INTRUSION DETECTION ON BIG DATA USING MACHINE LEARNING: A REVIEW

[1]Mukesh Choudhary & [2]Dr. Manish Shrimali
[1]Research Scholar [2] Professor
DCS & IT JRNRV
Udaipur, Rajasthan, INDIA

Received: May 07, 2019 Accepted: June 11, 2019

ABSTRACT: *The main objective of intrusion detection systems (IDS) is to discover the dynamic and the malicious form of network traffic that simply changes according to the characteristics of the network. The IDS methodology represents a prominent developing area in the field of computer network technology and its security. Different form of IDS has been developed working on distinctive approaches. One such kind of approach where it is used is the machine learning mechanism. In the proposed methodology an experiment is applied on the data-set named as KDD-99 including its subclasses such as denial of service (DOS), other types of attacks and the class without any form of attack. Depending upon the machine learning algorithms various distinct forms of IDS have been developed which further checks the optimization based potential features in connection with the neural network classifier for the various forms of IDS based attacks.*

Key Words: *Intrusion detection systems, denial of service, convolution neural network*

1. INTRODUCTION

In the present scenario the use of internet is growing at a large pace with is highly developed and emerging forms of ever growing network and its connectivity but the use of internet poses a great threat to cyber security. In order to maintain the high level of security there is an important need to overcome the cyber threats posing problems to various organizations, companies, and the firms. One of the major challenges among the cyber-security is to maintain the integrity of the intrusion detection system (IDS) thereby protecting it from major forms of attacks and to conquer the various form of risks of the intruded system [3]. The main function of the IDS is to identify a more precise form of intrusion. The illegal hackers of the security have found a large number of ways to break the security of the system whether it is a cloud network or the wireless-based network. Many researches have been performed by the technologists to curb the security threats from distinct forms of intrusions done to the cloud computing systems and the wireless system. So, the main objective of IDS is to protect the information whether it is governmental, public or private entity [7]. The use of IDS is mainly required in detecting the false and the poor detection rates. Whenever an attack is observed by the system or a harmful activity is done to the system, it automatically generates an alarm resulting in a false-positive alarm [3, 5]. The research mainly focusses upon the enhanced capabilities of the intrusion detecting system and thereby reduces the occurrence of the false type alarms. The basic operation of an intruder to search the faulty operative conditions in the network or the systems. So, an intruder helps to find out the best optimized solutions to identify the intrusions in the data. The main requirement of the IDS is not only to encounter the intruders in the data path but also to supervise the intruders of the data. The most important security aspects of an intrusion detection system consist of maintaining the following conditions.

- *Confidentiality:* Only an authorized user can detect the system.
- *Availability:* Here, the computer technology provides various forms of resources and the access to the legal users of the system without disturbing the working operation of the system.
- *Integrity:* The information must be protected from any kind of malicious act.

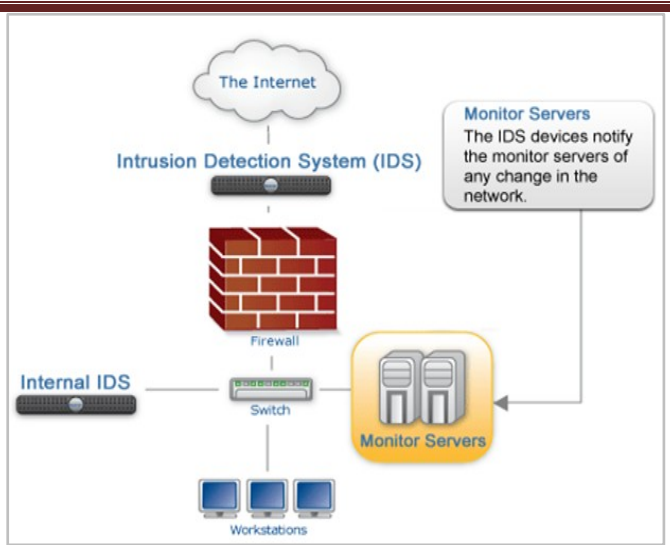

Figure 1: Intrusion detection system

1.1 IDS: Classification and Types

There are numerous classes of IDS based on structure or detection. The IDS are classified based on characteristics as represented below in figure 2.

1.1.1. Based on Structure

1.Network Based Intrusion Detection System [NIDS]: It represents a passive network analyzing the traffic related to the network and for finding out the evidence of various forms of attacks When a NIDS detects an attack, it provides an instant report to the administrator. It basically checks the types of attack that are incoming and outgoing networks and is usually placed inside the router. But the NIDS is unable to find out the encrypted source of information and is not able to distinguish some forms of attacks. There is no effect of system-failure over the NIDS. Being autonomous in nature these systems are simple to run and easy to install [5]. The first step is to install the NIDS then to perform some of the configurations (counter-active) and in the end plugging the required network and authorizing it to response the traffic network-based communication. The main function after the installation process is to identify and match the signatures present in the data-base with the attacking form of signatures.

2. Host Based Intrusion Detection System [HIDS]: This type of detection that is placed in the computer server represents the host of the system usually called as HIDS.

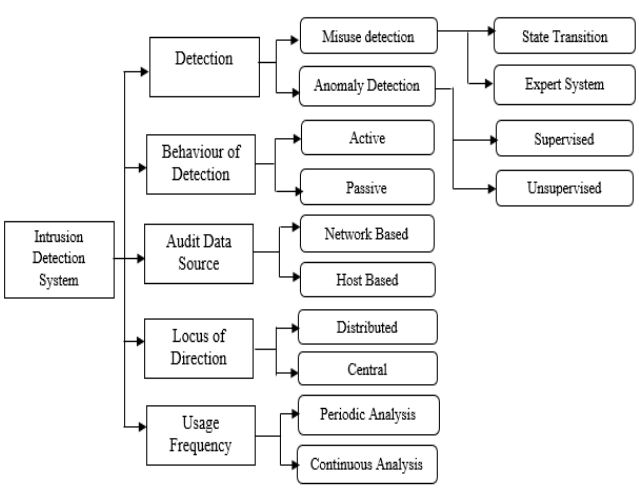

Figure 2: IDS Classification based on its characteristics

As the name suggests a mechanism that helps in analyzing the stored and the system files and further tells about the changes or the deletions done by the attacker in the system files. The HIDS simply detects the part i.e. not detected by the NIDS mechanism.

3. Application based IDS: The application-based IDS is another development of HIDS which monitors the different types of events such as the inspection of the files, checking the abnormal functions like exceeded permission, void-file execution, etc. It helps in analyzing the communication between the user and the application and monitors the traffic of the network i.e. encrypted [9].

1.1.2 Based on Detection Method

1. Misuse detection: It is also called as the signature-based IDS designed to compare the signatures or the patterns that are made over the incoming path of the traffic network. These signatures help in detecting the attacks in a very accurate manner. The main objective of misuse detection is that it helps in finding the eminent forms of attack. But one major drawback of the system is that it cannot detect the new forms of attack with the changed form of signatures resulting in negative false alarms due to which it deals with a vast number of negative false alarms.

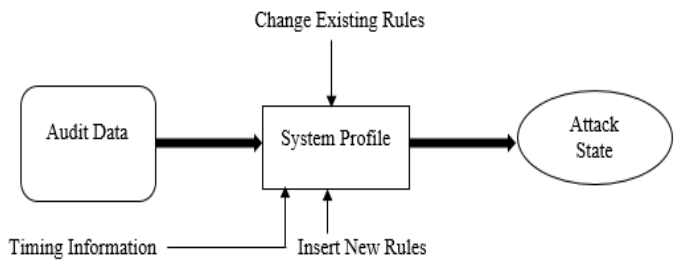

Figure 3: Typical Misuse Detection

2. Anomaly IDS: This term anomaly IDS is also known as statistical IDS i.e. it monitors the network traffic identified as a normal method deriving a potential base-line [8]. For determining the intrusion activities of the system, each network is observed at regular intervals and further matched with the base-line of the system. The process basically requires statistical as well as the behavioral models that are used for detecting the attacks that allows the false-negative rate whereas the presence of an attack is determined by the patterns of the programs or the users depending upon the normal or the abnormal activities of the system.

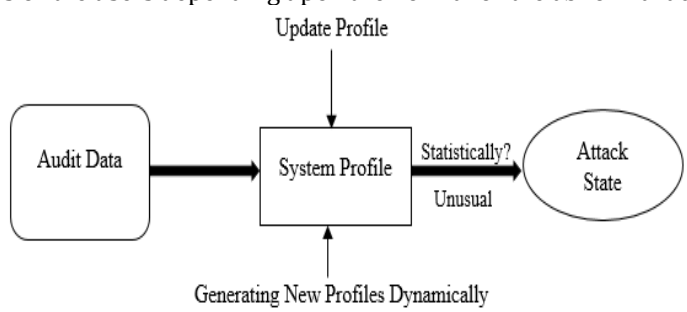

Figure 4: Typical anomaly detection

There are generally two types of detectors. One is the static anomaly detector and the other is the dynamic anomaly detector [8].

(a) Static Anomaly Detector: It helps in the prediction of an element based on the supervised method. The system makes use of the static-segment where the system is registered with string of binary bit nature or it may be a set of strings.

(**b) Dynamic Anomaly Detector**:The name itself represents an active form of operation. Here, the records that are present in an operating system are generally use to examine the events if the IDS. The activity gets monitored only when the audit-records are formed by the operating system. These represents the activity following a stringent methodology.

1.1.3 Based on attack

The attack-based IDS are categorized as follows [4][13][14]

1. Normal Category*:* This category does not have any form of data attack. It consists of a state where the system has no alteration and no such kind of abnormality occurs in the state of the system.

2. DOS-Attack: This is generally called as the denial of service (DOS) attack. Here, in this form of attack, the hacker or the attacker of the system perform various form of illegal activities such as illicit calculations,

makes the data memory typically jammed by sending the malignant data sources or the data packets in such that it is not able to maintain the authentic activity of the system. The attacker performs a Botnet attack and takes the advantage of the distance. The process of DoS consists of various types of attacks [9]

- **Operating DoS Attack**: The operating form of attack deals with bugs created by the system and fixes them with the help of patches. This form of attack is also known as "Teardrop" where the attacker of the system takes the advantage of TCP/IP fragmentation creating risk to codes of re-assembly.
- **Networking Attacks***:*This type of attacks puts certain restrictions on the protocols of the network. One such example of example of this kind of networking is "SYN flood" attack. Here, the attacker creates an IP spoofing with excessive links that are half-open. Further, the attacker implements the operation by sending the data to the victim in the form of SYN-packets with IP addresses that are spoofed. At the end, the victim checks the data sent and generates the SYN/ACK response to the spoofed (fooled) IP address. The attacker in response blocks the computer of the victim.

3. Probe Attack: This type of attack consists of collecting the information, analyzes the network operation in order to extract the valid form of IP address to pin-point the distinct services used for the network for performing a smart and wise attack on these services [14]. Various forms of probe-attack include the following:

- IPsweep: Identifies the service on a particular (specific) port.
- Portsweep: Detects and monitors the port services that are hosted by the single host).
- Nmap: It represents a form of tool for network mapping

4. Remote to Local (R2L) Attack: Attack is done when the user gets the access of system or it finds a root/link through the system (remote) to perform an attack. Sometimes in case of R2L attacks, the most common pathway to enter into a system is the internet. The R2L attacks commonly includes getting access through phf attack software that grants the users or the attackers to perform the inconsistent command operations on the server of the system and the other R2L attacks involves the password-guessing mechanism i.e. the guest and dictionary attacks.

5. User to Root (U2R) Attack: The process of user to root attack defines the activity where an attacker opens a fake account, make the system weak or creates the bugs into the system by squandering the authorization processes. The most commonly used U2R attack is the flow of the buffer where an attacker takes the advantage of the fault occurring in the program and congregate the additional information into a buffer i.e. kept on an execution stack. Thus, the main use of buffer is to carry the actual or necessary amount of data and the rest of the data overflows in the neighboring buffers resulting in loss of some amount of data.

Table.1: Detail of attacks and their patterns

Types of Attack	**Attack-Pattern**
Denial of Service (DoS)	Back, Land, Neptune, Pod, Smurf, Teardrop
Probe	Portsweep, Nmap, Ipsweep, Satan
Root to Local (R2L)	Guess Password, Imap, Ftp_Write, Spy, Multihop, Phf, Warezmaster, Warezclient,
User to Remote	Perl, Rootkit, Loadmodule, Buffer Overflow

2. INTRUSION DETECTION SYSTEM ACHITECTURE

The architecture of IDS comprises of its unique core element i.e. sensor popularly known as the analyzing engine to pin-point the intrusions occurring in the system. The sensor consists of a mechanism that helps in detecting the intrusions. In the following figure 1.2 the sensor gets the data (raw) from the given sources as shown which consists of the audit trails, knowledge-based data and, syslog. The 'syslog' includes the authority to the particular system or the system file configuration [1]. The sensor consists of a component known as event generator which performs the data collection shown in figure.3. It detects the way of collecting the data. The event generator consists of network, operating system and the network applications where it generates a set of events including audit (log) of the system or the packets of the network.

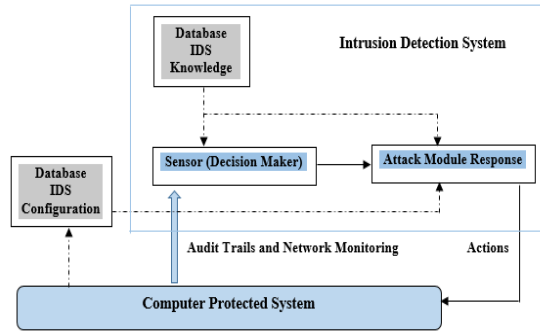

Figure 2.1: Sample IDS (arrow width ∞ information between system components)

This form of set events also involves the policy of information collection i.e. in or out of the system. Sometimes it is not necessary to store the data as it reaches simply to the analyser. So, basically the key role of the sensor is to extract or filter the data and remove the unwanted form of the data that is achieved from the event data set system [6]. Additionally, the database holds the configurational parameters of IDS that includes its mode of communication methods based on the response module. The sensor itself contains its own data observing all the historical multiplex forms of intrusions. Practically, the IDS may follow a structure based on an 'agent' principle where small modules (autonomous) are designed on 'per-host' basis approach. The agent mainly monitors and filters the activities scheduled within the area i.e. fully protected and further starting its initial analysis by undertaking a response action [12]

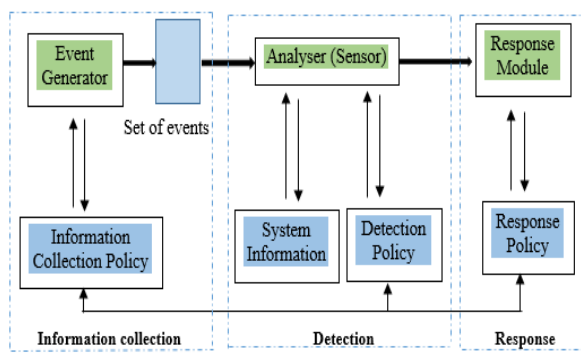

Figure 2.2: IDS components

When a suspicious act or event is detected, an agent issues an alarm. These can be shifted or cloned on another system. The system further may include the transceivers monitoring all the operations effected by agents of another host i.e. specific. The results fetched by the transceivers are provided to a single unique monitor where the monitor can coordinate the distributed form of information. In addition, some filters are used for aggregation and the selection purpose [10, 12]. The Interfacing of the IDS results in linking or providing the interactions between its components. These can be protected for an extended time period but the monitoring process requires synchronization of these components.

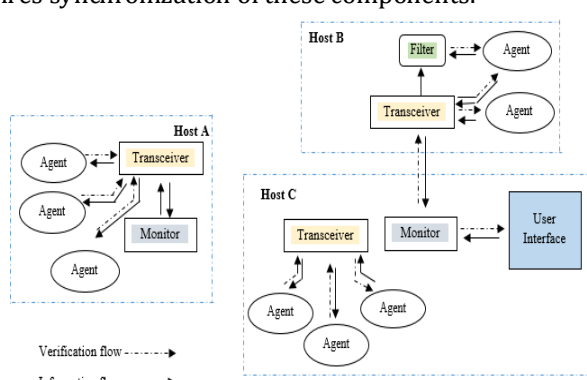

Figure 2.3: IDS Interface

3. RELATED WORK

Dias GV et.al [1] conducted a study indicated an intrusion detection system based on SVM methodology that combines an algorithm (hierarchical clustering), feature selection method and the technique of SVM. The algorithm i.e. used helps in providing the support vector machine with maintaining an abstracted form of high level of trained examples obtained from the trained set-up of KDD Cup 1999. The study indicates high level performance of SVM based technology which further resulted in a reduced form of training-time. The method of feature-based selection was adopted to remove the un-necessary features of the training set in order to maintain the levels of accuracy. The dataset of KDD cup-1999 was used to analyze the proposed system. When the system was compared with the other forms of data set, the experimental analysis showed that the result based on the performance analysis was not so good as compared to KDD Cup-1999 dataset. So, the methodology based on this dataset showed better analysis in detection of probe and DoS based attacks, maintaining accuracy globally. Cannady et.al [2] proposed a study on the process of misuse detection which is defined as a process to recognize the instances of different types of attacks by measuring the unexpected activity and the activity that is going currently. Mostly, the present processes based on misuse detection uses a technology of rule-based systems with the aim to identify the provoked nature of the attacks known to us. But the above process was less reliable to guess the forms of distinct attacks done on the system. The use of ANN technology gave a potential to search and identify the activities of the network that rely on the incomplete, non-linear, and limited amount of sources. Kemmerer et.al [3] presented a study by framing a simple question of why there is a need of intrusion detection system. Suppose, the owner of a house is out of town and he has locked his home with all the windows and doors closed. But, there is someone outside his home who wants to enter. Firstly, he rings the bell and checks the main door if it is locked or not then after sometime he checks the windows of the house that too are locked which makes sure that the house is safe. So, the question is why an alarming bell is installed. This question particularly sticks to the IDS. Why there is a need to plant the detection systems if the security is tight and secure. The reason to install these detective systems is that the intrusions still exist because sometimes the people may forget to lock their doors or windows, the same case occurs with the computer based networks which do not provide us 100% security of the system to work accurately. So, based on this study the researchers has tried to explain the techniques based on IDS to deal with these kind of intrusions present in the network. Steven T et.al [4] proposed a study on an application of STATL that represents a descriptive language based on a transition-based attacking system that is constructed to support the IDS. This form of descriptive language describes a process of penetration done to the computer network implemented by a hacker. These type of penetrations includes attacking activities performed by the hacker. The STATL description is used by the IDS to extract the stream events and the ongoing intrusions occurring in the system. As the IDS works under distinct environments such as Windows NT, Linux etc. and the domains like the host or the network. So, this extensible form of language helps in dealing with different targets as required. This language basically describes both the host and the network attacks. Here, in this paper an IDS based tool-set i.e. based on the descriptive language has been executed. This tool-set depicts various favorable and the desires results. There is a deep study of syntax based on the STATL language. Common real examples of both the network and the host are also described in the paper. Pi-Cheng et.al [5] conducted a research based on two of its issues related to the IDS designs. The two issues include the selection based on optimization of rule-based selection and the discovery in case of attack. This type of approach provides a connection between the junked packets. An algorithm is implemented for the attack identification and the rule based selection. The study is performed on the threats and describes the relationship for an application based web-server and the gateway. The algorithm is implemented over a signature-based IDS for having the better form of results. Carl, Glenn, et.al [6] suggested a study based on detection using Denial-of-service (DoS) techniques that includes change-point detection, activity profiling, and a signal analysis (wavelet-based) that further faced a major challenge to analyze the attacks on network that generated from the sudden unexpected activities or flash-events. This survey of techniques and testing results provided a mechanism to identify DoS based flooding attacks. As the detectors used in the process are quite good but none of them has shown the complete accurate detection. The adjoining of various methodologies with smart and intelligent network handlers would definitely produce excellent results. Kim, Jungwon, et.al [7] conducted a research on the use of artificial immune systems in IDS which is an interesting concept thatrelied on two main reasons. Firstly, the immune system of a human provides the best protection. Secondly, the present techniques used for maintaining the computer security are less reliable and complex in nature. Here, the researchers have used various distinct algorithms for the development of the systems and the best possible outcomes. The analysis has been done based on the important developments within this area of research, in addition to forming suggestions for future research options.P. Garcı´a-Teodoro, et.al [8] conducted a study on IDS i.e. an anomaly based network technique which

consists of protecting the system target against all the harmful activities. This paper starts with study and a method to review the anomaly based IDS. Further, the development of the system based on detection methods and various research projects are explained. The paper states the major challenges of anomaly based intrusion detection system, dealing with special issues based on its applications. Wolfgang Banzhaf, et.al [9] researched on Intrusion detection based that relies on the computational-based intelligence In order to build a good model of IDS, it should include the important features of computational intelligence (CI) systems that consists of high computational speed, fault tolerance, adaptation, and error
resilience properties. Here, the study has provided an overview to the problem of intrusion detection based on CI systems. The scope has encompassed CI core-method, including evolutionary computation, artificial immune systems, ANN evolutionary computation, fuzzy systems, soft computing, and swarm-based intelligence. The research has summarized that allowed us to clarify the research challenges that are existed already, and highlights the methods by promising new research solutions. The findings survey has provided useful methods to conduct the research in the current IDS technology. Muhammad HilmiKamarudin, et.al [10] proposed their study on technology of network security that has become a supreme method for the protection of information or the data. With the excessive growth of internet technology, various forms of attack cases are observed in a day to day life. So, to tackle such kind of attacks, a methodology of IDS is adopted and the process of Machine Learning is the most used technology in the IDS. The study based on recent years has shown that the Machine Learning Intrusion Detection system provides a good detection rate and a high accuracy. Thus this paper includes performance analysis based on Machine Learning algorithm known as Decision Tree (J48) where a comparison has been done with two of the other machine learning algorithms named as the NN and the SVM's. These algorithms were tested on the strategy of false alarming rate, rate of detection, and accuracy of four classes of attacks. From the experimental analysis it was detected that the J48 (Decision-tree) algorithm performed well as compared to the other two machine learning algorithms.

Table.1 Existing Scheduling Model

Author's Name	Year	Methodology Used	Proposed Work
Cannady*et.al.*	1998	ANN technology	Proposed a study on the process of misuse detection which is defined as a process to recognize the instances of different types of attacks by measuring the unexpected activity and the activity that is going currently.
Steven T*et.al.*	2002	STATL description Environment: Windows NT, Linux	Proposed a study on an application of STATL that represents a descriptive language based on a transition-based attacking system that is constructed to support the IDS.
P. Garcı´a-Teodoro,*et.al.*	2009	Anomaly based network technique	Conducted a study on IDS i.e. an anomaly based network technique which consists of protecting the system target against all the harmful activities
Shikha, *et.al.*	2015	Anomaly based network technique with hybrid approaches	Worked on the need of the present world dealing with vast amounts of data i.e. transferred and stored from location or another.
Elshoush,*et.al.*	2011	CIDS i.e. collaborative, intelligent intrusion detection system	Focused on proper prevention of attacks that were linked to the computer-based systems.

Elshoush, et.al [11] focused on proper prevention of attacks that were linked to the computer-based systems. As the motive of complete prevention of attacks is not possible so the process of using the IDS plays a crucial role to overcome the harm that is done to the operating systems. Two most important forms of methods based on intrusion detection were used, the first one was misuse-based detection and the second was the anomaly-based detection. A CIDS i.e. collaborative, intelligent intrusion detection system was proposed to examine both the methods, as the individually obtained results from both the methods resulted in less form of accuracy. Specifically there are two major challenges in CIDSs research strategy. Both of them were reviewed and highlighted. The two challenges were the architecture of CIDSs and alert-correlation

algorithms. The different forms of CIDSs architectures has been explained and compared accordingly. Using the CIDSs with other forms of security systems (multiple) explained some of the major issues in case of alert-correlation algorithm. So, various forms of techniques for alert correlation has been discussed. The main focus was based on the property of correlation of CIIDS alerts. So, the main focus was on the computational analysis, intelligence-based approaches, along with the applications on IDSs. In the end the paper suggested a fuzzy- based logic, and other techniques of AI required to reduce the negative false alarm rates while keeping the rate of detection high. Further it concluded, the occasion for the integrated-solution to large-scale CIIDS. Muamer N., et.al [12] conducted a study on using smart and intelligent form of data-mining methods to observe the incursion occurring in the local-networks. This paper suggested a better-quality strategy for IDS that combines the expert systems, the processes of data mining as employed in WEKA. The classification generally entails detection-based principle along with some of the phases of WEKA such as the processes of open-source data-mining. The joined methodology gives better performance of IDS based systems, and helps to maintain the process of detection more effectively. The experimental result was based on evaluating a novel strategy created a better form of detection based on efficiency. So, the study presented a good approach to analyse the experiments on behalf of intrusion detection. Nadiammai, et.al [13] focused upon the security issue of the networks and various developments in applications running on distinct platforms capturing an attention towards security of the network. This type of paradigm exploited the vulnerabilities of security that on technical basis was expensive and difficult to resolve. Hence intrusion can be used as a significant factor to compromise the confidentiality, availability, and integrity of a computer-based resources. IDS performs an essential part in discovering attacks and anomalies inside the network. In this ongoing working method, data exploration notion was usually combined with an IDS to recognize the kind of, hidden and relevant interested data for an individual efficiently and with a smaller amount execution time. Four type of problems such as for example Classification of Data, Conversation based on High Level Human, Insufficient Tagged (labelled) Data, and Efficiency of Distributed DoS (Denial of Service Attack) attack was being resolved using the suggested algorithms just like Hybrid IDS model, Semi-Supervised Method, EDADT algorithm, and HOPERAA Varied Algorithm. Our recommended algorithm continues to be tested applying dataset (KDD Cup). All of the proposed protocol (algorithms) showed improved accuracy and reduced rate of fake alarm in comparison to existing algorithms. Shikha, et.al [14] worked on the need of the present world dealing with vast amounts of data i.e. transferred and stored from location or another. When the data gets transferred or is stored somewhere then it gets exposed to many forms of attack. However, many types of techniques and the detection mechanism has been established to overcome the issues of data risk. Thus to examine the data and to identify the type of attack done on the various techniques of data mining have emerged to make it free from any kind of loss related activity. The process of anomaly detection uses mining techniques of data to recognize the hidden behaviour inside the whole set of data which might increase the chance of being attacked in an easy way. The use of hybrid-based approaches have also been made to judge the form of attacks whether known or unknown in nature. This research has reviewed the techniques of data-mining for anomaly-based detection in order to provide better understanding among the existing techniques that may help the interested researchers to work in future.

4. CONCLUSION

Intrusion can be characterized in terms of confidentiality, integrity, and availability. An event or action causes a breach of confidentiality if itallows to access resources, residing in a computer in an unauthorized manner. An event or action causes a 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 a 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 analyzing them for signs of intrusions. An intrusion detection system is a software or hardware that automates the process of monitoring and analyzing of events. The present scenario experiences various forms of developments and huge growth in advanced processing technologies consisting of connectivity among different networks but the methodology is vulnerable by the activities of the intruders or the attackers of the system.

5. REFERENCES

1. Snapp, Steven R., James Brentano, Gihan V. Dias, Terrance L. Goan, L. Todd Heberlein, Che-Lin Ho, Karl N. Levitt et al. "DIDS (distributed intrusion detection system)-motivation, architecture, and an early prototype." In Proceedings of the 14th national computer security conference, vol. 1, pp. 167-176. 1991.
2. Cannady, James. "Artificial neural networks for misuse detection." In National information systems security conference, vol. 26. 1998.

3. Kemmerer, Richard A., and Giovanni Vigna. "Intrusion detection: a brief history and overview." Computer 35, no. 4 (2002): supl27-supl30.
4. Eckmann, Steven T., Giovanni Vigna, and Richard A. Kemmerer. "STATL: An attack language for state-based intrusion detection." Journal of computer security 10, no. 1-2 (2002): 71-103.
5. Hsiu, Pi-Cheng, Chin-Fu Kuo, Tei-Wei Kuo, and Eric YT Juan. "Scenario based threat detection and attack analysis." In Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on, pp. 279-282. IEEE, 2005.
6. Carl, Glenn, George Kesidis, Richard R. Brooks, and Suresh Rai. "Denial-of-service attack-detection techniques." IEEE Internet computing 10, no. 1 (2006): 82-89.
7. Kim, Jungwon, Peter J. Bentley, Uwe Aickelin, Julie Greensmith, Gianni Tedesco, and Jamie Twycross. "Immune system approaches to intrusion detection–a review." Natural computing 6, no. 4 (2007): 413-466.
8. Garcia-Teodoro, Pedro, Jesus Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. "Anomaly-based network intrusion detection: Techniques, systems and challenges." computers & security 28, no. 1-2 (2009): 18-28.
9. Wu, Shelly Xiaonan, and Wolfgang Banzhaf. "The use of computational intelligence in intrusion detection systems: A review." Applied soft computing 10, no. 1 (2010): 1-35.
10. Jalil, KamarularifinAbd, Muhammad HilmiKamarudin, and Mohamad NoormanMasrek. "Comparison of machine learning algorithms performance in detecting network intrusion." In Networking and Information Technology (ICNIT), 2010 International Conference on, pp. 221-226. IEEE, 2010.
11. Elshoush, HuwaidaTagelsir, and Izzeldin Mohamed Osman. "Alert correlation in collaborative intelligent intrusion detection systems—A survey." Applied Soft Computing 11, no. 7 (2011): 4349-4365.
12. Mohammed, Muamer N., and NorrozilaSulaiman. "Intrusion detection system based on SVM for WLAN." Procedia Technology 1 (2012): 313-317.
13. Nadiammai, G. V., and M. Hemalatha. "Effective approach toward Intrusion Detection System using data mining techniques." Egyptian Informatics Journal 15, no. 1 (2014): 37-50.
14. Agrawal, Shikha, and Jitendra Agrawal. "Survey on anomaly detection using data mining techniques." Procedia Computer Science 60 (2015): 708-713.