ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Exploration of Anomaly Based Intrusion Detection System: A Security Framework

Harsh Arora, Govind Murari Upadhyay

Assistant Professor, Institute of Innovation in Technology & Management, GGSIP University New Delhi, India

ABSTRACT: Now a day's usage of internet and world wide connectivity has been grown, well-proportionate with cyber attacks. With the level of automation in attack tools, attacks are increased continuously, the information requires to infringe the security is minimized and the complication also increases proportionally which make the tasks of security professional very intricate. Maintaining Cyber security is a severe universal fright. Intrusion Detection System (IDS) has turn out to be an indispensable part of system security to identify several attacks with an intension of shielding systems from extensive harms and recognizing risks of the intruded system. Therefore finding intrusions accurately becomes chief functionality of most Intrusion Detection Systems. IDS can be seen or analysed as an anomaly based and signature based IDS. Here in this paper we are throwing light on anomaly based Intrusion Detection System. The considered concepts for anomaly based intrusion detection system are apache storm, neural network, artificial immune system, genetic clustering method and Linear Discriminant Analysis & Logistic Regression. All these concepts are compared based on the detection rate and false positive rate value for anomaly based intrusion detection system.

KEYWORDS: Anomaly based Intrusion detection system, cyber security, wireless network, neural network, genetic algorithm

I. INTRODUCTION

Current world is associated and interconnected with computer networks in a wide range of processes, events and applications. Since these networks are scalable and support emerging large number of users, it is essential to fulfill enhanced capacity and performance [1]. At this perspective, every segment of the operation is supposed to carefully maintain the systems in an outstanding part of security. The network systems are more exposed to large extents of security warnings due to scalability of networks, numerous applications, technology growth, added users and the usage of immense data for economic transactions. But the computers connected to the network must support confidentiality, integrity and guarantee against any attacks. So, networks need various expert security practices.

Intrusion detection is an essential module in network security, for preserving network resources. There is no magic ammunition for security. Even, not a single existing intrusion detection technology is able to protect our resources and information infrastructure. There are always loopholes in a certain part of security deployment. In field of intrusion detection, depend on type of methodology utilized for intrusion detection, Intrusion Detection Systems (IDSs) can be taken in the form of signature based and anomaly based IDS [2]. With the rapid development in the network technologies, the priority of intrusion detection has transferred from easy signature matching processes to identifying attacks based on analysing contextual information. Intrusion Detection System (IDS) is a distinguished component in providing security to information systems and is capable of detecting and preventing attacks by scanning network data. It is made up of many methods which are created and operated to find system intrusions [3].

As the main idea is to focus on some efficient intrusion detection system and highlighted their key features for the IDS. The considered concepts for anomaly based intrusion detection system are apache storm, neural network, artificial immune system, genetic clustering method and Linear Discriminant Analysis & Logistic Regression.

DOI: 10.15680/IJIRCCE.2017. 0503360

The rest of the paper is organized in the following manner: Section II describe the basic concept of Intrusion Detection System and their categorization Section III explains the considered efficient approaches with their comparative review and Section IV concludes the paper with some future references.

II. INTRUSION DETECTION SYSTEM

This section covers the basic concept of Intrusion Detection System and their categorization of Anomaly based and signature based IDS. These concepts are explained as below.

A. Intrusion Detection System

Specifically an intrusion is defined as a set of events which are unknown and unforeseen to the user, which compromises the protection of a computer system. It can be done from external side or internal side of the system.

IDS detect intruders that are accessing the network or those that are already in the network. Hence in other words we can say that it plays the role of burglar alarm that detects any kind of violation in the network and alarm signals are generated in the form of audio or video. Further messages like e-mails can also be generated. On the whole, IDS is primarily exploited for stopping defective activities that may attack or misuse the system by identifying attacks through providing desirable support for defense management and also give constructive information regarding intrusion. But structure of IDS should possess low fake alarms while undertaking the discovery of attacks. IDSs have become shielding mechanisms everywhere in current networks. There is no thorough and proficient methodology offered in checking the strength of these systems [4]. A general framework for IDS is shown by figure 1.

Attacks could be internal or external or both at the same time.So accordingly regular security measures detect activity which is intruding the system in all over network. IDS can be either passive or reactive. Out of this, passive systems are used to detect intrusion activities, to generate logs and account to the administrators. It does not take any action. It is up to the administrators to determine the type of response that should take place to resolve the problem. On other side, reactive systems are more usually recognized as intrusion prevention systems. These systems take step by resetting the network connection or blocking the network intruder with automatic provision or by an operator. The selection of system relies on the requirements of the business.

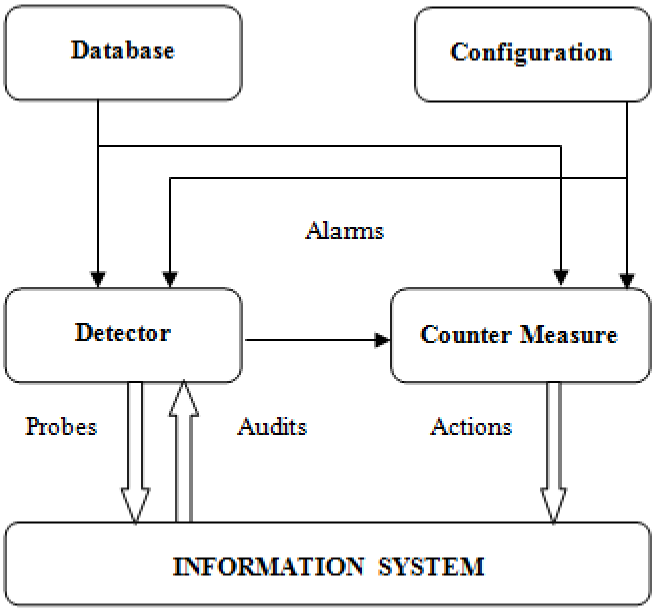

Figure 1: General Framework for Intrusion Detection System

DOI: 10.15680/IJIRCCE.2017. 0503360

B. Types of IDS

There can be various types of categorization of IDS like host based, network based and application based etc. But we mainly focus on application based IDS which are anomaly based and signature based IDS.

(1) Signature Based IDS

Signature based IDS is the one that matches signatures or patterns of the known attacks occurring in the incoming traffic of the network. So every time, the signature is used to detect attacks accurately. The major concern in signature detection system is writing signatures that completely includes possible transformations of the relevant attack. As well as writing signatures that does not match non-intrusive events. The gratification of signature based method is that it holds very good accuracy in discovering notorious attacks [5].

Unfortunately, newly created attacks with changed signatures are not detected by the system and eventually considered as false negatives. Therefore signature based IDS deals with large number of false negatives. So, it is wellknown as knowledge based IDS. It is successful in noticing attacks without producing vast number of false warnings.

(2) Anomaly Based IDS

The anomaly detection or statistical anomaly based Intrusion Detection System makes use of statistical analysis by keeping track of the traffic which is identified to be normal and a potential baseline is evolved. The foremost functionality of anomal detection is the capability of discovering unknown attacks [6]. The network events are regularly observed and matched with the baseline to determine intrusions. Generally, the statistical and behavioral models which are used to detect attacks allow a low false negative rate. Moreover, behavioral patterns of users or programs are developed based on a pattern of normal and abnormal activities, which are used in detecting the existence of an attack. Accordingly, any divergence from normal activity by a user or program would be detected, thereby produces an alarm. Unfortunately, most alarms are favorable and false positives are derived as an outcome. It is also considered as behavior based IDS. The basic principle of anomaly IDS is concerned with intrusive activity, defined to be as a section of abnormal activity. The intrusion may be identified based on anomalous actions.

The anomaly detection can be categorized based either static behavior or dynamic behavior. The static anomaly detector presumes as an element of the supervised method acts as a stable or static mechanism. The dynamic anomaly detector, with the name entails its active actions. Therefore the functioning of the system is given as a series of varied events.

III. METHODS OF ANOMALY BASED IDS

This section covers the anomaly based considered concepts of IDS. Also a comparative detail for the all these methods is shown in table I.

Al-Janabi and Saeed [7] has used the back propagation neural network method for anomaly based intrusion detection system that can promptly detect and classify various attacks. Authors have used KDD’99 dataset for experimentation. Authors have classified the concept into four stages of monitoring module, detection module, classification module and alert module. In context of ANN method training and testing have been done using back propagation ANN method for classifying various actions. The Detection Rate (DR) and False Positive rate (FP) have been calculated for different scenarios. However, the other aspect is that it takes very large amount of data and much time to ensure the accurate results. Another issue is that there is some kind of compromise between increasing the classification levels and the percentage of detection. Thus, a trade off is required. Furthermore, the obtained results of training with 41 features have been better than those with training with 22 features.

Mylavarapu et al. [8] has used the Apache Storm based hybrid approach for anomaly based intrusion detection system. The proposed concept is implemented on the real time application of big data. Apache Storm serves as a distributed, fault tolerant, real time big data stream processor. The hybrid detection system consists of two neural networks. The CC4 instantaneous neural network acts as an anomaly-based detection for unknown attacks and the Multi Layer Perceptron neural network acts as a misuse-based detection for known attacks. Based on the outputs from these two neural networks, the incoming data will be classified as ”attack” or ”normal.” Authors found the average accuracy of hybrid detection system is 89% with a 4.32% false positive rate. Authors show the commitment for the appropriate results and real time detection to handle big data.

Subba et al. [9] has used Linear Discriminant Analysis and Logistic Regression model for anomaly based intrusion detection system. The performance of these IDS models on the benchmark NSL-KDD data set and analyzes their performance against other IDS models based on Naive Bayes, C4.5 and Support Vector Machine (SVM). Author has considered the performance parameters of Accuracy and detection rate for evaluation. LDA and LR based intrusion detection models perform well on both the binary class and multiclass classification problem. Their performance are at par with the SVM and C4.5 based intrusion detection models, while they outperform the Naive Bayes based model. Due to lower computation overhead of proposed algorithm, it can be efficiently used for the deployment of real time network system.

Narsingyani and Kale [10] has used Genetic Algorithm for anomaly based intrusion detection system. The proposed concept is implemented to reduce the value of false positive rate. Reduction in False positive rate, increases the accuracy and performance of the system. The proposed genetic algorithm is implemented on KDD99cup dataset. Authors have classified the proposed concept into two modules of training phase in which rules are generated and Intrusion detection phase where real time intrusions are detected by using the genetic algorithm. The rules generated in the first phase are used for 2nd stage of intrusion detection. The further experimentation is done with population and fitness value of genetic algorithm. Overall authors have successfully implemented the intrusion detection system with lower false positive rate value.

Abas et al. [11] has used Artificial Immune System for anomaly based IDS. Authors has used GureKddcup database set for intrusion detection and accuracy by using r-chunk algorithm of immune system and enhance the performance of the system by reducing the complexity of the intrusion detection system. The anomaly detection setup based on AIS negative selection algorithm and a better detection algorithm R-chunks bit matching. Using feature selection of rough set theory to reduce the complexity of training data set, this is effecting on the computing time and the longer time responding. Overall authors have achieve the performance in terms of accuracy of the system and less time consumption in detection system.

Aissa and Guerroumi [12] has used genetic clustering algorithm for anomaly based IDS. The complete system is structured into k clusters, where certroid of clusters are represented by the chromosomes of genetic algorithm. The proposed concept is experimented on KDD99 dataset and overall results are compared with individual k-means clustering. The proposed concept shows high detection rate upto 98% accuracy and low false positive rates upto 0.12%. whereas k-means clustering shows detection rate maximum upto 81% and false positive rate 0.26%. So, we can say that genetic clustering algorithm is better as compare to k-means clustering.

Table I
Methods for Anomaly Based Intrusion Detection System

Anomaly Based IDS	Authors & Year	Key Features
Back Propagation Neural Network	Al-Janabi and Saeed (2011) [7]	1. Authors have classified the concept into four stages of monitoring module, detection module, classification module and alert module. The training and testing. 2. The training of the ANN requires a very large amount of data and considerable time to ensure that the results are accurate. Another issue is that there is some kind of compromise between increasing the classification levels and the percentage of detection.
Apache Storm	Mylavarapu et al. (2015) [8]	1. Apache Storm serves as a distributed, fault tolerant, real time big data stream processor. 2. The CC4 instantaneous neural network acts as an anomaly-based detection for unknown attacks and the Multi Layer Perceptron neural network acts as a misuse-based detection for known attacks. 3. Authors found the average accuracy of hybrid detection system is 89% with a 4.32% false positive rate.

Linear Discriminant Analysis and Logistic Regression Model	Subba et al. (2015) [9]	1. The performance of these IDS models on the benchmark NSL-KDD data set and analyzes their performance against other IDS models based on Naive Bayes, C4.5 and Support Vector Machine (SVM). 2. Their performance is at par with the SVM and C4.5 based intrusion detection models, while they outperform the Naive Bayes based model. 3. Due to lower computation overhead of proposed algorithm, it can be efficiently used for the deployment of real time network system.
Genetic Algorithm	Narsingyani and Kale (2015) [10]	1. The proposed genetic algorithm is implemented on KDD99cup dataset. 2. Overall authors have successfully implemented the intrusion detection system with lower false positive rate value.
Artificial Immune System	Abas et al. (2015) [11]	1. Authors has used GureKddcup database set for intrusion detection and accuracy by using r-chunk algorithm of immune system and enhance the performance of the system. 2. Using feature selection of rough set theory to reduce the complexity of training data set, this is effecting on the computing time and the longer time responding.
Genetic Clustering Algorithm	Aissa and Guerroumi (2015) [12]	1. The complete system is structured into k clusters, where certroid of clusters are represented by the chromosomes of genetic algorithm. 2. Genetic Clustering algorithm shows batter results as compare to k-means clustering.

IV. CONCLUSIONS

In this research work, it is brought out, today's security need or requirement is at very high demand to protect the organization information infrastructure resources and data from attackers. On other hand, with little expertise with computer, internet knowledge one can have information security network. But still there are some existing concepts for intrusion detection system. We have compared the existing anomaly based IDS by considering the parameters of false positive rate and detection rate. The considered concepts for anomaly based intrusion detection system are genetic algorithm, apache storm, neural network, artificial immune system, genetic clustering method and Linear Discriminant Analysis & Logistic Regression. Each concepts shows efficient results in their own aspect of dataset and consider circumstances as compare to some other algorithm. But Genetic clustering algorithm shows more efficient for anomaly based IDS. A comparative structure is show in table 1.

V. FUTURE SCOPE

From the existing concepts, we can say that results are efficient for IDS. But for future reference, we recommend to use nature inspired swarm intelligence based technique for anomaly based IDS. Swarm intelligence techniques are self optimized methods having strategy to solve the problem with efficient research solution.

REFERENCES

[1]. Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2007.

[2]. Debar, Hervé, Marc Dacier, and Andreas Wespi. "Towards a taxonomy of intrusion-detection systems." *Computer Networks* 31, no. 8 (1999): 805-822.

[3]. Garcia-Teodoro, Pedro, J. Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. "Anomaly-based network intrusion detection: Techniques, systems and challenges." *computers & security* 28, no. 1 (2009): 18-28.

[4]. Lunt, Teresa F. "A survey of intrusion detection techniques." *Computers & Security* 12, no. 4 (1993): 405-418.

[5]. Kruegel, Christopher, and Thomas Toth. "Using decision trees to improve signature-based intrusion detection." In *Recent Advances in Intrusion Detection*, pp. 173-191. Springer Berlin Heidelberg, 2003.

[6]. Jyothsna, V., VV Rama Prasad, and K. Munivara Prasad. "A review of anomaly based intrusion detection systems." *International Journal of Computer Applications* 28, no. 7 (2011): 26-35.

[7]. Al-Janabi, Sufyan T. Faraj, and Hadeel Amjed Saeed. "A neural network based anomaly intrusion detection system." In *Developments in E-systems Engineering (DeSE), 2011*, pp. 221-226. IEEE, 2011.

[8]. Mylavarapu, Goutam, Johnson Thomas, and Ashwin Kumar TK. "Real-Time Hybrid Intrusion Detection System Using Apache Storm." In *High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on*, pp. 1436-1441. IEEE, 2015.

[9]. Subba, Basant, Santosh Biswas, and Sushanta Karmakar. "Intrusion Detection Systems using Linear Discriminant Analysis and Logistic Regression." In *2015 Annual IEEE India Conference (INDICON)*, pp. 1-6. IEEE, 2015.

[10]. Aissa, Naila Belhadj, and Mohamed Guerroumi. "A genetic clustering technique for Anomaly-based Intrusion Detection Systems." In *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2015 16th IEEE/ACIS International Conference on*, pp. 1-6. IEEE, 2015.

[11]. Abas, Eman Abd El Raoof, Hatem Abdelkader, and Arabi Keshk. "Artificial immune system based intrusion detection." In *2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)*, pp. 542-546. IEEE, 2015.

[12]. Narsingyani, Dipika, and Ompriya Kale. "Optimizing false positive in anomaly based intrusion detection using Genetic algorithm." In *MOOCs, Innovation and Technology in Education (MITE), 2015 IEEE 3rd International Conference on*, pp. 72-77. IEEE, 2015.