Empowering Cyber Security Operations: A Deep Learning Agenda with User-Centric Focus

Dr.M.Supriya supriya@stellamaryscoe.edu.in

Mr.C.Bastin Rogers bastinrogers@stellamaryscoe.edu.in

J. Sunanthini SUNANTHINI@stellamaryscoe.edu.in

Mrs.Breethy.S.V breethy@stellamaryscoe.edu.in

Mrs. G.Sutherlin Subitha sutherlinsubitha@stellamaryscoe.edu.in

Department Of Computer Science Engineering

Stella Mary's College Of Engineering, Tamilnadu, India

ABSTRACT- A SIEM (Security Information and Event Management) framework is set up to work on the different safeguard advances and banner admonitions for security episodes to safeguard an organization's Internet security. Auditors (SOC) investigate admonitions to check whether they are precise. Be that as it may, the main part of the admonitions is inaccurate, and the number of alerts is more prominent than SCO's ability to deal with every one of them. Therefore, the malicious expectation is plausible. It's conceivable that assaults and compromised have are wrong. AI may be utilized to lessen the number of misleading up-sides and increment the usefulness of SOC experts. We foster a client-driven designer learning structure for the Internet Safety Functional Center in a true setting in this article. We go through normal information sources in SOC, their work process, and how to investigate this information to construct an AI framework that works. This exposition is composed of two crowds. The main gathering comprises brilliant analysts who have no foundation in information science or PC security but who should fabricate AI calculations for machine wellbeing. The second arrangement of guests are Internet security experts with broad information and involvement with the field, yet no Machine Learning encounters exist, and I might want to fabricate one for them. We use the record as an illustration at the finish of the paper to show each of the stages from information assortment to name advancement, highlight designing, AI calculation, and test execution appraisals using the PC made in Seyondike's SOC production.

I. INTRODUCTION

Ever since the introduction of credit cards and online payments, many scammers have found ways to exploit people and steal their credit card information to use them for unauthorized purchases. This leads to a huge amount of fraudulent purchases every day. Banks and eCommerce sites are attempting to recognize these fake exchanges and prevent them from reoccurring. With Machine learning and Deep Learning strategies, they are attempting to stop the fraudsters before the exchange is endorsed. AI is perhaps the most sizzling subject of this ten years and a subset of Artificial Intelligence. An ever increasing number of organizations are hoping to put resources into AI to work on their administrations. AI is a blend of different PC calculations and factual demonstrating to permit the PC to perform undertakings without hard coding. The obtained model would gain from the "preparing information". Forecasts can be made or activities can be performed from put away experiential information. Profound learning models are a piece of AI methods which includes Artificial Neural Networks. Convolutional neural organizations, Deep Belief Network, Auto-encoders, Recurrent Neural Network, and Restricted Boltzmann Machine are on the whole different techniques. An appropriately prepared NN would have the capacity to catch remarkable connections over the entire dataset. Mastercard extortion is a type of misrepresentation including the utilization of phony or taken Visa data and truly hurting account holders or shippers included. The complete number of Visa extortion in Single Euro Payments Area (SEPA) in 2016 was 1.8 Billion Euros out of the all out 4.38 Trillion Euros exchange, which is 0.4% lower than the past year[1]. In 2015, as per the Nelson report, the complete misfortune from the charge cards on the planet was $21.84 billion and projected that in 2020 it would be $32 billion. [2] In this paper, we will be investigating 3 informational indexes. They are the European dataset [3], the Australian dataset [4] and the German dataset [4]. In this work we expect to benchmark different ML and DL procedures. An ensemble of the best 3 performing models is also applied the all 3 datasets. We present our conclusions based on an empirical study comparing different ML.

II. EXISTING SYSTEM

The majority of business security techniques have concentrated on safeguarding network infrastructure while paying little or no attention to end users. As a result, traditional security functions and devices, such as firewalls and intrusion detection and prevention systems, are primarily concerned with network level protection. Despite the fact that such an approach is still part of the broader security storey, it has limits in light of the new security problems discussed in the preceding section.

Data Analysis for Network Cyber-Security is concerned with monitoring and analyzing network traffic data in order to detect and prevent harmful behavior. A quantitative risk assessment was conducted after risk values were incorporated into an information security management system (ISMS). According to the quantitative analysis, the recommended remedies might minimize risk to some amount. The cost-effectiveness of the recommended countermeasures will be investigated in the future. It gives users attack details including the type of attack, the frequency, and the target and source host IDs. Ten et al. presented a cyber-security framework for the SCADA system as vital infrastructure, based on real-time monitoring, anomaly detection, impact analysis, and mitigation methods utilizing an attack tree-based methodology.

DISADVANTAGE:

1. Firewalls can be challenging to set up correctly.
2. Incorrectly designed firewalls may prevent users from completing Internet operations until the firewall is properly configured.
3. Slows down the system compared to previously.
4. New software must be updated on a regular basis to maintain security.
5. It may be too expensive for the ordinary consumer.
6. The only constant is the user.

III. PROPOSED SYSTEM:

By bringing security closer to end users, user-centric cyber security helps businesses decrease the risk associated with rapidly changing end-user realities. User security is not the same as user-centric cyber security. Answering people's demands in ways that protect the corporate network and its assets is what user-centric cyber security is all about. User security might appear to be about safeguarding the network from the user — securing it against vulnerabilities introduced by the user's requirements. User-centric security is more beneficial to enterprises. Self-contained, real-time, and resilient cyber-security systems with high performance needs. They're employed in a variety of applications, including essential infrastructures like the national power system, transportation, healthcare, and military. These applications necessitate the integration of computer, communication, and control technological systems in order to achieve stability, performance, dependability, efficiency, and resilience. Because of their complexity and cyber-security connection, critical infrastructures have long been a target for thieves and are vulnerable to security risks. When people, processes, technology, or other components are attacked then the risk management measures are missing, insufficient, or fail in any manner, these CPSs face security breaches. The attackers want sensitive information. The main goal of this project is to decrease the amount of unnecessary data in the dataset.

ADVANTAGES:

1) Defends the computer against viruses, worms, spyware, and other malware.

2) Anti-theft protection for data.

3) Prevents hackers from gaining access to the computer.

4) Reduces the chances of your computer stalling or crashing.

5) Provides users with privacy

6) Securing the network edge that is user-aware

7) Protecting the communications of mobile users

8) User-centric security management.

Proposed System Modules

CYBER ANALYSIS

Cyber threat analysis is a process in which an organization's understanding of internal and external information vulnerabilities is compared to real-world cyber-attacks. In terms of cyber security, this threat-oriented strategy to countering cyber-attacks provides a seamless shift from reactive to proactive protection. Furthermore, the goal of a threat assessment is to provide best practises for maximising protective instruments in terms of availability, confidentiality, and integrity, without compromising usability or functionality. CYPER ANALYSIS, CYPER ANALYSIS, CYPER ANALYSIS A danger might be anything that causes the firm's valued services or items to be disrupted, meddled with, or destroyed. Regardless of whether it is of "human" or "nonhuman" origin, the investigation must examine every aspect that might pose a security concern.

DATASET MODIFICATION

You can conceal certain dataset items from display in the Datasets panel if a dataset in your dashboard has several dataset objects. To conceal dataset objects in the Datasets panel, for example, if you decide to import a huge quantity of data from a file but do not delete every undesirable data column before importing the data into Web, you may hide the undesired characteristics and metrics. To see hidden items in the Datasets panel, click the Show Hidden Objects button. To rename a dataset object, follow these steps. To construct a metric based on an attribute, follow these steps. To build an attribute based on a metric, follow these steps. To define a geo role for an attribute, follow these steps. To add further time information to an attribute, do the following: In the dashboard, to replace a dataset item.

DATA REDUCTION

Improve storage efficiency by employing data reduplication, compression, snapshots, and thin provisioning, as well as other data reduction and capacity optimization approaches. The most efficient approach to decrease a storing data is by simply eliminating undesirable or unnecessary info.

RISKY USER DETECTION

Immunity against false alarms to avoid consumer humiliation To safeguard all types of products from theft, there is a high detection rate. Entrance/exit layouts are more flexible with wide-exit coverage. A wide selection of appealing designs may be used to enhance any store's decor. For optimum system performance, sophisticated digital controller technology is used.

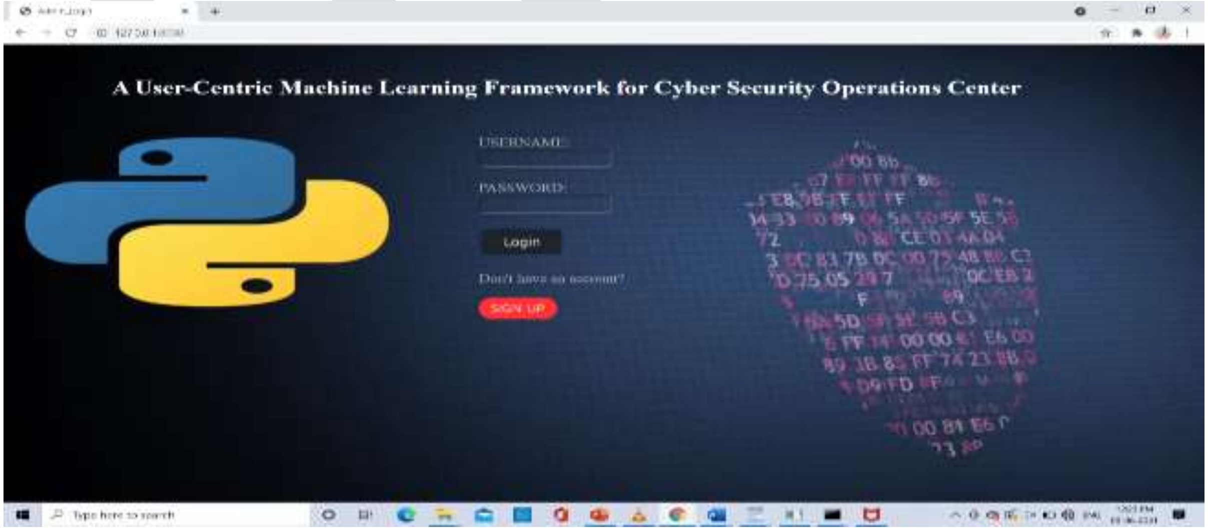
ALGORITHM: SUPPORT VECTOR MACHINE (SVM)

SVM (Support Vector Machine) is a supervised machine learning method that may be used to solve classification and regression problems. It is, however, mostly employed to solve categorization issues. The value of each feature is the value of a specific coordinate in this technique, which plots each data item as a point in n-dimensional space (where n is the number of characteristics you have). Then we do classification by locating the hyper-plane that best distinguishes the two classes (look at the below snapshot). A kernel is used to implement the SVM algorithm in practice. In linear SVM, the hyper plane is learned by converting the issue using some linear algebra, which is outside the scope of this SVM primer. The linear SVM may be rewritten using the inner product of any two supplied data rather than the observations themselves, which is an important discovery. The total of the multiplication of each pair of input values is the inner product of two vectors. The inner product of the vectors [2, 3] and [5, 6], for example, is 2*5 + 3*6 or 28. The following is the equation for creating a prediction for a new input using the dot product of the input (x) and each support vector (xi):

$$f(x) = B0 + sum(ai * (x,xi))$$

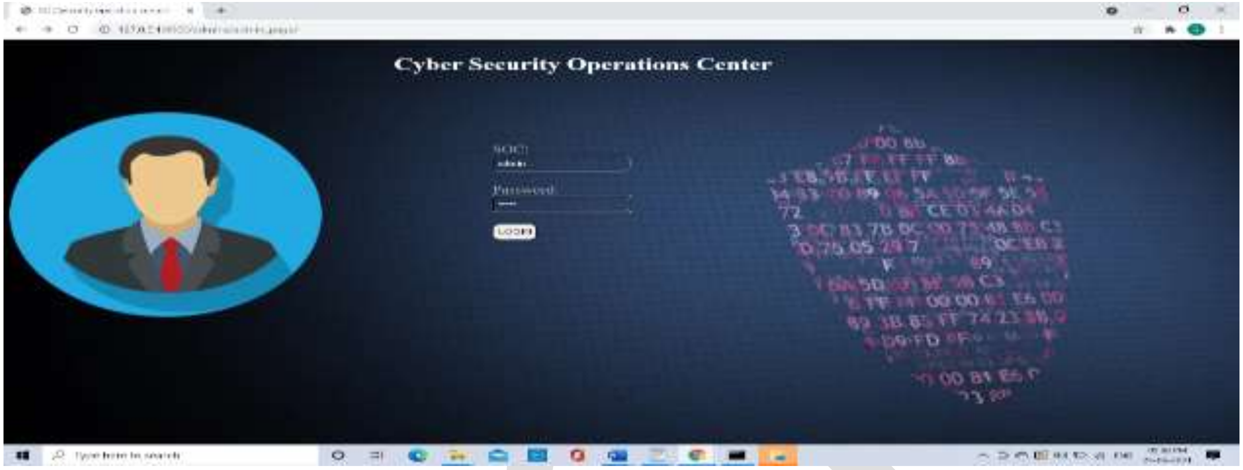
Calculating the inner products of a new input vector (x) with all support vectors in training data is the goal of this equation. The learning algorithm must estimate the coefficients B0 and ai (for each input) from the training data.

IV. EXPERIMENTAL RESULT:



A User-Centric Machine Learning Framework for Cyber Security Operations Center

Fig 1: User login page.

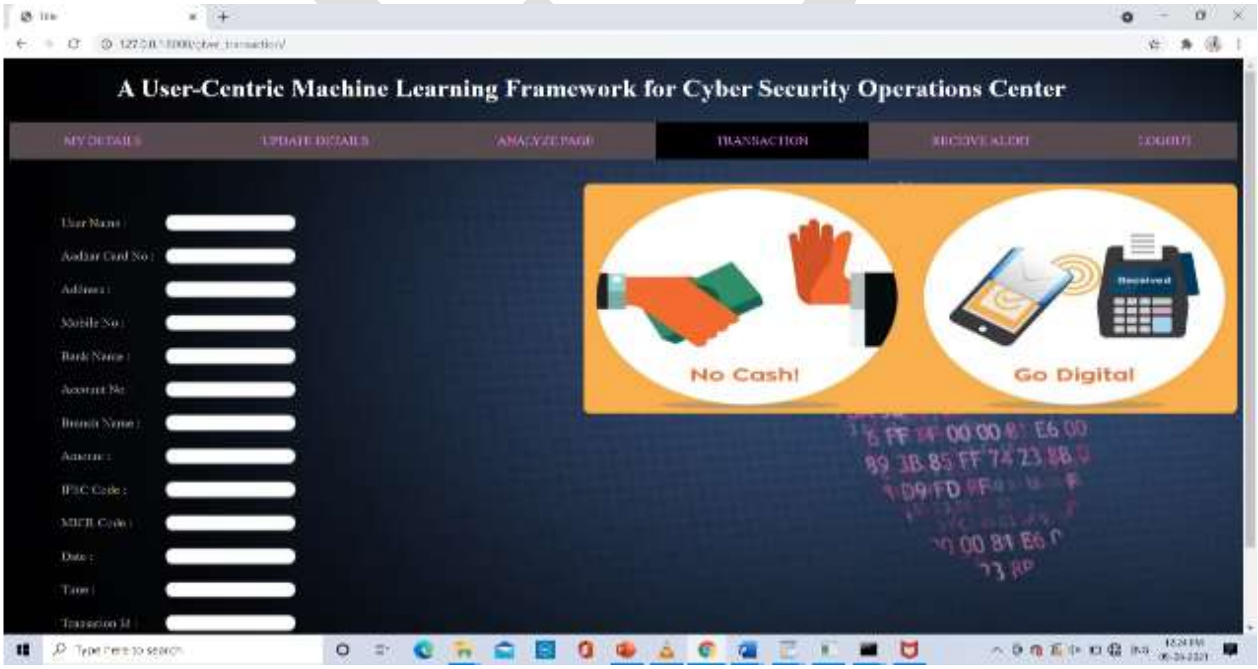


Cyber Security Operations Center

SOC!
admin

Password
*****

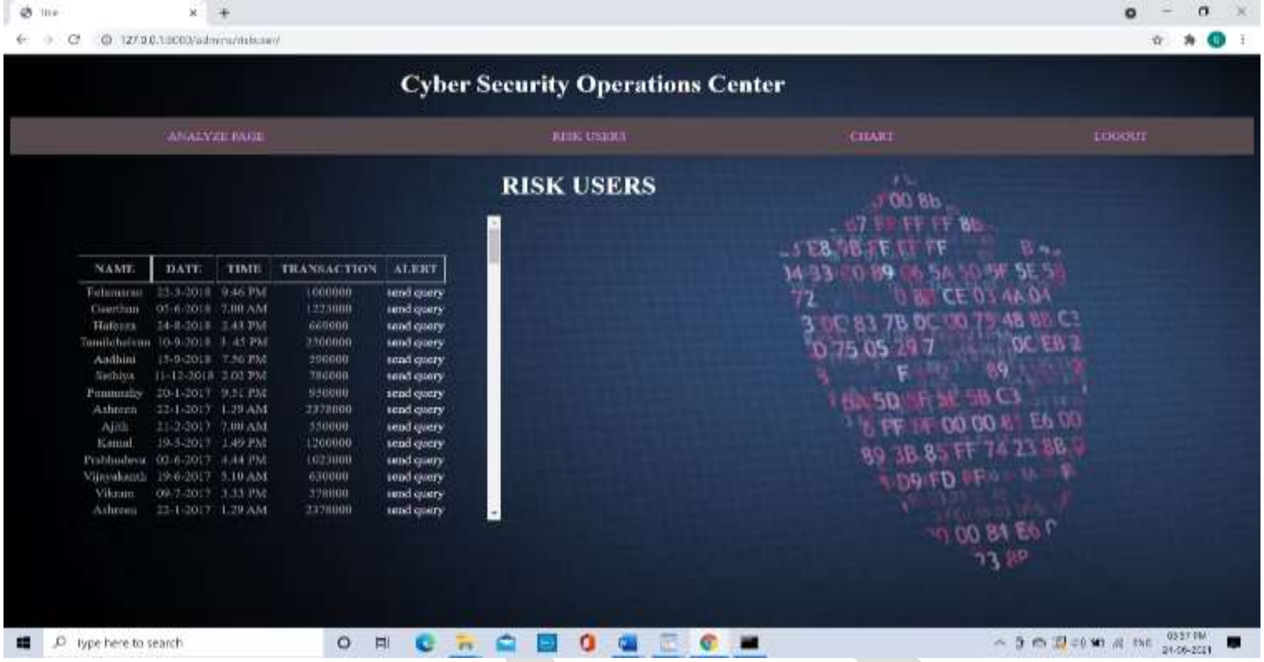
Fig 2: Login credentials for soc.



A User-Centric Machine Learning Framework for Cyber Security Operations Center

User Name :
Aadhar Card No :
Address :
Mobile No :
Bank Name :
Account No:
Branch Name :
Amount :
IFSC Code :
MICR Code :
Date :
Time :
Transaction Id :

Fig 3: Transactions of the user.

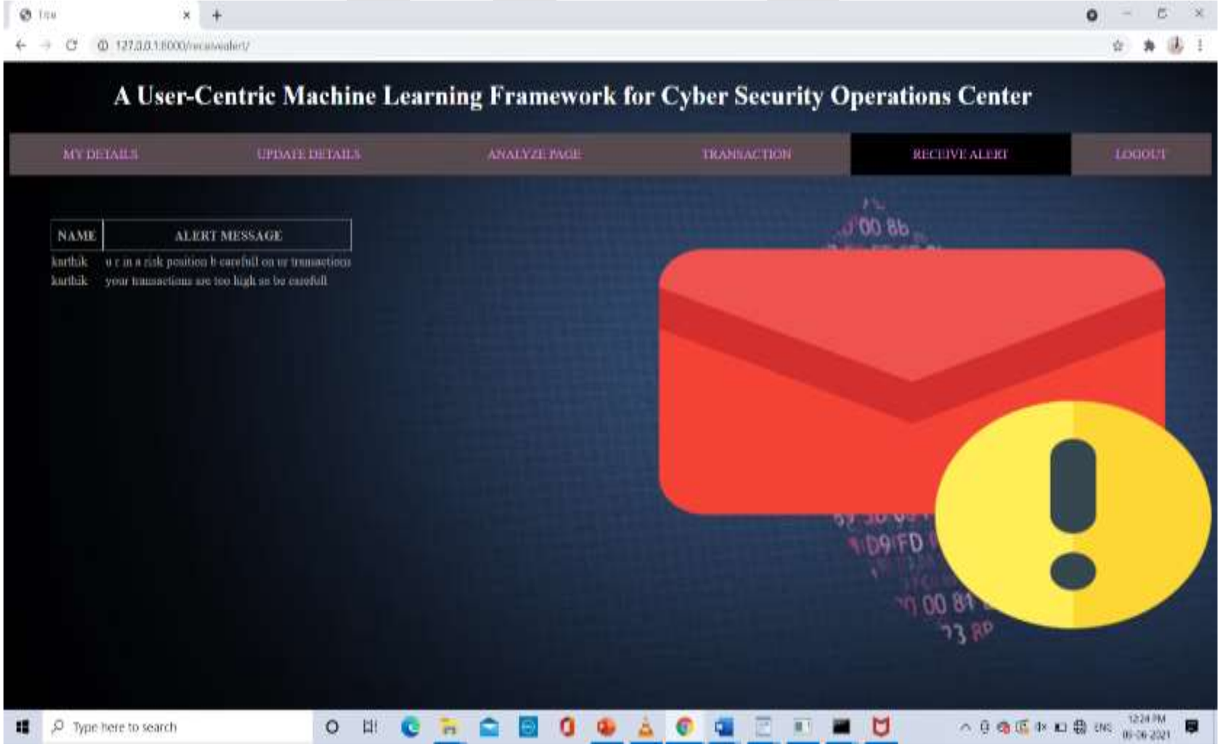


Cyber Security Operations Center

RISK USERS

NAME	DATE	TIME	TRANSACTION	ALERT
Felumurai	22-3-2018	9:46 PM	1000000	send query
Geethan	05-6-2018	7.00 AM	1223000	send query
Hafeeza	24-8-2018	2.43 PM	660000	send query
Tamilchelvan	10-9-2018	3.45 PM	2300000	send query
Aadhini	15-9-2018	7.56 PM	290000	send query
Sathiya	11-12-2018	2.02 PM	786000	send query
Ponmudiy	20-1-2017	9.51 PM	950000	send query
Ashreen	22-1-2017	1.29 AM	2378000	send query
Ajith	21-2-2017	7.00 AM	550000	send query
Kamal	19-5-2017	1.49 PM	1200000	send query
Prabhudeva	02-6-2017	4.44 PM	1023000	send query
Vijayakanth	19-6-2017	5.10 AM	630000	send query
Vikram	09-7-2017	3.33 PM	578000	send query
Ashreen	22-1-2017	1.29 AM	2378000	send query

Fig 4: Risk user detecting and sending query.



A User-Centric Machine Learning Framework for Cyber Security Operations Center

NAME	ALERT MESSAGE
karthik	u r in a risk position b carefull on ur transactions
karthik	your transactions are too high so be carefull

Fig 5: Receive alert message.

V. CONCLUSION

We provide a user-centered computer learning system that affects large data from various security logs, awareness information, and inspector intelligence. This strategy gives total design and answers for perilous client discovery for the Enterprise System Operating Center. Select AI strategies in the SOC item climate, assess productivity, IO, host, and clients to make client-driven elements. Indeed, even with straightforward mechanical learning calculations, we demonstrate that the gaining framework can see additional experiences from the rankings with the most lopsided and restricted marks. Over 20% of the neurological model of displaying is multiple times that of the current rule-based framework. To further develop the discovery accuracy circumstance, we will analyze other learning techniques to further develop the information securing, day-by-day model reestablishment, continuous gauge, completely improve and authoritative danger location and the executives. With respect to future work, we should look at other learning techniques to further develop discovery precision.

REFERENCES

[1] Cheshta Rani, Shivani Goel. An Expert System for Cyber Security Attack Awareness, International Conference on Computing, Communication, and Automation (ICCCA2015) ISBN:978-1- 4799-8890-7/15/$31.00 ©2015 IEEE 242 CSAAES.

[2] S. Poonia, A. Bhardwaj, G. S. Dangayach, (2011) “Cyber Crime: Practices and Policies for Its Prevention”, The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management, Vol. 19, No. SP1. Journal of Xi'an University of Architecture & Technology Volume XII, Issue V, 2020 ISSN No : 1006-7930 Page No: 2195

[3] Dr. Sunil Bhutada, PreetiBhutada.Applications of Artificial Intelligence in Cybersecurity International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018 All Rights Reserved © 2018 IJERCSE 214.

[4] NIKITA RANA, SHIVANI DHAR, PRIYANKA JAGDALE, NIKHIL JAVALKAR. Implementation of An Expert System for the Enhancement of ECommerce Security International Journal of Advances in Science Engineering and Technology, ISSN: 2321-9009 Volume- 2,

[5] M.M. Gamal, B. Hasan, and A.F. Hegazy, "A Security Analysis Framework Powered by an Expert System," International Journal of Computer Science and Security (IJCSS), Vol. 4, no. 6, pp. 505-527, Feb. 2011.

[6] K. Goztepe, "Designing a Fuzzy Rule-Based Expert System for Cyber Security," International Journal Of Information Security Science, vol.1, no.1, 2012.

[7] D. Welch, "Wireless Security Threat Taxonomy," Information Assurance Workshop. IEEE Systems, Man and Cybernetics Society, pp 76-83, June 2003.

[8] VidushiSharma, SachinRai, AnuragDev" A Comprehensive Study of Artificial Neural Networks" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 10, October 2012.

[9] ShaiquaJabeen, Shobhana D. Patil, Shubhangi V. Bhosale, Bharati M. Chaudhari, Prafulla S. Patil" A Study on Basics of Neural Network" International Journal of Innovative Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2017.

[10] Nalini, M. and Anbu, S., "Anomaly Detection Via Eliminating Data Redundancy and Rectifying Data Error in Uncertain Data Streams", Published in International Journal of Applied Engineering Research (IJAER), Vol. 9, no. 24, 2014.

[11] G. Jagga Rao, Y. Chalapathi Rao " Robust Bit Error Rate Optimization for MASSIVE MIMOCEM System using Channel Coding Method " International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume 8-Issue 4S2, pp. 180-184, March 2019.

[12] Nalini, M., and Uma Priyadarshini, To Improve the Performance of Wireless Networks for Resizing the Buffer, Proceedings of the 2019 international IEEE Conference on Innovations in Information and Communication Technology, Apr 2019.[DOI >10.1109/ICIICT1.2019.8741406]

[13] Shiny Irene D., G. Vamsi Krishna and Nalini, M., "Era of quantum computing- An intelligent and evaluation based on quantum computers", Published in International Journal of Recent Technology and Engineering (IJRTE), Vol. 8, Issue no.3S, pp.