (None, 30, 100)           0
_________________________________________________________________
bidirectional_4 (Bidirection (None, 30, 128)           84480
_________________________________________________________________
conv1d_1 (Conv1D)            (None, 27, 64)            32832
_________________________________________________________________
global_max_pooling1d (Global (None, 64)                0
_________________________________________________________________
dense_10 (Dense)             (None, 64)                4160
_________________________________________________________________
dense_11 (Dense)             (None, 3)                 195
=================================================================
Total params: 27,379,867
Trainable params: 121,667
Non-trainable params: 27,258,200
```

Fig.10. Model 4 Layers

The Bi-LSTM+CNN model is used on the dataset and the prediction accuracy of sentiment analysis on the twitter1.6Mdatasetisfoundtobe82.74%.

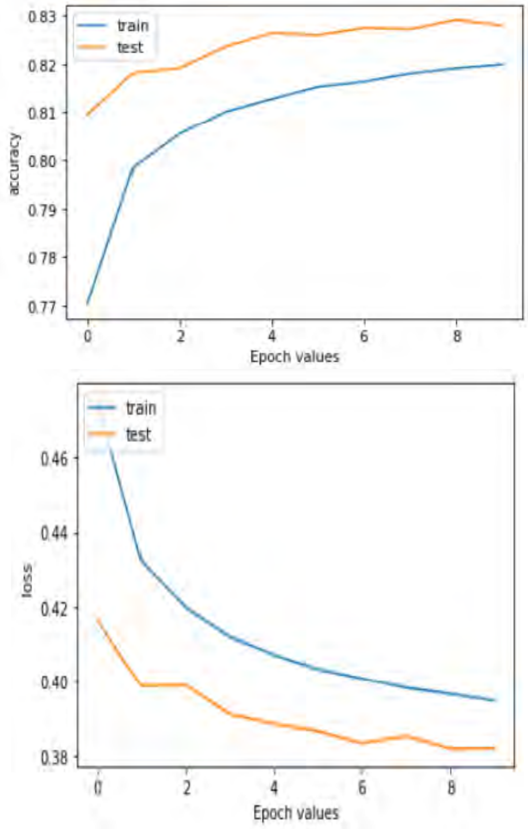


Fig. 11. Model 4 Accuracy and Loss plot

6. RESULTS

The LSTM model is used on the dataset and the prediction accuracy of sentiment analysis on the twitter 1.6M datasetisfoundtobe79.74%.

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

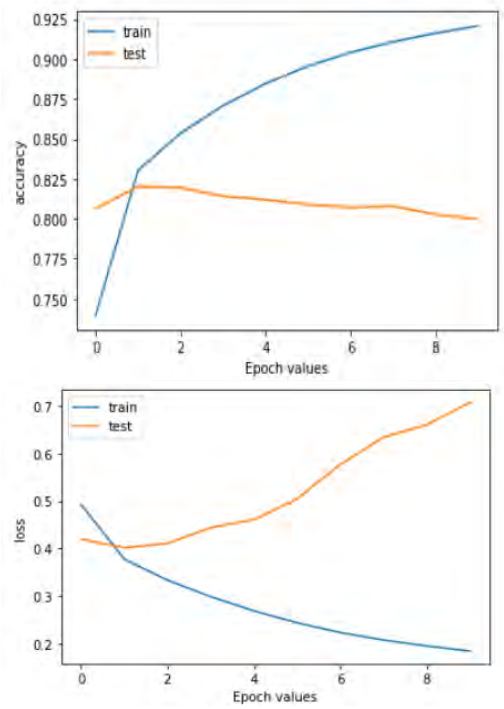


Fig.12. LSTM model Accuracy and Loss

The Bi-LSTM and additional dropout Layer model are used on the dataset and the prediction accuracyofsentimentanalysisonthetwitter1.6M datasetisfoundtobe82.28%.

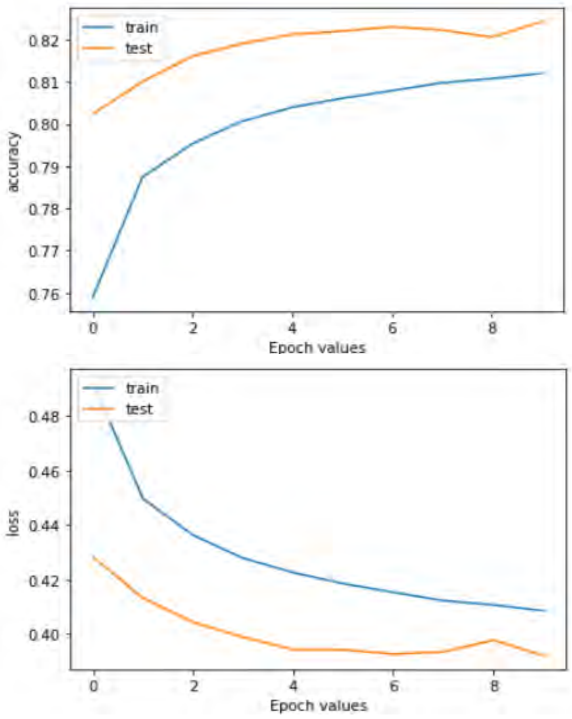


Fig. 13. Model 2 Accuracy and Loss plot

The CNN+Bi-LSTM model is used on the dataset and the prediction accuracy of sentiment analysis on the twitter 1.6M dataset is found to be 82.43%.

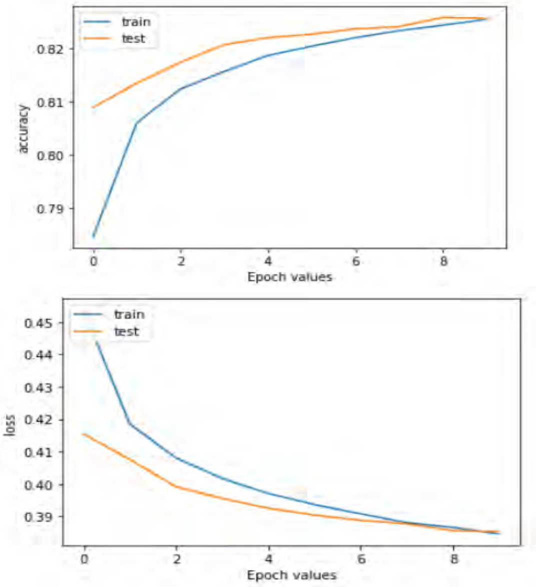
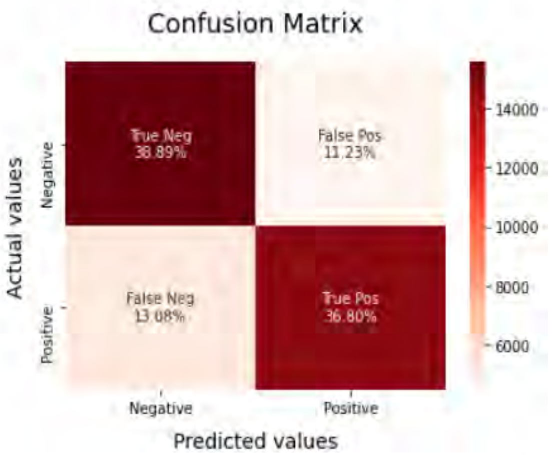


Fig. 14. Model 3 Accuracy and Loss plot

The Bernoulli Naive Bayes classifier model is used on the twitter1.6M dataset and the prediction accuracy of sentiment analysis on the given dataset is calculated and it is found to be 75.69%.TheConfusion Matrix values obtained from the model are given in Fig14.



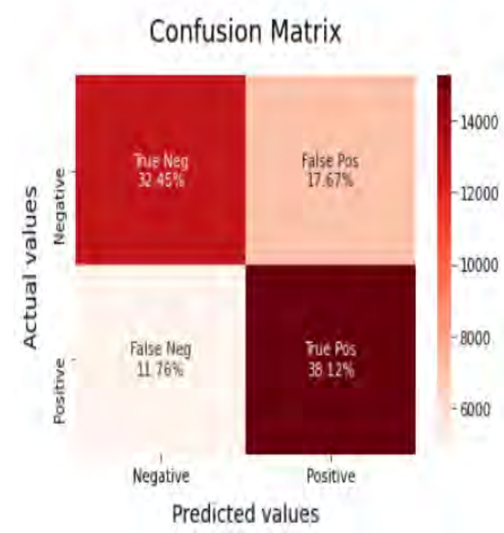
```
Accuracy of model on training data : 86.88
Accuracy of model on testing data : 75.69500000000001

              precision    recall  f1-score   support

    negative       0.75      0.78      0.76     20048
    positive       0.77      0.74      0.75     19952

    accuracy                           0.76     40000
   macro avg       0.76      0.76      0.76     40000
weighted avg       0.76      0.76      0.76     40000
```

Fig.15. Bernoulli Naive Bayes Confusion Matrix

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

The Random Forestclassifier model is used on the twitter1.6M dataset and the prediction accuracy of sentiment analysis on the given dataset is calculated and it is found to be 70.57%.

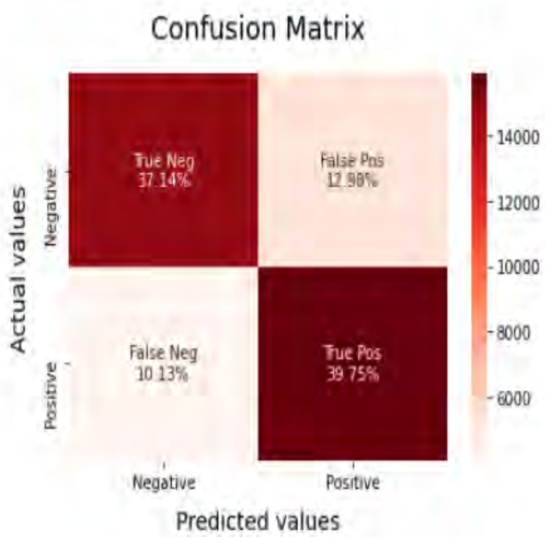
The Confusion Matrix values obtained from the model are given in Fig15.



```
Accuracy of model on training data : 75.655
Accuracy of model on testing data : 70.5725

              precision    recall  f1-score   support

    negative       0.73      0.65      0.69     20048
    positive       0.68      0.76      0.72     19952

    accuracy                           0.71     40000
   macro avg       0.71      0.71      0.70     40000
weighted avg       0.71      0.71      0.70     40000
```

Fig.16. The Confusion Matrix values obtained from the model

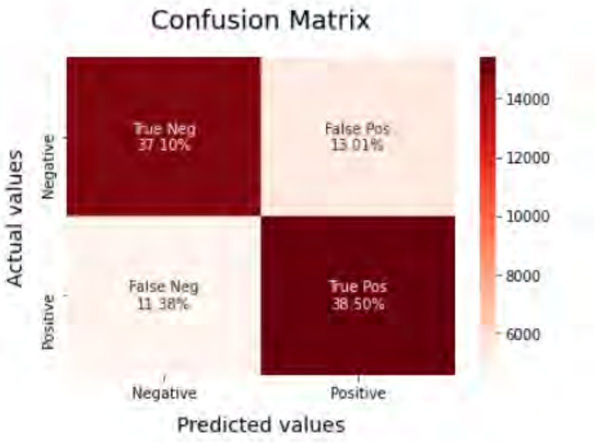
The Logistic Regressionclassifier model is used on the twitter1.6M dataset and the prediction accuracy of sentiment analysis on the given dataset is calculated and it is found to be 76.89%. The Confusion Matrix values obtained from the model are given in Fig16.



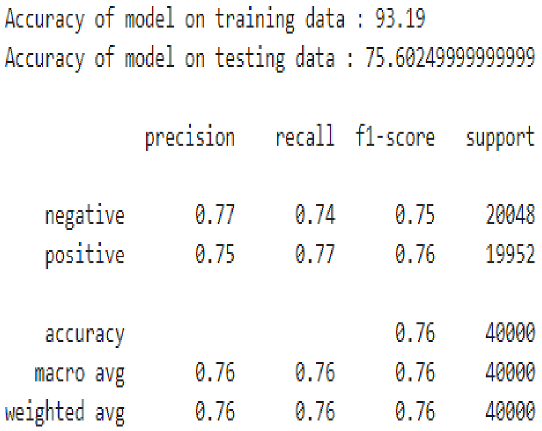
```
Accuracy of model on training data : 83.60562499999999
Accuracy of model on testing data : 76.8875

              precision    recall  f1-score   support

    negative       0.79      0.74      0.76     20048
    positive       0.75      0.80      0.77     19952

    accuracy                           0.77     40000
   macro avg       0.77      0.77      0.77     40000
weighted avg       0.77      0.77      0.77     40000
```

Fig.17. Logistic Regression Confusion Matrix

The SVM classifier model is used on the twitter1.6M dataset and the prediction accuracy of sentiment analysis on the given dataset is calculated and it is found to be 75.60%. The Confusion Matrix values obtained from the model are given in Fig17.



www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022



```
Accuracy of model on training data : 93.19
Accuracy of model on testing data : 75.60249999999999

              precision    recall  f1-score   support

    negative       0.77      0.74      0.75     20048
    positive       0.75      0.77      0.76     19952

    accuracy                           0.76     40000
   macro avg       0.76      0.76      0.76     40000
weighted avg       0.76      0.76      0.76     40000
```

Fig.18. SVM Confusion Matrix

7. MODEL COMPARISON

In the Model Comparison section, we display the results of our sentiment analysis tests using different Machine Learning & Deep Learning models. Aside from testing our CNN-Bi-LSTM and Bi-LSTM-CNN models, we also compare them with standard Bi-LSTM added with an extra dropout layer and then finally with LSTM networks. Furthermore, in our proposed work we also added the accuracy outcomes of our previous work which are carried out by ML classifiers (SVM,NB,RF) and Logistic Regression.

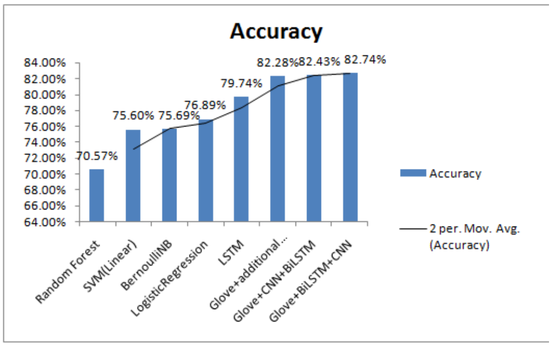


Fig.19. Model Accuracy Comparison

8. FUTURE WORK

For executing the deep learning models like ELMO and BERT, GPU and RAM requirements are very high. We were not able to fulfill these demands. So that's why we were tried to cut down the number of data sets to be used. If anyhow we could manage to increase the number of data sets, then results from inaccuracy would have been improved and the results would have been slightly different. Comparing its performance with BERT will be interesting.

9. CONCLUSION

In this proposed work, we have presented two models that aim to combine Bi-LSTM and CNN neural networks to obtain better performance on sentiment analysis by a quite good margin. Our CNN-Bi-LSTM model does 2.69% better than a regular LSTM model. On the other hand, the Bi-LSTM-CNN model does 3% better than a regular LSTM model and 7.05% better than a Bernoulli NB model. We hope that this proposed model may aid the future development of accurate sentiment analysis tools. The outcomes of all four machine learning models are evaluated, and the one that classifies the sentiment analysis the best is picked. The Bi-LSTM+CNN model was compared to LSTM, CNN+Bi-LSTM, and all four machine learning algorithms in the results obtained from the comparison of machine learning models, and based on the strong evidence from the results obtained, it can be concluded that the Bi-LSTM+CNN model classifies the sentiment analysis of the selected Twitter dataset with the highest accuracy. The consequences of the findings are examined, with substantial evidence indicating that the outcomes are correct. Threats to validity are also discussed in terms of the severity of the problem and how it might be overcome. The goal of this study is to find the best-fit algorithm for the chosen dataset for sentiment analysis of Twitter data classification. Monitoring and analyzing tweets are aided by the outcomes of the study, and valuable feedback for companies is supplied. This algorithm can be used to determine a user's opinion or sentiment. This algorithm decreases the computational complexity of the selected dataset by improving prediction performance, reducing time complexity in data prediction, and reducing time complexity in data prediction.

REFERENCES

[1] Ramos, C., , J.C. and Shapiro, D., 2008. Ambient intelligence—the next step for artificial intelligence. IEEE Intelligent Systems, 23(2), pp.15-18.

[2] "Comparative Study of Machine Learning Approaches for Amazon ScienceDirect."[Online]. Available:

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

[Accessed:2019]. https://www.ScienceDirect.com/science/article/PII/S1877050918308512.

[3] O'Shea, T. and, J., 2017. An introduction to deep learning for the physical layer. IEEE Transactions on Cognitive Communications and Networking, 3(4), pp.563-575.

[4] H., Deng, L., Y., J., He, X., Chen, J., Song, X. and Ward, R., 2016. Deep sentence embedding using long short-term memory networks: Analysis and application to information retrieval. IEEE/ACM Transactions on Audio, Speech, and Language Processing, 24(4), pp.694-707.

[5] “Random Forest and Support Vector Machine based Hybrid Approach to Sentiment Analysis - Science Direct.” [Online]. Available:2019

[6] D. L. and F. K. Espinoza-Vasquez, "From networked nominee to the networked nation: examining the impact of web 2.0 and social media on political participation and civic engagement in the 2008 campaign," J. Political Marketing, vol. 10, no. 1-2, pp. 189–213, Feb. 2011.

[7] Merriam-Webster, Merriam-Webster’s Collegiate Dictionary. Springfield, MA: Merriam-Webster, 2004.

[8] B., "Sentiment analysis and opinion mining," Synthesis Lectures on Human Lang. Tech., vol. 5, no. 1, pp. 1–167, Apr. 2012.

[9] A. Go, R. Bhayani, and L. Huang, “Twitter Sentiment Classification uses DistantSupervision,”p. 6.

[10] C. and R., "Learning to identify emotions in text," in . 2008 ACM., Brazil, 2008, pp. 1556–1560.

[11] Govindarajan, M, "Sentiment analysis of movie reviews using a hybrid method of naive Bayes and geneticalgorithm.”

[12] B. Yang and C. Cardie, "Context-aware learning for sentence-level sentiment analysis with posterior regularization." in. 52nd. Meeting on Assoc. Computational Linguistics, Baltimore, 2014, pp. 325–335.

[13] M. and B., "Mining and summarizing customer reviews," in . 10th ACM SIGKDD Int. . Knowledge Discovery and Data Mining, Seattle, WA, 2004, pp. 168–177. 47 48

[14] T. Wilson, J., and P., "Recognizing contextual polarity in phrase-level sentiment analysis," in . . Human Lang. Tech. Empirical Methods in Natural Lang. Process., Vancouver, B.C., Canada, 2005, pp. 347–354.

[15] T. Wilson, J., and R., "Just how mad are you? strong and weak opinion clauses," in. 19th Nat. . ., vol. 4, San Jose, CA, 2004, pp. 761–769.

[16] Z., D., and B. Yuan, "Context-dependent sentiment classification using antonym pairs and double expansion," in Web-Age Inform. Manage., China, 2014, pp. 711–722.

[17] N. and B., "Mining comparative sentences and relations," in . 21st Nat. . ., Boston, MA, 2006, pp. 1331–1336.

[18] A. and F., ": a publicly available lexical resource for opinion mining," in . Lang. Resources and Evaluation ., Genoa, Italy, 2006, pp. 417–422.

[19] P. J. Stone, D. C., and M. S. Smith, "The general inquirer: a computer approach to content analysis." in. Spring Joint. ., New York, NY, 1966, pp. 241–256.

A NOVEL VIEW ON RAINFALL PREDICTION MANAGEMENT SYSTEM

Anusha J[1], Chandan N[2]

[1,2]Department of Computer Science and Engineering, BITM, Ballari, India.

E-mail: anushamrb@gmail.com[1], chandann@gmail.com[2]

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Abstract- India Meteorological Department (IMD) has upgraded the Agro-Meteorological Advisory Service from agro climate zone to district level. IMD started issuing district level weather forecasts from 1 June 2008 for meteorological parameters such as rainfall, maximum and minimum temperature, relative humidity, surface wind and cloud octa up to 5 days in quantitative terms. In present studies rainfall prediction was based on NWP Numerical Weather Prediction methods are used which has given better results and played important role. The Multi-Model Ensemble (MME) technique is used for high resolution rainfall forecasts over Indian region. At 50 km resolution, Multi-Model Ensemble (MME) could cover only 250 districts. The results of the study motivated authors for further research to increase the forecast period and model resolution using improved rainfall outputs. This was done to meet the operational requirement of farming community during monsoon 2009.

Keywords— RailFall, Numerical Weather Prediction (NWP) Models, Multi-Model Ensemble (MME).

1. INTRODUCTION

Data prediction and analysis has created lot of scope in different areas for improving better services. Comparing to existing models developed using NWP for rain fall prediction machine learning based models are giving better accuracy. Machine learning provides option for dealing with structured and unstructured data with effective predictive models. Rain fall forecasting is one of the most important analysis and prediction method which is required for predicting upcoming rainfall in coming years based on previous dataset. In this project past 10 years dataset for different states and districts are taken as input and weather forecast is predicted. In present studies rainfall prediction was based on NWP numerical weather prediction methods are used which has given better results and played important role. Even though this methods are used in present systems there are many areas accuracy can be increased like dealing with Indian monsoon. This is because large variation of data at different times and limitation of NWP models.

There has been long demand from the user community for district level quantitative weather forecasts in short to medium range time scale. The quantitative rainfall forecast for smaller spatial distribution such as district level over highly complex inhomogeneous region like India is a very challenging task. For the generation of district level quantitative rainfall forecasts, one has to depend on the forecasts from dynamical Numerical Weather Prediction (NWP) models. During the last two decades, NWP methods have acquired greater skills and are playing an increasingly important role in the operational weather forecasting. But rainfall prediction skill of NWP models is still not adequate to satisfactorily address detailed aspects of Indian summer monsoon. This is because of large spatial and temporal variability of rainfall and some inherent limitations of NWP models. There are various factors like topography, prevailing synoptic situation and its interaction with mesoscale systems, lack of observations, etc., are some of the key factors which pose difficulties for numerical weather prediction of any region, and so Indian region is not an exception. Considering the need of farming sector, India Meteorological Department (IMD) has upgraded the Agro-Meteorological Advisory Service from agro climate zone to district level. As a major step, IMD started issuing district level weather forecasts from 1 June 2008 for meteorological parameters such as rainfall, maximum and minimum temperature, relative humidity, surface wind and cloud octa up to 5 days in quantitative terms. These forecasts are generated through Multi-Model Ensemble (MME) system making use of model outputs of state-of the-art

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

three global models from the leading global NWP centers. These forecasts are made available on the national website of IMD. During summer monsoon 2009, the number of ensemble members is increased from three to five. In the present study, we describe the development strategy of the MME technique, used for high resolution rainfall forecasts over Indian region and demonstrate the prediction skill of the technique during summer monsoon 2009. In our previous study, performance skill of MME at 50 km horizontal resolution for district level short range rainfall forecasts during summer monsoon 2007 was demonstrated from the use of four coarser grid models namely (i) IMD limited area model at 75 km horizontal resolution, (ii) IMD MM5 at 45 km horizontal resolution, (iii) National Centre for Medium Range Weather Forecasting (NCMRWF) MM5 at 30 km resolution, and (iv) NCMRWF T-80 (grid space ~156 over the tropics). At 50 km resolution, MME could cover only 250 districts. The encouraging results of the study motivated authors for further research to increase the forecast period and model resolution using improved rainfall outputs of state-of-the-art high resolution global models from leading NWP centers to meet the operational requirement of farming community.

2. LITERATURE SURVEY

Improved Weather And Seasonal Climate Forecasts From Multimodel Super Ensemble[1]. India Meteorological Department has implemented district level medium range rainfall forecast system. System uses multimodal ensemble technique, making use of model outputs of state-of-the-art global models from the five leading global NWP centres. In this paper, we describe the development strategy of the technique and performance skill of the system during summer monsoon 2009. The study demonstrates the potential for improving rainfall forecasts over Indian region. Improving Tropical Precipitation Forecasts From A Multi Analysis Super Ensemble[2]. This paper utilizes forecasts from a multianalysis system to construct a super ensemble of precipitation forecasts. The method partitions the computations into two time lines. The first of those is a control (or a training) period and the second is a forecast period. The results for day 1, day 2, and day 3 forecasts are compared to various conventional forecasts with a global model. Day 3 forecasts clearly have the highest skill in such comparisons.[3] Experimental Realtime Multi-Model Ensemble (Mme) Prediction Of Rainfall During Monsoon 2008: Large Scale Medium Range Aspects Multi-model ensemble (MME) forecasting is gaining popularity, as it has the potential to provide more information for practical forecasting in terms of making a consensus forecast and handling model uncertainties. During monsoon 2008, on an experimental basis, an MME forecasting of large-scale monsoon precipitation in the medium range was carried out in real-time at National Centre for Medium Range Weather Forecasting (NCMRWF), India. The skill score for the Indian domain and other sub-regions indicates that the BCEMn produces the best result, compared to EMN and MME. For higher rainfall values, the skill of the global model rainfall forecast decreases rapidly beyond day-3.[4] High Resolution Daily Gridded Rainfall Data For Indian Region: Analysis Of Break And Active Monsoon Spells Researchers developed a very high resolution (0.5° x 0.5 °C) daily rainfall data-set for mesoscale meteorological studies over the Indian region. The dataset was developed using quality-controlled rainfall data from more than 3000 rain gauge stations over India. Since the data density is not kept uniform, there is a possibility of temporal in homogeneity and cannot be used for trend analysis.[5] Rainfall Analysis For Indian Monsoon Region Using The Merged Rain Gauge Observations And Satellite Estimates Analysis of daily rainfall at the resolution of 1° grid for the Indian monsoon region has been carried out. This daily analysis, being based on high dense rain gauge observations was found to be very realistic and able to reproduce detailed features of Indian summer monsoon. When this product was used to assess the quality of other available standard climate products (CMAP and ECMWF reanalysis) at the gird resolution of 2.5°, it was found that the orographic heavy rainfall along Western Ghats of India was poorly identified by them.

3. OBJECTIVES

- The main motive of the paper is to predict the amount of rainfall in a particular division or state well in advance. We predict the amount of rainfall using past data.

- Design machine learning based prediction model for prediction rain fall by taking past 15 years data from different stats and districts.

4. IMPLEMENTATION

Implementation is the stage in the project where the theoretical design is turned into a working system and is giving confidence on the new system for the users that it will work efficiently and effectively. It involves careful planning, investigation of the current system and its constraints on implementation, design of methods to achieve the changeover, an evaluation of change over method. Apart from planning major task of preparing the implementation are education and training of users. The implementation process begins with preparing a plan for the implementation of the system.

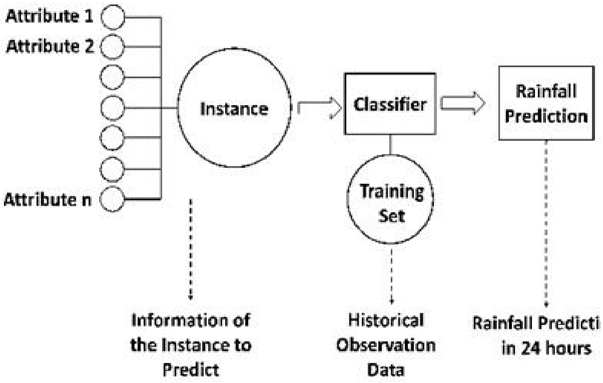

Attribute 1
Attribute 2
Attribute n
Instance
Classifier
Rainfall Prediction
Training Set
Information of the Instance to Predict
Historical Observation Data
Rainfall Predicti in 24 hours

Fig.1. Structure of rainfall

According to this plan, the activities are to be carried out, discussions made regarding the equipment and resources and the additional equipment has to be acquired o implement the new system. Implementation is the final and the most important phase. The most critical stage in achieving a successful new system is giving the users confidence that the new system will work and be effective. The system can be implemented only after thorough testing is done and if it is found to be working according to the specification. This method also offers the greatest security since the old system can take over if the errors are found or inability to handle certain type of transactions while using the new system.

Screen Shots are shared below:

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

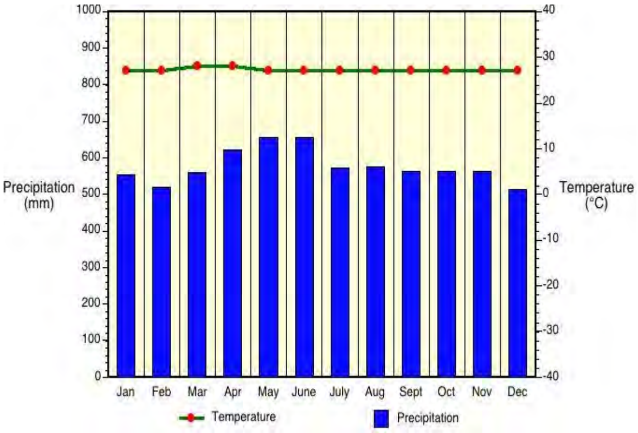


Fig.2. Amounts of rainfall over the reasonably months

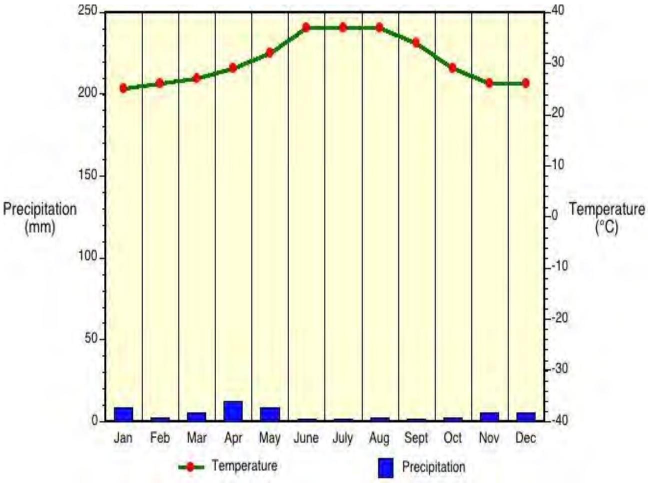


Fig.3. Distribution of rainfall over months

5. CONCLUSION

Various visualizations of data are observed which helps in implementing the approaches for prediction.

• Prediction of amount of rainfall for both the types of dataset.
• Observations indicate machine learning models won't work well for prediction of rainfall due to Fluctuations in rainfall.

Results of this study showed that all these models, in general, have the capability to capture large scale rainfall features of summer monsoon, such as heavy rainfall belt along the west coast, over the domain of monsoon trough and along the foothills of the Himalayas. It has clearly emerged from the results of the skill score that MME is superior to each member model. For the district level forecast, the procedure has showed appreciable skill to predict occurrence and non-occurrence of rainfall, as well as for the rainfall category of moderate rainfall. But it fails to capture heavy rainfall events. Otherwise, performance of the district level forecast for most of the districts has been fairly good, particularly over the monsoon affected states.

REFERENCES

[1] Brooks H E and Doswell C A 2017 New technology and numerical weather prediction; Weather 48 173–177. Krishnamurti T N, Kishtawal C M, Larow T, Bachiochi D, Zhang Z, Willford E C, Gadgil S and Surendran S 1999 Improved weather and seasonal climate forecasts from multimodel super ensemble; Science 285 1548–1550.

[2] Krishnamurti T N, Kishtawal C M, Shin D W and Willford E C 2018 Improving tropical precipitation forecasts from a multi analysis super ensemble; J. Climate 13 4217–4227.

[3] Mishra A K and Krishnamurti T N 2007 Current status of multi-model super-ensemble operational NWP forecast of the Indian summer monsoon; J. Earth Syst. Sci. 116(5) 1–16.

[4] Mitra A K, Iyengar G R, Durai V R, Sanjay J, Krishnamurti T N, Mishra A and Sikka D R 2011 Experimental realtime multi-model ensemble (MME) prediction of rainfall during monsoon 2008: Large scale medium range aspects; J. Earth Syst. Sci. 120(1) 27–52. Rajeevan M, Bhate J, Kale J D and Lal B 2018 High resolution daily gridded rainfall data for Indian Region: Analysis of break and active monsoon spells; Curr. Sci. 91(3) 296–305.

[5] Rajeevan M and Bhate J 2009 A high resolution daily gridded rainfall dataset (1971–2005) for meso-scale meteorological studies; Curr. Sci. 96(4) 558–562. Roy Bhowmik S K and Das Ananda K 2007 Rainfall analysis for Indian monsoon region using the merged rain gauge observations and satellite estimates: Evaluation of monsoon rainfall features; J. Earth Syst. Sci. 116(3) 187–198.

[6] Roy Bhowmik S K and Durai V R 2008 Multimodel ensemble forecasting of rainfall over Indian monsoon region; Atmosfera 21(3) 225–239. Roy Bhowmik S K and Durai V R 2010 Application of multimodel ensemble techniques for real-time district level forecasts in short range time scale over Indian region; Meteor. Atmos. Phys. 106 19–35.

[7] Roy Bhowmik S K, Durai V R, Das Ananda K and Mukhopadhaya B 2009 Performance of IMD multi-model ensemble based district level forecast system during summer monsoon 2008; Meteorological Monograph Synoptic Meteorology No. 8/2009, India Meteorological Department, New Delhi, 43p.

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

A SECURE INCREASED KEY POLICY ATTRIBUTE IN CLOUD COMPUTING

V Swathi[1], M P Vani[2]

[1,2]School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology, Vellore, India
E-Mail: swathivelugoti@gmail.com[1], mpvani@vit.ac.in[2]

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Abstract- Attribute-based keyword search (ABKS), is a very important sort of searchable coding, has been widely used for secure data storage in cloud during a key policy attribute-primarily based temporary keyword search (KP-ABTKS) theme, a non-public secret's related to associate degree access policy that monitors the ability search of the user, whereas an exploration token is related to a amount that monitors the search time of the cloud server. However, once a careful study, we tend to uncover that the sole existing KP-ABTKS construction [1] isn't secure. Through two fastidiously designed attacks, we tend to first show that the cloud server will search the encrypted text in any time. As a result, their theme cannot support temporary keyword search. to deal with this drawback, we tend to gift associate degree increased KP-ABTKS theme and prove that it's by selection secure against chosen-keyword attack within the random oracle model. The planned theme achieves each fine-grained search management and temporary keyword search at the same time. Additionally, the performance analysis indicates that our theme is sensible. The objective of the study is to support temporary keyword search. For that we've got planned increased KP-ABTKS theme and prove that it's by selection secure against chosen-keyword attack within the random oracle model.

Keywords— Cloud Computing, Attribute Based Keyword Search, Key Policy Attribute, Keyword Attack.

1. INTRODUCTION

Cloud computing is associate degree rising web technique that gives unlimited computing and mass service of storage for people and corporations. Being a big service of security in cloud computing, cloud storage will work with efficiency and privacy in data and notice knowledge sharing. because of its cheapness and convenience, additional and additional knowledge house owners store their sensitive knowledge within the cloud. However, this causes vast considerations for the reveal of the sensitive knowledge, as a result of {the knowledge the info the information} house owners lose management over the native knowledge after they source the data to the cloud. For instance, data related to personnel, email knowledge and monetary documents keep in iCloud could also be managed by the attacks from intruders and also the legal issues faced by the cloud vendor. One methodology for securing sensitive knowledge is to convert the knowledge and transfer encrypted text to the cloud. However, ancient coding techniques build knowledge, but the users can't access those techniques while retrieving the data. to deal with this issue, Boneh et al. the construct of public key coding based on keyword search (PEKS), this may succeed knowledge confidential and searchable at the same time. during a PEKS theme, {the knowledge the info the information} house owners write the keyword of every file and store the encrypted data within the cloud; the cloud server World Health Organization contains a search token related to a keyword will retrieve data by testing based on the token of search and also the encrypted text corresponds to a keyword which is similar to search.

Basically, PEKS are able to do knowledge confidential and searchable at the same time, it cannot support the user at the time of accessing and also the permissions related to data retrieval. to deal with this drawback, Zheng et al. planned the model of attribute-based keyword search (ABKS) supported PEKS and attributed-based coding (ABE). In ABKS, an exploration token is related to associate degree access policy (resp., attributes) and a ciphertext is related to attributes (resp.,

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

associate degree access policy); a user will retrieve the encrypted text only if the attributes satisfy the access policy related to a search token.as an example, think about a personnel health record cloud system supported ABKS, every personnel health record consists of a medical information and a keyword. A patient solely permits the feminine doctors to go looking his or her medical information by encrypting the keyword with a policy ("Doctor" AND "Female"). However, once the cloud server has the search token in ABKS schemes, it will search the old data and future encrypted texts, which can cause privacy escape. to improve the protection of ABKS, Ameri et al given the model of key-policy attribute-based temporary keyword search (KPABTKS) during which the search token will solely be utilized in a amount instead of any time. during a KP-ABTKS theme, an exploration token is labeled with associate degree access policy and an amount, whereas a ciphertext is labeled with attributes associate degreed an encrypting time; the search token can solely enable the cloud server to retrieve the ciphertext once the attributes satisfy the access policy and also the amount contains the encrypting time. Ameri et al planned the primary construction of KP-ABTKS and claimed their construction (we consult with as ADMS for short) is by selecting secure against chosen-keyword attack. However, once fastidiously finding out, we discover the ADMS construction isn't safe, and existing ABKS schemes cannot succeed fine- grained search management and temporary keyword search at the same time.

Cloud computing plays a very important role in our way of life, as a result of it provides effective, reliable and ascendable resources to store knowledge and procedure activities at a really low value. However, the users directly access the cloud for sensitive information which threatens their privacy. A trivial resolution to deal with this drawback is converting the knowledge to encrypted form before outsourcing it to the cloud. However, looking on the encrypted knowledge is incredibly tough. In Key-Policy Attribute primarily based Temporary Keyword Search (KP-ABTKS) schemes, the information owner generates an exploration able cipher text associated with a keyword and also the time of encrypting in step with associate degree absolute amount and generates a search token for supposed keyword to search out the cipher text. Then, he/she sends the token which is generated by the access policy to the cloud to run the search operation. By receiving the token, the cloud appearance for the documents contains the keyword which is to be supposed. The search result on a encrypted text is acceptable if

- the information related to user's attributes satisfies the access management policy,
- The amount of the search token encampments the time of encrypting, and
- The search token and also the encrypted text field associated with a appropriate keyword.

To accomplish the planned notion, we tend to additionally propose a concrete internal representation for this new scientific discipline primitive supported linear map. we tend to introduce the novel notion of KP-ABTKS, and propose a concrete construction for this new scientific discipline primitive which might be applied within the cloud storage services. The planned concrete theme is meant supported linear pairing. within the planned KP-ABTKS, every user is known with associate degree access management policy. the information owner selects associate degree attribute set, and runs the coding algorithmic program with relation to it. If an information user's attributes set satisfies the access tree of the information owner, then he/she will generate a legitimate search token. The cloud applies the generated search token to search out the corresponding cipher texts that are encrypted during a amount such that by the information user. we tend to formally outline 2 security definitions for KPABTKS within the commonplace model. one amongst them defines its security against by selection chosen keyword attack (KPABTKS-SCKA), and also the different one defines the keyword secrecy of KP-ABTKS. we tend to formally prove that our planned theme satisfies these security definitions beneath the hardness of the Decisional Diffe- dramatist (DDH) assumption.

We given a secure KP-ABTKS theme within the prime order teams, that achieves fine-grained search management and temporary keyword search and temporary keyword search at the same time. additionally, the performance analysis indicates that our theme is sensible. The objective of the study is to support temporary keyword search. For that we've got planned increased KP-ABTKS theme and prove that it's by selection secure against chosen-keyword attack within the random oracle model.

2. ADMS

The existing KP-ABTKS theme, particularly ADMS, by presenting 2 fastidiously designed attacks against ADMS theme, we tend to showed that the cloud server will retrieve the ciphertext created in any time that causes the ADMS theme insecure. Through two fastidiously designed attacks, we tend to first show that the cloud server will search the ciphertext in any time. As a result, their theme cannot support temporary keyword search.

Disadvantages

- Less secure.
- didn't attain keyword search.

3. Secure KP-ABTKS

In this work, we tend to implement our secure KP-ABTKS construction and compare its performance with different connected works. The comparison and experimental results show that our theme is economical and sensible. we tend to gift associate degree increased KP-ABTKS theme and prove that it's by selection secure against chosen-keyword attack within the random oracle model.

Advantage

- Secure against attacks.
- Achieves keyword search management.

4. KP-ABTKS theme

In this work, we tend to style possible attacks against ADMS theme and construct a safe increased KP-ABTKS theme. the most contributions area unit summarized as follows: we tend to first suggests that ADMS theme isn't secure by constructing 2 complete attacks. within the first attack, by modifying the recent search token, the cloud server will construct a replacement search token which will be utilized in any fundamental measures. Within the second attack, we tend to show that anyone will amendment the encrypting time to anytime he needs. As a result, albeit a cipher text isn't created within the amount that the search token is related to, it also can be searched by this search token. Hence, alike with different ABKS schemes, the ADMS theme cannot support temporary keyword search. we offer a construction of KP-ABTKS and prove that it's by selection secure against chosen-keyword attack within the random oracle model. In our system, an information user's secret secret's admire associate degree access tree, and an information owner will management the search permission by encrypting the keyword with attributes. an information user will source the temporary keyword search operations to the cloud by making an exploration token that's admire associate degree access tree and a amount. The cloud server will search the encrypted knowledge only if the attributes satisfy the access tree and encrypting time is enclosed within the amount at the same time. To the simplest of our information, this is often the primary public key coding that achieves attribute primarily based search management and temporary keyword search at the same time. we tend to implement our KP-ABTKS construction and compare its performance with different connected works. The comparison and experimental results show that our theme is economical and sensible. In a key-policy attribute-based temporary keyword search (KP-ABTKS) theme, a non-public secret's related to associate degree access policy that controls the search ability of the user, whereas an exploration token is related to a amount that controls the search time of the cloud server. but we tend to uncover that the sole existing KP-ABTKS construction isn't secure. Through 2 fastidiously designed attacks, we tend to 1st show that the cloud server will search the cipher text in any time. As a result, their theme cannot support temporary keyword search.

5. Enhanced KP-ABTKS Theme

We gave a secure KP-ABTKS theme within the prime order teams that achieves fine-grained search management and temporary keyword search. In our implementation, the text area is allowed to go looking the cipher text once their attributes satisfy the access tree, whereas the cloud server is just allowed to go looking the cipher text during a limit amount. Finally, we tend to give the protection and performance analysis to point out that our theme is secure and sensible.

6. Architecture

In this work authority will a login. Authority can facilitate the attackers it'll send

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

search response. Authority also can a read files within the cloud computing. Authorities will read users within the information. Authority have read house owners within the cloud computing. User will login within the cloud server. Cloud server contains a take a look at tokens generation. Cloud server additionally contains a delete tokens. User can have associate degree own knowledge. Within the knowledge owner 1st register all the user details within the information.

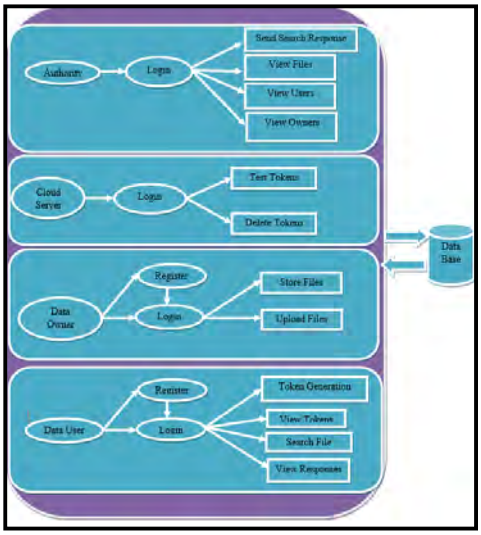


Fig.1. System Architecture Diagram of a Secure Enhanced KPABTK

7. CONCLUSION

In this research, we tend to first mentioned the prevailing KP-ABTKS theme particularly ADMS. By presenting two fastidiously designed attacks against ADMS theme, we tend to showed that the cloud server will access the encrypted text originated in any time that causes the ADMS theme insecure. Then, we tend to given a secure KP-ABTKS theme within the prime order teams that achieves fine-grained search management and temporary keyword search. In our construction, the use area unit allowed to go looking the encrypted text once their attributes satisfy the access tree, whereas the cloud server is just allowed to go looking the encrypted text during a prescribed amount. Finally, we tend to give the protection and performance analysis to point out that our theme is secure and sensible.

REFERENCES

[1] M. H. Ameri, M. Delavar, J. Mohajeri, and M. Salmasizadeh, "A key policy attribute-based temporary keyword search scheme for secure cloud storage," IEEE Transactions on Cloud Computing, pp. 1–1, 2018.

[2] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public keyencryption with keyword search," in International conference on the theory and applications of cryptographic techniques. Springer, 2004, pp. 506– 522.

[3] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attribute-based keyword search over outsourced encrypted data," in IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, 2014, pp. 522–530.

[4] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute- based keyword search with fine-grained owner-enforced search authorization in the cloud," in IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, 2014, pp. 226–234.

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2005, pp. 457–473.

[6] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006, pp. 89–98.

[7] J. Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policy attribute-based encryption," in 2007 IEEE symposium on security and privacy (SP'07). IEEE, 2007, pp. 321–334.

[8] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in International Workshop on Public Key Cryptography. Springer, 2011, pp. 53–70.

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

CLOUD GAMING USING THIN CLIENT

M A Ghaffar[1], Arshiya Naheed[2]

[1]Department of Computer Science (Data Science)- GITAM University, Hyderabad, India.
[2]Intern Analyst at Deloitte, Hyderabad, India.
E-mail: Ghaffar.ma2003@gmail.com[1], Arshiyanaheed98@gmail.com[2]

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Abstract- Cloud Gaming using Thin Client can be described as the unloading of a game logic in the cloud. And game can be rendered as a video streaming. This video stream is transferred to the user. The remote server receives user instructions from thin client. The remote server executes the game logic. Modified game scene is sent back to the user. This game scene is in the form of a video, which is decoded at the client-end. People gets help from this scheme, so that they can play games on their system irrespective of the machine. Cloud gaming further helps to overcome traditional gaming problems like unsuitability and movability. Cloud gaming using Thin Client is different from that of online gaming in performing the logic of the main game. Game logic performed at the server-end and also at the client-end. This paper, presents diverse features of cloud gaming that are deliberated to elucidate the several rewards and influencing this concept. In this paper parameters related to Quality of Service (QoS) in detail.

Keywords- Cloud, Quality of Service (QoS), Thin Client, System Architecture.

1. INTRODUCTION

Remote sources are used to play games on the local system.Thin client is used to send input events. After executing game logic on the remote server, the input sprang back to client in the form of a video [1].This videois played with the help of the thin client [1]. The games, in generalare graphically substantial and henceforth are in demand for new computer hardware which can encounter these high-end requirements [1]. This limitation affects the discrete gamer. The gamer tries to improve computer hardware whenever a new incompatible version of a game is released [1]. Likewise, the system hardware or software unsuitability and the extra time and exertion needed in making the game is also need to be improved. The Gamercan access the cloudhardware in cloud gaming,thus exterminating the need to adjust their hardware, download the game or bother about incompatibility of Hardwar /Software. Additional note worthy benefit is that the gamers can play these games on any arrangement such as computer system, Smartphone [5]. And games can be played even on televisions with Set-top boxes, provided reliable adequate internet connectivity [5].There is a noteworthy difference between the Cloud Computing and online gaming [5]. Online games can take benefit of far-off sources that are oncloud, still, game logic is executed at the client-end only.The servers are able to manage the reliability between the states of several games played on it [1]. In the design of cloud games, the execution of logic is done at the server-end [1].

2. BENEFITS OF CLOUD GAMIN USING THIN CLIENT

Let's take an example of a racing game, "Forza Horizon 4". The minimum requirement to run this game on any device is (a) Quad-Core Processor with 8GB RAM, (b) 64GB memory, and (c)NVidia 650TI or NVidia GT 740 OR AMD R7 250x graphics card, which is seriously expensive. The recently launched Computersnot even encounter these requirements. The mobiles and Computers don't have the same design, have same power limitations, diverse OS. We can solve all these using Cloud Gaming using thin client. The Cloud Gaming using thin client bidsis a benefit of better Digital Rights Management (DRM) [1].In this hardware being used is managed by the owner of the cloud system rather than the user [1]. Cloud gaming is a complex project, users might not understand the remote performance of the main game logic [1].

3. WORKING OF CLOUD GAMING

Usually, there are three types of remote translation methods in the real-time:

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

a) Streaming of 3-D Graphics
b) Streaming of Video
c) Streaming of Video using post-Rendering techniques

Streaming of 3-D Graphics: In this system, the cloud server sends the graphics-related commands to the client, interpret them and tends render the scene accordingly [1]. Streaming of Video: In this the server generates the 3D controls, changes them to 2D, and sends the video stream to the client [1].

Streaming of Video using post-Rendering techniques:. Here the huge work of rendering the 3D graphics is done at server while some low processor-exhaustive work is accomplished on the client-side via Thin Client [1].Aiming at distributed gaming systems, there have been many thin client designs. These are divided into two sections referred as instruction-based systems and image-based systems. There are few differences between the two systems. In instruction-based systems, only the instructions for generating the graphics corresponding to control event are sent over the network [1]. In contrast, in image-based systems, each computationally intensive rendering of the game scene is completed on the server-side and sent over the network in the form of a video stream. CGSs use image-based thin client designs because they don't require computing resources from the client . This is the main benefit of cloud gaming.

What is a thing client: It has User Interaction module and a video decoder . The User Interaction module captures all the control movements performed by the end-user with the help of input device like a mouse or keyboard. In response to the players actions, the video decoder plays the video.

There are four modules:

i) Thin Client Interaction
ii) Game Logic
iii) GPU Rendererand
iv) Video Encoder.

Thin client interaction: This module handles all the client commands. This module is also responsible for converting the messages. These are sent over the network into relevant game actions.

The game logic module: This module interprets messages in the game world.

GPU Renderer: This module will execute the scene.

Video Encoder: Encoder compresses scene which is sent by video streaming service, and sends this to the thin client [1]. Thus, stream is decoded and plays the video frames to the client.

Various QoS Parameters:

Cloud gaming service's benefits can be viewed from multiple perspectives. The provider's perspective, and the user's perspective. Allotting the resources is essential from the perspective of providers, and from the perspective of user the things which affect the gaming experience are essential. One need to quantify the quality of service from the time scale. Longer time scale will last multiple gaming sessions and a shorter time scale will last an individual game session.

We are focusing only on shorter timescale systems, because most of the cloud gaming systems use only a single Virtual Machine without any offloading to attend to each client [1].

Metrics focused here are-

Traffic Characteristics: The amount of bandwidth used in a single gaming session is called as traffic characteristics. This includes the payload size and packet rate .

Latency: The most crucial standard for measuring the performance of cloud gaming systems is latency. It is actually the response time of a machine [2]. It includes all the individual latencies acquired by several components.

Graphics Quality: The quality of the frames streamed over the network is crucial for the users. [3]

Measurements include the changes in quality over the varying network conditions. Streaming quality is typically measured with frame rate. The Latency quantifies game play responsiveness and it is a measure of Response Delay. Response is delayed when a user sends their command, and the appropriate game frame is shown to the user .Response Delay (RD) contains four individual delays, and they are:

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

- Network Delay (ND): It calculates the amount of time taken by a client's command to contact the server, and it also calculates the time taken by the game to contact the client [3].

- Processing Delay(PD):The time taken by the server to receive and understand the gamer's instructions. It also includes the time to encode and packetize the framerate, which is currently running for the gamer[4].

- Game Delay (GD):Calculation of time taken by the game's software to understand the gamer's action and generate the required game frame. This is the same for cloud gaming as well as standalone gaming[5] .

- Playout Delay (OD):In this we calculate the time taken by the client to receive, decode and play the current running frame .

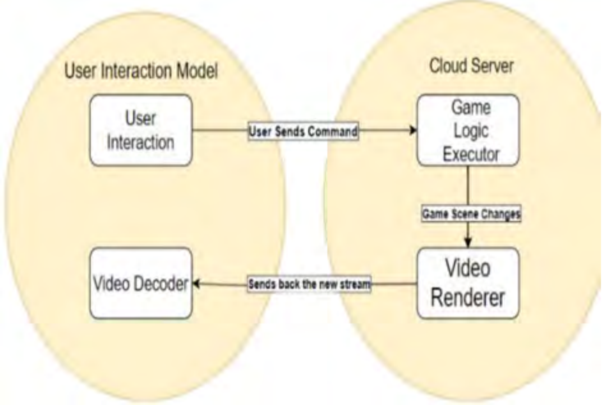


Fig.1. Cloud gaming in thin client

Using response delay we know about the quality of cloud gaming [6]. The Response delay]is calculated as the sum of Network delay, Processing delay, Game delay, and Playout delay, so

$$RD = ND + PD + GD + OD \quad (1)$$

4. CONCLUSION

This work amasses different aspects of cloud gaming and deliberates some of its characteristics. This platform is gaining much popularity in attractive graphics and dispensation of heavy games on the mobile platforms, which have fewer resources than a public computer [1]. Cloud gaming also has some shortcomings like high network latency and the effectiveness of thin client [1]. Still, future of cloud gaming looks good as network latencies are becoming shorter with faster network connections [1]. There are various cloud platforms for games in the market like stadia and PlayStation.

REFERENCES

[1] www.cpuh.in Paper submitted to Hoa Sen University Shea, R. Cloud Gaming: Architecture and Performance, Eisert, P. and Fechteler, P. 2008. Low delay streaming of computer graphics," in Proceedings of IEEE ICIP 2008. 2704–2707.

[2] Kiki Fakhri Dermawan, Rahadian Yusuf. "Moving Mixed Reality Game to the Cloud: A Survey on Feasibility" , 2020 6th International Conference on Interactive Digital Media (ICIDM), 2020 Publication.

[3] Nave, I., David, H., Shani, A., Tzruya, Y., Laikari, A., Eisert, P. and Fechteler, P. 2008. Games@Large graphics streaming architecture," in IEEE International Symposium on Consumer Electronics 2008.

[4] Claypool, M. and Claypool, K. 2006. Latency and player actions in online games. Communications of the ACM, 49: 40– 45.

[5] Shi, S., Hsu, C. Nahrstedt, K. and Campbell, R. 2011. Using graphics rendering contexts to enhance the real-time video coding for mobile cloud gaming. In Proc. of ACM Multimedia'11. 103– 112.

[6] Claypool, M. 2009. Motion and scene complexity for streaming video games," in Proceedings of the 4th International Conference on Foundations of Digital Games. ACM. 34–41.

FOREST FIRE DETECTION USING INTERNET OF THINGS

G Sreeja[1], B Sampath Kumar[2], D Kalyan[3], M Nimish[4]

[1,2, 3, 4] Department of Computer Science and Engineering, Anurag Group of Institutions,
Hyderabad, India.
E-mail: sreejacse@cvsr.ac.in[1], 17h61a05j7@cvsr.ac.in[2], 17h61a05k3@cvsr.ac.in[3], 17h61a05m7@cvsr.ac.in[4]

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Abstract- Forest Fire Accidents are main reasons for destruction of wealth of the forest. A Forest fire cause serious threat to the environment, disturbs the forest wealth, and imposes a natural disaster. The response time of emergency teams greatly affects the consequences and losses caused by them, so by implementing this forest fire detection using IoT systems can be considered a main objective for protectingthe environment. In this proposed system, the real-time monitoring of certain environmental parameters may make the forest fire prevention, detection, and fighting more efficient and cause less damage to forest wealth. Ecosystem of the forest is under high risk. The delay in reaching of the emergency services to the fire accident location may damage eco-system of the project. The proposed system detects the fire using the fire detection sensors like temperature sensor, infrared sensor, smoke sensor and the exact location of the fire in the forest which is obtained by GPS module is send to the emergency team using GSM module. This proposed IOT based forest fires detection system helps to reduce the damage to the forest due to fire. This design focuses on providing basic information on the fire accident site to the emergency contacts. As a results of the sudden help, precious forest wealth may get saved. This design detects fire accidents in less time and sends this information to the specified authorities. On account of a fire accident, with help of employed sensors the system detects an emergency and fetches the location details immediately

Keywords: Arduino, GSM Module, GPS Module, Infrared Sensor, LM35 Sensor, MQ-2 Gas Sensor, Buzzer.

1. INTRODUCTION

This proposed systemmainly focuses on providing information on the fire accident site to the emergency contacts as soon as fire occurs in the forest. As results of the sudden help, precious forest wealth may get saved. This design detects fire accidents in less time and sends this information to the specified authorities. On account of a fire accident, with help of employed sensors the system detects an emergency and fetches the location details immediately. This data along with an alert is sent to the concerned bodies through GSM module. Fire accidents happen frequently which causes huge loss of forest wealth and animals life due to the poor emergency facilities. This proposed system is a few systems which was developed to detect a fire accident and alert the emergency services regarding the location of the fire accident. With respect to this, the real-time monitoring of certain environmental variables may make the forest fire detection, and fighting more efficient. This situation prevails, just because there is a lack of emergency facility that could in time to reach the accident location in time. We are in the process of solving this issue by proposing an efficient solution and to reduce the loss of forest wealth as much as possible. This design focuses on providing basic information on the fire accident site to the emergency contacts. As a result of the sudden help, precious forestwealth may get saved. This design detects fire accidents in less time and sends this information to the specified authorities. On account of a fire accident, with help of employed sensors the system detects an emergency and fetches the location details immediately. This data along with an alert is sent to the concerned bodies through GSM module. Fire accidents happen frequently which causes huge loss of forest wealth and animals life due to the poor emergency facilities.This proposed system is a few systems which was developed to detect a fire accident and alert the emergency services regarding the location of the fire accident. This system can locate the exact co-ordinates of the fire accident so the emergency services are directed immediately towards the fire accident location. The system comprises of

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

infrared sensor, temperature sensor, smoke sensor, GPS and GSM Module support in sending message. Infrared sensor detects the fire, temperature sensor detects the temperature of the fire and smoke sensor detects the surrounding smoke occurred due to fire and GSM module sends the alert message to mobile with the situation of the accident. Location of fire accident is consigned within the kind of Google Map link, derived from the latitude and longitude from GPS module. Once the fire accident location is identified necessary action are going to be taken and this can help to achieve the rescue service in time and save the precious animal life and forest wealth.

1. RELATED WORK

In paper [1], Researchers from all around the world have conducted several studies on forest fire accidents, Ignacio Bosch, Soledad Gomez, Luis Vergara et al have proposed a paper based on a scheme of infrared sensors. This scheme based on infrared image processing performs the immediate detection of any fire in the forest to determine the presence or absence of fire. Sensor networks are widely used and help the human capabilities to monitor large forest areas. This paper describes a scheme for automatic forest surveillance with the help of IR sensors. The paper describes only about detecting the fire.

2. PROPOSED SYSTEM

Our design focuses on providing basic information on the fire accident site to the emergency contacts. As a results of the sudden help, precious forest wealth and animal's life may get saved during this work. This design detects fire accidents in less time and sends this information to the specified authorities. Fire accidents happen frequently which causes huge loss of forest wealth and animals life due to the poor emergency facilities. This proposed IOT based forest fires detection system helps to reduce the damage to the forest due to fire. This design focuses on providing basic information on the fire accident site to the emergency contacts. This design detects fire accidents in less time and sends this information to the specified authorities. The system comprises of infrared sensor, temperature sensor, smoke sensor, GPS and GSM Module support in sending message. Infrared sensor detects the flame/fire, LM35 sensor detects the temperature of the fire/flame and MQ-2 sensor detects the surrounding smoke occurred due to fire/flame and GSM module sends the alert message to mobile with the situation of the accident. Location of fire accident is consigned within the kind of Google Map link, derived from the latitude and longitude from GPS module.

Hardware Requirements:

- Arduino Micro-Controller
- GSM Module
- GPS Module
- Infrared Sensor
- LM35 Sensor
- MQ-2 Gas Sensor
- Buzzer

Software Requirements:

- Arduino IDE

3. IMPLEMENTATION

The foremost aim of the system is to develop a sophisticated system that efficiently alert concerned bodies on the account of a fire accident, providing the exact geographical location of the event, ultimately help in reducing the spread of fire reported in fire accidents. The proposed system works in two phases, within the primary phase, the Arduino monitors the pin at which the impact sensor is connected and waits for the input to urge active. within the second phase, the GPS receiver fetches the GPS location, after calculating the precise location, the GSM module helps us in sending a SMS which includes location of the accident, temperature and smoke levels and sends it to respective emergency teams. Arduino IDE: The Arduino integrated development environment could even be a cross-platform application written in Java, and derives from the IDE for the Processing programing language Arduino programs are written in C or C++. The users need only to define two functions to make an executable cyclic executive program:

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

BASIC BLOCK DIAGRAM

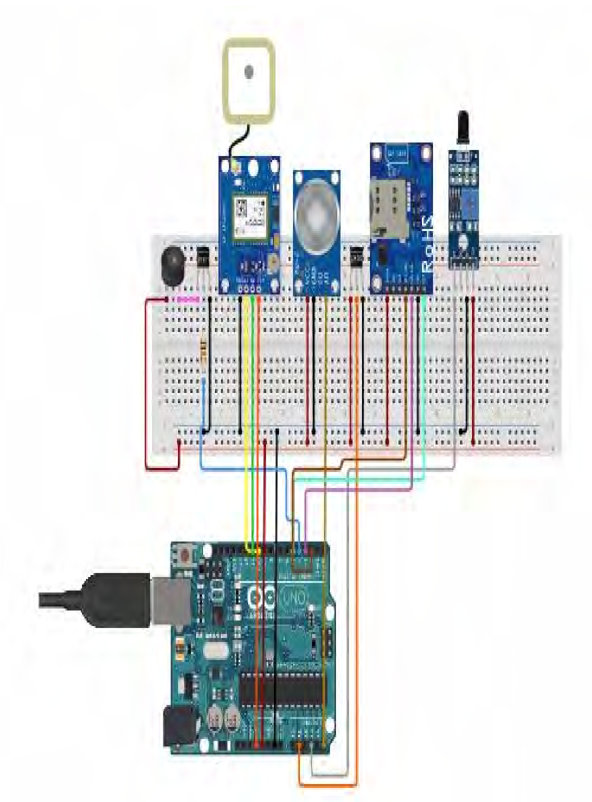


Fig. 1. Block Diagram

This paper is a few systems which is developed automatically to detect a fire accident and alert the closest emergency services.This design detects fire accidents in less time and sends this information to the specified authorities. On account of a fire accident, with help of employed sensors the system detects an emergency and fetches the location details immediately. The system comprises of infrared sensor, temperature sensor, smoke sensor, GPS and GSM Module support in sending message. Infrared sensor detects the fire/flame, LM35 sensor detects the temperature of the fire/flame and smoke sensor detects the surrounding smoke occurred due to fire/flame and GSM module sends the alert message to mobile with the situation of the accident. Location of fire accident is consigned within the kind of Google Map link, derived from the latitude and longitude from GPS module. Then after confirming the fire accident necessary action are going to be taken and this can help to achieve the rescue service in time and save the precious forest wealth and animal life.

Infrared Sensor

A flame detector sensor is used to detect the presence of a “flame or fire” which helps in detecting the fire. With the help of infrared sensor, we can detect the fire and raise an alarm and acts accordingly.It can be used to turn off the ignition system though in many cases they take no direct action beyond notifying the operator or control system.

LM35 (Temperature) Sensor

LM35is used to find the temperature of the surroundings. It is a measuring device having an analog output voltage proportional to the temperature. It provides output voltage in Centigrade i.e. degree C. The LM35 series are precision integrated-circuit temperature devices with an output voltage linearly-proportional to the Centigrade temperature. The range of LM35 device is over a −55°C to 150°C temperature range, while the range of LM35C device is −40°C to 110°C range with −10° with improved accuracy.

MQ-2 Gas Sensor

The Grove Gas Sensor (MQ2) is used to detect smoke and leakage of harmful gases such as hydrogen, liquefied petroleum gas, methane, carbon-monoxide, alcohol etc. This sensor can be used for both industrial and household purpose. Due to its high sensitivity and fast response time, measurement can be taken as soon as possible. Potentiometer is used to set the sensitivity of the sensor.

GSM Module

GSM is used to send voice messages and data in the form of SMS. GSM module is an affordable device through which we can send SMS and voice messages. User can use this device to communicate with other over internet/network, using this module user can send information to large distances. The controlling unit contains the microcontroller and also the GSM modem interfaced to that. The microcontroller continuously checks whether it's received any message from the modem. Finally, it receives the message and transmits the data to owner

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

of the vehicle. GSM module belongs to second generation mobile. This is used everywhere in this world for communicating. This module consists of sim slot where we have to place sim to make. In our project the device is used for transmitting data the info from GPS is transmitted to given mobile through this GSM itself.

GPS Module

GPS abbreviates global positioning system and this can be accustomed detect the latitude and longitude of the actual position and it also shows the precise time. It detects these values anywhere on the world. In our project it plays main role and it's the most source of the latitude and longitude of the vehicle to grasp the accident occurred location, or perhaps for theft tracking of the vehicle. A GPS receiver acquires these signals and provides the user with information. Using GPS technology, we can find location, 24 hours daily, in any type of atmospheric conditions within the world at no cost.

Overall working flow of the research

- setup(): a function that runs once at the start of a program which may initialize settings.
- loop(): This function is called repeatedly until the board powers off.
- Flowchart for accident tracking:
  - Start
  - Power on all the modules
  - await the infrared sensor to detect fire
  - Get this location from the GPS modem
  - Check whether the GSM modem is registered on the network
  - Send the SMS

This system shows the location where the fire accident has occurred with the help of the GPS module connected to it and hence that information is added in the form of latitude and longitudinal values in fire accident alerting message and reduce the loss of forest wealth and animals lives due to the delay in reaching to the emergency services in remote areas and reduces the communication gap between the emergency services in reaching the fire accident location.

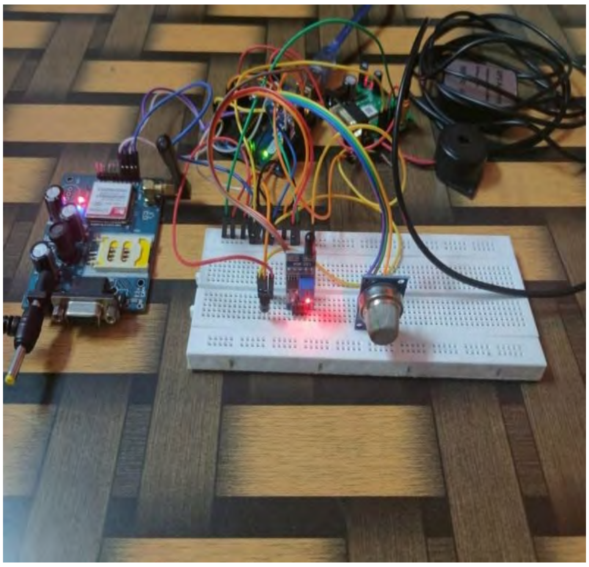


Fig. 2. Accident Tracking Connectivity

4. CONCLUSION

With the development of sensor technology, with all components, we have given the hardware connections successfully. We try our best to produce an exact data on our surroundings. Then software and hardware also interfaced effectively. We executed the hardware and we got the required output. In future, more advanced features (add a voice recognition system to make the way easier and more secured, to provide an alert message when the firebreaks out) will be integrated with this system which will provide users with more safety and relaxation. Whenever fire accident occurs, then the device sends a message with the information of fire accident location to the predefined numbers so that help can be made available. The message sent with the help of the GSM module will appear like this – 'I need help, fire accident occurred at latitude and longitude position, temperature, smoke of the surroundings and link to track exact location of accident' occurred place.

REFERENCES

[1] J. Zhang, W. Li, Z. Yin, S. Liu and X. Guo, "Forest fire detection system based wireless sensor network," 4th IEEE Conference on Industrial Electronics and Applications, 2009, pp. 520-523, doi:10.1109/ICIEA.2009. 5138260.

[2] Losso A., Corgnati L., Perona G., " Early Forest Fire Detection: Smoke Identification using Commercial Sensors", Environment Including Global Change, Palermo, Italy, 2009.

[3] Dubey V, Kumar P, Chauhan N (2018) Forest fire detection using IoT. In: International conference on innovative computing and communication (ICICC-2018)Google Scholar

[4] Bouabdellah K, Noureddine H, Larbi S (2013) Using wireless sensor networks for reliable forest fires detection. Procedia Comput Sci 19:794–801CrossRefGoogle Scholar

[5] Cantuna JG, Bastidas D, Solorzano S, Clairand J (2017) Design and implementation of a wireless sensor network to detect forest fires. In: 2017 Fourth international conference on eDemocracy & eGovernment (ICEDEG)Google Scholar

[6] Lloret J, Garcia M, Bri D, Sendra S (2009) A wireless sensor network deployment for rural and forest fire detection and verification. Sensors 9:8722–8747CrossRefGoogle Scholar

[7] Sharma A, Ansari M, Siddique M, Baig M (2017) IOT enabled forest fire detection and online monitoring system. Int J Curr Trends Eng Res (IJCTER) 3(5):50–54Google Scholar

[8] Shinde R, Pardeshi R, Vishwakarma A, Barhate N (2017) Need for wireless fire detection systems using IOT. Int Res J Eng Technol (IRJET) 4(1)Google Scholar

[9] Yu L, Wang N, Meng X (n.d.) Real-time forest fire detection with wireless sensor networks. In: Proceedings 2005 international conference on wireless communications, networking and mobile computingGoogle Scholar

[10] Sowah R, Ampadu K, Ofoli A, Koumadi K, Mills G, Nortey J (2016) Design and implementation of a fire detection and control system for automobiles using fuzzy logic. In: 2016 IEEE industry applications society annual meetingGoogle Scholar

[11] Pant D, Verma S, Dhuliya P (2017) A study on disaster detection and management using WSN in Himalayan region of Uttarakhand. In: 2017 3rd International conference on advances in computing, communication & automation (ICACCA) (Fall)Google Scholar

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

PRIVACY CLOUD STORAGE WITH DATA DYNAMICS USING PRIVATE NETWORK CODING TECHNIQUES

Gnanedra Kotikam[1], Ravi Aavula[2]

[1]Assistant Professor, Department of Computer Science and Engineering Narasaraopet Engineering College, Andhrapradesh, India.

[2]Associate Professor, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Telngana, India.

Email: k.gnanendra@gmail.com[1], aavularavi@gmail.com[2]

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Abstract- Limited Storage Cloud users can communicate their data in cloud computing age to remote servers. Instead of financial advantages, these servers provide customer data irretrievability at any moment. A customer monitors the integrity of outsourced data using cloud storage technologies. We are investigating the possibility of creating secure cloud storages for dynamic data using secure network coding techniques in this project. We demonstrated how multiple safe network coding methods may be used to create efficient, secure cloud storage protocols for dynamic data and a network secure coding protocol. DSCS I is the first secure cloud storage protocol for dynamic data, based on secure network coding methods and safe in the standard model. While generic dynamic data enable arbitrarily inserted, deleted and modified data, only supplementary data may find various real-world uses. To evaluate their performance, we created a secure DSCS II Cloud Storage Protocol (DSCS II) devoted to add-on only data that circumvents numerous DSCS limitations.

Keywords— DSCS I, DSCS II, Cloud Users, Data Owners, SNC, MAC, DPDP, PDP

1. INTRODUCTION

Cloud servers provide their customers (cloud users) numerous services with the introduction of cloud computing, including the delegation of massive volumes of computing and the outsourcing of large numbers of data. For example, a client with an intelligent gadget with a low-level processor or limited storage will be unable to do complex calculations or store large amounts of data. Under specific circumstances, she may outsource her computation/storage to the cloud server. The cloud server maintains huge data for its customers in the event of storage outsourcing (data owners). However, a rogue cloud server may remove specific client information, visited rarely for space retention. Secure cloud stock protocols are used to detect unhindered data storage from servers (two-state client-server storage protocols). These protocols are classed as secure cloud data storage techniques, based on the nature of the outsourced data. In case of static data, following the first outsourcing (e.g. backup/archival data) customers cannot alter their data. Dynamic data are general since the customer may change his data as much as necessary. The client can monitor outsourced data without accessing all data files in secure cloud storage protocols and yet identify undesirable data alteration from a rogue server. The client provides the server, during an audit, with a random difficulty producing storage evidence that meets this challenge (computed using the saved data). The use of public parameters to conduct a cloud storage audit (TPA) is publicly available for secure protocols, or privately available for auditors who need certain confidential client information. The auditors may use the public parameters. Figure 1 shows the entities engaged in and interaction with a secure cloud storage technology. A network coding protocol mixes input packages to output a different packet with each intermediary node (excluding sender / receptor nodes) over a network path.

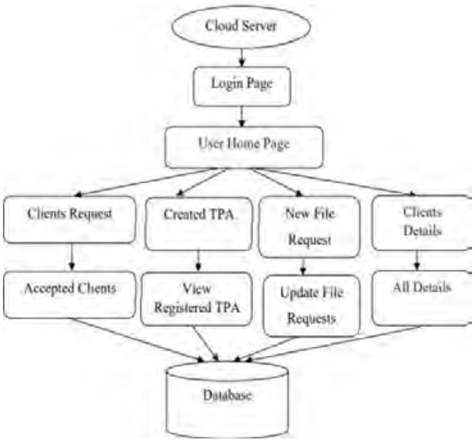


Fig. 1. DFD of DSCS protocol

These protocols have greater performance, efficiency and scalability than the storage and forward routing, but can be infected with rogue intermediate nodes that inject erroneous packages.

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Downstream more packages of this sort are generated and the receiver cannot decode the file sent by the node of the sender. Secure network coding protocols (SNC) use encryption methods to prevent such attacks. The sender authenticates each packet by sending a small tag to the network. These authentication tags are created using homomorphic MAC or homomorphic signatures. Becoming packets (and their tags) can be joined together into a packet and their tag by an intermediary node because of homomorphic feature. In the present article, we examine the challenge of creating a secure dynamic data cloud storage protocol (DSCS). We investigate if it is possible to construct an efficient DSCS protocol using an SNC protocol. In a previous piece, Chantal. Reveal a relationship between secure cloud storage and encryption of the security network. You may construct a secure cloud storage system for static information using an SNC protocol algorithm. But its structure does not deal with dynamic data — it is not enough for a client to update (insert, remove, or change) three distant data quickly in many applications. Further research are required with the aid of a secure network coding protocol (SNC) for effective DSCS development. Network coding technology has been used to build distributed storage systems that spread client data across several servers.

The main objective is to decrease the bandwidth of the repair, however, if certain servers fail. On the other side, we look at whether we can use SNC protocol techniques to build a cloud storage protocol for dynamic data that is efficient and safe (for a single storage server). Although dynamic data is broad in the sense that it supports unrestricted updating (installation, deletion and modification), the add-only data, which is put at the end of the file only, finds a number of applications. These apps retain both archive and current data largely by the addition of the current data to older databases. Examples of data collected via CCTV cameras, monetary transaction-containing ledgers, patient medical history, append only databases, etc. Data supply alone are also helpful for various log structures (e.g., certificates are stored using append-only log structures in certificate transparency schemes). The data owner wants a cloud server in many such applications to store the bulk data in a constantly recoverable way with just one change permitted. While safe cloud storage techniques also work for append only data for generic dynamic data, an even more efficient (specific to appended data files) solution would be useful.

2. PROBLEM STATEMENT

In this study, we presented a secure dynamic data cloud storage (DSCS I) protocol based on the SNC protocol. This is the first SNC-based DSCS protocol to our best knowledge, which is safe in the standard model and is publicly verified. In building an effective DSCS protocol of an SNC protocol we have highlighted several problems. We also found several constraints of the dynamic data SNC-based secure cloud storage system.

3. LITERATURE REVIEW

Cloud service providers give their customers with storage outsourcing. The integrity of customer data is preserved via a secure cloud storage (SCS) protocol. B. Sengupta and the S. Sengupta Alexandria, 2015. [1] In this study the client may update external data as required by building the publicly-verifiable cloud secure storage protocol, based on the SNC protocol. [1] [11]Our method is the first dynamic data SCS protocol to be safe in our standard model, providing privacy-reserving audits in a publically verifiable environment, to our best of our knowledge. [11] In addition, the overall structure of a dynamic data (DSCS protocol) efficient protocol may be (un)built on the arbitrary SNC protocol[12] discussed in detail. Furthermore, to facilitate privacy audits, we adapt the current DSCS system (DPDP I). Compared with previous SCS systems our DscS protocol is (including the modified DPDP I scheme). Finally, several inconveniences are highlighted in a SCS design based on the SNC protocol. Z. N. J. N. J. And D, Peterson. And D, Peterson. X. 2007 Song, and so forth. [2] A PDP paradigm is in place that enables a client who has saved data on an unconfident server to verify if the original data is available on the server without being retrievable.

A sample of random sets of server blocks create probability evidence of possession, which decreases I/O costs substantially. The customer keeps metadata to validate the evidence. [9] The protocol challenge/response sends a minimal, consistent quantity of information which reduces communication in the network. The remote data monitoring PDP paradigm supports huge amounts of data in a widespread storage system. In comparison with schemes with lower guarantees, we provide two proven PDP plans which are more effective than prior methods. [10] The overhead of

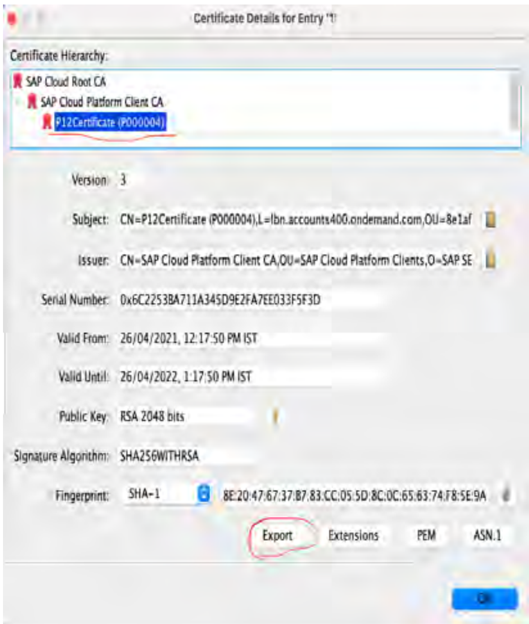
www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

the server is, in particular, minimal, or even constant, compared with linear data size. Experiments performed with our implementation demonstrate that PDP is feasible and reveal PDP's performance is limited by disk I/O rather than cryptographic computing. H. Shacham and B. Shacham. Food..and, 2013. [3] A data-storage center satisfies a verifier in a proof-of-retrievability system that all data is truly stored by a client [4]. Erway, C. Papamanthou, A. Kupcu, and R. Moscow College, 2015. The challenge of demonstrating effectively the integrity of the data kept on untrusted servers has gained increasing attention because storage-outsourcing and resource-sharing network is becoming widespread. The Client pre-processes the data and transmits it to an unauthorized server under the Povable Data Possession (PDP) paradigm while retaining a little bit of meta-data. The customer then requests the server to show that the stored information was not deleted or manipulated (without downloading the actual data). However, only static (or append-only) files are covered by present PDP systems. [5] We provide the Dynamic Provable Data Possession (DPDP) defining framework and efficient construction to expand the PDP paradigm to enable the updating of data stored. We utilize a new ranking-based authenticated dictionary version. [6] Dynamic update prices are the performance shift for the file with n blocks from O(1) to O(logn n (or O(nȚlog n) when the likelihood of mis-compliance is kept. [7] Our tests demonstrate that this lag in practice is quite minimal (e.g., 415KB proof size and 30ms computational overhead for a 1GB file). [8] We illustrate additionally how our DPDP technique is used to outsourced file systems and version management systems (e.g., CVS).

4. METHODOLOGY

DSCS Protocol Chen et al. suggests that any SNC protocol of static data generally offer a secure cloud storage protocol. You perceive F as m chunks or gathered vectors (each of dimension n). In addition to authentication marks, the client output his vector to the server. This tags may be calculated using the SNC technique. TagGen. During an audit, the client sub-sets Q of {1,2. M } for the server. The server raises the requested vectors in line with the SNC and combines them. Send the output vector to merge the customer tag (blockless verification). The customer then checks the genuineness of the vector received (using SNC. Verify). The number of vectors in the transmission file is fixed in an SNC protocol. Since a priori it should be known the dimension of the coefficient vectors used to increase the original vectors. A general design of a secure cloud storage as described is therefore suited only for static data. However, following initial outsourcing, customers inside the DSCS protocol can change their data (insert, remove and edit them). In order to provide an effective DSCS Protocol We emphasize some of the issues for the SNC as follows. For details, please see Appendix A. 1) For insertions and deletions, the DSCS protocol must handle m values that are variable. 2) A vector index is not to be included into its tag. If not, the client must reputate tags for all subsequent vectors to insert or delete a vector as their indices change too. 3) Customer data must be fresh, i.e. up-to-date data should be stored on the server. (4) A third party auditor (TPA) may frequently be required to audit the auditor on behalf of the customer. In this part we are creating the DSCS protocol (DSCS I) which is publicly verified and is safe in the standard model, based on the proposed SNC protocol. For the quality of the dynamic data, DSCS I utilizes a ranked authenticated skiplist. May h be the haze resistant to collisions utilized in the authenticated skip list depending on rank. We assume that the outsourced F file is a collection of m (or blocks as defined in 2) size n. We can notice that the file is divided into a data block of 20 such that each block receives an authentication tag (thus, in this paper, a block represents a vector). Every part of a vector is called a segment. Every segment is Ț-bit long, we presume. As follows, we describe the DSCS I algorithms. In addition to other Skip List activities.

5. RESULTS



Certificate Details for Entry '1'

Certificate Hierarchy:

SAP Cloud Root CA
SAP Cloud Platform Client CA
P12Certificate (P000004)

Version: 3

Subject: CN=P12Certificate (P000004),L=lbn.accounts400.ondemand.com,OU=8e1af

Issuer: CN=SAP Cloud Platform Client CA,OU=SAP Cloud Platform Clients,O=SAP SE

Serial Number: 0x6C2253BA711A345D9E2FA7EE033F5F3D

Valid From: 26/04/2021, 12:17:50 PM IST

Valid Until: 26/04/2022, 1:17:50 PM IST

Public Key: RSA 2048 bits

Signature Algorithm: SHA256WITHRSA

Fingerprint: SHA-1 8E:20:47:67:37:B7:83:CC:05:5D:8C:0C:65:63:74:F8:5E:9A

Fig.2. Accept Client Details in Cloud Section

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

6. CONCLUSION

In this study, we presented a secure dynamic data cloud storage (DSCS I) protocol based on the SNC protocol. This is the first SNC-based DSCS protocol to our best knowledge, which is safe in the standard model and is publicly verified. In building an effective DSCS protocol of an SNC protocol we have highlighted several problems. We also found several constraints of the dynamic data SNC-based secure cloud storage system. However, the underlying SNC protocol utilized has certain restrictions. A more effective SNC protocol might offer us a more efficient DSCS protocol. We also found certain SNC procedures suited for data supplements, and we developed a DSCS protocol (DSCS II) that is efficient for data supplementation purposes alone. DSCS II has been found to exceed several of DSCS I's restrictions.

8. FUTURE ENHANCEMENT

In order to illustrate the practicality and performance of DSCS I, the DSCS II prototype implementations were carried out in conjunction with SNC based, static, cloud, and the DPDP I cloud storage performance.

REFERENCES

[1] B. Sengupta and S. Ruj, “Publicly verifiable secure cloud storage for dynamic data using secure network coding,” in ACM Asia Conference on Computer and Communications Security, 2016, pp. 107–118.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, “Provable data possession at untrusted stores,” in ACM Conference on Computer and Communications Security, 2007, pp. 598–609.

[3] Juels and B. S. Kaliski, “PORs: Proofs of retrievability for large files,” in ACM Conference on Computer and Communications Security, 2007, pp. 584–597.

[4] H. Shacham and B. Waters, “Compact proofs of retrievability,” Journal of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.

[5] C. C. Erway, A. K ¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” ACM Transactions on Information and System Security, vol. 17, no. 4, pp. 15:1–15:29, 2015.

[6] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling public audit ability and data dynamics for storage security in cloud computing,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011.

[7] D. Cash, A. K ¨upc¸ ¨u, and D. Wichs, “Dynamic proofs of retrievability via oblivious RAM,” in EUROCRYPT, 2013, pp. 279–295.

[8] E. Shi, E. Stefanov, and C. Papamanthou, “Practical dynamic proofs of retrievability,” in ACM Conference on Computer and Communications Security, 2013, pp. 325–336.

[9] R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung, “Network information flow,” IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1204–1216, 2000.

[10] S. R. Li, R. W. Yeung, and N. Cai, “Linear network coding,” IEEE Transactions on Information Theory, vol. 49, no. 2, pp. 371–381, 2003.

[11] S. Agrawal and D. Boneh, “Homomorphic MACs: MAC-based integrity for network coding,” in International Conference on Applied Cryptography and Network Security, 2009, pp. 292–305.

[12] D. X. Charles, K. Jain, and K. E. Lauter, “Signatures for network coding,” International Journal of Information and Coding Theory, vol. 1, no. 1, pp. 3–14, 2009.

IMPLEMENTATION OF CRYPTOGRAPHY USING AES ALGORITHM AND SHA256 HASHING TECHNIQUE FOR SECURE COMMUNICATION

J Priyanka[1], A Shriya[2], K Snehith[3], Deepika Vodnala[4]

[1, 2, 3,4]Department of Computer Science and Engineering, Vignana Bharathi Institute of Technology, Telangana, India.
E-mail: joganolapriyanka@gmail.com[1], shriya.annamaneni2000@gmail.com[2], snehithkumar44444@gmail.com[3], deepuvodnala19@gmail.com[4]

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Abstract- Nowadays, to Implement Communication Applications, security is quite possibly the main feature, particularly when sharing private documents. One strategy that can be utilized to get information by encoding and decoding data is Advanced Encryption Standard (AES). AES is the most widely used and best secure algorithm as it implements the encryption process very quickly during the transfer of data over the network. This algorithm is open-source cryptography that uses symmetric keys to perform encryption and decryption of documents. This algorithm is used to encrypt any media file like pictures, audio, and video. In this paper, the importance of secure communication using cryptography has been addressed, also various existing Cryptography mechanisms have discussed. The proposed system uses AES and SHA256 algorithms to perform encryption and decryption of user documents. The file is encrypted using a secret key which is given by the user and the encrypted file can be decrypted by using the same key. In this way, only authenticated users can perform decryption and restricts access to unauthenticated users. The results section illustrates the successful implementation of encryption and decryption of user documents using the secret key.

Keywords- Advanced Encryption Standard (AES), Cryptography, SHA256, Secret Key.

1. INTRODUCTION

Our Endeavour will be beneficial to the client who will be able to access the records and edit them through the process of encoding and decoding, which is known as cryptography. By encoding and unscrambling the report, the client can make his record private. The report might be scrambled or decoded by the customer who took part with no cryptographic information and the ability to look through the archive. To ensure the information or keep the information hidden, the documents in the framework were initially covered up or secured with a secret word. However, the records were frequently covered up, which has some disadvantages. If the other client modifies the framework's settings, he will be able to see the hidden documents and steal the information. As Rijndael has existed as the Advanced Encryption Standard since 2000, there are already many implementations of this algorithm. These implementations are available in many different programming languages. As the AES standard is open, organizations or users who wish to implement the Rijndael algorithm are free to do so. Cryptography is the workmanship and study of encryption of the data so that except the client, nobody can understand the authentic information which is a type of safety through haziness. In other words, cryptography conceals authentic information, however, it doesn't cover the way that it's anything but the real information. Various existing systems are implemented using the AES algorithm which is illustrated in section 2. As technology progressed, new methods were developed to keep records safe. They can be kept safe by employing cryptography. In the proposed work, AES calculations were used in conjunction with SHA256 hashing algorithms. The proposed framework cryptography furnishes an agreeable climate to manage information. By and large, cryptography devices support numerous sorts of calculations. Our application upholds AES Algorithm and SHA256 hashing. This application has been created utilizing Visual studio and python language. The proposed system will provide a proper amount of security to all the documents that

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

are in the user's laptop thus, gives an amicable climate to the clients.

The organization of this paper is as follows: in section 2, various existing Cryptography mechanisms have been discussed. In section 3, provides the proposed system architecture. In Section 4, the overview of the proposed system and its methodology have discussed. In Section 5, simulation results are provided and section 6 concludes the paper.

2. LITERATURE SURVEY

Advanced Encryption Standard (AES) algorithm to encrypt and decrypt data. Nowadays, the use of the internet and networks is quickly rising. Every day, a large amount of digital data is being exchanged between the users. Some data is important and must be kept safe from attackers. Encryption [2] methods are critical in preventing unauthorized access to original data. To encrypt data, a variety of algorithms are available. One of the most efficient algorithms is the Advanced Encryption Standard (AES) [2], which is extensively supported and used on both hardware and software. The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher method that is extensively applied around the globe. This technique, which has its structure for encrypting and decrypting sensitive data, is used in hardware and software all around the world. When using the AES method to encrypt data, it is exceedingly difficult for hackers to decrypt the data. There is no indication to date that this algorithm is broken. AES can handle three alternative key sizes: 128, 192, and 256 bits, with each of these ciphers having a 128-bit block size. The purpose of this paper is to describe a few key elements of the AES algorithm and to discuss some past research that has been done on it to evaluate the performance of AES to encrypt data under various conditions. According to research findings, AES can give significantly better security in comparison with competing algorithms such as DES, 3DES, and Blowfish [2]. Performance Improvement of Advanced Encryption Algorithm using Parallel Computation. The need for network information security is becoming increasingly crucial. Cryptography[3] is a technique for ensuring the confidentiality, authenticity, and integrity of data. The implementation of cryptography algorithms has numerous problems, including execution time, memory requirements, and compute power. Parallel processing is a possible way for improving cryptography performance. Parallel processing is a possible way for improving cryptography algorithm performance. In parallel computation, the divide-and-conquer approach is commonly used to perform algorithms in parallel by partitioning and allocating the number of provided subtasks to available processing units. By parallelizing the execution of an algorithm across multiple cores, multicore computers may conduct parallel processing. In this paper, the author had focused on how to minimize the execution time of the AES (Advanced Encryption Algorithm) cryptography algorithm on a dual-core processor by leveraging the OpenMP API.

The concept of parallel programming using a multi-core CPU is explained and illustrated the usage of multicore systems and the openMP API [3] to efficiently and effectively implement the Advanced Encryption Algorithm, extracting as much parallelism as feasible from the algorithm in a parallel implementation approach. This paper represents a thorough quantitative analysis of execution time for both sequential and parallel implementations. The result analysis shows that with the AES block cipher and comparable algorithms, multi-core machines can be used efficiently for parallel implementation. Multi-core processors are efficient and reliable to perform the AES cryptographic method.

Implementation of advanced encryption standards algorithm

The study of mathematical approaches connected to characteristics of information security such as confidentiality, data integrity, entity authentication, and data origin authentication is known as cryptography. Cryptography is required in data and telecommunications when communicating over an unstable medium, which includes any network, particularly the internet. In this research, the Rijndael algorithm (Advanced Encryption Standard algorithm) [4] is used to synthesize a 128-bit AES encryption and decryption that may be easily implemented on an FPGA. The cipher, inverse cipher, and Key Expansion are the three essential components of the algorithm. The cipher transforms data into plaintext, which is incomprehensible. Key

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Expansion creates a Key schedule, which is used in the cipher and inverse cipher procedures. A cipher and an inverse cipher are both made up of a specific number of rounds. The AES algorithm uses a round function that is made up of four separate byte-oriented transformations: Sub Bytes, Shift Rows, Mix Columns, and Add Round Key to determine the number of rounds to be executed throughout the algorithm's execution. The implementation of the AES algorithm on a 128-bit message concluded this study effectively. The decoded and encrypted ciphertexts are analyzed and found to be correct. The proposed AES algorithm's encryption efficiency was investigated and found to be satisfactory.

Report on the Development of the Advanced Encryption Standard (AES)

In this work, the author had focused on the creation of a Federal Information Processing Standard (FIPS) [5] that specifies an encryption algorithm capable of safeguarding sensitive (unclassified) government data well into the twenty-first century. The algorithm is expected to be employed by the US government and, voluntarily, by the commercial sector, according to NIST. The finalist competition was fierce, and after a lengthy and complicated examination procedure, NIST chose Rijndael as the proposed AES algorithm. This report explains the methodology and includes many of the algorithm characteristics discovered during the public review periods.

3. SYSTEM ARCHITECTURE

The System Architecture of the proposed system i.e. Implementation of Cryptography Using AES Algorithm and SHA256 Hashing Technique for Secure Communication shown in Figure 1. which describes various components and communication between those components. The ciphertext is data or text which is encrypted into a secret code using a mathematical algorithm; it can be deciphered using different mathematical Algorithms. Encryption is converting the text into a secret message, technically known as converting the plaintext to ciphertext, and Decryption is converting the ciphertext back to plaintext so that only the authorized users can decipher and use the data. Generally, it uses a key that is known to both the sender and the receiver so that they can cipher and decipher the text.

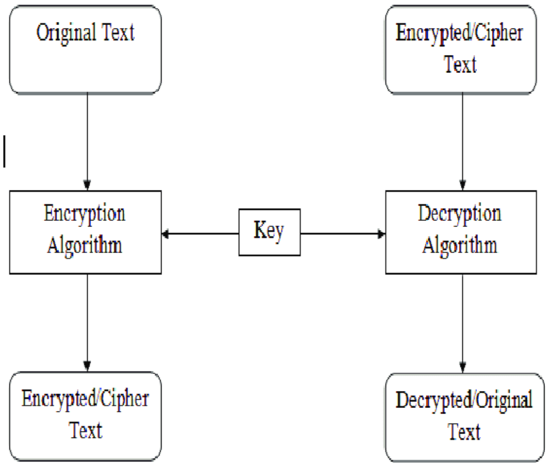


Fig.1. System Architecture

4. PROPOSED SYSTEM

The proposed system i.e. “Implementation of Cryptography Using AES Algorithm and SHA256 Hashing Technique for Secure Communication” is implemented using AES and SHA256 algorithms which are explained below.

AES algorithm

Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES supports key lengths of 128, 192 and 256 bit. AES comprises of 3 block ciphers AES-128, AES-192 and AES-256, each cipher encrypts and decrypts the data in the block of 128 bits using the secret key of 128, 192 and 256 bits respectively. AES algorithm both encrypts and decrypts the plain to ciphertext and ciphertext to plain text with the same secret key. AES has key lengths of 128, 192, and 256 bit which encodes and decodes the information present in the document or file in the square of 128 pieces with the secret key. It is possible because of the Cipher class which handles both encryption and decryption. When the document is encrypted successfully with the secret key, it converts the text into some gibberish language, and when decrypted with the right secret key which is used for encryption then it converts the ciphertext into plain text. The AES algorithm is implemented with three modules, that are:

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

- **Secret Keys**

In this module, we utilize two mystery keys for Encryption and Decryption of the record. Both the mysterious keys must be comparative. The keys we use for encryption can just give the correct data present in the record after decoding. Wrong keys can likewise decode the record however it shows the wrong substance in the archive.

- **Encryption of the Document**

In this module, the first record is encoded when given the comparable mystery keys. At the point when the report is scrambled, the first archive is erased without anyone else from the framework. The document that is uploaded will be encrypted with the help of the secret keys mentioned by the users.

- **Decryption of the Document**

In this module, the encoded report is decoded with similar mystery keys, and really at that time, one can have the correct substance present in the archive. It unscrambles the report with some unacceptable mystery keys however the substance won't be the first.

- **SHA256 Algorithm**

In SHA256 Algorithm, the password entered twice matches with the hash function. This ensures that the password entered twice is accurate, which helps in gathering useful data and save them in an encrypted format. In the SHA256 algorithm, it secures the data and the password by performing the hash function. When a password is entered it encrypts the password by executing the hash function and stores it in the database. To retrieve the file, one has to re-enter the password. The file gives permission only if the password is right. It verifies the password in hash format. If the passwords do not match, it shows an error.

5. RESULTS

The proposed system i.e. Implementation of Cryptography Using AES Algorithm and SHA256 Hashing Technique for Secure Communication is implemented using Visual studio and python programming language. The proposed system provides more security to any kind of document that is available on the user's laptop, thus, gives an amicable climate to the clients. This section provides the result analysis of the encryption and decryption process using the proposed application. Figure 2 shows application menu page where the user can select either encryption or decryption to process the document. the actual file before initiating the encryption process. The file contains some text messages as shown in the figure.

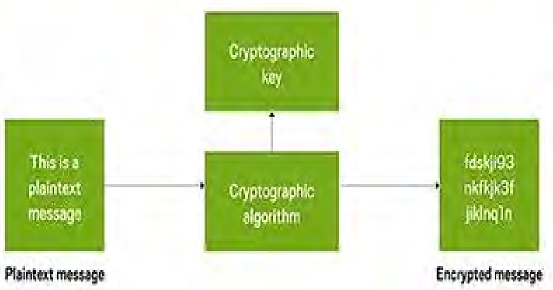


Fig.2. The Encryption Process

Fig 2. shows the encryption process using the proposed application. To do encryption, the user has to load the document into the application by selecting a file. Once the document is uploaded successfully, he has to enter the secret key and select encrypt option from the menu as shown in the figure. Once the process is done, the application displays the "File Encryption Successful !!" message on the screen. The user has to remember the secret key to do the decryption process whenever he needs the file. Otherwise, he can't decrypt the file.

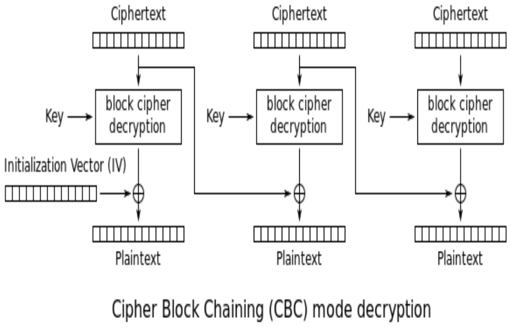


Fig. 3. Decryption Process

Figure 3 shows the Decryption process. For this process, the user has to upload the encrypted file and enter the same secret key which was used during the encryption process of the same file.

Then he has to select the Decrypt option to decrypt the file. Once the process is completed, the "File Decryption Successful !" message is displayed on the screen as shown in the figure. Once the decryption process is done successfully then the user receives the original file as shown in Figure 3. If any unauthenticated user tries to decrypt the file, then he will get a decryption successful message though he gives an invalid secret key the decrypted file contains data in unreadable format as shown in figure 7. In this way, the proposed system prevents access to unauthenticated users.

6. CONCLUSION

Privacy is everyone's need nowadays. The proposed system is successfully implemented using the AES algorithm along with the SHA256 hashing technique. These approaches are being used for the encryption and decryption process where the user file is encrypted and decrypted by using the same valid secret key. The proposed system is useful to the users who want to maintain their documents securely in the local system and to prevent access to unauthenticated users.

REFERENCES

[1] Singh, G. A study of encryption algorithms (RSA, DES, 3DES, and AES) for information security. International Journal of Computer Applications, 67(19), 2013.

[2] Yenuguvanilanka, J., &Elkeelany, O. Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm. In Southeast conference, 2008. IEEE pp. 222-225, April, 2008.

[3] Diaa, S., E, Hatem M. A. K., &Mohiy M. H., Evaluating the Performance of Symmetric Encryption Algorithms. International Journal of Network Security, Vol.10, No.3, pp.213-219, May, 2010.

[4] C. Parikh and P. Patel, "Performance Evaluation of AES Algorithm on Various Development Platforms", Consumer Electronics, ISCE 2007. IEEE International Symposium, (2007), pp. 1-6.

[5] Abdullah, A. M., & Aziz, R. H. H. New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4, pp. 11-17, June 2016.

[6] R. Anderson, E. Biham, and L. Knudsen, Serpent: A Proposal for the Advanced Encryption Standard, AES algorithm submission, June 1998.

[7] L. Bassham, NIST Efficiency Testing of Round 2 AES Candidate Algorithms, The Third AES Candidate Conference, April 13, 2000.

[8] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999.

[9] J. Nechvatal, Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

CREDIT CARD FRAUD DETECTION

Shenaz Begum[1], Srinivas V B[2], Usha V Ballolli[3], Vaishnavi J[4], Varsha B[5]

[1,2,3,4,5] Department of Computer Science of Engineering, Ballari Institute of Technology and Management,
Ballari, Karnataka, India.
E-mail: shehanazbitm@gmail.com[1],b_srinivas274912@gmail.com[2], balloli_ushamallabollolli@gmail.com[3,]
J_vaishnavijois2@gmail.com[4], b_varshab@gmail.com[5]

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

Abstract- Due to the increase in fraud leading to global financial losses, many issues and methods designed to detect involves analyzing user activities in order to understand the malicious behavior of users. Cruelty is a broad term that includes Delinquency, Fraud, Intrusion Fraud Detection, and Account Error. This paper introduces a study of current strategies used in detecting credit card fraud. This paper also discusses popular algorithms used for unsupervised and supervised learning.

Keywords- Fraud Detection, Malicious Behavior, Credit Card

1. INTRODUCTION

With the rise of technology today, the dependence of e-commerce and online payments has grown exponentially. As the credit card provides convenience to users but fraud caused by these activities creates disruption. Credit card information is private, anonymous and some financial institutions do not want to disclose information about their customers. Risk management is essential for financial businesses to survive in this competitive industry. Temporary losses arise because "bad" bank accounts lend money to customers who end up not being able to pay. In risk management, the chances of having a negative (positive "false" accounts) are still high. However, by using their functionality such as using credit, payment details, risks can also be controlled to control temporary losses. In this paper, the focus is on disaster management and fraud detection.

In 2019 Sahaya sakila V, D.Kavya Monisha Aishwarya, Sikhakolli Venkata visalak shiswshai Yasawi described key strategies of Twain [8] which are Whale Optimization (WOA) and SMOTE (Synthetic Minority Oversampling Techniques). The main purpose is to progress the swiftness of combination and crack the problem of information inequality. The difficulty of class inequality is control by utilizing the SMOTE process and WOA process. The SMOTE process favors against completely re-sampled transactions to check data accuracy and improvements using the WOA process.

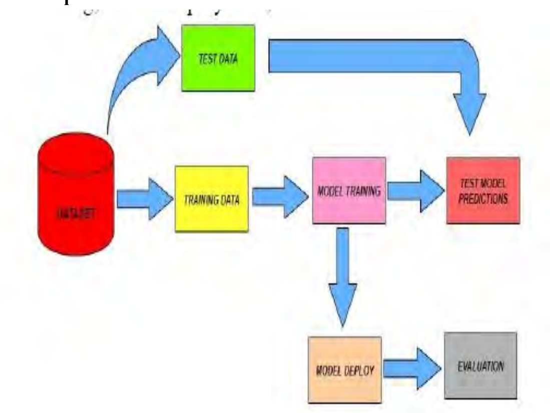


Fig.1. Block Diagram of Credit Card Fraud Detection

2. LITERATURE SURVEY

A. Mishra and C Ghorpade[1], "Credit Card Fraud Detection on Bonded information using many Divisions, Integration Methods", 2018 International Students' Conference on Economics and Technology (SCEECS), pages 1-5. These days, as the speed of the internet has increased and mobile prices have dropped dramatically in the last few years. And data prices are also more affordable for most people. This has led to the creation of as many computing computers as it is suitable for everyone and also the record keeping authority. As a result, most banks and other institutions have received and transferred credit cards. Opportunities for transaction fraud.

Transactions are very small but not bad and if it detects even one fraud is improper because it is a crime and we cannot ignore it even if it is very small as it damages the customer and the

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

reliability of the institution. This consequently intentions to analyze different classification strategies using different system of measurement to judge different dividers. This prototypical goals to improve scam discovery rather than unlawfully sell the real thing as fraud. 1. Andrea Dal Pozzolo,“ Calibrating Probability with Under sampling aimed at Instable division” at the Symposium on Computational Intelligent. Below the sample is a popular method for unlimited data shares to reduce skew in class delivery. However, it is well known that under the sample one phase changes the essence of the training set and as a result chooses to look forward to the opportunities behind the division. In this paper, we read by analyzing and experimenting how the sub-sample affects the posterior possibilities of the machine learning model. We make the issue legal for making low-level examples. Although the bias due to the sample does not affect the order of the rate returned by the background opportunities. N. Malini and M. Pushpa, "Strategic Investigation of Credit Card Fraud Policies Based on KNN and Outlier Detection. General expense style approved for both offline and online is a credit that offers free transactions.

3. MODULE DESCRIPTION

- The Convolutional Neural Network (CNN) is also a field of intensive education. Plotting contribution in hidden layer characterizes a single feature plot respectively represents a single way of compressing neurons compression features in a feature chart called convolution. CNN is very effective in face recognition, letter recognition, image classification etc.
- It has two stages of training and testing: The training phases involve building a isolation forest, and the testing phases involve passing each data point in each tree to calculate the average number of edges needed to reach the external node.

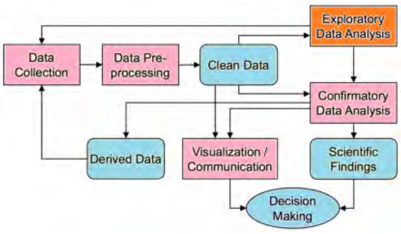


Fig.2. Exploratory Data Analysis

- **ADA BOOST ALGORITHM:**

Ada boost Algorithm Boosting is one of the ways to integrate. This algorithm is used to build strong separators from weak partitions. This can be done by building a strong model using a weak model in the series. Initially, the model was built from training data. After that the second model was built from the first model by correcting the errors represented in the previously made model. This is a repetitive process and continues until a large number of models or a complete training database is well predicted. Ada boost was one of the most successful growth algorithms designed for binary division.

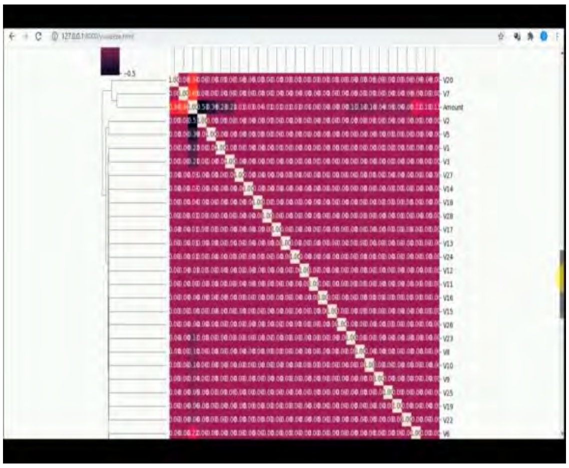


Fig.3. Confusion Matrix

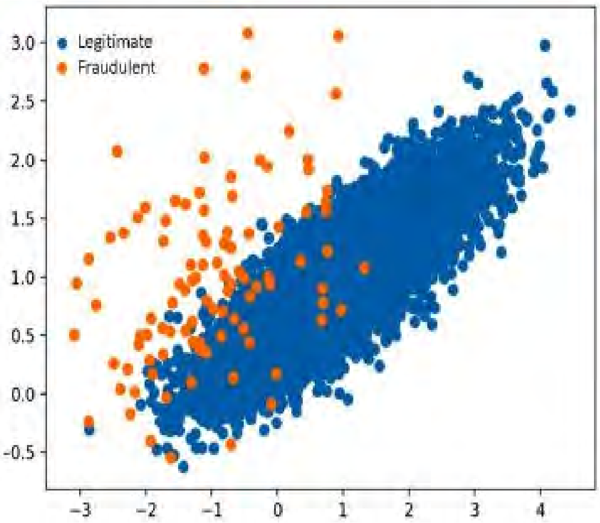


Fig.4. Model Performance and Visualize Plots

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022

4. IMPLEMENTATION

A. Tensor Flow

Tensor Flow is a free and open source software for data flow and partitioning programs that can be used to solve various problems. It is a symbolic mathematical library that is also used in neural networks and other system learning tools. At Google, it is used for research and production. The Google Brain team has created a Tensor Flow for Google's internal use. Tensor Flow is a low-level framework for performing complex calculations aimed at professionals who understand how to create exploratory learning frameworks, play with them, and implement practical programs.

B. Scikit-funda

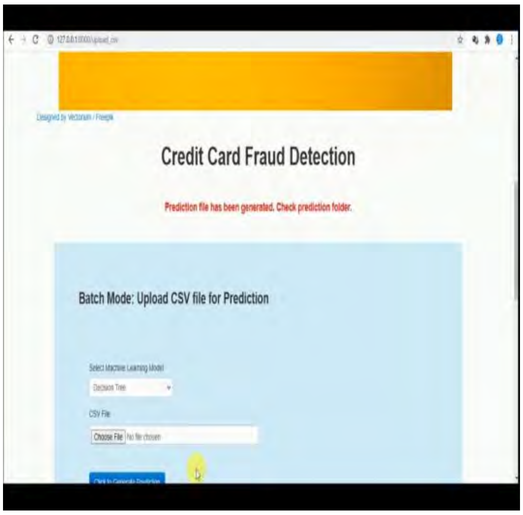
Scikit Read is a free python programming language package. It includes vector support equipment, random forests, gradient enlargement and k-means and other subdivisions, regression, and integration methods, and is designed to work with numerical and scientific libraries Python NumPy and SciPy.

C. Python

Python is a flexible programming language that can be used for a variety of tasks. Python has grown in popularity as a result of this. Python as two electronic learning libraries are SciPy and NumPy, which are used in direct algebra and kernel learning methods. Language is ready to work with machine learning algorithms and has simple and logical syntax. This is an excellent language for beginners to learn and use. Python's syntax, considered both "good" and "mathematical", is one of the advantages. NumPy has one of the many frameworks and modules, as well as extensions that make python functions easier to use. As a result, the context of the programming language plays a role in the complaint f or specific applications.

5. RESULTS

The proposed method is tested using a credit card database for all training and testing. After loading the database, if the generated value is 0 then it should be a valid transaction and 1 means it is considered fraud. The following figure shows some of the sample images from a sample credit card database used to train and evaluate their predictions.



127.0.0.1:5000/upload_csv
Designed by Vectorium / Freepik
Click to Generate Prediction

Credit Card Fraud Detection

Prediction file has been generated. Check prediction folder.

Batch Mode: Upload CSV file for Prediction

Select Machine Learning Model

Decision Tree

CSV File

Choose File No file chosen

Fig.5. Database testing to generate predictions

6. CONCLUSION

In this research we compared Logistic Regression and Auto encoder Neural Network for scam detection in banking operations. The Logistic Regression model achieves 58% accuracy. Since then, the quintessential target for increased accuracy has been satisfied with the Auto encoder Neural Network with 99.83% accuracy. By analyzing the result, it is clear that the Auto encoder Neural Network is a clear Logistic Regression model. AS a result, even the most computer neural network as the advantage of learning complex and indirect tasks.

REFERENCES

[1] "Credit Card Fraud Detection Based on Transaction Behaviour -by John Richard D. Kho, Larry A. Vea" published by Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017

[2] CLIFTON PHUA1, VINCENT LEE1, KATE SMITH1 & ROSS GAYLER2 " A Comprehensive Survey of Data Mining-based Fraud Detection Research" published by School of Business Systems, Faculty of Information Technology, Monash University, Wellington Road, Clayton, Victoria 3800, Australia .

[3] "Survey Paper on Credit Card Fraud Detection by Suman" , Research Scholar, GJUS&T Hisar HCE, Sonepat published by International Journal of Advanced Research in Computer

Engineering & Technology(IJARCET) Volume 3 Issue 3, March 2014 .

[4] "Research on Credit Card Fraud Detection Model Based on Distance Sum – by Wen-Fang YU and Na Wang" published by 2009 International Joint Conference on Artificial Intelligence .

[5] "Credit Card Fraud Detection through Parenclitic Network Analysis-By Massimiliano Zanin, Miguel Romance, Regino Criado, and Santiago Moral" published by Hindawi Complexity Volume 2018, Article ID 5764370, 9 pages.

[6] "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy" published by IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, VOL. 29, NO. 8, AUGUST 2018

[7] "Credit Card Fraud Detection-by Ishu Trivedi, Monika, Mrigya, Mridushi" published by International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016

[8] David J.Wetson,David J.Hand,M Adams,Whitrow and Piotr Jusczak "Plastic Card Fraud Detection using Peer Group Analysis" Springer, Issue 2008.

www.IndianJournals.com
Members Copy, Not for Commercial Sale
Downloaded From IP - 136.233.95.6 on dated 1-Apr-2022