A Comprehensive Survey on Intrusion Detection Systems and its Various Approaches

Danish Akhtar[1], Narendra Parmar[2] and Gagan Sharma[3]

[1]Department of Computer Science & Engineering, RKDF University, Gandhinagar, Bhopal, India
[2] Department of Computer Science & Engineering, RKDF University, Gandhinagar, Bhopal, India
[3] Department of Computer Science & Engineering, RKDF University, Gandhinagar, Bhopal, India

[1]danishakhtar.010@gmail.com, [2]narendrarkdf.ac@gmail.com, [3]gagansharma.cs@gmail.com

* Corresponding Author: Gagan Sharma
Manuscript Received: Manuscript Accepted:

Abstract: *With the rapid growth of internet and web based technologies, people's lives have become more and more connected to the cyberspace which in turn increases the risk of intrusions and cyber-attacks on the network systems we are associated with. Network security has now become a very important concern these days because intellectual properties, confidential data and personal data are on stake. Lately a rapid increase in the number of attempts of data theft and hacking has been witnessed which increases the need and demand of intensive research in the field of intrusion detection. The traditional methods of securing the computers or any network are not much capable of securing the network from these daily threats. The objective of this paper is to discuss Intrusion Detection Systems and Various approaches that are being used to address the issues of Intrusion Detection.*

Keywords: ***Intrusion, Data mining, Support Vector Machines, IDS, Clustering***

I. Introduction

Intrusion Detection can be defined as detection of any malicious of suspected activity to safeguard out computer system or any network. The intrusion detection system monitors the system under observance and checks if there is any malicious activity which can hamper the integrity and confidentiality of the system [1]. The Intrusion Detection System (IDS) plays a very important role in maintaining the security and integrity of any system. A robust IDS lays the foundation of a robust and secure system. Whether an activity is malicious or not is defined in the security policy of that system [2]. When any such malicious activity is detected the intrusion system raises alarm for the administrator to look after that activity and take necessary actions. Early and timely detection of any such malicious activity lets the administrator takes proper action to stop such malicious attack [3]. While Intrusion Detection systems are strong enough for detection of intrusion, they are not reliable enough to be trusted on its own. In many cases human intervention also becomes important.

II. Related Work

The term Intrusion Detection was first coined in early 1980's by James P Anderson [4]. By the end of the 1980's the intrusion detection systems were widely accepted and adopted around the world.
Sannasi Ganapathy, et al [5] discussed various intelligent algorithms for classification and feature selection to develop a robust Intrusion Detection System.

A Novel hybrid KPCA SVM with GAs model for intrusion detection has been proposed by Fangjun Kuang, et al [6].

Jasmin Kevric, et al [7] proposed a Classifier model with the help of tree based algorithms for detection of intrusions in networks. Their aim was to classify the incoming traffic if they were normal or malicious

Rana Aamir Raza Ashfaq, et al [8] proposed a unique SSL Algorithm for the improvement of the performance of the classifier using the divide & conquers tactics where they categorized unlabeled samples along with the predicted labels.

Abien Fred M. Agarap [9] Suggested an amendment to the already existing schema of GRU RNN with the help of Support Vector Machines.

Longjie Li, et[10] al Proposed a novel hybrid model for detection of intrusion in network precisely and effectively using the Gini Index.

A framework for perseverance of privacy for signature based intrusion detection was developed by Yu Wang, *et al* [11] which was based on fog devices. The approach they followed was evaluated in different environments.

Soroush M. Sohi, et al [12] used Pattern Machine Algorithm along with Rule Structure Generation to develop an effective and powerful framework for Host Based Intrusion Detection.

III. Types of Intrusion Detection System

The Intrusion Detection Systems are broadly classified into two types which are Network Based Intrusion Detection System and the other one is Host Based Intrusion Detection System.

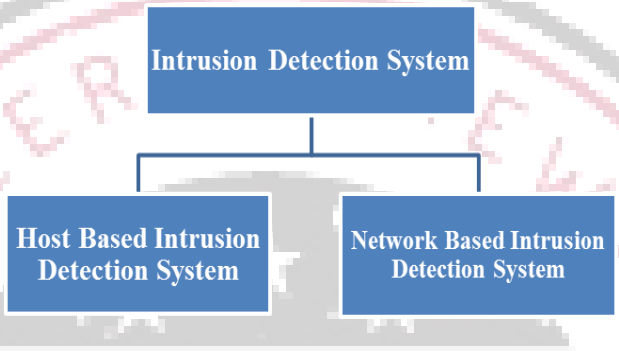

Fig.1. Types of Intrusion Detection System

The most common difference between both the Intrusion Detection Systems is that the Host Based IDS has Host based sensors while the network based IDS has Network based sensors.
References

3.1 Host Based Intrusion Detection System

These IDS's are installed on the host system to be monitored [13]. It checks the various activities of the host system to identify any suspected or malicious attempt of attack. The Host Based IDS is most significant in the case when any unauthorized attempt is made to access a file which is stored on the host system. Such kind of IDS strongly relies on audit trials. The Host Based Intrusion Detection system monitors the activity log of the system to check any malicious or suspected behavior.

3.1.1 Advantages of Host Based IDS:

1. It continuously monitors the system activities for any suspicious access to the files and services of the host system.
2. It can identify intrusion attempts which Network Based IDS fails to do.
3. No specific hardware devices are required.
4. It monitors the system's event logs frequently and thus is capable of identifying the system behavior more accurately.

3.1.2 Disadvantages of Host Based IDS:

1. This cannot be installed in switches and routers.
2. A network with a large number of computers is difficult to manage with Host Based Intrusion Detection System.

3.2 NETWORK BASED INTRUSION DETECTION SYSTEM:

A Network Based Intrusion Detection System is responsible of monitoring the suspicious behaviors by intruders in a network by observing packets in the network traffic [4]. The traffic of the network is observed and a log is maintained which helps in identifying suspicious or malicious packets present in the system.Network node agents are installed in all the host computers of the network.

3.2.1 Advantages of Network Based IDS:

1. The network based Intrusion Detection system captures the details of all the packets moving towards any host system.
2. Easy to deploy
3. The Network based IDS is useful in detecting network based attacks.
4. A single NIDS is capable of monitoring a large number of systems in a network.

3.2.2 Disadvantages of Network based IDS:

1. The Network based IDS is not capable of analyzing encrypted traffic.
2. The network based IDS may miss some packets due to high utilization of bandwidth by other packets on different routes.

IV. Intrusion Detection System Techniques

4.1 Anomaly Based Intrusion Detection:

The Anomaly Based Intrusion Detection detects any abnormal behavior of the system in respect to the already defined behavior or activities of the system [14]. It is also known as Behavior based Intrusion Detection. Any deviation from the normal behavior leads to a suspicion and treated as an anomaly. It thus compares the current state of the system and the predefined behavior to detect or identify any intrusion. The Anomaly Based Intrusion Detection Method is further divided into two types i.e. Static Anomaly Detection and Dynamic Anomaly Detection.

4.2 Signature Based Intrusion Detection:

The Signature Based Intrusion Detection is also known as the Misuse Detection. This is based on the principle of pattern matching to detects intrusions [15]. Such detection is also known as knowledge based detection as the knowledge of known attacks plays a very important role in detecting the new incoming attacks. So whenever a pattern of previously known attack is found, an alarm is raised for the administrator. But sometimes it becomes difficult if the attack is not previously known or there is not pattern match for that attack. Such attacks may also be missed by the detection system. The Signature Based Intrusion Detection is also known as the Misuse Detection. This is based on the principle of pattern matching to detects intrusions [15]. Such detection is also known as knowledge based detection as the knowledge of known attacks plays a very important role in detecting the new incoming attacks. So whenever a pattern of previously known attack is found, an alarm is raised for the administrator. But sometimes it becomes difficult if the attack is not previously known or there is not pattern match for that attack. Such attacks may also be missed by the detection system.

V. Data Mining Approaches to Intrusion Detection

5.1 Association Rule Mining

The Association Rule mining finds association between different item sets in a database. The best example of Association Rule mining is the Market-basket analysis. The intrusions and the following user activities have a lot of relationships in a network. Such behavior of the network and its systems may help to suspect any unusual behavior in the network. Thus we achieve the ability to extract behavioral patterns for precisely detecting intrusions through association and thus can reduce the false alarms rate.

5.2 Classification

Classification is a supervised learning technique. The process of Classification can classify all the packets of a network into two distinct groups. They may be normal packets or they may be malicious packets. For the classification tasks an algorithms should be developed which would act as the classifier. This approach is best suited for the anomaly based intrusion detection.

5.3 Data Clustering

The clustering approach maps the packets or the data into similar groups depending upon their distance among themselves and similarity with each other. This method may be applied to both the signature based intrusion detection and the anomaly based intrusion detection. Clustering method is an unsupervised learning method. Different clusters have different members, not similar to each other's. Several Clustering methods like the Fuzzy C-means, K- Means and Y- Means Clustering are being used for intrusion detection purposes. Clustering techniques are very fruitful in classification of the data of a network for the detection of intrusions or malicious attacks.

5.4 Decision Tree

A decision tree is a mechanism to arrive at a decision using a tree like model containing conditional statements. Decision trees are also extensively used for intrusion detection systems. Decision trees are capable of analyzing the network data and identifying important features that indicate suspicious activities. Decision trees help the analyst to arrive at significant decisions through tree like graph, even for very large data sets. The decision trees are very significant in use for the intrusion detection because they provide a rich set of protocols for the network which are easy to go through and are easy to be integrated with real-time techniques. They have very high intrusion detection accuracy and have good speed of operation, even while dealing with large volumes of data.

5.5 Support Vector Machines

Support Vector Machines have also been used extensively for intrusion detection. They are primarily used for the anomaly based intrusion detection [17]. It performs classification of data with the help of support vectors. The support vector machine is a machine learning algorithm for binary classification of data. The support vector machines can deal with large dimensional data and may be used for the multiclass classification and the binary classification. The SVM is one of the fastest techniques that can be used for the purpose of intrusion detection.

VI. Conclusion

In this paper we have discussed about the Intrusion Detection System and its types. The various approaches and techniques used for the intrusion detection have also been discussed and we found that data mining techniques are widely used in intrusion detection due to their vast capability of improving the scalability, usability and the performance of the intrusion detection system. Various data mining methods like Clustering, Association Rule Mining, Classification, Decision Tree, Support Vector machines and others have proved to be very effective for the task of intrusion detection. These techniques are capable of extracting useful patterns even form a large dimensional data store. The future lies in the study of application based intrusion detection system. A lot of scope is there for the researchers and the analysts.

References

[1] D. Selvamani, V Selvi, A Literature Survey on the Importance of Intrusion Detection System for Wireless Networks, Asian Journal of Computer Science and Technology, Vol.7 No.3, 2018

[2] Kruegel, Christopher, Fredrik Valeur, and Giovanni Vigna. Intrusion detection and correlation: challenges and solutions. Vol. 14. Springer Science & Business Media, 2005

[3] Aleksandar Milenkoski, Marco Vieira, Samuel Kounev, Alberto Avritzer, and Bryan D. Payne. 2015. Evaluating computer intrusion detection systems: A survey of common practices. ACM Comput. Surv. 48, 1, Article 12 (September 2015), 41 pages. DOI: http://dx.doi.org/10.1145/2808691

[4] Deepa A J, Dr. V. Kavitha, A comprehensive survey on Approaches to Intrusion Detection System, International Conference on modeling optimization and computing, Elsevier

[5] Sannasi Ganapathy, et al., "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey," EURASIP Journal on Wireless Communications and Networking, Vol.1, pp.271, 2013.

[6] Kuang, Fangjun, Weihong Xu and Siyang Zhang, "A novel hybrid KPCA and SVM with GA model for intrusion detection," Applied Soft Computing, Vol.18, pp.178-184, 2014.

[7] Kevric, Jasmin, Samed Jukic and Abdulhamit Subasi, "An effective combining classifier approach using tree algorithms for network intrusion detection," Neural Computing and Applications, Vol. 28, No.1, pp.1051-1058, 2017.

[8] Rana Aamir Raza Ashfaq, et al, "Fuzziness based semi-supervised learning approach for intrusion detection system," InformationSciences, Vol. 378, pp. 484-497, 2017.

[9] Abien Fred M. Agarap, "A Neural Network Architecture Combining Gated Recurrent Unit (GRU) and Support Vector Machine (SVM) for Intrusion Detection in Network Traffic Data," Proceedings of the 2018 10th International Conference on Machine Learning and Computing, ACM, 2018.

[10] Li, Longjie, *et al.,* "Towards Effective Network Intrusion Detection: A Hybrid Model Integrating Gini Index and GBDT with PSO," *Journal* of *Sensors*, 2018.

[11] Yu Wang, *et al.,* "A fog-based privacy-preserving approach for distributed signature-based intrusion detection," *Journal of Parallel and Distributed Computing*, Vol. 122, pp. 26-35, 2018.

[12] Soroush M. Sohi, Fatemeh Ganji, and Jean-Pierre Seifert, "Recurrent Neural Networks for Enhancement of Signature-based Network Intrusion Detection Systems," arXivpreprintarXiv: 1807.03212, 2018.

[13] Jayesh Surana, et al, A Survey on Intrusion Detection System, Internation Journal of Engineering Development and Research, Vol 5, issue 2, 2017

[14] W. Lee and S. J. Stolfo. Data mining approaches for intrusion detection. In Proceedings of the 7th USENIX Security Symposium, San Antonio, TX, January 1998.

[15] Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019). https://doi.org/10.1186/s42400-019-0038-7

[16] W. Lee, S.J. Stolfo, K.W. Mok, Algorithms for Mining System Audit Data, in Proc. KDD, 1999

[17] Burge, C.: A Tutorial on Support Vector Machines for Pattern Recognition. Data mining and knowledge discovery journal. 2(2) (1998) 121–167.