ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-4, 2019

Intrusion Detection Techniques: Survey & Discussions

Amita Tiwari[1], Prof. Atul Shrivastava[2]

[1]M. Tech Scholar, Department of CSE, SIRTE, Bhopal (India)

[2]Professor, Department of CSE, SIRTE, Bhopal (India)

[1]amitatiwari777@gmail.com, [2]akshri5@gmail.com

ABSTRACT

Cyber security is becoming increasingly important; therefore, countries have started to make big investments in order to protect their critical infrastructures. The IDS is tasked with monitoring and analyzing network activity to differentiate between normal and anomalous activities. If anomalous activity goes undetected, this could potentially cause severe damage to the infrastructure and reliability of a computer system. Therefore, the detection rate of anomalous activity must be maximized. In this paper we present the comparative performance evaluation for the various techniques in intrusion detection system.

Keywords:- Intrusion detection system, Neural network, Cyber security, KDDCUP, Attack.

INTRODUCTION

Due to extensive usages of internet, electronic assaults on network and information system of the financial organizations, military and energy sectors are increasing. Large web sites of any organization are attacked by various intruders and hackers. The information of government and private organizations may be leaked or damaged by unauthorized users. Intruders can have many forms such as viruses, spyware, worms, malicious logins, spamware, etc.. The information security is very important aspect to protect the valuable data of any organization. The organizations need security applications that effectively protect their networks from malicious attacks and misuse. Intrusion detection system can detect the intrusions and protect the information system from the security violations.

Intrusion detection system detects intruder and take the action against intruder. It is used to recover the information by repairing the damage caused by unauthorized user of the organization [2]. It is used to identify the malicious use of computer and computer network. It detects access to un-authorized user, the violation of security and finds illegal users [2].

The attackers act like normal users, generate data and hide their malicious activities under terabytes of data. They know that many security mechanisms cannot protect the networks due to the large amount of data stored, scalability issues or due to the lack of detection capabilities. The enterprises and government agencies need to monitor their network traffic to detect malicious activities and perform analysis to differentiate the malicious and legitimate user activities to protect their networks. Detecting malicious activities require intrusion detection systems (IDS) and in today's secure ICT infrastructure, the IDSs are part of most networks. However, the IDSs are only good if they have elite detection capabilities. It is critical that an IDS detection mechanism is accurate enough to differentiate between legitimate and malicious traffic that enter and leave the network. The possible results of using an IDS are as follows: detected malicious traffic (real alarms), undetected malicious traffic, legitimate traffic that IDS detect as malicious (false alarms) and legitimate traffic that IDS detect as good [7].

Network Intrusion Detection System (NIDS) constitutes an essential security tool for organizations to monitor network traffic and

identify network attacks. NIDSs can be categorized into three main categories based on the detection method they use in identifying potential attacks as signature-based, anomaly-based or specification-based NIDS [1]. Due to the continuous change of attacks signature and the emerging of new threats and normal traffic alike, the research community is always in need for modern datasets that accurately reflect the current status of security threats as well as benign applications traffic. UNSW-NB15 is a new dataset for evaluating NIDS created by the Cyber Security Research Group at the Australian Centre for Cyber Security (ACCS), which contains over 2 million labeled modern normal and abnormal network traffic.

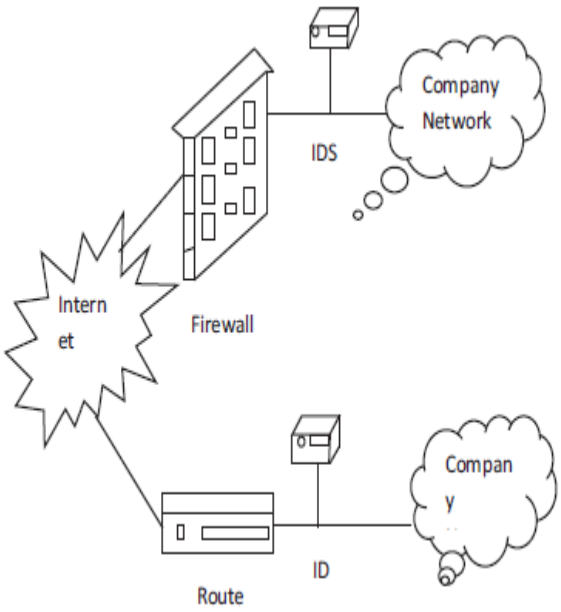

Fig 1: Process for Intrusion detection system.

The various network attacks can be categorized as User-to-Root (U2R) attacks, Denial-of-Service (DoS) attacks, Remote-to-Local (R2L) attacks and probe attacks [9]. In DoS attack, the attacker interrupts or denies the user access to the server. Examples are Neptune, Ping of Death, Mailbomb, etc. In U2R, the attacker is allowed privileged access by the extension of the root permissions like those of the administrator, the most common example being the buffer overflow attack. In R2L attack, the assailant intrudes the target system illegally, without any permission from the owner. Last of all, probe attack gathers and analyses information with an aim to map the network system, e.g., scanning software like Satan, Mscan and Nmap collect information from the target system such as hostname, service application, IP address and operating system. Though this attack gathers only data, this information can be employed in attacks of various kinds in the future.

The rest of this paper is organized as follows in the first section we describe an introduction of about cyber security, attacker and threats occurred in a computer network generally. In section II we discuss about the intrusion detection system, In section III we discuss about the literature survey in the intrusion detection system, finally in section IV we conclude the about our paper.

II INTRUSION DETECTION SYSTEM

The computing world has changed over the past decade due to the rapid development of internet and new privacy enhancement technologies to circumvent internet censorship. Tor which is popular in fighting internet censorship has been deployed to serve thousands of users transferring terabytes of data daily. Intrusion detection system is a software application or a device placed at strategic places on a network to monitor and detect anomalies in network traffic [6] as shown in below figure. The main features of IDS are to raise an alarm when an anomaly is detected. A complementary approach is to take corrective measures when anomalies are detected, such an approach is referred to as an intrusion Prevention System (IPS). Based on the interactivity property of IDS, it can be designed to work either on-line or offline. Onine IDS operates on a network in real time by analyzing traffic packets and applying rules to classify normal and analogous traffic. Off-line IDS operates by storing data and after processing to classify normal and anomaly.

ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-4, 2019

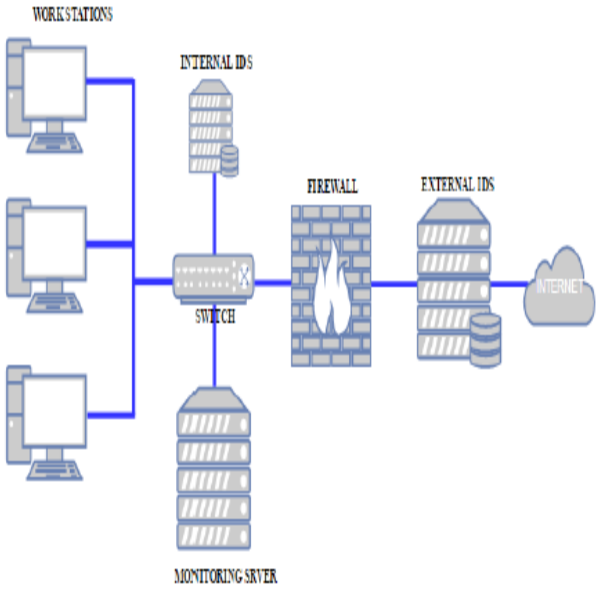

Fig 2: Intrusion Detection System model.

III RELATED WORK

Intrusion Detection Systems is a mechanism, which protects resources and data from unauthorized access, misuse, and malicious intrusions in a distributed computing environment. Machine learning techniques, such as Neural Networks, Support Vector Machines, Naïve Bayesian Classifiers, etc. are common techniques for intrusion detection. IDSs constantly monitor and analyze the system, which allows the machine learning model to recognize common/normal behavior. This allows the model to detect abnormal/anomalous behavior and react with the appropriate response. The common dataset used for IDS developments and testing is the KDD99 dataset [4].

[1] In this paper, a deep learning model based on a multilayer Feed forward artificial neural network using back propagation and stochastic gradient descent method has been evaluated as a binomial classifier for Network Intrusion Detection System. Three different experiments were executed in order to determine the optimal activation function, then to select the most important features and finally to test the proposed model on unseen data. The evaluation results show outstanding performance with extremely high accuracy (i.e. 98.99%) and very low false alarm rate (i.e. 00.56%).

[2] In this paper, a novel intrusion detection technique based on ensemble method of machine learning is proposed. The Bagging method of ensemble with REPTree as base class is used to implement intrusion detection system. The relevant features from NSL_KDD dataset are selected to improve the classification accuracy and reduce the false positive rate. The performance of proposed ensemble method is evaluated in term of classification accuracy, model building time and False Positives. The experimental results show that the Bagging ensemble with REPTree base class exhibits highest classification accuracy. One advantage of using Bagging method is that it takes less time to build the model. The proposed ensemble method provides competitively low false positives compared with other machine learning techniques.

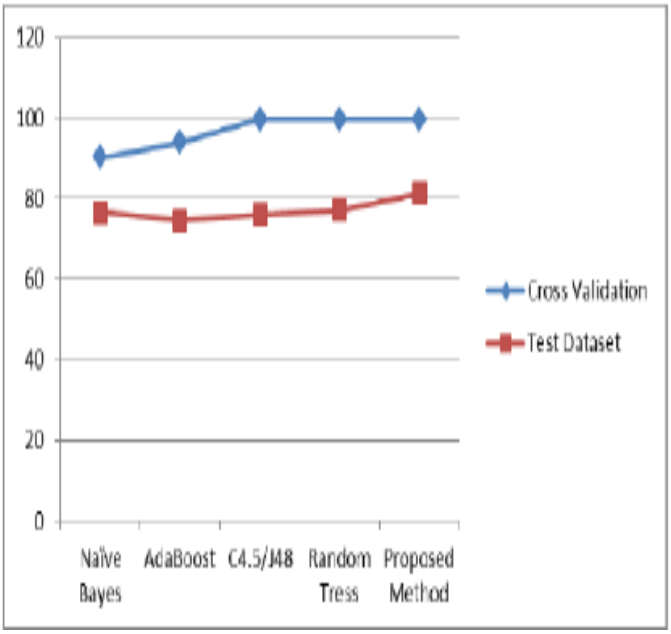

Fig 3: Classification Accuracy of machine learning techniques.

[3] In this paper, novel method is for intrusion detection with feature reduction using partially ID3 algorithm to find higher information gain for attribute selection and KNN based GA (genetic algorithm) is applied for classification and detection of intrusions on KDD dataset. The simulation & analysis of the method is done on MATLAB2012A. The experimental scenario of proposed methodology produces better result when it compared with some existing approaches, for the measurement of the result comparing with the different performance metrics parameters such as sensitivity, specificity and accuracy.

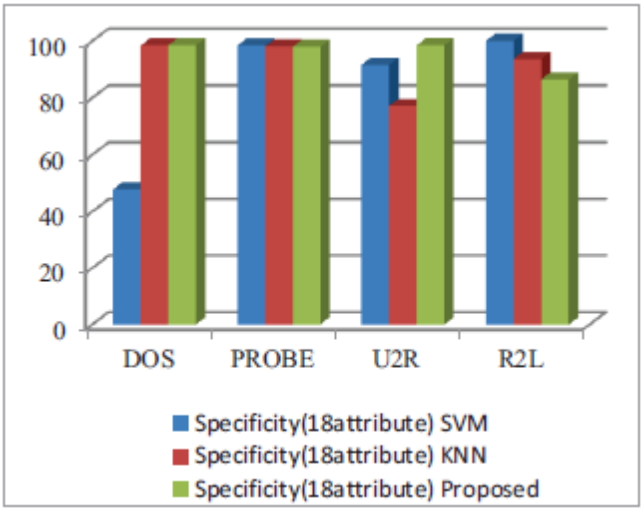

Fig 4: Specificity (18attribute).

[4] In this paper, they implemented an Evolutionary General Regression Neural Network (E-GRNN) as a two-class classifier for intrusion detection based on features of application layer protocols (e.g., http, ftp, smtp, etc.) used in simulated network traffic activities. The E-GRNN is an evolutionary search-inspired General Regression Neural Network, which extracts the most salient features to reduce computational complexity and increase accuracy. Their research shows that the E-GRNN classifier was able to achieve a DR of 95.53% and an FAR of 2.11%.

[5] In this paper, firstly network anomaly and attack detection studies on big data has been reviewed. Then, a public big network data was analyzed with a new unsupervised anomaly detection approach on Apache Spark cluster in Azure HDInsight. Finally, the results obtained from a case study were evaluated, %96 accuracy was achieved. The results were visualized after dimension reduction using Principal Component Analysis (PCA). The identified anomalies may provide usable outputs to understand the behavior of the network, distinguishing the attacks, providing better cyber security, and protecting critical infrastructures.

[6] This work focuses on the classification of Tor traffic and nonTor traffic to expose the activities within Tor traffic that minimizes the protection of users. A study to compare the reliability and efficiency of Artificial Neural Network and Support vector machine in detecting nonTor traffic in UNB-CIC Tor Network Traffic dataset is presented in this paper. The results are analysed based on the overall accuracy, detection rate and false positive rate of the two algorithms. Experimental results show that both algorithms could detect nonTor traffic in the dataset. A hybrid Artificial neural network proved a better classifier than SVM in detecting nonTor traffic in UNB-CIC Tor Network Traffic dataset.

[7] This study investigates the performance of two open source intrusion detection systems (IDSs) namely Snort and Suricata for accurately detecting the malicious traffic on computer networks. Snort and Suricata were installed on two different but identical computers and the performance was evaluated at 10 Gbps network speed. It was noted that Suricata could process a higher speed of network traffic than Snort with lower packet drop rate but it consumed higher computational resources. Snort had higher detection accuracy and was thus selected for further experiments. It was observed that Snort triggered a high rate of false positive alarms. To solve this problem a Snort adaptive plug-in was developed. To select the best performing algorithm for the Snort adaptive plug-

in, an empirical study was carried out with different learning algorithms and Support Vector Machine (SVM) was selected.

[8] This paper proposes a novel approach for intrusion detection system based on sampling with Least Square Support Vector Machine (LS-SVM). Decision making is performed in two stages. In the first stage, the whole dataset is divided into some predetermined arbitrary subgroups. The proposed algorithm selects representative samples from these subgroups such that the samples reflect the entire dataset. An optimum allocation scheme is developed based on the variability of the observations within the subgroups. In the second stage, least square support vector machine (LS-SVM) is applied to the extracted samples to detect intrusions. They call the proposed algorithm as optimum allocation-based least square support vector machine (OA- LS-SVM) for IDS.

IV CONCLUSIONS

The detection and prevention of the intrusion from the network is an important issues and it is not possible to violate security completely on using the existing approaches. The intrusion detection helps security organization accordingly by enhancing the efficiency and it is easy to use. In this paper we present the survey for the intrusion detection using various techniques and the number of application with security of a network.

REFERENCES:-

[1] Malek Al-Zewairi, Sufyan Almajali, and Arafat Awajan, “Experimental Evaluation of a Multi-Layer Feed-Forward Artificial Neural Network Classifier for Network Intrusion Detection System”, International Conference on New Trends in Computing Sciences, IEEE 2017, pp 167-172.

[2] D.P.Gaikwad, Ravindra C. Thool, “Intrusion Detection System Using Bagging Ensemble Method of Machine Learning”, International Conference on Computing Communication Control and Automation, IEEE 2015. Pp 291-295.

[3] Preeti Singh, Amrish Tiwari, “An Efficient Approach for Intrusion Detection in Reduced Features of KDD99 using ID3 and classification with KNNGA”, Second International Conference on Advances in Computing and Communication Engineering, IEEE 2015. Pp 445-452.

[4] James Brown, Mohd Anwar, Gerry Dozier, “An Evolutionary General Regression Neural Network Classifier for Intrusion Detection”, IEEE, 2016. Pp 1-5.

[5] Duygu Sinanc Terzi, Ramazan Terzi, Seref Sagiroglu, “Big Data Analytics for Network Anomaly Detection from Netflow Data”, IEEE, 2017. Pp 592-598.

[6] Elike Hodo, Xavier Bellekens, Ephraim Iorkyase, Andrew Hamilton, Christos Tachtatzis, Robert Atkinson, “Machine Learning Approach for Detection of nonTor Traffic”, ARES 2017. Pp 1-6.

[7] Syed Ali Raza Shah, Biju Issac, “ Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System”, 2017. Pp 1-25.

[8] Enamul Kabir, Jiankun Hu, Hua Wang, Guangping Zhuo, “A Novel Statistical Technique for Intrusion Detection Systems”, Pp 1-39.

[9] Rashidah Funke Olanrewaju, Burhan Ul Islam Khan, Athaur Rahman Najeeb, Ku Nor Afiza KuZahir, Sabahat Hussain, “Snort-Based Smart and Swift Intrusion Detection System”, Indian Journal of Science and Technology, 2018. Pp 1-9.

[10] Wrushal K. Kirnapure, Arvind R. Bhagat Patil, “ Survey on Classification, Detection and Prevention of Network Attacks using Rule based Approach”, International Journal of Computer Applications, 2017. Pp 11-17.

[11] L. Khalvati, M. Keshtgary, N. Rikhtegar, “Intrusion Detection based on a Novel Hybrid

Learning Approach", Journal of AI and Data Mining, 2018, Pp 157-162.

[12] Pratham Harshit Rajmahanty, S. Ganapathy, " Role of Decision Trees in Intrusion Detection Systems: A Survey", International Journal of Advances in Computer and Electronics Engineering, 2017. Pp 9-13.

[13] Sheetal Panjeta, Er. Kanika Aggarwal, "Review paper on Different Techniques in Combination with IDS", International Journal of Engineering Science and Computing, May 2017. Pp 11623-11630.