e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:02/February-2022 Impact Factor- 6.752 www.irjmets.com

ANOMALY ATTACK DETECTION OF AN INTRUSION DETECTION SYSTEM WITH DEEP LEARNING APPROACH

Vallabhi Bajaj*1, Nilesh Parmar*2

*1M. Tech Scholar, Computer Science And Engineering, Jawaharlal Institute Of Technology, Borawan, India.

*2Assistant Professor, Computer Science And Engineering, Jawaharlal Institute Of Technology, Borawan, India.

ABSTRACT

New innovation carries new difficulties with it. We should guarantee that information on a system must not be gotten to by any unapproved individual. The principle assignment of system security is to give a solid and effective Network Intrusion Detection System (NIDS). An interruption identification procedure may anticipate total up and coming and on-going interruption at a structure. Throughout the previous two-decade different AI procedures have been utilized for organize based interruption location. A decent interruption identification framework will consistently be a topic of conversation for quite a while to come. As the digital assaults and volume of system information increments exponentially, associations must grow better approaches to keep their systems and information secure from the gatecrashers. With greater security apparatuses being conveyed inside the cutting-edge endeavor arranges, the measure of security occasion and ready information being created keep on expanding, making it more difficult to find the assault and gatecrashers. Associations must depend on new strategies to help and supplement human investigators when managing the identification, and reaction to organize security occasions and possible assaults on their systems. The spotlight for this Thesis is on characterizing system traffic information as ordinary or pernicious. In this work first, Particle Swarm Optimization (PSO) is utilized to enhance the highlights of preparing system information and afterward completely associated Deep Neural Network (DNN) is utilized to prepare a Network Intrusion Detection System (NIDS) by means of directed learning. Profound neural system models are prepared utilizing NSL-KDD dataset that defeat impediments of KDD Cup2009 interruption recognition datasets which has been regularly utilized before. With NSL-KDD datasets, profound neural systems with molecule swarm enhancement are demonstrated to be powerful as far as exactness and recognition rate.

Keywords: IDS, NIDS, Deep Learning, NSL-KDD Dataset.

I. INTRODUCTION

The Internet has upset society — with an ever-increasing number of individuals interfacing consistently, it is quick turning into a need of everyday life and a pillar for directing everyday business. Proceeded with development in both system access and speed of system network has encouraged wide-spread appropriation by the world on the loose. While the development of the Internet keeps on empowering advancement developments and ground breaking benefits to society, it additionally opens the opportunities for enemies to direct vindictive action in this computerized field. While their inspirations might be differed, their points are the equivalent: influence the network of society through the Internet to complete a malignant objective. These objectives can differ from burglary of protected innovation, refusal of administration, interruption of business, robbery of by and by identifiable data (PII) or instalment card data (PCI), financial extortion, requesting a payment (for example emancipate product), demolition of physical property (for example Conflicker Warm), and other unfair purposes. It is commonly understood that there is no such thing as100%security. The aim instead is towards managing risk and reducing the chances for attack. Security is an intractable problem, as it is impossible to think of all the possible ways an attacker may break through the defences. Attackers continually try new avenues to compromise defences by altering their attack strategies and using never before seen techniques. Commonly referred to as a zero-day attack, these types of attacks can be very damaging and frustrating to the defender, as the attacker has developed a new exploit that bypasses the defences of a given system or software. One of the most effective ways to protect the confidentiality, integrity, and availability of information and enterprise systems once an attacker has compromised its defences is to deploy Intrusion Detection Systems (IDS).

There are two main types of Intrusion Detection Systems: Host-based and Networkbased. Host-based intrusion detection systems monitor and control data coming from an individual workstation using tools and techniques such as host-based firewalls, anti-virus/anti-malware agents, data-loss prevention agents, and via monitoring system call trees. Network-based defences monitor and control network traffic flows via firewalls, anti-virus, proxies, and network intrusion detection techniques. Network Intrusion Detection Systems (NIDSs) are essential security tools that help increase the security posture of a computer network. NIDSs have become necessary, along with firewalls, anti-virus, access control, and other common defense-in-depth strategies towards helping cyber threat operations teams become aware of attacks, security incidents, and potential breaches occurring on their networks.

A. Intrusion Detection Systems

Intrusion leads to violations of the security policies of a computer system, such as unauthorized access to private information, malicious break-in into a computer system, or rendering a system unreliable or unusable.

A full-blown network security system should include the following subsystems:

- Intrusion Detection Subsystem: Distinguishes a potential intrusion from a valid network operation.
- Protection Subsystem: Protects the network and security system itself from being compromised by the network intrusions.
- Reaction Subsystem: This part either traces down the origin of an intrusion or fights back the hackers. The focus of this thesis is on the intrusion detection subsystem, which constitutes the first line of defense for a computer network system.

There are a number of approaches in this field. Most of them fall into three primary categories: anomaly detection, misuse detection and hybrid schemes. The anomaly detection approach is based on a model of normal activities in the system. This model can either be predefined or established through techniques such as machine learning. Once there is a significant deviation from this model, an anomaly will be reported. By contrast, a misuse detection approach defines specific user actions that constitute a misuse and uses rules for encoding and detecting known intrusions [2] [3]. The hybrid detection approach uses a combination of anomaly and misuse detection techniques. Intrusion detection is the method of finding out the actions happening in a computer system as well as justifying them for the symbol of intrusion. An IDS (Intrusion Detection System) is a system that monitors network traffic to detect suspicious activity & issues warnings when such activity is found in network. It is an application software that scans a network and system for policy breaching & harmful activity. Any malicious event or violation is directly reported either to an administrator or collected centrally using a security information and event management system. In the modern network, IDS has become an important and integral part of over-all security architecture. In order to define an IDS, it is important to understand "what is an intrusion" and then "what is an intrusion detection." We take terminology and definitions from the NIST report. An intrusion can be characterized in terms of confidentiality, integrity, and availability. An event or action causes breach of confidentiality if it allows to access resources, residing in a computer in an 6 unauthorized manner. An event or action causes breach of integrity if it allows to change the states of resources, residing in a computer in an unauthorized manner. Similarly, an event or action causes breach of availability if it prohibits legitimate users to access resources or services, residing in a computer. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of intrusions. An intrusion detection system is a software or hardware that automates the process of monitoring and analysing of events.

Intrusion detection system can be comprehensively arranged dependent on two parameters.

- By Analysis technique, Misuse IDS and Anomaly IDS can be characterized 7
- By Source of information, Host based IDS and Network based IDS can be characterized

Types of Intrusion Detection System

A. **Network Intrusion Detection System:** Network intrusion detection systems are set up within the network to examine traffic coming from different devices on the network. NIDS performs an observation of passing traffic on the entire subnet & compares the traffic that is passed on the subnets with the collection of known attacks. If an attack or abnormal behaviour is recognised, then alert can be sent to the administrator. One example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.

B. Host Intrusion Detection System: Host intrusion detection systems run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing data packets from the device only and It will alert the administrator if malicious activity or any abnormal behaviour is found. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were altered or deleted, an alert is sent to the administrator to investigate.

B. Deep Learning

Deep Learning is a subset of Machine Learning, on the other hand which is part of Artificial Intelligence. Artificial Intelligence is a common term referring to techniques that allow computers to mimic human behavior. Machine Learning represents a set of data-trained algorithms that make all of this possible.

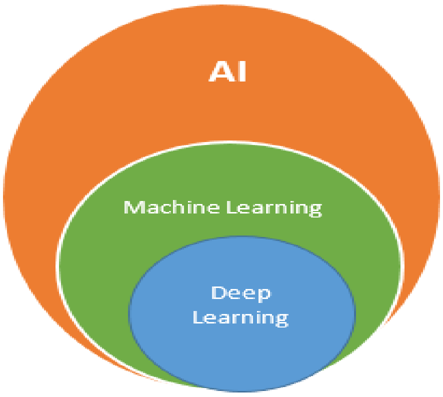

Figure 1: Deep Learning Subset

Deep Learning, on the other hand, is simply a form of machine learning, inspired by the formation of the human brain. In-depth learning algorithms attempt to reach the same conclusions as humans would by continuously analyzing data with a logical structure. To achieve this, in-depth learning uses a multi-layer structure of algorithms called neural networks.

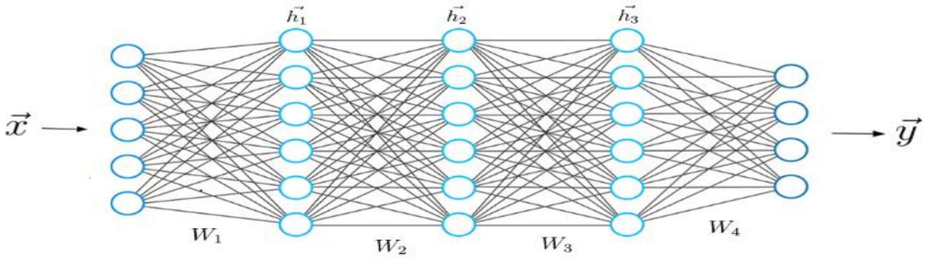

Figure 2: Deep neural networks

The structure of the neural network is based on the structure of the human brain. As we use our brains to identify patterns and separate different types of information, neural networks can be taught to perform similar functions in data.

Individual layers of neural networks can also be thought of as a type of filter that operates from negative to hidden, which increases the chances of finding and producing a positive result.

The human brain works the same way. Whenever we receive new information, the brain tries to compare it with the known. The same concept is used and deep neural networks.

Neural networks enable us to perform many functions, such as merging, splitting, or retrieving. With neural networks, we can collect or organize non-labeled data according to the similarities between the samples in this data. Or in the case of segregation, we can train the network in a labeled database to divide the samples into the database into separate categories.

Neural-generating networks with unique capabilities that enable in-depth learning models to solve tasks that machine learning models cannot solve.

a. Rectified Linear Activation Function

In order to use the stochastic gradient reduction and spread errors to train deep neural networks, an activation function is required that looks and acts as a line function, but, in fact, an indirect function that allows complex relationships in the data to be studied. The function should also provide extra sensitivity to the input function and avoid easy filling of space. The solution is to use an activated line function, or ReL for short. The node or unit that uses this activation function is referred to as the modified activation unit unit, or ReLU for short. Typically, networks that use the hidden layer repair function are called fixed networks. The adoption of ReLU can easily be considered as one of the few key steps in an in-depth learning transformation, e.g. strategies now allow for the general development of very deep emotional networks. The Rectified Linear Unit is a performance appliance that is commonly used in in-depth learning models. The function returns 0 if it receives any negative input, but for any positive xx value returns that value. Surprisingly, such a simple task (and one made up of two line pieces) can allow your model to respond to the linearity and interact smoothly. But the ReLU function works well in most systems, and is widely used as a result.

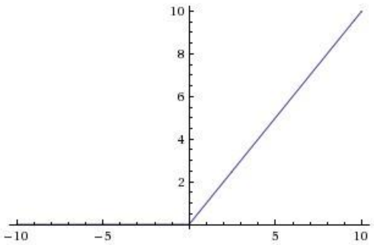

Figure 3: The ReLU function works

II. DATASET

Statistical analysis has shown that there are significant data set problems that significantly affect system performance, and have resulted in very poor estimates of unconventional detection methods. To address these issues, new data set such as, NSL-KDD [6] is proposed, containing the selected records of the complete KDD data set. The advantage of the NSL KDD database is this. There are no unnecessary records on the train set, so the divider will not produce any biased result

1. There is no duplicate record in the test set with better mitigation rates.
2. The number of records selected for each complex group equals the percentage of records in the original KDD data set.

The training data set was made up of 21 of the 37 different attacks present in the test data. The most common types of attacks are those in the training database while the novel attack is an additional attack on the experimental database i.e. not available for training data sets. The types of attacks are organized into four categories: DoS, Probe, U2R and R2L. Table 1 shows the major attacks on both training and database testing.

Table 1: Attacks in Testing Dataset

Attacks in Dataset	Attack Type
DOS	Back, Land, Neptune, Pod, Smurf, Tear drop, Mail bomb, Process table, Udpstorm,Apache2,Worm
Probe	Satan, IP sweep, Nmap, Port sweep, Mscan, Sa int
R2L	Guess_password, Ftp_write, Imap, Phf, Multi hop, Warezmaster, Xlock, Xsnoop, Snmpgue ss, Snmp get attack, Http tunnel, Send mail, Named

U2R	Buffer_overflow,Loadmodule,Rootkit,Perl ,Sqlattack,Xterm,Ps

III. EXPERIMENTAL RESULTS

NSL-KDD dataset is the benchmark in modern-day to investigating new methodologies for better IDS. We have selected 10% dataset of NSL-KDD for training and testing dataset with 3,11,029 records with two ways to deal with accurately group the ordinary and intrusions in the informational index.

Table 2: Result Analysis of various Algorithm.

		Accuracy	Precision	Recall	F-Score
Algorithm	**Linear Regression**	84.8	98.9	82.4	89.7
	Decision Tree	93	99.9	91.4	95.4
	Naive Bayes	92.9	98.9	92.3	95.5
	Random Forest	92.7	99.9	91	95.2
	Adaboost	92.5	99.5	91.1	95.1
	DNN_1	92.9	99.8	91.4	95.4
	DNN_2	93.1	99.9	91.5	95.5
	DNN_3	**93.1**	**99.8**	**91.6**	**95.5**
	DNN_4	**93.1**	**99.8**	**91.6**	**95.5**
	DNN_5	93.1	99.9	91.6	95.5

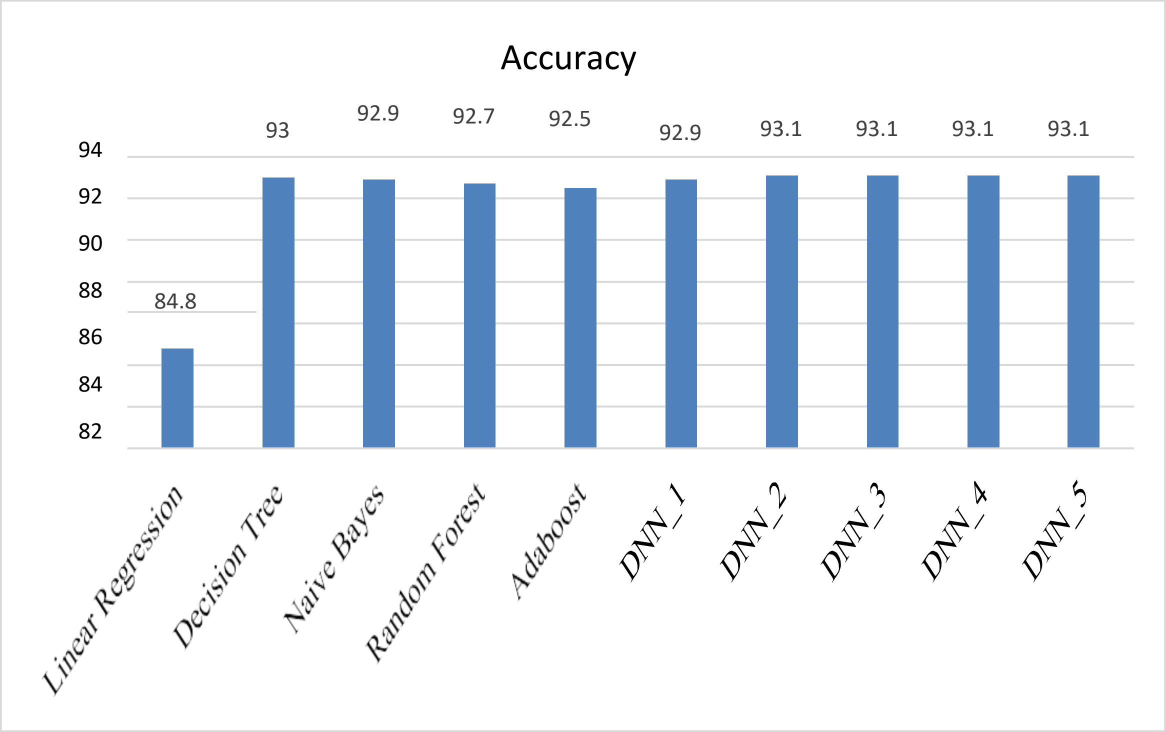

Figure 4: Accuracy of different algorithms.

IV. CONCLUSION

Deep neural Network system are prepared utilizing NSL-KDD dataset that beat impediments of KDD Cup2009 interruption identification datasets which has been normally utilized previously. With NSL-KDD datasets, profound neural systems with molecule swarm enhancement are demonstrated to be successful regarding precision and discovery rate.

V. REFERENCES

[1] Ripon Patgiri, Udit Varshney, Tanya Akutota, Rakesh Kunde, "An Investigation on Intrusion Detection System Using Machine Learning", 2018 IEEE Symposium Series on Computational Intelligence (SSCI), Nov 2018 pp1684-1691.

[2] Marzia Zaman, Chung-Horng Lung, "Evaluation of Machine Learning Techniques for Network Intrusion Detection", IEEE/IFIP Network Operations and Management Symposium, 23-27 April 2018 // Taipei, Taiwan, Cognitive Management in a Cyber World.

[3] Amol Borkar Akshay Donode Anjali Kumari - "A Survey on Intrusion Detection System and Internal Intrusion Detection and Protection System" - Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017)

[4] Jiadong Ren, Jiawei Guo, Wang Qian, Huang Yuan, Xiaobing Hao & Hu Jingjing – "Building an Effective Intrusion Detection System by Using Hybrid Data Optimization Based on Machine Learning Algorithms" Published 16 June 2019.

[5] B.M. Beigh, U. Bashir and M. Chachoo - "Intrusion Detection and Prevention System: Issues and Challenges" - International Journal of Computer Applications (0975-8887), Volume 76-No.17, August 2013.

[6] P.S. Rath, Dr.N. Barpanda and S. Panda - "Intrusion Detection System Built around Hybrid Technology: A Review" - International Advanced Research Journal in Science, Engineering and Technology, Vol.3, Issue 4, (April 2016).

[7] R. D. Kulkarni - "Using Ensemble Methods for Improving Classification of the KDD CUP '99 Data Set" - IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 16, Issue 5, and e- ISSN: 2278-0661, p-ISSN: 2278- 8727, PP 57-61, (Sep-Oct.2014).

[8] U. Albalawi, S.C. Suh and J. Kim - "Incorporating Multiple Supervised Learning Algorithms for Effective Intrusion Detection" - World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, Vol. 8, No 2, (2014).

[9] S. Choudhury and A. Bhowal - "Comparative Analysis of Machine Learning Algorithms along with Classifiers for Network Intrusion Detection" - International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015, pp.89-95.

[10] P.S. Rath, M. Hohanty, S. Acharya and M. Aich - "Optimization of IDS Algorithms Using Data Mining Technique" - Proceeding of 53rd IRF International Conference, Pune, India, 2016, ISBN: 978-93-86083-01-2.

[11] K. Murugan, P. Varalakshmi, R.N. Kumar and S. Boobalan - "Data Mining Using Integration of Clustering and Decision Tree" - ISSN (Online): 2347 – 2812, Vol. 1, Issue 2, (2013).

[12] V. Malviya and A. Jain (HOD) - "An Efficient Network Intrusion Detection Based on Decision Tree Classifier & Simple K-Mean Clustering using Dimensionality Reduction" – A Review", International Journal on Recent and Innovation Trends in Computing and Communication, Vol .3, Issue 2, ISSN: 2321 –8169, (February 2015).

[13] V. Rao - "A Clustering Algorithm for Intrusion Detection using Hybrid Data Mining Technique" - International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, Vol. 3, Special Issue 1, (April 2015).

[14] P. Singha, R. Lakkadwala, A. Sheth, A. Gaikwad and M.V. Kadam - "Improving Efficiency of Hybrid Intrusion Detection System Using Kmeans and Naïve Bayes" - International Journal of Engineering and Computer Science Vol. 4, Issue 3, Page No. 10842-10845, ISSN: 2319- 7242 (March 2015).

[15] K. Rajasekhar, B.S. Babu, P.L. Prasanna, D.R. Lavanya and T.V. Krishna - "An Overview of Intrusion Detection System Strategies and Issues" - International Journal of Computer Science & Technology, Vol. 2, Issue 4, ISSN: 0976-8491 (Online), ISSN: 2229-4333(Print), (Oct- Dec. 2011).

[16] V. Richhariya, Dr. J.L. Rana, Dr. R.K. Pandey and Dr. R.C. Jain - "An Efficient Classification Mechanism

Using Machine Learning Techniques for Attack Detection from Large Dataset" - International Journal of Innovative Research in Science, Engineering and Technology, Vol. 1, Issue 2, (December 2012).

[17] Roshani Gaidhane, C. Vaidya and Dr. M. Raghuwanshi – "Intrusion Detection and Attack Classification using Back-propagation Neural Network"- International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181 Vol. 3 Issue 3, March – 2014

[18] WANG Huai-bin, YANG Hong-liang, XU Zhi-jian and YUAN Zheng – "A clustering algorithm use SOM and K Means in Intrusion Detection" - 2010 International Conference on E-Business and E-Government

[19] Varuna and Dr.P. Natesan – An Integration of K-Means Clustering and Naïve Bayes Classifier for Intrusion Detection - 3rd International Conference on Signal Processing, Communication and Networking (ICSCN) 978-1-4673- 6823- 2015

[20] Sinem Osken; Ecem Nur Yildirim; Gozde Karatas; Levent Cuhaci, "Intrusion Detection Systems with Deep Learning: A Systematic Mapping Study", Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), 20 June 2019, pp. 1-9

[21] Hamidreza Sadreazami, Arash Mohammadi, Amir Asif and Konstantinos N. Plataniotis, "Distributed-Graph-Based Statistical Approach for Intrusion Detection in Cyber-Physical Systems", IEEE Transactions on Signal and Information Processing over Networks, Vol. 4, 2018, pp. 137-147,.

[22] Jaime Zuniga Mejia, Rafaela Villalpando Hernandez, Cesar Vargas Rosales and Andreas Spanias, "A Linear Systems Perspective on Intrusion Detection for Routing in Reconfigurable Wireless Networks", Vol.7, 2019, pp. 60486- 60500.

[23] Panagiotis I. Radoglou Grammatikis, Panagiotis G. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems", Journal Article| IEEE Access, 2019, pp. 46595-46620.

[24] Amol Borkar, Akshay Donode and Anjali Kumari, "A Survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and Protection System" , Proceedings of the International Conference on Inventive Computing and Informatics, 2017, pp. 949-953.

[25] Rui Zhao, Ruqiang Yan, Zhenghua Chen, Kezhi Mao, Peng Wang, and Robert X. Gao, "Deep Learning and Its Applications to Machine Health Monitoring: A Survey", 2015, pp. 1-14.

[26] Dimitar Nikolov, Iliyan Kordev, Stela Stefanova, "Concept for network intrusion detection system based on recurrent neural network classifier", Proc. XXVII International Scientific Conference Electronics, 2018, pp.13-16.

[27] Aumreesh Ku. Saxena, Dr. Sitesh Sinha, Dr. Piyush Shukla, "General Study of Intrusion Detection System and Survey of Agent Based Intrusion Detection System", International Conference on Computing, Communication and Automation, 2017, pp.417-421.

[28] Bo Dong, Xue Wang, "Comparison Deep Learning Method to Traditional Methods Using for Network Intrusion Detection", International Conference on Communication Software and Networks, 2018, pp. 581- 585.

[29] Anuja S. Desai and D. P. Gaikwad, "Real Time Hybrid Intrusion Detection System usingSignature Matching Algorithm and Fuzzy-GA", IEEE International Conference on Advances in Electronics, Communication and Computer Technology, 2016, pp. 291-294.

[30] Mohammed Anbar, Rosni Abdulah, Izan H. Hasbullah and Omar E. Elejla, "Comparative Performance Analysis of classification algorithm for Internal Intrusion Detection", 14th Annual Conference on Privacy Security and Trust,2016, pp. 109-120.

[31] Dewan Md. Farid, Nouria Harbi, and Mohammad Zahidur Rahman, "Combining Naive Bayes and Decision tree for Adaptive Intrusion Detection", airccse.org/journal,2017, pp. 12-25.

[32] Marzia Zaman , Chung-Horng Lung , "Evaluation of Machine Learning Techniques for Network Intrusion Detection" , IEEE/IFIP Network Operations and Management Symposium , 2018, pp. 1-5.

[33] X. Fan, C.-H. Lung and S. Ajila, "An Adaptive Diversity Based Ensemble Method for Binary Classification", Proc. of the 41st IEEE International Computer Software and Applications Conference (COMPSAC), July 2017.