International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 2, Mar-Apr-2019, ISSN (Online): 2395-566X

A Survey on Robust Intrusion Detection System Methodology and Features

M. Tech. Scholar Jyotsna Purohit
Dept. of Computer Science & Engg.
Mittal Institute of Technology
Bhopal, Madhya Pradesh, India
jyotsnapurohit28@gmail.com

Asst. Prof. Jayshree Boaddh
Dept. of Computer Science & Engg.
Mittal Institute of Technology
Bhopal, Madhya Pradesh, India
jayshree.boaddh@gmail.com

Asst.Prof. Akrati Shrivastava
Dept. of Computer Science & Engg.
Mittal Institute of Technology
Bhopal, Madhya Pradesh, India
aakratishrivastava93@gmail.com

***Abstract* - To improve network security different steps has been taken as size and importance of the network has increases day by day. In order to find intrusion in the network IDS (Intrusion detection system) systems were developed which were broadly classified into two category first was anomaly based and other was misuse based. In this paper survey was done on the various techniques of intrusion detection system where some of supervised and unsupervised intrusion detection techniques are discussed. Here methodology of various researchers are explained with their steps of working. Different types of attacks done by the intruders were also discussed.**

***Index Terms* - Anomaly Detection, ANN, Clustering, Genetic Algorithm, Intrusion Detection..**

I. INTRODUCTION

Information security considered as main issue in information system. Computer Network security has long been recognized as a serious issue. The problem of computer security was first formulated in a general fashion. Since these beginnings, computer security has continued to receive attention due to the rapid increase in security incidents. For the purpose of this work, a security violation will be defined as any activity that is not explicitly permitted in a security policy [1]. This security policy may or may not be formally defined. It should be noted that the security of a system and its usability are tradeoffs. Increasing the security of a system will tend to decrease its usefulness.

Internet attacks are rising, and there have been different attack detection methods accordingly. As a practical matter, this makes it impossible to guarantee the security of a useful system. Intrusion detection improves this tradeoff by allowing activities to continue, but by trying to identify those activities which may lead to security violations [3].

1. Host based IDs Get audit data from host audit trails and detects attack against a single host. It works in switched network environments. It operates in encrypted environments and detects and collects the most relevant information in the quickest possible manner. It requires the use of the resources of a host server – disk space, RAM and CPU time. It does not protect entire infrastructure

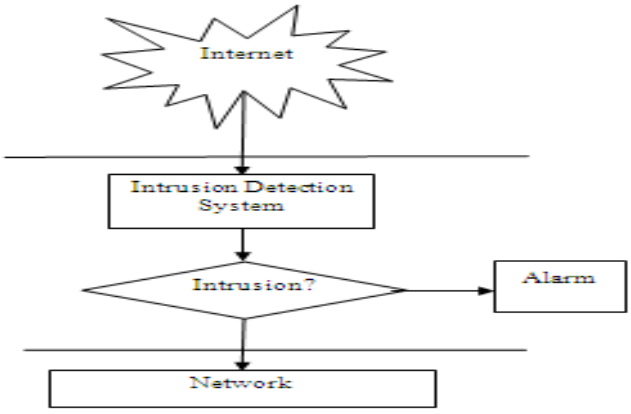

Figure 1 Intrusion Detection System [14].

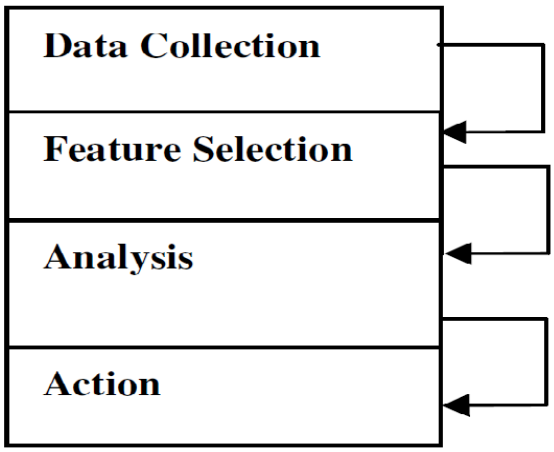

Figure 2 Key functionalities of an Intrusion Detection System [14].

© 2019 IJSRET

1.1 Data Collection- This module collects the real world data in system and provided it as the input to the IDS. In case of network based IDS, packets of data in the transmission are get collected and within the host dependent IDS, details such as disk usage, system process, call stack etc are logged.
1.2 Feature Selection- Large amount of data is available in the network and a subset of it is usually analyzed for the intrusion. As an example, Internet-Protocol (IP) address of source and the target system, protocol type, header length and size could be studied for possible intrusion.
1.3 Analysis-This module defines the method that is used to analyze data. One approach which is the use of the rule dependent IDS in which the incoming-traffic is checked against pre-defined signature or pattern. Another method is the use of anomaly dependent IDS in which the behavior of the system is analyzed and mathematical models are employed.
1.4 Action- This scheme explains how a system should act to the possible attacks within a system. It can either inform the system administrator with entire data which is needed via icons of alarm/email or it can play an active part in the system by dropping packets so that it does not enter the system or closing ports [1].

2. Distributed IDs It gathers audit data from multiple hosts and possibly the network that connects the host. It detects attacks involving multiple hosts.

3. Network based IDs It uses network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services. It detects attack from network. NIDS uses a passive interface to capture network packets for analyzing. NIDS sensors placed around the globe can be configured to report back to a central site, enabling a small team of security experts to support a large enterprise. NIDS systems scale well for network protection because the number of actual workstations, servers, or user systems on the network is not critical – the amount of traffic is what matters .Provide better security against DOS attacks.

Whole paper is organized into few section where second section gives summary of the work done by different author in this field of IDS, here comparison table of researcher approach was shown with their limitations. Third section explained various techniques for intrusion detection include supervised and unsupervised both. Finally types of attacks were brief in fourth section.

III. TECHNIQUES OF IDS

1. Misuse identification [9] utilizes examples of the definitely known attacks or the framework's delicate spots to coordinate and distinguish intrusions. For example, in the event that somebody tries to figure a secret key, a mark manage for this sort of conduct could be that 'excessively numerous fizzled login attempted in indicated time' and occasion of his compose may bring about rising an alarm. Misuse recognition observed to be not proficient against the not known attacks that have no coordinated guidelines or examples yet.

2. Anomaly location [9] banners watched exercises that withdraw impressively from the customary use profiles as inconsistencies, that is, conceivable intrusions. For example a profile of a client may contain the found the middle value of frequencies of some framework summons in his or her logging sessions. Also, for a logging session that is being observed on the off chance that it has altogether lower or higher frequencies an abnormality ready will be raised.

Anomaly identification is a successful strategy for discovering perfect or not referred to attacks as the learning is never required with respect to the intrusion attacks. Be that as it may, in the meantime it tends to raise a larger number of cautions than misuse identification since whatever occasion occurs in a session, ordinary or unusual conduct, if their frequencies are significantly separate among the threshold found the middle value of frequencies of the client it will raise an alarm.

3. Supervised learning
In conceptual terms the supervised learning can be seen as a teacher having knowledge of the environment derived from input-output examples. The teacher provide consultancy to the neural network telling it what is normal and abnormal traffic pattern, in the sense of what is classified as malicious and non-malicious.

Basically the supervised learning operates as a portion of network connection is to be analyzed and labeled with the help of the teacher [2, 11]. Afterwards the labeled training data is used by the learning algorithm to generalize the rules. Finally the classifier uses the generated rules to classify new network connections and gives alert if a connection is classified to be malicious.

4. Unsupervised learning
Unlike the supervised learning, unsupervised learning does not have a teacher to tell what is a ’good’ or ’bad’ connection. It has the ability to learn from unlabeled data and create new classes automatically. In with the use of a clustering algorithm it is illustrated how unsupervised learning operates [8]. First, the training data is clustered using the clustering algorithm. Second, the clustered weight vectors can be labeled by a given labeling process, for example by selecting a sample group of the data from a cluster and label that cluster center with the

© 2019 IJSRET

major type of the sample. Finally, the labeled weight vectors can be used to classify the network connections.

5. Compare Supervised and unsupervised

Monitoring network traffic shows a lot of activities in the sense of different data packets being sent forth and back constantly. Of course the magnitude of this activity depends on the network monitored. If a network of a home computer, which is only used for e-mail checking and internet browsing, is monitored, it will show little traffic activity, but if a busy server on the Internet is monitored, it will show a great deal of activity.

Intrusion detection systems should be able to monitor and categorize (or label) traffic at the same time regardless of the size of the traffic activity. But in networks with large traffic rate, labeling data becomes a tough task. It is time-consuming and normally only the small part of provided data may be labeled [7]. At packet level it may be impossible to unambiguously assign label to data. On the other hand in real application one can never be sure that a set of labeled data examples are enough to cover all possible attacks [10]. These considerations are important and should be taken into account when choosing network paradigm.

6. Genetic Algorithm

Genetic algorithms are unsupervised search procedures often used for optimization problems. Genetic algorithm is based on the principles of evolution and natural selection of chromosomes. An initial population of chromosomes is generated randomly where each chromosome represents a possible solution to the problem (an set of parameters).The evaluation function is used to calculate the "goodness" of each chromosome. In evaluation, two operators, crossover and mutation, are used to generate the new population or rules. Then, the best individual or chromosome is selected as the final result once the optimization criteria in met

III. RELATED WORK

Shaohua Teng et. al. in [1] this work present an adaptive collaboration intrusion detection method to improve the safety of a network. A self-adaptive and collaborative intrusion detection model is built by applying the Environments classes, agents, roles, groups, and objects (E-CARGO) model. The objects, roles, agents, and groups are designed by using decision trees (DTs) and support vector machines (SVMs), and adaptive scheduling mechanisms are set up. The KDD CUP 1999 data set is used to verify the effectiveness of the method.

Kai Peng et. al. in [2] In this study, this work propose a clustering method for IDS based on Mini Batch Kmeans combined with Principal Component Analysis. Firstly, a preprocessing method is proposed to digitize the strings and then the dataset is normalized so as to improve the clustering efficiency. Secondly, the Principal Component Analysis method is used to reduce the dimension of the processed dataset aiming to further improve the clustering efficiency, and then Mini Batch Kmeans method is used for data clustering. More specifically, this work use Kmeans++ to initialize the centers of cluster in order to avoid the algorithm getting into the local optimum, in addition, this work choose the Calsski Harabasz indicator so that the clustering result is more easily determined.

Barolli Leonard et al [4] researches the utilization of IDS utilizing neural network for giving IDS arrangement in a Tor (The Onion Router) organize. Tests did utilized a Tor server and customer with back engendering NN to reproduce exchanges over the Tor organize while catching for examination. The framework proposed is a prepared ANN with information caught from Wire shark, at that point the server and customer information are analyzed, contrasts will recognize an interruption or misuse. The outcomes from testing were fruitful in giving viable exactness when assessed in the test condition.

Chuanlong Yin at. Al. in [11] In this paper, this work explore how to model an intrusion detection system based on deep learning, and this work propose a deep learning approach for intrusion detection using recurrent neural networks (RNN-IDS). Moreover, this work study the performance of the model in binary classification and multiclass classification, and the number of neurons and different learning rate impacts on the performance of the proposed model. this work compare it with those of J48, artificial neural network, random forest, support vector machine, and other machine learning methods proposed by previous researchers on the benchmark data set.

Zhiyuan Tan et. al. [13] place associate degree interconnected systems, like web servers, database servers, and cloud computing servers and so on, are currently under threads from network attackers. Collectively of commonest and aggressive suggests that, denial-of-service (DoS) attacks cause serious impact on these computing systems. A DoS attack detection system that uses multivariate correlation analysis (MCA) technique for accurate network traffic characterization by selecting the geometrical correlations between network traffic choices.

MCA-based DoS attack detection system uses the principle of anomaly based detection in attack recognition. This makes answer capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic. A triangle-area-based technique is planned to enhance and to speed

© 2019 IJSRET

up the process of MCA. The effectiveness of planned detection system is evaluated using KDD Cup 99 data set and the influences of each non-normalized data and normalized data on the performance of the planned detection system are examined. The results show that system outperforms two different previously developed state-of-the-art approaches in context of detection accuracy.

Snort [15] product provides high flexibility that allow to the user to self configure and modify its source code by using source fire. The major drawback of Snort is that it uses only signature based technique to detect the intrusion but if anomaly behavior occur then it will not be possible for SNORT to detect that anomaly attack [5].

This paper [16] provides a technique of secure mobile agent in IDPS for the security of system. Secure mobile agent monitors the system, processes the logs, detects the attacks, and protects the host by automated real time response. Major disadvantage is that if the target of the attackers is mobile agent then it will be difficult to protect the system from being hacked. So it needs to adopt some security infrastructures for the protection of mobile agent.

IV. NETWORK ATTACKS

A more profound comprehension of PC attacks is required to distinguish intrusion and security dangers. An ordinary PC attack can be summed up into a five stage approach.

1. Reconnaissance - The assailant gathers abnormal state data of the framework.
2. Scanning- Using the data gathered in the past advance, the assailant distinguishes potential vulnerabilities in the framework and gathers point by point data about the system, for example, arrange topology, ports utilized and firewall rules.
3. Gaining Access-There are two approaches to access the framework relying on the authenticity of the client. An approved client misuses the provisos in the working framework or different applications running in the framework. An ill-conceived client makes utilization of the system to join the framework. DoS (Denial of Service) are one such case in which the web server is shelled with different demands all the while that it in the long run crashes.
4. Maintaining Access-The invader approaches the framework and tries to extricate data from the framework and hold control.
5. Covering Tracks- with a specific end goal to practice nonstop control over the framework, the invader alters framework logs and other pertinent data to guarantee that there is no hint of contradiction in the security framework.The easy and common criterion for describing all computer network attacks and intrusions in the respective literature is to the attack types [1]. In this chapter, these works categorize all computer attacks into the following classes:

6. Denial of Service (DoS) attacks- Denial of Service (DoS) attacks mainly attempt to "shutdown a whole network, computer system, any process or restrict the services to authorized users" [2]. There are mainly two types of Denial of Service (DoS) networking attacks.
- Operating system attacks.
- Network attacks.

In denial of service attack, operating system attacks targets bugs in specific operating system and then can be fixed with patch by patch, on the other hand networking attacks exploits internal limitation of particular networking protocols and specific infrastructure.

7. SSH- Secure Shell is a protocol that provides authentication, encryption and data integrity to secure network communications. Implementations of Secure Shell offer the following capabilities: a secure command- shell, secure file transfer, and remote access to a variety of TCP/IP applications via a secure tunnel. Secure Shell client and server applications are widely available for most popular operating systems. The secure shell protocol allows users to log in remote terminals in a secure fashion. It does this by performing authentication using a passphrase and a public keying, and subsequently encrypts all information transmitted or received, guaranteeing its confidentiality and integrity.

8. Probing (surveillance, scanning)- Probing (surveillance, scanning) attacks scan the networks to identify valid IP addresses and to collect information about them (e.g. what services they offer, operating system used). Very often, this information provides a tacker with the list of potential vulnerabilities that can later be used to perform an attack against selected machines and services. These attacks use known vulnerabilities such as buffer overflows [8] and weak security points for breaking into the system and gaining privileged access to hosts. Depending upon the source of the attack (outside attack vs. inside attack), the compromises can be further split into the following two categories:

9. R2L (Remote to Local)- Attacks, where an attacker who has the ability to send packets to a machine over a network (but does not have an account on that machine), gains access (either as a user or as the root) to the machine. In most R2L attacks, the attacker breaks into the computer system via the Internet. Typical examples of R2L attacks include guessing passwords (e.g. guest and dictionary attacks) and gaining access to computers by exploiting software vulnerability (e.g. phf attack,

© 2019 IJSRET

which exploits the vulnerability of the phf program that allows remote users to run arbitrary commands on the server).

10. U2R (User to Root)- Attacks, where an attacker who has an account on a computer system is able to misuse/elevate her or his privileges by exploiting a vulnerability in computer mechanisms, a bug in the operating system or in a program that is installed on the system. Unlike R2L attacks, where the hacker breaks into the system from the outside, in U2R compromise, the local user/attacker is already in the system and typically becomes a root or a user with higher privileges. The most common U2R attack is buffer overflow, in which the attacker exploits the programming error and attempts to store more data into a buffer that is located on an execution stack.

V. CONCLUSION

This paper provides an detailed survey of intrusion detection system where for detecting various types of intrusion in the network and host were explained. Comparison of various approaches of researchers for intrusion detection shows there merits and issues in the work. Various techniques are explained for increasing the detection accuracy like neural networks, genetic programming or algorithms are explained. So this work conclude that soft computing is very useful in intrusion detection because this give accurate result with high speed and good efficiency.

REFERENCES

1. Shaohua Teng, Naiqi Wu, Senior, Haibin Zhu, Senior, Luyao Teng, and Wei Zhang. "SVM-DT-Based Adaptive and Collaborative Intrusion Detection". IEEE/CAA JOURNAL OF AUTOMATICA SINICA, VOL. 5, NO. 1, JANUARY 2018.
2. Kai Peng, Victor C.M. Leung, Qingjia Huang. "Clustering Approach Based on Mini Batch Kmeans for Intrusion Detection System over Big Data". IEEE Transaction 2169-3536 © 2017. .
3. Aljurayban, N.S Emam, A. (21-23 March 2015). Framework for Cloud Intrusion Detection System Service. Web Applications and Networking (WSWAN), 2015 2nd World Symposium on, p1-5
4. Barolli Leonard, Elmazi, Donald; Ishitaki, Oda, Tetsuya; Taro; Yi Liu, Uchida, Kazunori. (24-27 March 2015). Application of Neural Networks for Intrusion Detection in Tor Networks. Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on, p67-72.
5. Koushal Kumar, Jaspreet Singh Batth "Network Intrusion Detection with Feature Selection Techniques using Machine-Learning Algorithms" International Journal of Computer Applications (0975 – 8887) Volume 150 – No.12, September 2016
6. R. Karthik, Dr.S.Veni, Dr.B.L.Shivakumar "Improved Extreme Learning Machine (IELM) Classifier For Intrusion Detection System" International Journal of Engineering Trends and Technology (IJETT) – Volume-41 Number-2 - November 2016
7. Premansu sekhara rath, 2manisha mohanty, 3silva acharya, 4monica aich "optimization of ids algorithms using data mining technique" International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-4, Issue-3, Mar.-2016
8. Mohammadreza Ektefa, Sara Memar, Fatimah Sidi, Lilly Suriani Affendey "Intrusion Detection Using Data Mining Techniques", 978-1-4244-5651-2/10/$26.00 ©2010 IEEE
9. YU-XIN MENG," The Practice on Using Machine Learning For Network Anomaly Intrusion Detection" Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong, 978-1-4577-0308-9/11/$26.00 ©2011 IEEE
10. Liu Hui, CAO Yonghui "Research Intrusion Detection Techniques from the Perspective of Machine Learning" 2010 Second International Conference on MultiMedia and Information Technology 978-0-7695-4008-5/10 $26.00 © 2010 IEEE
11. Chuanlong Yin , Yuefei Zhu, Jinlong Fei, And Xinzheng He. "A Deep Learning Approach For Intrusion Detection Using Recurrent Neural Networks" current version November 7, 2017. Digital Object Identifier 10.1109/ACCESS.2017.2762418.
12. Nouf Saleh Aljurayban, Ahmed Emam "Framework for cloud intrusion detection system service". DOI: 10.1109/ WSWAN.2015. 7210298, IEEE, 20 August 2015.
13. Zhiyuan Tan, Aruna Jamdagni, Xiangjian, Priyadarsi Nanda, Ren Ping Liu, "A System for Denial-of-Service Attack Detection Based on Multi- variate Correlation Analysis", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:25 NO:2 YEAR 2014.
14. Mr Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan. "Intrusion Detection System". International Journal of Technical Research and Applications e-ISSN: 2320-8163, Volume 5, Issue 2 (March - April 2017), PP. 38-44.
15. Mario Guimaraes, Meg Murray. Overview of Intrusion Detection and Intrusion Prevention, Information security curriculum development Conference by ACM (2008).
16. Muhammad Awais Shibli, Sead Muftic. Intrusion Detection and Prevention System using Secure Mobile Agents, IEEE International Conference on Security & Cryptography (2008).