Volume - 4, Issue - 2
Jan – Jun, 2019

ISSN : 2581 - 4125

HMR Interdisciplinary Journal of Science, Technology & Education Management

HMR Institute of Technology & Management
(Affiliated to Guru Gobind Singh Indraprastha University, Delhi)
Hamidpur, Delhi – 110 036

HMR INTERDISCIPLINARY JOURNAL OF SCIENCE, TECHNOLOGY AND EDUCATION MANAGEMENT

Advisory Board

Editorial Board

ABOUT THE JOURNAL – HMRIJSTEM

(ISSN: 2581- 4125)

HMR Interdisciplinary Journal of Science, Technology & Education Management is published by HMR Institute of Technology & Management, Hamidpur, Delhi, on bi – annual basis. HMRIJSTEM is approved by National Science Library (NSL), National Institute of Science Communication And Informational Research, Council of Scientific and Industrial Research (NISCAIR), Government of India. The of this Journal is aim to provide a suitable platform presenting well considered, meaningful, constructively thought provoking, non-political and non controversial but critically analyzing and synthesizing present and future aspects of technical and interdisciplinary education particularly reference to our country. The authors and contributors are expected to highlight various research issues along with meaningful suggestions for solution, refinement and innovations.

Authors are requested to follow the IEEE Conference Paper Template. The authors are fully responsible for the contributions. Articles will be selected by the Editorial Board and are subject to editorial modification, if necessary. All data, views opinion etc being published are the sole responsibility of the author. Neither the publisher nor the HMRITM is anyway responsible.

THERE IS NO PUBLICATION FEE.

For detail regarding guidelines, copyright and paper template visit Institute website: www.hmritm.ac.in

Paper / Manuscripts are invited for Jan – June Issue and Jul – Dec Issue

Send your manuscripts to editor.journal@hmritm.ac.in

Editorial

We, at HMRITM are delighted to announce the release of Volume 4, Issue 2, of HMR Interdisciplinary Journal of Science, Technology and Education Management. HMRIJSTEM publishes articles which present novel research in the areas of engineering, science, technology and management. The Editorial Team encourages interdisciplinary research and the current issue publishes seven research papers and the efforts of all the corresponding author' s are significant for the successful operation of the journal.

This edition of HMRIJSTEM contains articles "Encrypting Electronic Cash System", Producing Energy Using Blind Man Stick", "Smart Diagnosis Using Machine Learning", "Ethical Hacking: A Necessity", "Cardiac Arrest Prediction using Artificial Neural Networks" and " Managing WSN by Technical Tools".

We take this opportunity to thank all those contributors, reviewers, in making this issue an unforgettable one. We would also like to thank our Chief Patron - Hon'ble Shri A K Gupta, Our mentor Prof Ramjee Prasad, Founder Chairman, Global ICT Standardization Forum for India (GISFI), AARHUS University, Herning Denmark, Chief Executive Officer - Mr S N Jha (IAS – Retired) , Director - Prof V C Pandey, Deputy Director - Prof Shalini Gupta and all Advisory Board Members for their motivation and support in bringing out this edition of HMRIJSTEM. Suggestions and feedback from our readers are welcome for the overall improvement of quality.

Delhi
25/07/2019

Editorial Board

Encrypting Electronic Cash System

Rajeev Kumar

KIRAS, GGSIPU, New Delhi
rajeev974@gmail.com

***Abstract*—** The bitcoin system is a digital asset. Since it is computational, it allows online transactions without the need of any third party. It is an improved method where we can directly make the payments instead of paying extra money from our pocket to the ban or any other financial institution. Basically the solution is that the bitcoins are given an address generated by hash. Transaction takes place and is checked by the miners. Digital signatures are helpful, but main benefit is lost if any third party (miner) is still required to check for double-spending.

Keywords— Digital Currency; Bitcoin; Hash Cash; Encryption.

I. INTRODUCTION

Bitcoin is a digital currency in which encryption techniques are used for the generation of currency, transfer of funds without any central bank or any other party. This currency can be created and held electronically, this means that they aren't printed and no institution controls this. This can be used to buy or pay or to send money to other person. The software used for this was developed by Satoshi Nakamato and is based on mathematical proof. Being an open-source network, it allows any two parties to transact directly with each other without spending anything extra on any third party. These transactions cannot be reversed so this avoids any frauds, but in case of any loss of the money, the funds cannot be refunded. In this paper, we redefine an improved method which uses timestamp server to generate the order of transactions.

First we download the software and set up a bitcoin wallet. Now we can send, receive, or store bitcoins. The software develops a bitcoin address through hash[1] [2]. We can buy bitcoins either from user or through any other bitcoin exchange. Now we can perform the transactions. The miners confirm the transaction and these transactions are collected in a block. Every account consists of a public key[3] [4] and a private key. To spend bitcoins we need to know the private key[5] [6] to access the account. To send bitcoins, we need to know the public key of the receiver. Miners checks for double spending. After every transaction the coin must be returned to the miner to issue a new coin. Only the coins issued from the miners are trusted not to be double spent. Problem with this solution is that the money system depends on company running the miner, and every transaction goes through them, just like bank.

We now need a way so that the payee gets to know that previous owner did not sign the earlier transactions. For our purpose, the earliest one is the one that counts, so we don't care about any later attempts to double spend. To confirm the absence of a transaction, we need to be aware of all transactions. In the miner based model, the miner is aware of all the transactions and they decide which arrived first. To accomplish this without any trusted party, transactions must be publicly announced, and now we need the system for participants to agree on single history of the order in which they were received. The payee needs a proof that at the time of transaction, majority of nodes agree it was the first one to be received.

II. EXISTING WORK

The solution we propose consists of a timestamp server which works by taking a hash of the block of items which is to be time stamped and then widely publishing the hash, such as publishing it in a newspaper. This way the timestamp proves that the data must have existed at thattime, in order to get into hash. Each next timestamp includes previous timestamp inits hash, which forms a chain, with each new timestamp reinforcing the ones which it has before it.

III. METHODOLOGY

To implement distributed timestamp server as a useful solution, we will use a methodology which is somehow similar to Adam Back's Hashcash, rather than depending upon the newspaper or any other media.

This methodology involves scanning for a value such that when hashed, such as with SHA-256, the hash begins with a particular number of zero bits. The average amount of work required is exponential in number of the zero bits required which then can be verified by execution of a single hash.

For this timestamp network, we implement this methodology by incrementing a nonce in that block until such a value is found that gives block's hash it's required zero bits. Once the CPU's effort has been expended to make it work such that it satisfies the methodology, then that block cannot be changed without redoing the whole work. Since the later blocks are chained after it, so the work to change the block thenwould include redoing all those blocks which are after it.

Apart from this the methodology also solves the issues of determining the representation in major cases of decision making. If the majority of them is based on one-IP address-one-vote, it can be subverted by any person who is capable of allocating many IPs[7]. Method here is basically one-CPU-one-vote. The majoritydecision comes out to be represented by the longest chain, in other ways one which has the greatest amount of work effort invested in it. If the majority of the CPU power is controlled by honest nodes, then that honest chain will be the one to grow the fastest of all and also will outpace all the other competing chains. In case of modification of any past block, an attacker will have to firstredo all the previous methodology of the block and also for all blocks after it and then have to catch up with the work of the honest nodes and

also surpass the work of those honest nodes. We will be showing later on that the probability of a slower attacker trying to catch up with the methodology of each block decreases exponentially as subsequently more blocks are added.

IV. Network Design

To run a network first all the new transactions are broadcasted to all the nodes. After this each separate node collects the new transactions in a block. Each separate node then works on finding the proof-of-work for its own block and when a node finds a methodology, it transmits the block to all the other nodes. Now the nodes will accept the block if and only if the transactions in it are valid and also are not already spent. Nodes will then accept the block by creating next blocks of the chain by using hash of the accepted block as previous hash. Nodes will always consider longest chain to be correct one, so they will keep working on ways to extend it. If there are two nodes broadcasting different versions of next block simultaneously, somenodes might receive one or the other one first. So in that case, they start working on that first one they received, but they save the other branches in case it becomes longer. Tie will be broken when next methodologies are found and one of the branches become longer, nodes that were operating on the other branches will then switch to longer one. New transaction broadcasts may not necessarily reach all the nodes. It might happen that a node does not receive any block. In that case it will simply request it when it just receives the next block and will realize it has now missed one.

V. Results and Discussions

A. Incentive

We set up a convention and accordingly the first transaction done in the block is a special type of transaction that starts a new coin which is owned by the creator of that block. This will then add an incentive for the nodes to support network. Now this provides a way to distribute the coins since there is no authority to issue the coins initially. Now we can steadily add a constant amount of new coins. CPU time and electricity are the resources that are expended. We can also provide funds to the incentive by the transaction fees. This means that if the output amount of a transaction is less than the input amount then the difference of them is added to incentive as the transaction fees for that block which contains the transaction. This will make the incentive completely free of any inflation.

B. Disk Space

We also need an efficient way to save our disk's space. So once the latest transaction of a coin is buried under many blocks, the earlier spent transactions before it can be readily discarded. This will in turn help in saving the disk space. But discarding the transaction might break the hash of the blocks. So now to save the disk space without breaking the hash, transactions can be readily hashed in a Merkle Tree. Only the root of the tree is to be included in block's hash. The older blocks can then be discarded. The interior hashes don't need to be stored.

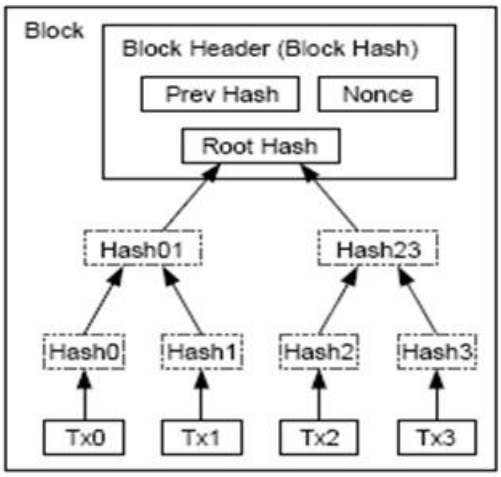


Fig. 1. Transaction Hashed in a Merkle Tree

C. Payment Verification

To verify the payments the user just need a copy of block headers of longest proof-of-work chain. The user can then obtain the Merkle branch linking transaction to the time stamped block. He can't check the transaction by himself, but by linking it to any place in the chain, he will be able to see that the network node has accepted it, also the blocks added after it further confirm that the network has accepted it.

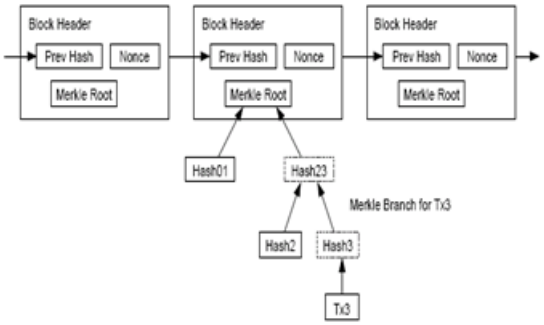


Fig. 2. Hash Function and Verification

This verification is reliable but only as long as the honest nodes control network, but it is vulnerable if network is overpowered by attacker. This simplified method for payment verification can be fooled by an attacker's composition of transactions, as long as the attacker can do this he can overpower the network. So one solution to this is to accept alerts created by the network nodes when they detect a suspicious attempt, any invalid block.

D. Privacy

Privacy in banking models is achieved by limiting the access to information to the parties involved that is by not making things public. In the bitcoin system privacy can be maintained by announcing the transactions publicly. In other words privacy can be maintained by keeping the public keys

anonymous. This means that the public will be able to see that someone is sending some amount to someone else, but without any information linking transaction to anyone. A new key must be used for each transaction. This will avoid them from being linked to any common owner.

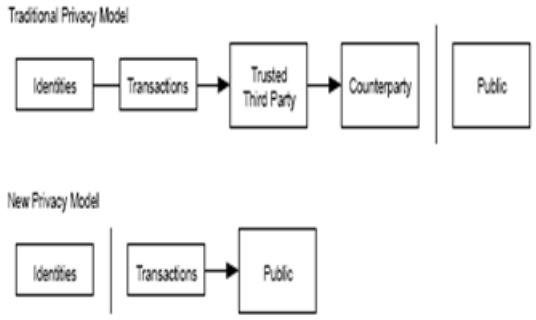


Fig. 2. Traditional Privacy Model

VI. Bionomial Random Work

We assume that an attacker is trying to generate an alternate chain faster than the honest chain. So there is a race between the honest chain and an attacker chain. This race can be named as a Binomial Random Walk. When the honest chain extends it's one block, the event is a success event increasing itslead by +1. When the attacker's chain extends it's one block, the event is failure event reducing the gap by -1.

We can even calculate the probability if an attacker ever catches up with the honest chain. The probability will drop exponentially if the number of blocks he has to catch with increases. If he does not move forward early, his chances will become really small and he will fall further behind. We will now consider how long the recipient of any new transaction will have to wait before being sufficiently sure that the sender cannot change the transaction. We can assume that the sender is an attacker who wants to make the recipient believe that he had paid him, and then toggle it to pay back to himself after some time. Receiver will be alerted whenever that happens, but it might be too late till then. The receiver can generate new keys and give public key to sender soon before signing. This will prevent sender from preparing any chain of blocks ahead of time by trying to work on it constantly until he is able to get sufficiently far ahead, and then executing transaction at that time. Once that transaction is sent, that dishonest sender starts working on another parallel chain which contains an alternate version of that transaction.

VII. Conclusion

We have proposed an efficient system for electronic transactions without relying on any trusted party. We initially started up by generating the coins and assigning them the address generated by hash. But this is incomplete without a way to prevent the problem of double-spending. As a solution to this, we proposed another efficient network using proof-of-work to record a history or an order of transactions which becomes impractical for any attacker to change if the honest nodes control the majority of CPU power. Network is stout. Nodes work with little coordination. Also they don't need to be identified. The messages aren't routed to any particular place, they only need to be delivered on best effort basis. Nodes can depart and rejoin the network at their own will, accepting methodology chain as the proof of what had happened while they moved out. They basically vote with their CPU power, express their approval of valid blocks by working on ways to extend them and rejecting invalid blocks.

References

[1] Lee,D "Hash Function Vulnerability function and Hash Chain Attacks" at 3rd IEEE workshop,2017,pp 1-6.
[2] Bradford,P.G; Gavrylyako,O.V "Hash chainswith diminishing ranges for sensors" at International conference,2014, pp 77-83.
[3] Al Housani,H;Baek,J; Chan Yeob Yeun "Survey on certificateless public key cryptography" at International conference,2011,pp 53-58.
[4] Al-Janabi, S.T.F.; Rasheed; M.A .-S "Public-Key Cryptography Enabled Kerberos Authentication" at Development in E-systems Engineering[DeSE],2011,pp 209-214.
[5] Feng Bao "A generic method of detecting private key disclosure in digital signature schemes" at 5th InternationalICST conference,2010,pp 1-5.
[6] Liping Zheng; Yujuan Zhao "Research on managing private key of PKI users" at International confenrence,2015,pp 2411-2414.\
[7] Karni,R ; Dror,S "Determinants of value creation and customer value in IPs operation phase" at International ICE conference,2014,pp 1-11.

Producing Energy Using Blind Man Stick

Depender Kumar Soni

CSE, HMRITM, GGSIPU, Delhi, Indiai
dependerkumarsoni@gmail.com

***Abstract*—** We all are familiar with the problems a blind person faces while walking on road. Of course, many of us come ahead to help them, but sometime it becomes a matter of self-respect or say the person is not willing to take help from others or even it is possible that nobody may be available to help. Think of a situation when a blind person is alone and an Electronic Travel Aid Stick suddenly stops working due to completely discharged battery system. This paper aims to build a device which can generate that much amount of energy which is required to run the electronic system efficiently so that it can prevent visually impaired people from suffering.

Keywords— Wiring Duct; Piezoelectric Plate; Light Spring; Piston System; Aluminum Cylindrical Pipes; Crankshaft.

I. INTRODUCTION

In our day – to – day life we come across many people who are visually impaired and are unable to walk independently. According to a report by Times Of India [1] out of 37 million blind population of world 15 million are from India. Such people carry a white cane, some carry a guidance dog or they are simply dependent on others. Also there are some Electronic Travel Aids (ETAs) available in market which are helpful in guiding obstacles and potholes present on the road. But there is a possibility for that person to fall in a great trouble when the battery of ETA device suddenly gets discharged. Aiming to solve this problem, the objective of this project is to develop a guiding stick which will be able to generate electricity and store that energy in the battery already present in the device.

II. LITERATURE SURVEY

A lot of work has been done to make it easy for a blind person to walk on a road or anywhere else independently. These Guiding Machines (ETAs) are able to detect for obstacles in surrounding.

A. PIC Based Blind Man Stick

This stick is completely based on Programmable Interrupt Controller (PIC) [2] and the main component of this stick is Ultrasonic Sensor which detects obstacles near it. But lack in identifying shape of the obstacle. The PIC 16F877A is used to run overall microcontroller unit.

B. Intelligent Guide Stick

This Device is a Smart Stick which can detect for obstacles in both the sides, in front and in back of the stick. This stick implements Artificial Intelligence to decide better path and the main components used here are Sonar Sensors and a Camera for intelligent detection. [3]

C. IR Based Smart Stick

It works with the help of IR Sensors which make this device much Cheaper and Fast Responsive. Here only two IR sensors are used to detect for obstacles and staircases. [4]

D. Electric Walking Stick

It is a system which can be applied in straight path, right angled path or curved path with a width of at least 1 m. The main functions of this device are clear path indication and the recognition of environment. This system uses Microcontroller (AT mega 328). [5]

E. Intelligent Walking Stick for Blinds

This is a tremendous stick which can be connected to a smartphone for live location guiding. Also it provides a dynamic navigation through speech output to a person roaming in an unfamiliar location.

III. SYSTEM DESCRIPTION

A Piezoelectric Plate

It is a sensor which contains a piezoelectric material, most often, a piezoelectric crystal. When we press this disc like sensor it produces opposite charges on different sides of plate. Due to this a potential difference is generated to provide current.

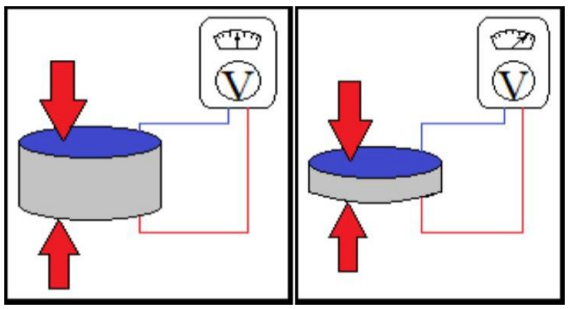


Fig. 1. Schematic Diagram of Piezoelectric plate

B. IR Sensors

These sensors consist of two parts, one is an emitter and other is a receiver. The emitter emits an Infrared Radiation which hits the obstacles and reflects back from the obstacle. The receiver receives the reflected radiation and the in-built system detects the distance between the stick and obstacles

C. Buzzer

This is a device which produces buzzes to indicate for any obstacle, pothole or any staircase. We can manage the frequency and number of vibrations to provide different signals for different situations.

D. Switch

This Switch is installed in handle to Switch ON or Switch OFF the whole device.

E. Arduino Nano or ATMEGA328 Microcontroller

It is a microcontroller unit which can be programmed and can be used for multiple functions such as controlling sensors and buzzers. It lacks in only a DC power jack. It works on an input power supply of 6 – 20 V and provides an output of 5V.

F. *Battery*

Here we will be using a lithium – ion chargeable battery for continuous power supply to our proposed system.

IV. Functional Description

The functionality of this device is divided in two parts, one is detection of obstacles, potholes, and staircase in path and other is charging battery system present in device.

A Pain Detection

The basic structure of this device is made up of two hollow aluminum pipes, a circuit box embedded into the handle and the Wheel Structure.

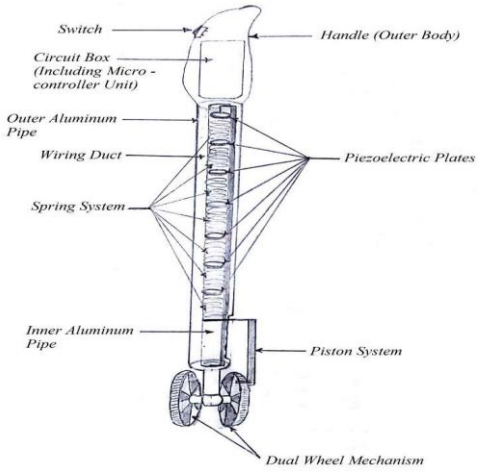


Fig. 2. Basic Structure of Stick

The Dual Wheel Structure is designed to help users to check for sudden inclinations and irregular surfaces. Most often it happens with the user of simple white cane that they become unable to check for sudden little inclinations in streets which is common in Indian cities and some rural areas. It may result in falling off on to the path. Also stepping suddenly on an irregular path or an area near any construction site, visually impaired people usually fall off. With help of this Dual Wheel Structure, it will be easy to detect for such drastic situations and to be prepared for it before stepping into the situation. Also the wheels are connected to piston system which is explained later.

The combination of outer and inner aluminum pipes creates an empty space in between both the pipes which is named as wiring duct in the proposed device. This empty space will be used for wiring purposes, that is, for connecting different electronic devices to the microcontroller and for making other connections.

The inner pipe contains a system of parallel connected piezoelectric plates and in between every two plate there is a light spring. The lower end of spring is connected to a crankshaft which is later connected to the wheel. This shaft along with wheel makes a piston system. When the wheel start rotating, the shaft begins its to and fro motion and a continuous compression and expansion process takes place in the inner cylindrical pipe which contains the complete system of springs and piezoelectric plates. Due to this regular compression and expansion process, piezoelectric plates produce voltage which is used in charging battery of device.

The handle of this device will contain the complete microcontroller system, the battery system and the charging circuit. And the outer body of this device will have IR sensors on front side and the back side will carry the Buzzers.

One of the IR sensors is placed near handle focusing towards floor and another near wheel pointed upwards. The upper sensor1 is able to detect for obstacles, potholes (shown in fig 2) and downward stairs. (shown in fig 3)

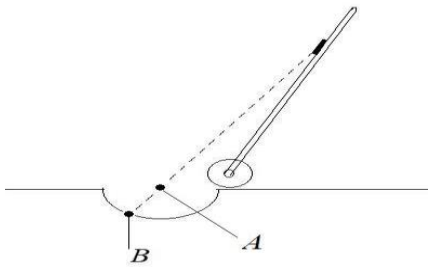


Fig. 3.Detection of pothole

For this purpose, the sensor measures the distance between floor and stick, if distance increases in a regular manner than it confirms for stairs but if distance increases in an irregular manner i.e. if there is a sudden increase and decrease or if the sensor doesn't receive back signal, it informs for a pothole.

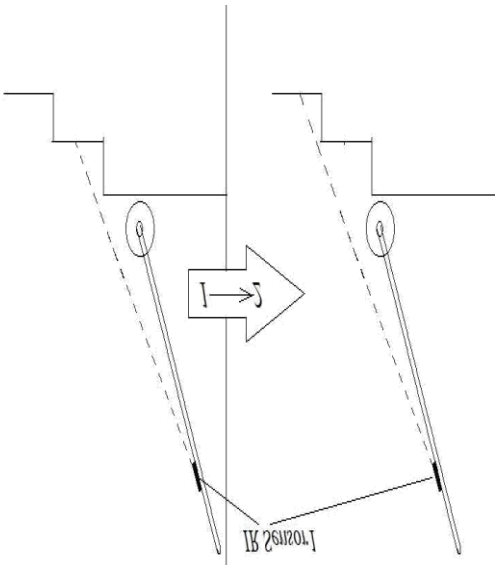


Fig. 4. Detection of downwards staircases

Similarly, the case may arise when a blind person is travelling in a narrow street and there is a window opened outwards, which is very common in crowded streets. For this problem, the lower sensor2 , which is deployed near wheel, detects for the obstacles present at certain height above the ground level also the sensor is able to check for the upward staircases as shown in picture given below in fig 5.

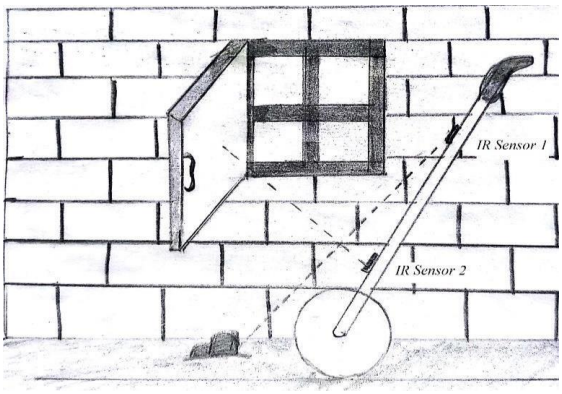


Fig. 5.Detection of Obstacle above ground

B Charging Battery

Piezoelectric system produces a voltage across its plates. This voltage provides current which passes through rectifier circuit for conversion into DC current. Also a capacitor is included in this circuit to make a continuous supply to the battery. This current is then passed to battery for charging via voltage sensing switch. Finally Using USB, energy is provided to Sensors and Micro – controller Unit. The Circuit diagram for charging is shown in fig 5 below.

When sensors detect for any obstacle, pothole, or staircase they send a signal to Micro – controller Unit (MCU). Then MCU send message to Buzzer which is fitted inside the handle. We can program different patterns of buzzer signals for telling the user about different types of obstacles. For example: a single buzz for an obstacle in between path, double buzz for pothole, zig – zag buzzing for raised obstacles and continuous buzzing for staircases.

In this way a blind person who cannot hear will also be able to use this stick.

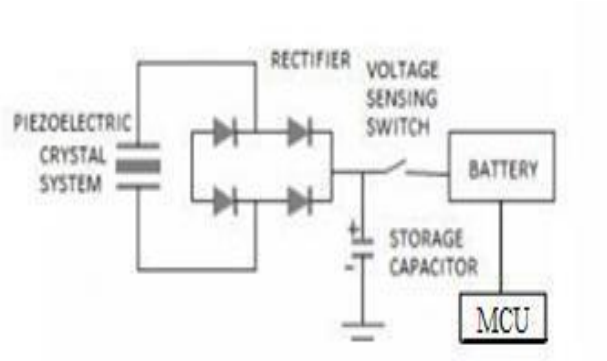


Fig. 6.Charging Circuit

Thus the working of overall device can be understood with the block diagram given below (fig 6)

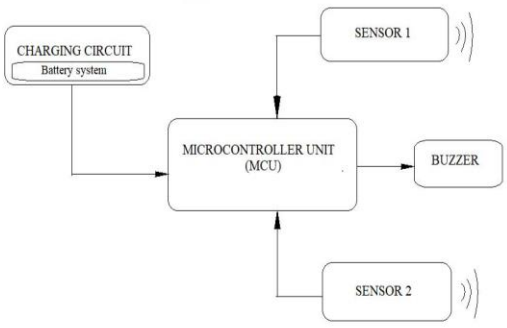


Fig.7. Block Diagram for working of overall device

V. Advantages and Disadvantages

Advantages:

- It will provide an emergency backup for power supply to sensors used in device.
- The device is able to detect for almost all type of obstacles.
- Reducing extra usage of sensors, speaker systems and an easily available structure makes this device cheaper and economically affordable by needy people.
- Spare parts for this device are easily available.

Disadvantages:

- Buzzer system may be confusing for the first time but with second or third use, it will become handy.
- Piezoelectric Plate sensors contain lead which may be harmful for children if damaged.
- The current design is not that much portable as other white canes are.

VI. Conclusion

This paper aims to propose an Idea of energy conservation by producing energy to help out blind or visually challenged people. This will provide a cheaper device, which will be easily available to needy people and will secure for their safety on roads and crowded streets. Also this device aims to solve the problems of sudden battery discharging on roads when the user becomes unable to replace or recharge battery.

VII. Future Scope

- We can make a segmented body design, which will be easy carry able.
- We can implement artificial intelligence with camera for better detection of pbstacles.
- We can connect the device with GPS system to guide a better path as per requirement. This will be helpful in determining for less hindered path.
- We can build an automatic switching circuit to switch off the overall device when not in use.

References

[1] Kounteya Sinha, “India Has Largest Blind Population”(2007, October 11) [Online] https://timesofindia.indiatimes.com/india/India-has-largest-blind-population/articleshow/2447603.cms

[2] A Parikh, D. Shah, K. Popat, H. Narula, “Blind Man Stick Using Programmable Controller (PIC)”,International Conference on Advanced Computing Technologies and Applications (ICACTA – 2015).

[3] S.J. Kang, Y.H. Kim, I.H. Moon, “Development of an Intelligent Guide – Stick for the Blind”, International Conference on Robotics & Automation Seoul, Korea, May 21 – 26, 2001.

[4] A.A. Nada, M.A. Fakhr, A.F. Seddik, “Assistive Infrared Sensor Based Smart Stick for Blind People”, Science and International Conference 2015, London, U.K. , July 28 – 30, 2015.

[5] S. Chaurasia, K.V.N. Kavith, “An Electric Walking Stick For Blinds”, ICICES 2014 – S.A. Engineering College, Chennai, Tamil Nadu, India.

[6] K.Chaitrali, D.Yogita, K.Snchal, D.Swati, D.Arti, “An Intelligent Stick for the Blind”, International Journal of Engineering Research and General Science Volume 3, Issue 1, January – February 2015

Smart Diagnosis Using Machine Learning

[1]Ujjwal Mittal, [2]Sanya Swain

[1,2] CSE, HMRITM GGSIPU, Delhi, India
[1]ujjwal.hmritm@gmail.com , [2]sanyaswain16@gmail.com

Abstract— We discuss a plausible way for smart diagnosis. Theuse of Deep Learning in image processing can enable us to build Models to detect the presence of ailments in Diagnostic Images such as X-Ray or CT Scans performing as a diagnosis tool. These trained models can be effortlessly added into an easily accessible portal like a website or a phone application providing ease of use even for a non-practitioner. Further, we have covered a case study on how we built a Convolution Neural Network Model over a set of X-Ray Images of Lungs to determine the presence of pulmonic disease like Pneumonia using Keras framework.

Keywords— Smart Diagnosis; Machine Learning; Deep Learning; Convolution Neural Networks.

I. INTRODUCTION

Machine Learning, subset of Artificial Intelligence, is a broad area of study whose use as a technology has proliferated in the recent times due to its wide and ambitious applications. It deals with developing algorithms that can utilize a large amount of data to 'train' itself to recognize similar data without any explicit programming. These 'trained' models can predict or classify the resultant attribute of similar data. It possesses the ability to solve numerous real world problems as we can process not only textual, but moving visuals and audio too. Its current applications are widespread over domains like Computer Vision, Pattern Recognition, Language Processing, Monitoring, and Diagnosis and so on. For example, Microsoft's InnerEye, which began in 2008, is an initiative on diagnostic imaging using Machine learning.

Researchers of Google Brain are taking a pilot at Aravind Eye Hospital in Madurai and planning a similar one at Sankara Nethralaya Hospital to grade photos of patients' retinas via AI to detect Diabetic Retinopathy in the World's Diabetic Hotspot – India [2]. These examples clearly display prevalent research and development of AI and Machine Learning in Health Care Sector. But there are certain problems which restricts complete deployment of AI for replacement of human experts. Practitioners often argue that increment of tools in diagnosis will just augment the detection process and amalgamating the result will be a hassle.

Also, introduction of AI will generate contraptions that may need additional expertise to comprehend the working and produced output. The recent rise in research on AI for health diagnosis provides us plausible plan. The easy coding provides us with functional ML models which can process Diagnostic images and classify them as containing abnormality or are benign to high accuracy (up to 96%)[4]. These models are utilizing algorithms such as Support Vector Machine, Naive Bayes, Artificial Neural Networks and further derivation of these [3]. The detection by these trained models is being stated as better than bare eye human expertise. Moreover, due to the flexibility of technology provided by Tensor Flow, we propose that these 'trained' models can be added to everyday use interfaces such as Phone Applications .

Conclusively, this means that we could upload a photograph of a scan or X-ray image on our Android Device Application and develop an estimated report for the illness in the patient, if it exists. We are investing in a system that is extremely user friendly and provides user interface comprehensible even for non-technical crowd .This reduces the complexity of medical diagnostic procedure aligning to time and cost restraints. To illustrate our methodology, we have implemented a Convolutional Neural Network model over X-ray images of lungs of children to detect presence of Pneumonia. CNN is efficient for Image Processing due its multi-layer model structure and was an optimum choice [6]. The model displays accuracy to certain extent. Tensor Flow Library will further enable us to add our model to a Android application. We can further construct a user friendly Interface and display result in a comprehensible format.

II. SMART DIAGNOSIS

A. Problem In Diagnosis using Machine Learning

AI has gained a lot of attention and research for health care and detection. Researchers have constructed Machine Learning models that are around 95-96% accurate in detecting diseases [4], which is statically better than how doctors detect it using their personal expertise. But these tools remain unimplemented in the actual sector probing the question on what improvement can we bring about in these ideas to make them adaptable to the current health diagnosis setup. We try to see it from the perspective of both the patient and practitioner. The factors of a diagnostic process that matter the most to a patient is - the communication of an accurate and timely explanation of their health problem which is cost and time efficient. While for the doctor, the diagnostic tool must be easy to use, reducing the complexity of diagnostic procedure without need of external technical expertise. With the availability of numerous tools, the diagnostic process has become a time consuming and costly process. Moreover, the patient, who may be a non-practitioner, may not understand the need of such a lengthy diagnostic process[3].

B. Solution Devised

Our plausible idea is to build a ML model which can classify diagnostic images like X Rays and CT Scans to detect presence of any disease .These models will intake labeled images of scans as input data to train itself to recognize similar images and whether they are infected or not. If trained suitably, it will be able to spot any anomaly in the given diagnostic

image and give out a report depending on the kind of abnormality it witnesses. These models can be added to Mobile or Web Applications using suitable libraries, thus simplifying the process. Thus, a doctor could simply upload a Diagnostic Image of the patient to the application to get a report .This procedure would be fundamentally easy, quick and transparent which can even be apprehensive for the non-technical crowd. To test out idea, we tried to implement a basic Artificial Neural Network Model over a data of X-ray images to diagnose an illness. Hence is the case study of the methodology we followed.

III. Case Study

Pneumonia is an infection in the lungs affecting mostly children below the age of 2 years and adults aged 65 years and older. It affects the lungs by inflaming the air sacs present there with fluid or pus, making it difficult for the patient to breathe and causing incessant coughing. [18] While it usually is not a life threatening disease, it is a major cause of child mortality in many developing countries, causing almost 2 million pediatric deaths every year. [4].

A. Present Diagnostic Procedure of Pneumonia

Diagnosis of pneumonia is conducted by healthcare professionals by conducting thorough history and physical examination of the patient. Further a series of tests are recommended depending on the severity of symptoms and obscurity of diagnostic results. These tests range from Blood Tests, Chest X Ray imaging, Pulse Oximetry and Sputum test. If you are a patient of high risk, due to your past health history or present age and health status, further tests like CT Scans may be advised to get a better look of chest inflammation. [7]

B. Reducing the Need of Multiple tests

We present the scope of detection solely using X Ray Scans in an effortless manner.

- Machine Learning Algorithms for Image Processing can enable us to classify images as malign or benign.
- The normal chest X-ray depicts clear lungs without any areas of abnormal opacification in the image. Bacterial pneumonia typically exhibits a focal lobar consolidation, whereas viral pneumonia manifests with a more diffuse ‘‘interstitial’’ pattern in both lungs. [10] These are the patterns that the ML algorithm builds on to make predictions on the test set.

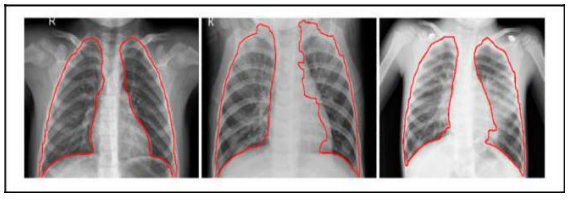


Fig. 1. The highlighted parts display the Lung which are processed during building model.

- We will use Machine Learning and Deep Learning libraries, functions, and algorithms to build the main working algorithm for this software. We will use CNN, an abbreviation for Convolutional Neural Network, for building the framework of this software. CNN is a class of deep neural networks used for analyzing visual imagery. They are a type of multilayer perceptrons, also known as fully connected layers wherein each neuron in a layer is connected to all the neurons in the next layer. [17].

C. Convolution Neural Network

Convolution Neural Network has 4 main steps – Convolution, Max Pooling, Flattening, and Full Connection. The convolution layer is the main building block of a convolution neural network. Its main aim is to extract high-level features such as edges etc. from the input image. The input image is divided into a matrix of pixels. To perform the convolution operation, a kernel or filter is selected – it is a matrix having smaller pixels than that of the input image. This kernel traverses the entire image to provide us with feature maps (the output received on convolving the image with a particular filter is called a feature map) [8].

The next layer is the pooling layer. It is used to further reduce the spatial size of the feature map. It extracts the dominant features of the image and gets rid of the redundant parameters, thereby reducing the computational power of the network and effectively training the model. Each feature map is operated upon individually. The most common approach used in this layer is max pooling. It has a better performance as compared to average pooling since it returns the maximum value from the portion of the image covered by the feature maps [9].

The next step is flattening wherein the matrix is flattened into a one dimensional matrix, analogous to a chain of neurons. It is called the column vector. This flattened output is fed to a feed-forward neural network in the fully connected layer and back propagation is applied to every iteration of training. The fully connected layer of neurons at the end of CNN has full connections to all activations in the previous layer. Over a series of epochs, the model is able to distinguish between dominating and certain low-level features in images and classify them accordingly [9].

D. Data Used

- The data set which we will work on is organized into 2 sets (train, test) which contained images of each category (Pneumonia/Normal). There are 5,863 X-Ray images (JPEG) divided into 2 categories-Pneumonia and Normal, which were kept in separate Sub directories under the Train and Test Directories.
  •Chest X-ray images (anterior-posterior) were selected from retrospective cohorts of pediatric patients of one to five years old from Guangzhou Women and Children’s Medical Center, Guangzhou.
- For the analysis of chest X-Ray images, all chest radiographs were initially screened for quality control

by removing all low quality or unreadable scans. The diagnoses for the images were then graded by two expert physicians before being cleared for training the AI system. In order to account for any grading errors, the evaluation set was also checked by a third expert. [10]

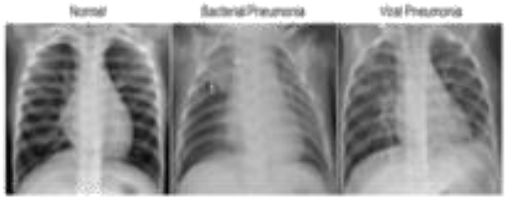


Fig. 2. Sample Images of Data showing Normal, Bacterial Pneumonia and Viral Pneumonia [10]

E. Process and Code

- Initially, the images in Pneumonia Sub Directories were labeled as Positive of '1.0' and the Normal Images were labeled as Negative or '0.0'.
- Using an object of Sequential model from Keras Framework we build a model adding layers.
- *Convolution2D*: Convolution matrices were builtand images were resized into 64*64.
- *Pooling2D:* Pooling matrix size was adjusted to2*2.
- *Flattening*: We have used the flatten function toconvert the output into 1D vector for further processing by the last step called the dense.
- Final step of full connection where we add multiple layers to the model for neural network. Relu was used as the activation function for final layers. A compilation function was used with suitable optimizer, loss and metrics.
- Finally, the data from train and test data was fit into the model to produce a prediction data frame for the test data.

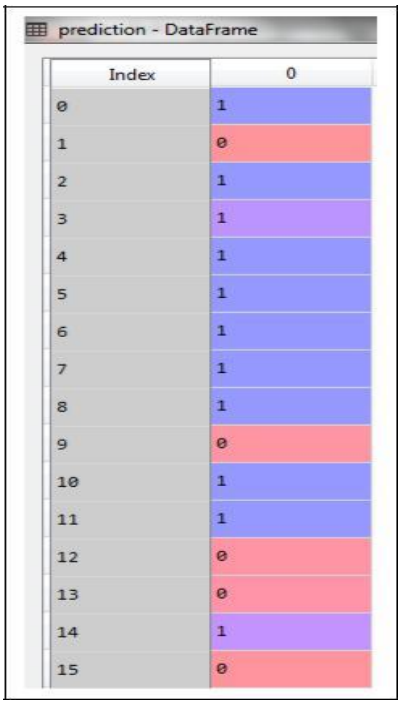
F. Outcome

The test data comprised of 15 images which were a mixture of both benign and malign Pneumonia. The prediction for Each image is given against it's index in Fig. 2. As per the labeling we followed, a '1' depicts a chance of lungs being infected with pneumonia, while a '0' indicates a negative result. On comparing with the original labeling through confusion matrix, 50% of the results were accurate. We plan to improve the accuracy by working on the various hyper parameters.

G. Improvement

Our model is an illustration and needs improvement in its accuracy. Related works tell that researchers have been effective in developing more precise classifiers for similar models. A similar lung classifier built for Lung Cancer Detection claims of 79.6% accuracy [11].

Also, we plan to add our model to a mobile application to feature its graspable employment using Tensor Flow Library. Steps include converting the trained model into Tensor Flow model, adding Tensor Flow as a dependency in the application and putting down Java code to perform inference in your app with the Tensor Flow model [5]. Further, we need to add user interface that will enable uploading X Ray Images to get the prediction and exhibit it in a perceivable form.



Index	0
0	1
1	0
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	0
10	1
11	1
12	0
13	0
14	1
15	0

Fig. 3. Output Window of Test Data Comprising of 15 images displayed in the index. While the second column displays the estimated predictory value-1s and 0s.

IV. RELATED WORK

There are a bundle similar works in field of Diagnosis using Deep Learning that can be spotted. Visualization and Interpretation of Convolution Neural Network Predictions in Detecting Pneumonia in Pediatric Chest Radiographs have been reportedly been performed in past with good precision[4]. In the field of Dermatology, Stanford researchers have trained an algorithm to diagnose skin cancer with reliable accuracy and have successfully used it in medical practice over a web application[12][13].CT scans can be utilized to detect hemorrhage using Deep Convolution Neural Network[16]. Even more basic algorithms like Support Vector Machine (SVM) have been used in assistance to detect illness. For example - Breast Cancer has been reportedly detected by a CNN supported SVM Model with accuracy up to 83.3%[14,15]. There is a further wide variety of work on various diagnosis using Image Processing which can seek improvement to be deployed in medical practice.

V. Future Scope

A. Need for More Accurate Models

We have come across various models and researches detecting diseases at accuracy ~ 90% and more, but in case of fatal illnesses like Cancer we cannot afford to minute percentage of errors. A single false negative can be fatal if we rely solely on the existing Image processing models. Vice versa, a false positive could be ineffective too [3]. Thus, we seek algorithms and image processing techniques which are highly effective with nearly zero error rates. Else, a need for human expertise will still exist to decide in regard to diagnosis.

B. Building a Multi Diagnostic Application

As in the related work section, we saw the proliferating successful research in Deep Learning Models for Diagnosis, we could coalesce them into one single multipurpose Application to detect various ailments which can revolutionize medical diagnosis. The Application may provide options to choose the specific condition we want to diagnose for and provide support from the respective model . This would end the need for multiple diagnostic tools and will simplify the detection procedure. Currently, this is a vision and will require extensive improvement in the existing researches. Though, we view this consolidation as a complete possibility.

VI. Conclusion

Technology is seeping deep in every industry, and with the advent of new technologies like Machine Learning and Deep Learning, a question that arises is how every industry can benefit and excel in its field using the said technologies. Medicine and health is a field where it is pivotal to keep updating and improving the existing technologies and methodologies for better treatment purposes. We propose a system to incorporate the various concepts of Machine and Deep Learning in health diagnosis to build a portal effective and efficient enough to tackle modern day diagnostic hassles.

Acknowledgment

The success and final outcome of this research paper required a lot of guidance and assistance from many people and we are extremely privileged to have got this all along the completion of our paper. All that we have done is only due to such supervision and assistance and we would not forget to thank them.

We owe our deep gratitude to our guide Ms. Charu Chabbra, Assistant Professor, CSE Department, HMR Institute of Technology and Management, who took keen interest in our paper and guided us all along, till the completion of our paper by providing all the necessary information for developing a good paper.

We are thankful to and fortunate enough to get constant encouragement, support and technical guidance from Mr.Rohan Rana, our fellow batch mate, which helped us in successfully completing our research paper.

References

[1] Project Inner Eye - Medical Imaging AI to Empower Physicians, Microsoft, October 2008. Available: https://www.microsoft.com/en-us/research/project/medical-image-analysis/

[2] Alnoor Peermohmed, “With 98.6 accuracy, Google AI to tell if diabetes will hamper your eyesight”, *Business Standard*, May 3,2018.

[3] Yu, K.-H., Beam, A. L., & Kohane. “Artificial intelligence in healthcare*”. Nature Biomedical Engineering,* 2018.

[4] Sivaramakrishnan Rajaraman et al. , “Visualization and Interpretation of Convolutional Neural Network Predictions in Detecting Pneumonia in Pediatric Chest Radiographs”, Advanced Intelligent Imaging Technology), September 2018

[5] John Olafenwa, “Deploying PyTorch and Keras Models to Android with TensorFlow Mobile”, *HeartBeat,* Jun 2018 .

[6] Matthew D. Zeiler, Rob Fergus, “Visualizing and Understanding Convolutional Networks,” Computer Vision – ECCV 2014, September 2014

[7] Pneumonia Symptoms and Diagnosis, American Lung Foundation, Available:https://www.lung.org/lung-health-and-diseases/lung-disease-lookup/pneumonia/symptoms-and-diagnosis.html .

[8] Harsh Pokharna, “The best explanantion of Convolutional Neural etworks on the Internet”, Medium, Available: https://medium.com/technologymadeeasy/the-best-explanation-of-convolutional-neural-networks-on-the-internet-fbb8b1ad5df8

[9] Sumit Saha, “A Comprehensive Guide to Convolutional Neural Network – The Eli5 way”, Towards Data Science, Available: https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53

[10] Paul Mooney, Chest X Ray Images, Pneumonia, Kaggle. Available : https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia/activity .

[11] Wenqing Sun, Bin Zheng, Wei Qian, “Computer aided lung cancer diagnosis with deep learning algorithms,” Proceedings Volume 9785, Medical Imaging 2016: Computer-Aided Diagnosis, March 2016.

[12] Andre Esteva et al. , “Dermatologist-level classification of skin cancer with deep neural networks”, Nature, June 2017

[13] Taylor Kubota, “Deep learning algorithm does as well as dermatologists in identifying skin cancer”, Stanford, January2017

[14] Ruey Feng Chang et al. , “Support Vector Machines for Diagnosis of Breast Tumors on US Images”, Academic Radiology, Volume 10, Issue2, February 2003, Pages 189-197, February 2003

[15] Teresa Araújo, “Classification of breast cancer histology images using Convolutional Neural Networks”, Plos, June 2017

[16] Hyunkwang Lee et al. ,”An explainable deep-learning algorithm for the detection of acute intracranial haemorrhage from small datasets”, [17] Nature Biomedical Engineering, December 2018 Convolutional Neural Network”, Wikipedia, Available, https://en.wikipedia.org/wiki/Convolutional_neural_network

[18] “Pneumonia”, Mayo Clinic Available, https://www.mayoclinic.org/diseases-conditions/pneumonia/symptoms-causes/syc-20354204

.

Ethical Hacking: A Necessity

[1]Sagar Sharma, [2]Ashish Rana, [3]Rohit Prajapati
CSE, HMRITM, Delhi, India
[1]sagarshrm029@gmail.com, [2]ashishrana3435@gmail.com, [3]rohitpra.d16@gmail.com

***Abstract*—** In today's era, our data is as valuable as moneyand sometimes more. This is the reason the fear of information being compromised by a cybercriminal worries everyone including the government, private industry and the everyday computer user. Cyber Crime is estimated to cost $6 trillion by 2021. Because of the increasing number of attacks, people need ethical hackers. The task of an ethical hacker is to find vulnerabilities and weakness in the system or network that can be exploited to gain access to the data and then provide a solution to prevent this from happening. This paper will describe what is the need of ethical hacking, why it is so crucial regarding data security, and how it is performed.

Keywords— Cybercriminals; Ethical Hacker; Vulnerabilities; exploited.

I. INTRODUCTION

The term Hacker strikes a false image in the mind of a normal person who has no idea who a hacker really is. Originally, the term meant a person who is interested in learning about the computer system and wants to know the limits it can be stretched to bring out its capabilities, opposed to a normal user who only uses it to the amount required. A hacker is someone who enjoys programming rather then just study about it.It was extended to the verb form "hacking" which was used to describe the quickly creating a new program or making changes to an existing one.The term meant as a compliment changed its meaning shortly after. As the popularity of computers increased and the technology developed further, the cost became high and it was not accessible to everyone. Some users challenged the system to get through its security controls. They did this by stealing someone's password, exploring the bugs or even take control of the whole system.In the beginning, the most damage done was theft of time. Other time, they were in the form of practical jokes but not for long. Occasionally the intruders would accidentally bring down a system or damage its files, so that it had to be restarted or repaired. Once denied the access after being detected, they would react with intentionally harmful actions. As the number of these destructive computer intrusions became noticeable, media took no time and it became "news". When the news media picked up on the story, instead of using the more accurate term of "computer criminal" they began using the term "hacker" to describe individuals who break into systems for fun, revenge, or profit. Since calling someone a "hacker" was originally meant as a compliment, computer security professionals prefer to use the term "cracker" or "intruder" for those hackers who turn to the dark side of hacking.

II. LITERATURE SURVEY - ETHICAL HACKING

Hacking is using the knowledge of system and networks to access the protected data that may or may not be used to harm an individual or an organization.

Hacking can be broadly classified as:

- Ethical hacking
- Unethical hacking

Also known as penetration testing and intrusion testing or red teaming, ethical hacking is the act of employing the tools and tactics of hackers to test the security precautions protecting a network, but with the client's permission to do so. This is done with the help of tools which are made for testing the security level of a system by trying to breaking-in or bypassing the security.

Unlike malicious hackers, the purpose of ethical hacking is to improve the security of system by fixing the vulnerabilities found during the process. Tools and techniques used in ethical hacking are same ones used by the cyber criminals but with the authorized permission of the user to defend the system from the attacks. Initially it was started by the US government to hack its own systems in 1970s to check their if their system security is penetrable or not. Telecommunication companies began using ethical hacking in 1980s and banks caught on in the 1990s. Since then, most of the e-firms started practicing ethical hacking as a critical security measure because a single intrusion or interruption can cost massive financial loss as well as loss of potential customers.

The market for this service consists of clients worried about the security of their information that varies from emails to credit card numbers, phone number and their home address. Those vulnerabilities can be exploited to steal or manipulate the data which may prove harmful to the client personally or financially. The work of an ethical hacker is to report the client about their findings as a result and providing solutions to fix these vulnerabilities.

III. WHO IS ETHICAL HACKER?

A hacker is basically someone who gains access of a system without the permission of the user. Its opposite, an ethical hacker is a skilled professional with the same technical knowledge and skills as hacker, but he uses his skills to protect the system and networks from being attacked by hackers who can steal important information. To become a certified ethical hacker, they go through intense training programs and exam to pass. Their work is completely legit and they work with the permission of the target to break into their system or network to check its security. While testing the security of a system, an ethical hacker looks for answer to these three basic questions:

- What information an attacker can steal from the system?
- What can the attacker do with that information?
- Does the victim notice the attempts of attacker?

Unlike movies and TV series, hacking is a slow process hence requires a lot of patience. For penetration testing, it might take days and even months in some cases. Rushing the process can lead to damage or loss of data. They work carefully so that they don't interrupt the client's work. Hackers can be divided into three groups based on their work as: - Black hats, White hats and Grey hats.

A Black hat hacker

Black hat hackers are the bad guys who engage in hacking for illegal reasons. They are malicious hackers or crackers who use their skills to break into systems. By gaining unapproved access they steal data and simply cause problems for the targeted user. The "hacker poster boy" Kevin Mitnick, a black hat, was pursued by the authorities for very long. The Department of Justice described him as "the most wanted computer criminal in the United States history."

B White hat hacker

White hat hackersor the ethical hackers are thegood guys who provide their skills to protect the systems from computer criminals. With the help of their knowledge of hacking and toolset, they detect weakness and implement countermeasures. Stephen Wozniak, "Woz", the co-founder of Apple got his start in hacking making blue boxes, devices that bypass telephone-switching mechanisms to make free long-distance calls.

C Grey hat hacker

Grey hat hackers are the ones who work who work according to the situation. They can be offensive as well as defensive. There is a line between a hacker and a cracker. Grey hats qualify as both, but their existence clouds the difference between the above two.

IV. NEED FOR ETHICAL HACKING

Not everyone hacks for knowledge. Some engage in hacking for mischief and pranks while some intend to harm the files or even bring down the whole system. Ethical hackers are our walls of protection against the criminal hackers and they try to do their best to determine if a hacker was to attack a system or a network, how would they do it. The most basic way to avoid a hacker is to think like one. That is what ethical hacker does. An ethical hacker thinks like a hacker, how he can break into system security, what tools or technique he may use, keeping all this in mind he tries to increase the system security to prevent any malicious attack. Some of the many reasons we need ethical hackers are:

- Identifying vulnerabilities that other programs can't detect.
- Testing a networks defense against attacks of all sizes and finding holes in a Wi-Fi system
- Providing evidence that a security system may/may not need further investment.
- Educating a company on how easily it is to slip in through employee devices, flash drives, and simple passwords.

Some are afraid to give such access to a hacker in their company or private space who can steal the data easily. The data can cost them a lot and can be sold at high prices at black market. But certified ethical hackers go through very tough process to get certified. One of the important things is that ethical hackers are trustworthy, and they can be trusted with the sensitive data. That is the reason certified ethical hackers are preferred over black hat hackers who become white hat hackers, there is lack of trust.

V. STEPS FOR ETHICAL HACKING

There are five steps involved in the process of ethical hacking:

A Reconnaissance

This is also known as foot printing and information gathering, it means using tools and techniques for secretly gathering as much information as possible about the target system. There might be some information that may seem useless while gathering but during the next steps, it may prove very important. So, one should save any information we get about the target during the reconnaissance. Basic information like domain name, source code, metadata profile of a website or a network can be found easily using Google.

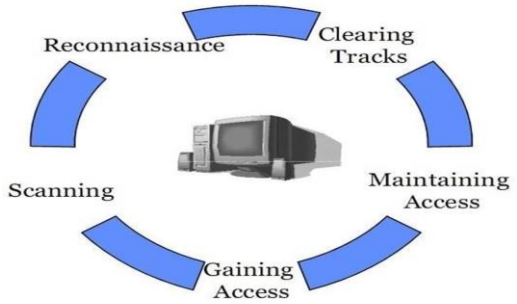


Fig. 1. Steps of hacking

The information collected is usually about the three groups: Network, Host and People Involved. Foot printing is of two types:

- Active: Information is collected using tools like Nmap by directly interacting with the targets.
- Passive: Information is collected indirectly from searching places like social media, public websites etc.

Tools used for reconnaissance are Whois Lookup, NSLookup, search engines like Google.

B Scanning and Enumeration

Next step in ethical hacking involves two terms that are scanning and enumeration. In this phase, hacker tries to find any open doors through which he can enters the system and look for information that can help in gaining higher access to modify or delete data.There are three types of scanning involved: Post Scanning, Vulnerability Scanning and Network Mapping.

Post Scanning is the Scanning the target for information like open ports, live system, operating system, services running on host based on the information gathered during reconnaissance.

In Vulnerability Scanning target is scanned for weaknesses and vulnerabilities with the help of automated tools. In Network Mapping Finding firewall servers, routers, topology of network of the target and creating a network diagram which is used as a map during the further process. Tools used for scanning are Ping, Tracert, Nmap, Netcraft.

C Gaining Access

After information is gathered and vulnerabilities are found, hacker tries to exploit those weaknesses in security with the help of tools listed below. Then he increases his privileges to administrator so that he can install required applications, modify or delete data.

Tools used for gaining access are John The Ripper, Konbot, Pwdump7, Wireshark, Fluxion.

D Maintaining Access

After gaining access, if the hacker wants to show what kind of damage can be done to the system, he tries to maintain the access without alarming the user. This can be done with trojan horses which have access to application level or with the rootkits with access to operating system level. The aim is to maintain access until the planned task, i.e., penetration testing is completed.Trojan horses can be used to steal information like emails, usernames, passwords and credit card information from the system. Tools used for maintaining access are Metasploit, Beast, Cain & Abel.

E Clearing Tracks

This step is all about destroying the evidence of any activity to evade trace back and further punishment as it is a cybercrime. If a hacker wants to remain anonymous, then removing any sign of presence is important. This includes clearing log files, caches and cookies, changing registry values, uninstalling the applications used and deleting the folders and files created during the process. First thing done security team is to monitor any suspicious activity which can be done by checking the log files, so it is important to change the log files to prevent the intrusion from being suspected and any further investigation to take place. Tools used for clearing tracks are Metasploit an OSForensics.

VI. TOOLS USED IN HACKING

There are various tools of hacking but widely used tools are as follows:

Tools	***Description***
Google	A search engine which is used to give all the basic information of the website.
Nmap	Network mapper, or Nmap, is used for network discovery and security auditing.
Netcraft	Used for internet security services, Netcraft provides anti-fraud and anti-phishing services, application testing using the analysis of the network.
John The Ripper	Also referred simply as 'John', it is a very popular password cracking tool used to carry out dictionary attacks
Pwdump7	Pwdump7 is the program that yield the LM and NLTM password hashes of local user accounts from the Security Account Manager (SAM).
Metasploit	Metasploit is a multi-purpose tool which is used in maintain access as well as clearing tracks. It provides vital information regarding known security vulnerabilities and helps to formulate penetration testing plans, strategies and methodologies for exploitation.
Cain & AbelIt	Cain & AbelIt is a tool used for both gaining access and maintaining access in system. It recovers passwords using network packet sniffing and by tools to crack passwords hashes.

VII. CONCLUSION

Today, when everything is getting connected to internet, cybercrime is becoming a greater threat and to tackle that ethical hacking is necessary, but not everyone is aware about it. This paper introduces us to the basic terms like hacking, ethical hacking, who are ethical hackers and why do we need them, and most importantly an overview on how ethical hacking is performed and tools used for it. Everyone should know the basics of ethical hacking to prevent their information like emails, passwords, home address, credit card

details and what not. The more aware we are about these attacks, more easily we can protect ourselves from them.

REFERENCES

[1] Hessa Mohammed Zaher Al Shebli, Babak D. Beheshti ,"A Study on Penetration Testing Process and Tools".

[2] Marilyn Leathers , " A Closer Look at Ethical Hacking and Hackers".

[3] Sonali Patil, Ankur Jangra, Mandar Bhale, Akshay Raina, Pratik Kulkarni, "Ethical Hacking: The Need for Cyber Security".

[4] Alok Singh, Brijesh kumar Pandey, Lovely Balani, "Ethical hacking(Tools, Techniques and Approaches)"

[5] Internet Security Systems, Network and Host based Vulnerability Assessment.

[6] https://phoenixts.com/blog/why-do-we-need-more-certified-ethical-hackers/

[7] https://www.greycampus.com/opencampus/ethical-hacking

[8] Information Security Media Group, Corp. [US] ,https://www.bankinfosecurity.com/interviews/we-need-ethical-hacking-i-1145

[9] http://www.corecom.com/external/livesecurity/pentest.html

[10] https://www.simplilearn.com/phases-of-ethical-hacking-article

Cardiac Arrest Prediction using Artificial Neural Networks

[1]Ayushi Batra, [2]Sakshi Kaushik, [3]Samarth Karan
Department of IT, HMRITM, Delhi, India

[1]ayushibatra0209@gmail.com, [2]sakshi24kaushik@gmail.com, [3]samarth176@gmail.com

***Abstract*—** Heart diseases are the leading cause of death around the world, if it isn't just sufficient, it is also a major cause of disability among all. But should it mean that it has to be accepted as a fate? Well no, although humans lack the power to change some risk factors — such as family history, sex or age — there are some key heart disease prevention steps one can take to reduce this risk. Before everything, it becomes really important to have an early diagnosis of the same heart disease that is supposed to be worked out a healthy lifestyle for. Although traditional track-and-trigger systems are used to predict cardiac arrests early, but these diagnostic methods have their own limitations, they are time consuming, less sensitive, invasive and/or have high false-alarm rates. In this research paper, a Heart Disease Prediction system (HDPS) is worked upon which uses artificial neural network. The HDPS system predicts the likelihood of a patient getting a heart disease and for this the system uses 11 clinical features as an input for the neural network and then the neural network has been trained to predict the absence or presence of heart disease. The accuracy is calculated and visualized as of 83.5% which was the most accurate out of all the implemented algorithms.

Keywords— Diagnosis; Prediction; Neural Networks; Health; Decision; Dataset.

I. INTRODUCTION

The heart is the main organ of the human body If it stops working correctly our whole body can get infected and in most cases, this disease leads to death. From 1990 to 2013 41% cardiovascular disease increased globally. Life is not possible without a functioning heart and so human beings cannot survive without it. It controls our blood pressure, body temperature and many other vital health aspects including oxygen regulation in the blood. Some of the most common factors that contribute to the heart disease include family genetic problems which come from generation to generation, high blood pressure, Cholesterol, Sex, Age mostly above 30, Poor diet, Calcium rate, a blood vessel of heart got over stretched, lake of exercise etc. Heart disease is a persistent apprehension of the whole world as it is frequently increasing in ratio per person. The heart is the main regulating organ of the human body. According to the Institute for Health Metrics and Evaluation (IHME) death rate due to this disease has shown an alarming 41% increase from 1990 to 2013 and a 9.83% further increase in 2014. Survey analysis of (WHO) shows 17 million deaths due to heart disease. If any disease gets predicted at earlier stages, then it becomes easier to find or apply a cure before it gets dangerous. Just like that, if a heart disease is predicted earlier, it becomes easier to find a cure. This type of prediction problem, related to medical diagnosis comes under the branch of computer science i.e., bioinformatics. In bioinformatics, for prediction, we need previous historical data of the patient and some pattern matching algorithms which can be trained on the respective data to generate results. In clinics and health centers, a lot of patients are being diagnosed daily so there is a lot of data collection, for example, in the form of Medical Reports. Collection of data from these reports can be used for extracting knowledge from data. This can be done by a well-known model of bioinformatics i.e., Knowledge Discovery from Data (KDD). Prediction should be done to reduce risk of Heart disease. Diagnosis is usually based on signs, symptoms and physical examination of a patient. Almost all the doctors are predicting heart disease by learning and experience. The diagnosis of disease is a difficult and tedious task in medical field. Predicting Heart disease from various factors or symptoms is a multi-layered issue which may lead to false presumptions and unpredictable effects. Healthcare industry today generates large amounts of complex data about patients, hospitals resources, disease diagnosis, electronic patient records, medical devices etc. The large amount of data is a key resource to be processed and analysed for knowledge extraction that enables support for cost-savings and decision making. Only human intelligence alone is not enough for proper diagnosis. A number of difficulties will arrive during diagnosis, such as less accurate results, less experience, time dependent performance, knowledge up gradation is difficult.

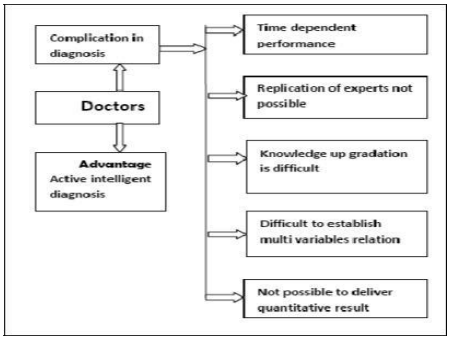


Fig. 1. Steps of diagnosis

In order to improve the accuracy of diagnosis and to reduce the diagnosis time, we have developed an efficient and reliable Decision Support System for Heart Disease using Neural networks. If by implementing any particular machine learning algorithm out of all the ones that we've considered for the project working, we can actually come through the occurrence of any of the heart diseases, then it should purely be seen as a milestone in the field of engineering and medical sciences and it doesn't really just achieve a huge recognition but also can be useful for the prevention or to the least reduction of death that can be caused by cardiac arrests upto a very noticeable level which eventually proportionate to the life expectancy rate.

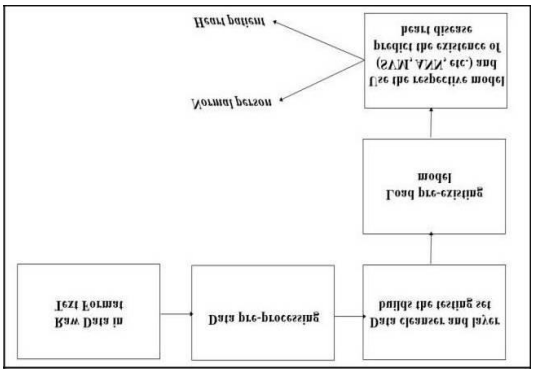


Fig. 2. Actual Implementation of the Project

The proposed system has been developed with the aim to classify people with heart disease and healthy people. The performances of different machine learning predictive models for heart disease diagnosis on full and selected features were tested. Feature selection algorithms such as Linear regression, SVM, ANN, Random forest, Decision tree have been used to select important features, and on these selected features, the performance of the classifiers is further tested. The model's validation and performance evaluation metrics have eventually been computed. The methodology of the proposed system is structured into five stages including (1) raw data gathering, (2) preprocessing of dataset, (3) load pre existing model, (4) machine learning classifiers, and (5) classifiers' performance evaluation and providing results to the end user.

II. Related Work

Work done in heart disease diagnosis using data mining and artificial neural networks are discussed below:

Sellappan Palaniappan et al. developed a prototype Intelligent Heart Disease Prediction System (IHDPS) using data mining techniques, namely, Decision Trees, Naïve Bayes and Neural Network. IHDPS can answer complex "what if" queries which traditional decision support systems cannot. Using medical profiles such as age, sex, blood pressure and blood sugar it can predict the likelihood of patients getting a heart disease. IHDPS is Web-based, user-friendly, scalable, reliable and expandable. It is implemented on the .NET platform.

Dilip Roy Chowdhury et al. represent the use of artificial neural networks in predicting neonatal disease diagnosis. The proposed technique involves training a Multi Layer Perceptron with a BP learning algorithm to recognize a pattern for the diagnosing and prediction of neonatal diseases. The Back propogation algorithm was used to train the ANN architecture and the same has been tested for the various categories of neonatal disease. About 94 cases of different sign and symptoms parameter have been tested in this model. This study exhibits ANN based prediction of neonatal disease and improves the diagnosis accuracy of 75% with higher stability.

Vanisree K et al., has been proposed a Decision Support System for diagnosis of Congenital Heart Disease. The proposed system is designed and developed by using MATLAB's GUI feature with the implementation of Back propagation Neural Network. The Back propagation Neural Network used in this study is a multi layered Feed Forward Neural Network, which is trained by a supervised Delta Learning Rule. The dataset used in this study are the signs, symptoms and the results of physical evaluation of a patient. The proposed system achieved an accuracy of 90%.

Niti Guru et al. proposed a system that uses neural network for prediction of heart disease, blood pressure and sugar. A set of 78 records with 13 attributes are used for training and testing. He suggested supervised network for diagnosis of heart disease and trained it using back propagation algorithm. On the basis of unknown data is entered by doctor the system will find that unknown data from training data and generate list of possible disease from which patient can suffer.

A proficient methodology for the extraction of significant patterns from the heart disease warehouses for heart attack prediction has been presented by Shantakumar B.Patil et al. Initially, the data warehouse is pre-processed in order to make it suitable for the mining process. Once the preprocessing gets over, the heart disease warehouse is clustered with the aid of the K-means clustering algorithm. Consequently the frequent patterns applicable to heart disease are mined with the aid of the MAFIA algorithm from the data extracted. In addition, the patterns vital to heart attack prediction are selected on basis of the computed significant weightage. The neural network is trained with the selected significant patterns for the effective prediction of heart attack.

III. Methodology

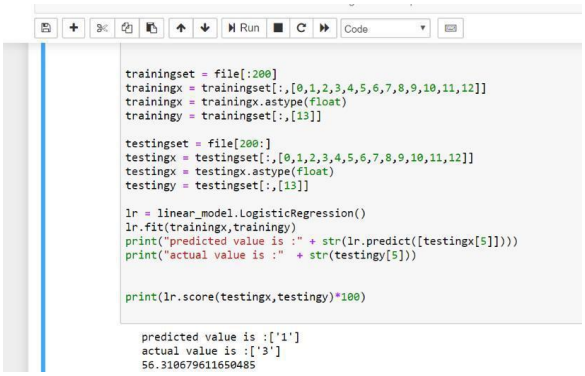
Machine learning, a type of artificial intelligence that "learns" as it identifies new patterns in data, enables data

scientists to effectively pinpoint revenue opportunities and create strategies to improve customer experiences using information hidden in huge data sets. The primary aim is to allow the computers learn automatically without human intervention or assistance and adjust actions accordingly. Machine Learning Algorithms we used are:

A Linear Regression

It is a machine learning algorithm based on supervised learning. It performs a regression task. Regression models a target prediction value based on independent variables. It is mostly used for finding out the relationship between variables and forecasting. Different regression models differ based on – the kind of relationship between dependent and independent variables, they are considering and the number of independent variables being used.

The accuracy for Logistic Regression is: 56.3106%



```
trainingset = file[:200]
trainingx = trainingset[:,[0,1,2,3,4,5,6,7,8,9,10,11,12]]
trainingx = trainingx.astype(float)
trainingy = trainingset[:,[13]]

testingset = file[200:]
testingx = testingset[:,[0,1,2,3,4,5,6,7,8,9,10,11,12]]
testingx = testingx.astype(float)
testingy = testingset[:,[13]]

lr = linear_model.LogisticRegression()
lr.fit(trainingx,trainingy)
print("predicted value is :" + str(lr.predict([testingx[5]])))
print("actual value is :"  + str(testingy[5]))


print(lr.score(testingx,testingy)*100)
```

```
predicted value is :['1']
actual value is :['3']
56.310679611650485
```

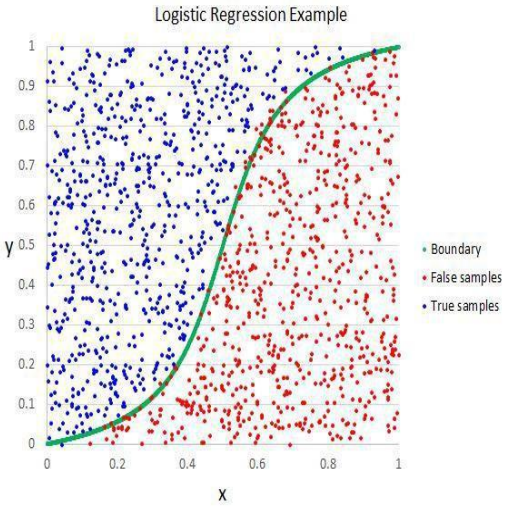
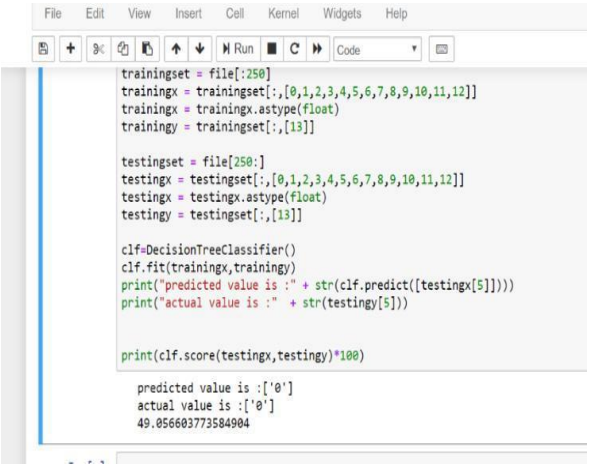


Fig. 3. Logistic Regression Example

B Decision Tree

They are a type of Supervised Machine Learning (that is you explain what the input is and what the corresponding output is in the training data) where the data is continuously split according to a certain parameter. The tree can be explained by two entities, namely decision nodes and leaves. The leaves are the decisions or the final outcomes. And the decision nodes are where the data is split.

The accuracy of the Decision Tree Algorithm came out to be : 49.0566%



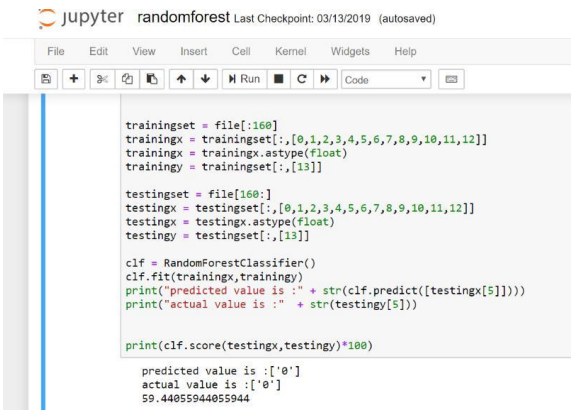
```
trainingset = file[:250]
trainingx = trainingset[:,[0,1,2,3,4,5,6,7,8,9,10,11,12]]
trainingx = trainingx.astype(float)
trainingy = trainingset[:,[13]]

testingset = file[250:]
testingx = testingset[:,[0,1,2,3,4,5,6,7,8,9,10,11,12]]
testingx = testingx.astype(float)
testingy = testingset[:,[13]]

clf=DecisionTreeClassifier()
clf.fit(trainingx,trainingy)
print("predicted value is :" + str(clf.predict([testingx[5]])))
print("actual value is :"  + str(testingy[5]))


print(clf.score(testingx,testingy)*100)
```

```
predicted value is :['0']
actual value is :['0']
49.056603773584904
```

C Random Forest

Random forest builds multiple decision trees and merges them together to get a more accurate and stable prediction. One big advantage of random forest is, that it can be used for both classification and regression problems, which form the majority of current machine learning systems. Random Forest has nearly the same hyper parameters as a decision tree or a bagging classifier. Fortunately, you don't have to combine a decision tree with a bagging classifier and can just easily use the classifier-class of Random Forest. Like we already mentioned, with Random Forest, you can also deal with Regression tasks by using the Random Forest regressor. Random Forest adds additional randomness to the model, while growing the trees. Instead of searching for the most important feature while splitting a node, it searches for the best feature among a random subset of features. This results in a wide diversity that generally results in a better model. Therefore, in Random Forest, only a random subset of the features is taken into consideration by the algorithm for splitting a node. You can even make trees more random, by additionally using random thresholds for each feature rather than searching for the best possible thresholds (like a normal decision tree does).

The accuracy of Random Forest was: 59.4405%

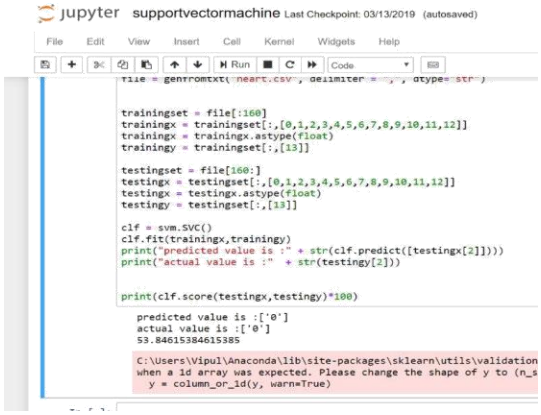


D Support Vector Machine

It is another simple algorithm that every machine learning expert should have in his/her arsenal. Support vector machine is highly preferred by many as it produces significant accuracy with less computation power. Support Vector Machine, abbreviated as SVM can be used for both regression and classification tasks. But, it is widely used in classification objectives.The objective of SVM algorithm is to find a hyper plane in an N-dimensional space (N-the number of features) that distinctly classifies the data points.To separate the two classes of data points, there are many possible hyper planes that could be chosen. Our objective is to find a plane that has the maximum margin, i.e. the maximum distance between data points of both classes. Maximizing the margin distance provides some reinforcement so that future data points can be classified with more confidence.

Support vectors are data points that are closer to the hyper plane and influence the position and orientation of the hyper plane. Using these support vectors, we maximize the margin of the classifier. Deleting the support vectors will change the position of the hyper plane. These are the points that help us build our SVM.

The accuracy of SVM: 53.8462%



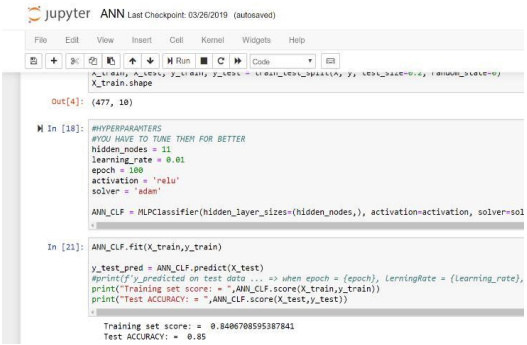
E Artificial Neural Networks

It is inspired by the biological neural network. It can learn to perform tasks by observing examples, we do not need to program them with task-specific rules. An ANN can look at images labeled ‘cat’ or ‘no cat’ and learn to identify more images itself.

Such a network is a collection of artificial neurons-connected nodes; these model neurons in a biological brain. A connection is like a synapse in a brain and is capable of transmitting signals from one artificial neuron to another. This neuron processes the signal it receives and signals to more artificial neurons it is connected to. Some applications of Artificial Neural Networks have been Computer Vision, Speech Recognition, Machine Translation, Social Network Filtering, Medical Diagnosis, and playing board and video games. It intended to simulate the behavior of biological systems composed of “neurons”. ANNs are computational models inspired by an animal’s central nervous systems. It is capable of machine learning as well as pattern recognition. These presented as systems of interconnected “neurons” which can compute values from inputs.

A neural network is an oriented graph. It consists of nodes which in the biological analogy represent neurons, connected by arcs. It corresponds to dendrites and synapses. Each arc associated with a weight while at each node. Apply the values received as input by the node and define activation function along the incoming arcs, adjusted by the weights of the arcs.

The accuracy of the ANN was: 83.50%



IV. DATASET

The experiment is carried out on a publicly available database for heart disease. The Cleveland dataset (UCI, 1990) used in this study was received from the University of

California Irvine (UCI) Machine Learning Repository heart disease dataset that includes four independent databases contributed by four independent medical institutions. The Cleveland dataset have 598 instances of patient data. The table shows the Cleveland dataset attributes with their definitions. In this study, 6 of the instances of the Cleveland dataset containing missing entries are omitted. The diagnosis of heart disease attribute (num) was categorized into two classes denoted as absence (num = 0) and presence (num = of the heart disease. The dataset separated into two sub-sets for training (80%) and testing (20%).

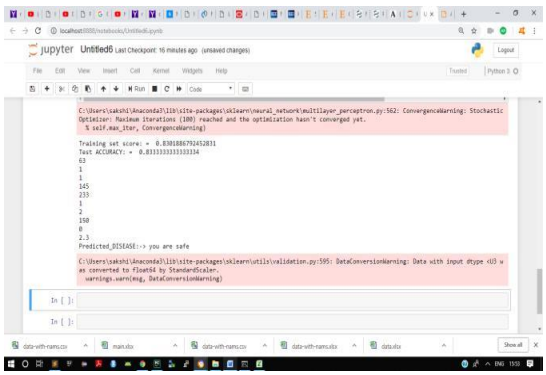
- Age
- Sex
- Chest pain
- Rest bp
- Chol
- Fbs
- Rest ECG
- Max HR
- ExAng
- Oldpeak
- Decision

V. Experimental Results

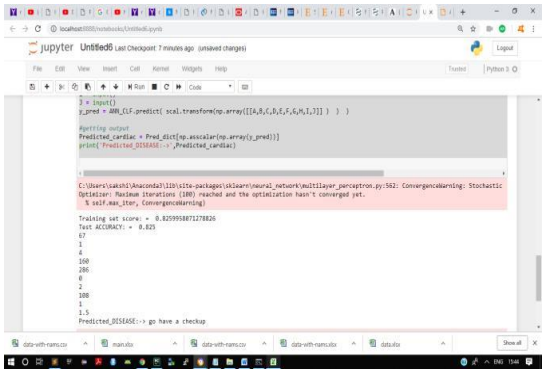
Finally, we train each of our machine learning models and check the cross-validation results. Here is the comparison between the various Machine Learning Algorithms by calculating different accuracies in accordance of the programs written individually for the same.

Algorithm	***Accuracy***
Linear Regression	56.31%
Random Forest	52.63%
SVM	53.85%
Decision Tree	50.94%
Artificial Neural Network	83.50%

VI. Output and Results



ANN predicting that the patient is safe



Accuracy using ANN warning patient to have a check up

VII. Conclusion

Artificial Neural Network are used to finds association rules of heart dataset attributes. Classification algorithms are used to predict small set of relationships between attributes in the databases to build an accurate classifier. The main contribution of the present study to attain high prediction accuracy for early diagnoses of heart diseases. Due to the significance of heart disease diagnosis in the medical field, we have compared various models for diagnosis of this disease. In our result, we discovered that artificial neural network is the best algorithm for diagnosis of heart disease which gave an accuracy rate of 83.5%. The experimental results show that large number of the rules support in the better discover of heart diseases that even support the heart specialist in their diagnosis judgments. Besides, in this research work, we have discovered that one of the major causes of death due to heart disease is unawareness at the initial stage of the disease, regular medical check-up can help to discover the disease at initial stage. If heart disease can be discovered in time, it can be properly managed or cured; especially coronary heart disease can be treated by proper diet, medication and exercises. Finally, the habits that lead to heart disease should also be stopped by an individual to avoid a critical case of the disease. Smoking habit, unhealthy diet and irregular exercises should be stopped. The proposed model acknowledging such characteristics was developed, which may aid in the prevention of heart disease in these individuals.

VIII. Future Work

Since the present study involved 11 attributes, the future scope will be directed in reducing numbers of attributes and to evaluate the significant attributes contributing towards the diagnosis of heart disease. There is a need to build a system

where every human can check the risk of heart diseases using minimum parameters and resources. Various parameters like processing time, resources and memory can be further enhanced.

REFERENCES

[1] Aliev, R.A., Aliev R.R., Guirimov, B.G. ,Uyar K., 2007. Recurrent Fuzzy Neural Network Based System for Battery Charging. Lecture Notes in Computer Science 4492-II. 307-316.

[2] J. S. Sonawane, D. R. Patil and V. S.Thakare, "Survey on Decision Support System for Heart Disease,''International Journal ofAdvancements in Technology, vol4, pp. 89-96, 2013.

[3] E. O.Olaniyi, K. Adnan., "Onset Diabetes Diagnosis Using Artificial Neural Network" International Journal of Scientific and EngineeringResearch, vol. 5, Issue 10, October (2014).

[4] R. Das, I. Turkoglu, A. Sengur, Effective Diagnosis of Heart Disease through Neural Network Ensemble, "ExpertSystems with Applications" vol. 36 issue 4, pp. 7675-7680, May (2009). [Available]:10.1016/j.eswa.2008.09.013.

[5] Christopher J.C. Burges, "A Tutorial on Support Vector Machines for Pattern Recognition, Data Mining and Knowledge Discovery, 2, 121–167 (1998).

[6] Mishra, Binod Kumar, Prashant Lakkadwala, and Naveen Kumar Shrivastava. "Novel Approach to Predict Cardiovascular Disease Using Incremental SVM." Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, 2013.

[7] Vanisree K, Jyothi Singaraju, Decision Support System for Congenital Heart Disease Diagnosis based on Signs and Symptoms using Neural Networks, International Journal of Computer Applications (0975 – 8887) Volume 19– No.6, April 2011.

[8] Shantakumar B.Patil, Y.S.Kumaraswamy, Intelligent and Effective Heart Attack Prediction System Using Data Mining and Artificial Neural Network, European Journal of Scientific Research, ISSN 1450-216X, Vol.31 No.4 (2009), pp.642-656.

[9] Niti Guru, Anil Dahiya, Navin Rajpal, Decision Support System for Heart Disease Diagnosis Using Neural Network, Delhi Business Review, Vol. 8, No. 1, January-June 2007.

[10] Amiri A.M., Armano, G., 2013. Early Diagnosis of Heart Disease Using Classification And Regression Trees. The 2013 International Joint Conference on Neural Networks (IJCNN), Dallas, TX.1-4.

Managing WSN by Technical Tools

Varun Tiwari

TIPS, GGSIPU, New Delhi, India
varuntiw1984@gmail.com

***Abstract*—** With the advancement of technology, the usage of networking sites has become common in our lives. In the field of social networking there are many security problems. The main purpose of the developers is to attract users and make their connection and security is not at all their priority. As a consequence, with the benefits of social networking sites, many security problems have resulted. Developers should provide its users with the tools that can handle security problems. Most of the current security systems do not provide the required protection level against ever-increasing security issues. The reason for their failure is the use of point solutions to protect host, and if the security is not given priority, it can lead to cyber-terrorism and further it can bring down an individual or organization. This paper is about the system overview, susceptibility analysis system, imposition detection system, imposition response system, security tools and security devices. It will give a wider perspective on security and a basic knowledge to how to reduce and manage risk personally in all situations.

Keywords— Cyber-Security; Cyber-Terrorism; Susceptibility Analysis; Imposition Detection; Imposition Response.

I. INTRODUCTION

This paper aims to describe the forensic security tools. Our team has developed to protect social network site users from the presently existing security intimidations. First we recognized the security problems in the social network sites; we engrossed on making tools to support in the chasing down of criminals. The tools we industrialized concern recovery of social network site user's non-personal-identifiable information, for instance operating system, IP address, MAC address etc. Recovery of this information is to ensue upon the simulated contact from the other person, be it by them merely browsing our personal page, by other person contacting by Virtual Meeting, for example chatting. This paper shields procedures used, test results, and future aims going forward. Good Information Security strategy is an acute constituent of an overall tactic to certify the triumph of the organization. The organization can lessen the effect of social engineering spasms by executing a widespread information security strategy. Such a plan would embrace methods ranging from printing a well written security policy, implementing enduring security awareness and education programs, following through with auditing programs to monitor policy compliance, installing security devices to avert unapproved admittance and buying insurance alongside security attacks.

II. RELATED WORK

First Mistreatment imposition structural design: Detect, Monitor, Recovery and Prevent Internal deception .

The article [1] describes structural design against mistreatment imposition used for detecting, monitoring, recovering and averting internal deception that are caused through workers. The structural design is based on a holistic proceed that considers different types of factors, both technical and non-technical. The structural design has technical, managerial, operational and other controls. The actions used for anticipation of worker frauds include perimeter defense technology training, supervision, screening, and segregation [1]. Measures for detecting frauds include internal auditing, conformity and also technical measures including both network and host based imposition detection systems. The measures for monitoring are placed at the operating system, network, and application levels [2]. At the network level measures include monitoring admittance to receptive assets, monitoring spamming and download. At the in service level monitoring is on system calls, on CPU usage, audit trails, and file access. At the submission level monitoring is done on communications of users with different applications like requirements and responses, access patterns, user inputs, and application inputs [2]. Recovery measures include fraud proof collection and explanation measures, which include confirmation recognition and compilation, examination storage, conservation shipping and presentations in courts. Incorporated instinctive beside among Adaptive Simulated Immune Systems applied to procedure incongruity recognition .

In the doctoral theory [3] simulated immune systems are applied to solve security issues in software systems. The organic immune properties were applied in growing the performance of simulated immune systems (SIS). The thesis presents nine design philosophies for the second generation's simulated immune systems. The First principle is that simulated immune systems are signified as independent agents. The second principle states problems when SIS is signified as external or antigens signals. The third principle states that the goal of the second generation SIS is to uphold themselves and their atmosphere. The fourth principle describes the roles of agents being to imprison antigens, to present, to identify, to process, to monitor process and create signals [3]. The fifth design principle states that agents have a lifecycle. The sixth design principle states that agent's contrary with the atmosphere at several levels. The seventh design principle states that signals can be internally or externally twisted. The eight design principle states that receptors can be internal or external, specific signals. The last principle states that agents are capable of concentrate in specific tasks [3].

Structural design for disruption Detection using Autonomous Agents (SDFDD) SDFDD [4], proposed at Purdue, is an agent built on hierarchal construction for IDS. It decays the old-style IDS into frivolous sovereign cooperating

agents, which can simply reconfigure. Autonomous agents used in SDFDD project, with inert and distinct purpose agent platform, are used to vigorously reconfigure IDS components. The other thing value perceiving is that SDFDD is based on a hierarchal construction, which is susceptible to direct attacks. If any of the inner bulges is conceded, the whole outlet is spiked. Secondly, the handover of huge logs thru the hierarchy also overloads the network traffic.

Automated recognition of susceptibilities in privileged programs by implementation monitoring (ARSP) ARSP project [4] worked on recognition of susceptibility misuses in privileged programs by monitoring operational audit traces. Their work is based on the hypothesis that privilege programs are more likely to deed susceptibilities. They have presented the Program Policy Specification Language based on a modest predicate logic and regular expressions.

III. METHODOLOGY – SYSTEM OUTLINE

We have urbanized the complete scheme in our so called MagicNET Environment. MagicNET is broad Mobile Agents System that provides features like review, design, privileges assignment, trust evaluation, and secure adoption of mobile agents and the secure runtime support for mobile agents' execution [5]. The proposed network security system contains four subsystems. It has the layered architecture of the system. The four subsystems are comparable to the human immune system functional concept. These subsystems are as follows: a. Susceptibility Analysis System (SAS)- Pre-imposition susceptibility Analysis , Post-imposition susceptibility Analysis and Susceptibilities Record Management b. Imposition Detection System (IDS) -Host based Imposition Detection and Distributed Imposition Detection c. Imposition Response System (IRS)- Host based Imposition Response , Distributed Imposition Response and Safety Management (SMS) d. Susceptibility Rule Updater Moreover, the following three components work with these systems to provide widespread network security system. e. Mobile Agents (MAs) f. ID\IP Components g. Administration Console (AMC) The presented elucidation is tightly attached with the number of mobile agents which provide scalability, suppleness, platform independence and consistency to the system. Moreover, mobile agents can execute autonomously, asynchronously and can adapt animatedly at different stages of attacks timeline and thus provide a vigorous safety mechanism. At the abstract level, these mobile agents are acting as middleware between ID/IP components and the overall system's interior functionality. AMC supplies graphical interface to Safety management position, in squat SecAdmin, and to remote servers. At SecAdmin, AMC helps safety administrator to perform different tasks and scrutinize activities and results of mobile agent's dispensation. At isolated servers, it provides mechanism to display information about different agents visiting and performing different actions. Mobile Agents interrelate with number of ID/IP Components on remote host en route for accomplish their tasks. These components are in fact still agents that perform certain predefined tasks. In our execution we have used five IDP components: Osiris, Windows firewall, SNORT, Nessus, jRegistry, and System logs [6]. We will not go into the details of these components due to space limitation.

A. Susceptibility Analysis System (SAS)

As the first step, SAS – Susceptibility Record Management provides safety administrator with up-to- date and rich information about vulnerabilities. This has been achieved by using three susceptibilities databases: NVD, OSVDB and Security Focus [7] [8], and generating IDP System's own database called Susceptibilities DB. Susceptibility DB is a rich database which contains related information about most of known susceptibilities to date. SAS updates DB daily, weekly, or monthly, depending on a local safety policy. Second, Pre-Imposition Susceptibility Analysis provides potential near query remote servers concerning their profile in terms of different software installed. It is important to acquire host profile for efficient Susceptibility Analysis. Two agents perform this activity: Agent_Susceptibility_Messenger and Agent_Susceptibility_Analyzer. SAS bring remote host profile and query Susceptibilities DB for susceptibilities. If they exist, it stores susceptibilities in the Susceptibilities DB and displays the outcome on the administrative interface. Most of the IDS and Imposition Response Systems (IRS) consider their task proficient after they detect and respond to imposition. It can be effortlessly inferred that impostors will try to exploit the same susceptibility at a different system in the network. Post-Intrusion Susceptibility Analysis provides capability to analyze the particular Susceptibilities that was being exploited by impostor in the most recent attack. The main intention of this analysis is to recognize the exploited susceptibility at a particular host and then apply control measure to the rest of the network against given susceptibility. This action is performed with the help of [9] Agent_Post_Intrusion_Susceptibilities_Analyzer. As soon as IRS finishesit's task and reports to the Administrative Server (the Server from where agents were launched the first time), the Administrative Server automatically launches Agent_Post_Intrusion_Susceptibility_Analyzer in order to analyze the particular host previously under attack by analyzing the system logs and logs generated by SNORT. Administrative Server stores susceptibility information in the Susceptibilities DB in the Exploited_Susceptibilities table .

B. Imposition Detection System (IDS)

In an IDP system, a team of mobile agents is dispatched in the network within response to a distrustful alarm. They scrutinize the statistical data related to different imposition attempts like DDoS , DoS attack, Doorknob- Rattling Attack [10] etc, and then appeal for underpinning from the Security Administrator. First SIDS, analysis of logs and reporting is performed on logs generated by system events and sensors, like Osiris or SNORT on remote hosts. Examination of logs notifies Security Administrator about the imposition. Agent_IPS_Logs agent along with the Agent_Leader agent analyze these logs, filter them, extract related and useful information, and display results to the Security Administrator. Second, Host–based Imposition Detection (HID) subsystem monitors the network hosts for different types of impositions and reports as soon as

some impositions occurs, so to facilitate suitable response measures by SIRS can be applied. Host monitoring is being implemented by incessantly analyzing SNORT logs. Agent_Host_Monitoring initially is not present at remote hosts. Security administrator launches Agent_Host_Monitoring agent. It along with Agent_Leader reach remote hosts and stays there permanently. They incessantly examine log entries generated by OSIRIS, SNORT and as so on. If they discover any imposition based on SNORT rules, they ask for help from the directorial server. Third, Distributed Imposition Detection (DID) sub- system works equivalent as Host–based Imposition Detection, but it is activated by the recognition of distrustful activity below the imposition threshold, by ID components. Agent_Host_Monitoring provides the signal for the commencement of DID. DID creates Suspicious Host List (SHL) [8], specific to each type of attack, and then logs the addresses of each host generating the same type of alert [11].

At this instance of time DID, launches Agent_Distributed_Intrusion_Analyzer (ADIA) along with Agent_Leader and Agent_Distributed_Messenger to visit each host in the SHL, analyze data from system logs, and subsequently associate and cumulative them with system logs of other entries of SHL to gather traces of the attack. If result is positive, then Agent_Distributed_Messenger straight away returns back to the organization Server and marks proved field as true in the SHL for hosts under the distributed imposition attack, notified by a message to the administrator. Before launching an ADIA, DID creates a static agent i.e. Agent_SHL_Monitoring that constantly monitors SHL for any change in the Proved fields of different entries. In order to recognize the described situation take an example of a Doorknob-Rattling Attack in which attacker tries few common password and username combinations on many computers that result in failed login attempts [7]. These failed login attempts, as events are logged into the system log. Agent_Host_Monitoring detects these events, marks them as distrustful and reports to the administrator, where DID creates SHL, fills host IP field and marks attack type as Doorknob-Rattling. DID then launches Agent_Distributed_Intrusion_Analyzer along with Agent_Leader and Agent_Distributed_Messenger to visit each host in the SHL, and analyze data from system logs for Doorknob-Rattling attack. When it is detected that a remote host is under Doorknob-Rattling attack, it reports with the confirmation message to the DID through Agent_Distributed_Messenger and asks for reinforcements.

C. Imposition Response System (IRS)

IRS is securely tied with the IDS and it is activated as soon as the IDS detect some imposition at remote hosts for both cases i.e. Host–based Imposition and Distributed Imposition. The purpose of the IRS is to avoid the imposition in real time. It launches Agent_Intrusion_Response to counter the attack by any mean, like blocking the address from where the attack started, closing the port, shutting down service or program, or shutting down of remote host which is beneath attack in order to stop contagion in the network. Agent_Imposition_Response along with Agent_Leader is automatically launched (event based) from the Administrative Serverto the host that reported an imposition. Agent_Imposition_Response reaches the preferred host, initialize the response, and then reports to the Administrator. The response is generated using decision tables. Decision table is a mechanism that joins each attack with a specific response. It is the basis for static mapping and does not consider any other factor, except the attack type. Agent_Imposition_Response is using firewall to create its responses against impositions. As soon as Agent_Distributed_Messenger mark, Proved field true Agent_SHL_Monitoring launches Agent_Imposition_Response along with Agent_Leader. Agent_Intrusion_Response applies appropriate response to all hosts in the SHL that have confirmed intrusion and reports back to the Administrator.

D. Safety Management System (SMS)

SMS also uses mobile agents to implement management action in the network. The motto of these tasks is to keep all hosts in line with respect to number of safety services, answers, or safety configurations. SMS performs three tasks. 1. Test connectivity of remote host, 2. Query remote host configurations, and 3. Apply a number of security management tasks to remote hosts and exploited vulnerability and SNORT rule mapping [12].

IV. DIGITAL FORENSIC TOOLS

Guidance Software EnCase Forensics is one of the industry's most famous tools toward demeanor computer forensic investigations. With an intuitive GUI, greater analytics, enhanced email/Internet support and a powerful scripting engine, EnCase provides investigators with a single tool, capable of conducting large-scale and composite investigations from beginning to end. Corporate investigators and consultants around the humanity advantage from the many features EnCase Forensic provides. AccessData Ultimate Toolkit (UTK) The Ultimate Toolkit comprise all needed to investigate, protected and scrutinize computer or digital data. The UTK includes the Forensic Toolkit, Registry Viewer, Password Recovery Toolkit, Distributed Network Attack (1-Server / 50 Client Licenses), FTK Asia, NTAccess, WipeDrive 20-Pak, FTK Imager and includes technical phone support with free software subscription service for twelve months. Maresware supports an important set of tools for searching computer records and protecting private information. It is greatly bendable to meet the requirements of all types of investigators including: intelligence agency, law enforcement, human resource personnel, corporate security officers, and private investigator. Used within a forensic archetype, the software enables discovery of proof intended for use in civil or criminal legal proceedings. Interior investigators can build up documentation to support disciplinary actions, yet do so non-invasively, to protect proof that could end up in court. X-Ways Forensics is a sophisticated work atmosphere for computer forensic examiners. Some of the functions implemented by this tool includes: reviewing slack space; file carving, support for FAT and NTFS, data recovery disk cloning and imaging; hard disk cleaning, and mass hash calculation for files. Spider shows all of the URLs and cookies stored in the index.dat file,

and will then allow the user to remove them. Following are the details on the software's usability: • Retrieve chat history files stored on your system or any other system on the network • Convalesce all encoded archive file of any yahoo account • Works with all versions of Yahoo Instant Messenger • Software can auto detects stored yahoo chat conversation logs and decode it • Program recovers all SMS messages that are sends from yahoo messenger to any mobile phone numbers • Enable and disable yahoo archive setting even you are not login • Import any external yahoo archive file and decode it when it is not in yahoo directory • View any yahoo archive file on your computer even you don't know the password of that account [13].

V. Data Recovery Investigation Tools

Rifiuti is a Recycle Bin Forensic Analysis Tool. Rifiuti, the Italian word meaning "trash", was developed to inspect the stuffing of the INFO2 file in the Recycle Bin.Rifiuti will parse the in sequence in an INFO2 file and output the fallout in a field surrounded manner so that it may subsist imported into your favorite spreadsheet program. Rifiuti is built to work on several stages and will execute on Windows, Mac OS X, Linux, and *BSD platforms [8].Registry Information Extractor is a test release of a software utility that is in progress and under trying. It is a Windows 95/98/ME system.dat registry information extractor. It will be updated to extract a lot more information from the registry. At present it will only extract system.dat information from Windows 95/95 and ME. It can extract the following information: Registered Owner, Registered Organization, Windows Version, Windows Version Number, Windows Installed Date & the Computer Name. RIE can also be used as a File Viewer from within EnCase. PC Inspector File Recovery is a data recovery program that ropes the FAT 12/16/32 and NTFS file systems. Some of the salient features in PC Inspector File Recovery 3.x are as follow : • Finds partitions robotically, even if the boot sector or FAT has been removed or destroyed (does not work with the NTFS file system) • Recovers files with the unique time and date stamp • Supports the economy of recovered files on network drives • Recovers files, even when header entry is no longer available Gargoyle Forensic Pro quickly and easily determines whether malware is present on a system under investigation. The Forensic Pro Edition is designed for dataset creator, private investigators, forensic investigators, law enforcement personnel, examiners and forensic lab use. The Forensic Pro version includes all the travelling license, dataset converter, malware datasets, a single-user license of Mount Image Pro™ allowing forensic image investigations and other tools including a USB thumb drive for covert investigations and a 1-year subscription to the Digital Evidence Time Stamping service.

A. PDA Investigation Tools

Pilot-Link is used to retrieve information from ROM and RAM of Palm PDA hand-held. Pilot-xfer can moreover be used to allow attainment. Paraben PDA Seizure is the only forensic tool designed to confine data and report on data from a PDA. As an inspector you know enhanced than anyone that the difference between making a case and losing a case is tough proof. And through additional horrific guys going high tech, obtaining that substantiation is becoming more complicated than ever. Paraben's PDA Seizure is all-inclusive tool that allows PDA data to be viewed, acquired and reported on, all within a Windows environment. Now with USB support.

B. Network Investigation Tools

Specters CNE can be used to verification all your employees do online, together with instant messages, chats, emails sent and received, web sites visited, applications launched, files downloaded and keystrokes typed.

VI. Conclusion

This paper has offered network security system that smears features from the protected system to secure systems. The system has features that support an information security classification to be trained to acclimatize to vibrant atmosphere. This system uses safer mobile agents to protect systems and networks. These mobile agents are created and tested by means of the negative and clonally selection algorithms. The secure mobile agents that pass these tests are permitted to perform the susceptibility analysis, imposition detection, imposition response, and safety management services. We have created the system using secure mobile agents which take input from sensors like, Nessus, SNORT, Firewall, and Osiris. Mobile agents course the inputs from sensors and based on subsystem functionality execute various activities and finally output using sensors again. Our paper displays important improvements in network security and as by deploying system, there is important diminution in imposition, as our system outfitted them using multifaceted method, similar to the human immune system.

Security has become a chief concern on Social Networks. It is very important that we find the right solutions to tackle the different security problems on the Social Network Site's today. The scripts described in this paper should be used to their completest advantage in the simulated communication world. The tools described here can be used to help in examinations of Social Network Site crimes, but can also be used to help protect users from the start of their Social Network Site interactions, to avoid crimes from even occurring. We should also operate the free software that is accessible on various websites to track the actions of the visitors on the website.

References

[1] Shafiqul Abidin "Enhancing Security in WSN by Artificial Intelligence", Springer International Conference on Intelligent Data Communication and Internet of Things (ICICI - 2018), Chapter 93 , Lecture Notes on Data Engineering and Communication Technologies Series, pp 814-821, January 2019.

[2] N.T. Baloyi. Misuse intrusion architecture: prevent, detect, monitor and recover employee fraud, The Proceedings of the Information Security South Africa 2015 New knowledge today conference. Sandtorn, South Africa.

[3] Furnell, S. Enemies within: the problem of insider attacks, Computer fraud & security. Volume 2004, issue 7, July 2004. IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.1, January 2009 .

[4] Twycross, J.P. Integrated innate and adaptive artificial immune systems applied to process anomaly detection. University of Nottingham. 2007. www.cs.nott.ac.uk/ ~jpt/papers/phd-thesis.pdf
[5] Ko, C. Fink, G. Levitt, K. Automated detection of vulnerabilities in privileged programs by execution monitoring, Proceedings of Computer Security Applications Conference, 1994. P 134-144.
[6] Shafiqul Abidin, Manu Ahuja and Mohd Izhar "Minimizing Risks in Wireless Sensor Network", IEEE International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing – EECCMC 18, January 2018.
[7] National Vulnerability Database, http://nvd.nist.gov/ last retrieved December 01, 2008.
[8] The Open Source Vulnerability Database, http://www.osvdb.org/ last retrieved December 01, 2008.
[9] S. Ahmed, S. Muftic, Intrusion Prevention System based on Secure Mobile Agents, Thesis Report, Department of Computer and Systems Sciences (DSV-KTH), March 2006.
[10] SNORT www.SNORT.org last retrieved December 01, 2008.
[11] Jung Won Kim, Integrating artificial Immune Algorithms for Intrusion Detection, Ph. D thesis, The Department of Computer Science, University of London, 2002
[12] Shibli, M. A., & Muftic, S. (Feburary 2009). MagicNET: Security Architecture for Creation, classification and validation of Trusted Mobile Agents. IEEE 11 International Conference on Advance Communication Technology. (Accepted for publication)
[13] P. Kannadiga, M. Zulkernine, DIDMA: A Distributed Intrusion Detection System Using Mobile Agents, Proceedings of the Sixth International Conference on SE. Vol, Issue, 23-25 May 2005 Page(s): 238 – 245.

Volume - 4, Issue - 2
Jan – Jun, 2019

ISSN : 2581 - 4125

Contents

HMR Institute of Technology & Management
(Affiliated to Guru Gobind Singh Indraprastha University, Delhi)
Plot # 370, Hamidpur, Delhi – 110036
www.hmritm.ac.in editor. journal@hmritm.ac.in