Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017)
IEEE Xplore Compliant - Part Number: CFP17L34-ART, ISBN: 978-1-5386-4031-9

A Survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and Protection System (IIDPS)

Amol Borkar
Dept. of Computer Engg
Sinhgad Institute of Technology
Lonavala, India
amolborkar30597@gmail.com

Akshay Donode
Dept. of Computer Engg
Sinhgad Institute of Technology
Lonavala, India
donodeakshay@gmail.com

Anjali Kumari
Dept. of Computer Engg
Sinhgad Institute of Technology
Lonavala, India
anjali.kumari135@gmail.com

Abstract— **Around the world, billions of people access the internet today. Intrusion detection technology is a new generation of security technology that monitor system to avoid malicious activities. The paper consists of the literature survey of Internal Intrusion Detection System (IIDS) and Intrusion Detection System (IDS) that uses various data mining and forensic techniques algorithms for the system to work in real time. Data mining methods are proposed for cyber analytics in support of intrusion detection.**

Keywords— **Internal Intrusion Detection System (IIDS), Intrusion Detection System (IDS), System Call (SC), Denial of Service (DOS).**

I. INTRODUCTION

In Today's world, several organisations store their data in several ways. These organisation's only requirement is to protect their private and official data from the intruders and external, internal intruders. It may also be possible that some authorised user may leak the data of the organisation for any purpose. In real-time, it is challenging to recognise the attacker because duplicate IP and attack packets can create. Techniques used before like firewall, and IDS was not able to detect the real-time attackers which occurred in the absence of the admin without his knowledge. A computer network is the combination of a set of hardware and software. Both components have their risks, vulnerabilities and security issues. The attack in the software makes the data vulnerable. The ones who know programming and systems can easily find out the various activities performed on the systems using log files. They can help in ensuring security. The problem arrives when people don't have any underlying knowledge of programming, and their system gets attacked by the intruders, and they can't find out the problem. There are various types of attacks. But the most challenging one is to find out the insider/internal attack. The network security is an area where every user wants his systems to protected from all the malicious attacks (internal or external attacks). The external attacks by the intruders can be detected by IDS, and IIDS can identify the internal intruders. In return, these techniques help us to protect our systems.

In this paper, section II presents the types of attacks. In section III, IIDS with their types is present. The literature survey shown in section IV. In the section, V paper concludes.

II. TYPES OF ATTACKS

The attacks can be passive or active [1]. The active attack is characterised by the attacker attempting to break into the system. During an active attack, the intruder will introduce data into the system as well as potentially change data within the system. The types of active attacks are distributed DOS, session replay and masquerade. Viruses, Worms, Trojan are the example of active attacks. The passive attack attempts to learn or make use of information from the system but doesn't affect system resources. Tapping, Encryption, Scanning are some types of passive attacks. An attack can also be wreaked by an outsider or an insider of the company. An insider attack is a malicious attack carried out on a network or computer system a person with authorised system access. UBS PaineWebber is one of the types of insider attacks. An outsider attack initiated by an illegal use of the system. Spoofing, Spam, Spin are some of the types outsider attacks.

Pharming:

Pharming involves a hacker infiltrating a computer system and installing malicious code that causes website traffic from the network to redirected to bogus sites developed by the hacker. Many websites require the user's personal information. Private and personal information entered into these fake sites is then captured by the pirate. DNS cache poisoning host file modification are the methods of pharming attacks.

DOS (Denial of Service):

DOS is an attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting service of a host connected to the internet. Flooding in the network, disrupting the connections, preventing the access of individuals are some examples of DOS attacks. DOS attacks deprive legitimate users of the service they expected.

Eavesdropping Attack:

Eavesdropping is an electronic attack where digital communication is interrupted by an individual whom they are not intended. Man in the middle attack is the best example of eavesdropping attack. Directly listening to digital or analog voice communication and shifting of data relating to any form of communication are two main types of eavesdropping attack.

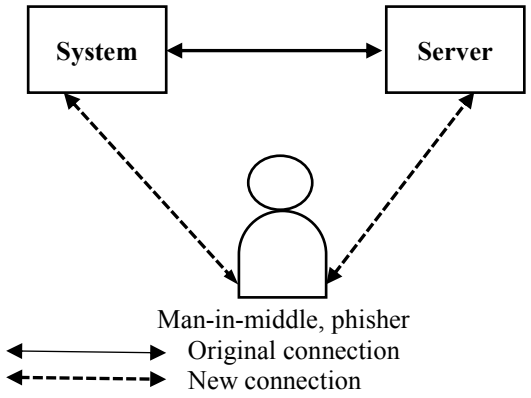

Fig. 1. Example of Eavesdropping Attack

Phishing Attack:

Phishing is an attack to obtain sensitive information for malicious reasons. These information's includes usernames, passwords, credit card details and more. Spear phishing, clone phishing, whaling are the types of phishing attacks.

Spear phishing:

Spear phishing is a type of e-mail spoofing which targets an individual or an organisation to access its sensitive information.

Clone phishing:

Clone phishing is a type of phishing where the recipient's address is duplicate for creating an identical e-mail having different content.

Whaling phishing:

Whaling phishing is a type of phishing which targets the high-profile group that includes senior executives, celebrities, businessmen's, politicians etc. Technical support scams, infected attachments, social media exploits, fraud scams are the examples of phishing.

DDOS (Distributed Denial of Service) Attack:

In DDOS, the incoming traffic flooding the victim originates from many different sources. In DDOS attack, the perpetrator uses more than one IP addresses. The primary difference between DOS and DDOS includes the usage of systems in both the attacks. DOS uses the single internet connections in a network whereas DDOS uses multiple links connected to various devices.

Brute Force Attack:

A Brute force attack is a trial-and-error method used to obtain information such as passwords, or PIN (Personal Identification Number). A dictionary attack, searches attacks rule-based search attacks are types of brute force attacks. This attack can avoid by having strong password content.

III. IIDS

Network-based attacks are threats that are originated and managed by a device or devices other than those under attack. DOS attacks and distributed- DOS attacks are examples of network-based attacks. Firewalls and intrusion prevention system are countermeasures to these types of attacks. A host-based IDS system monitors and analyses the internals of a computing system. A general IIDS uses a database of system objects it should monitor.

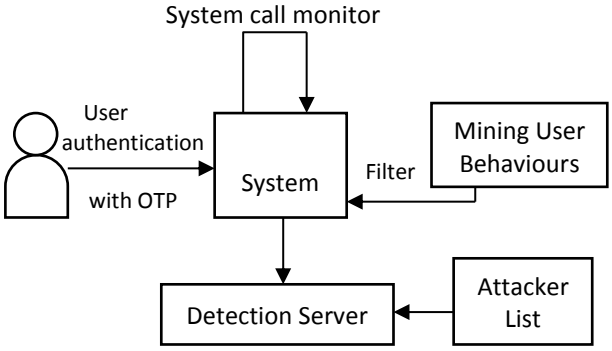

Fig. 2. Proposed System Architecture

IIDS were developed to detect the internal intruders. These systems were not as accurate as the proposed system. This method performs at real time and hence increase the accuracy by a noticeable percentage.To improve the security; a technique has proposed where the administrator will get an OTP on registered email id or the mobile number. Real-time images and activities are captures through webcam or screenshots which provides the intruder activity list.

IV. LITERATURE SURVEY

According to [2], a system to accurately detect potential attack has developed by using various techniques like decision free, Random forest and KNN.To overcome the limitation of the previous system that was not able to detect the IPV6 attacks, a new method are proposed. The developed system produce the impressive and efficient result in identifying IPV4-based attack keeping in mind the future scope. The effectiveness of various algorithm evaluated. Detection accuracy, precision, recall percentage were measured.

[3] Has stated that clustering and KDD can be efficiently used to detect novel anomaly called NEC. An unsupervised anomaly is used to produce high detection rate and less false passive rate. It is an appropriate way to solve the problem and

find the anomaly which does not need a labelled data set. The system is verified over NSL-KDD 2009 dataset. The preprocessing model transforms all features into the real number and normalised dataset at the end the evaluation component will compare predicate result an accurate result.

Concerning A Survey of Data Mining and Machine Learning for CSID [4], a survey of data mining and machine learning for cybersecurity instruction detection is performed to ensure cybersecurity. Packet-header and net flow packet header are used for the instruction detection system to be able to reach networks and kernel level data. The future scope that is kept in mind is that data mining and machine learning cannot ware without representative data and also it's very time-consuming. The complexity of different machine learning and data mining algorithm is discussed, The paper also provides a set of comparison criteria for machine learning/data mining methods Intrusion Detection System help discovered, determine and identify unauthorized used, duplication, alteration and destruction of the information system.

An [5], confirmed that on the advanced method for detection to improve the security by identifying and tracking the attacker using machine learning, ranking and Voronoi clustering is proposed the paper ensure reducing the size of data set and high detection accuracy. A data set called ISOT has been used keeping in mind the processing delay in the large-scale network UDP and TCP are examined to recognize achieve instruction growth in network traffic is taken care of machine learning modules act like deep neural network various botnet techniques are provided DNA based method is developed by the system help. The paper also uses characteristics of the network flow to detect the botnet intrusion despite packet payload content, which helps in encryption of packet.

According to An ADS-B IDS [6], an automatic dependent surveillance-broadcast IDS technique are proposed by using ADS-B techniques. HMAC data set has been used to increase the performance of air traffic control. The methods operate with minimal overhead. The future scope says for ADS-B position to be valid, its distance from the corresponding one at a time t as to be within the safe zone. ADS-B as emerged as an alternative to current radio, radar standards in aircraft signalling superior location accuracy are the provided by GPS using the cyber-physical environment the attack detection is confirmed. A mechanism is proposed to exchange the keys used for the HMAC algorithm securely. ATC Centre initiates firm handshakes with ATC's that control another zone in the flight-path to transfer the private key over public key infrastructure (PK1) schemes.

[7] This paper stated that using common path mining a hybrid IDS using data mining is developed for a power system that uses data logs the approach is an automated approach to build the hybrid IDS. One of the important advantages is detection accuracy which is up to 73%. But this method is not at all suitable for big data problem capturing such as data logs is also tricky. The system leverages features of signature-based and specification based IDS. The data mining technique that aggregates audit logs from multiple system devices to learn the standard path. The automated approach eliminates the need to manually analysis and manually code pattern.

According to Flow anomaly based. [9], this paper based on the flow anomaly Intrusion Detection System for Android mobile devices this approach uses ANN (Artificial Neural Network) on Android Operating System to detect anomaly behaviours in android mobiles. Accuracy and detection rate of this methodology reaches 85% and 81% respectively. Imitation is considered regarding CPU, memory and battery power this work endeavours to identify a lightweight, scalable an efficient IDS for an android environment various services are provided for addressing public attacks. The data streams are analysed by using efficient machine learning algorithms. The future scope includes the improvement in accuracy and detection rate.

As proposed [10], A Hidden Markow model based IDS is developed for software-defined networking (SDN). SDN network can help monitor the overall security of a system by analysing the web as a hole and making choices to defend the network based on the data from the entire network it includes uses of ANN IDS. This methodology allows greater dynamic control of a networking environment. The paper consists of the advantages like increased in the range of activities and also is the increase of security application. It has shown that machine learning application holds the potential to be used to access the risk in networking environment for the future scope expanding the feature vector used by HMM in determining the maliciousness of a set data are to be added.

[14] Referred that cybersecurity is severe issues in the cyberspace. The paper includes the demonstration of a neuromorphic cognitive computing approach for network IDS for cybersecurity using deep learning. This method uses Discrete Vector Factorization. The NSL-KDD dataset is used to increase accuracy and classification up to 90.12% and 81.31% respectively. Deep learning achieves human-level performance in particular for recognition tasks, in-depth learning approach combining the features of extraction classification. The future scope includes the challenge of determining the representation of data in spiking format for the use in the True- North-System.

According to [13], this paper based on the Intrusion detection system for PS-Poll DOS attack in 802.11 networks using real-time discrete event system. This approach uses RTDES on real-time discrete event system for detecting DOS attack. One of the important advantages is high accuracy and detection rate, but one of the major drawbacks is a loss of frames. Detect the PS-DOS attack require encryption change in protocol or installation of proprietary hardware.

TABLE I
DIFFERENT TECHNIQUES OF IDS

Algorithm/Technique Used	**Reference Paper**	**Test Data Used**	**Purpose of IDS**	**Advantages**	**Limitations/Future Scope**
Decision tree, random forest, K-NN.	[2]	NA	To accurately detect potential attacks.	Produce impressive and efficient results in detecting IPV4-based attacks.	IPV6 attacks cannot be detected yet.
Clustering and KDD.	[3]	NSL-KDD 2009 dataset.	To detect novel anomalies called NEC.	Quality labelled datasets are not required.	High false positive Rate and high detection rate.
Data Mining and Machine Learning.	[4]	Packet headers and net flow packet headers.	To ensure cybersecurity.	IDS can reach networks and kernel level data.	Data Mining and Machine Learning can't work without representative data and is very time-consuming.
Machine Learning, Ranking, Voronos clustering.	[5]	ISOT	Improve the security by identifying and tracking the attackers.	Reduce the size of the dataset, high detection accuracy.	Processing delays in the massive scale of the network.
Automatic Dependent Surveillance-Broadcast (ADS-B).	[6]	HMAC.	To increase the performance of air traffic control.	Operates with minimal overhead.	An ADS-B position to be valid, its distance from the corresponding one at a time t has to be within the safe zone.
Common Path Mining.	[7]	Data logs.	An Automated approach to building a hybrid IDS.	Detection accuracy is 73%.	Not suitable for big data. Problem capturing such as data logs is difficult.
Epigenetic algorithm.	[8]	KDD-NSL.	Additional an information of future offspring.	It helps to prevent more preciously the curable and not curable diseases based on environmental factors that do not fit in the sequenced gene.	Reduction of total iterations to obtain the optimal solution is a shorter time.
Artificial Neural Network (ANN), IDS.	[9]	Android OS	Detect the anamoly behaviours in android mobiles.	Accuracy and detection rate reaches 85% and 81% respectively.	Further, improving the accuracy and detection rate.
SDN, NIDS.	[10]	NA	Allows greater dynamic control of a networking environment.	Increase the range of activities, increase the efficiency of security applications.	Expanding the features vectors used by the HMM in determining the maliciousness of a set of data.
Genetic Programming Fuzzy Inference System for Classification (GPFIS-Class)	[11]	NSL-KDD	To solve the problem of classification in IDS.	Classification accuracy is higher.	New GFS hybridised with a neural network.
Hybrid Cryptography	[12]	NA	To reduce the network and routing overhead.	More powerful and secure than MANET	Reduce PDR PDR=total packet received / Total packet sent.

Real-Time Discrete Event System. (RTDES)	[13]	NA	A timed IDS based or real-time discrete event system for detecting DOS attack.	Preserves much energy, high accuracy, detection rate.	Loss of frames.
Discrete Vector Factorization (DVF) in-depth learning approach.	[14]	NSL-KDD	To demonstrate a neuromorphic cognitive computing approach for network IDS.	90.12% and 81.31 are the accuracy and classification respectively.	It is challenging to determine the representation of data in spiking format for the use in the True-North system.

V. CONCLUSION AND FUTURE SCOPE

As per the studied of techniques suggested by various authors, the ways it can detect the intruder are presented here. The conclusion that can be drawn from the survey stated above is the paper [7] [8] [14], has accuracy and detection rate maximised to 90.12% whereas the techniques proposed by us increase the accuracy and detection rate up to 95%. A Survey from [3] includes high false positive rate, but our system reduces the false positive rate comparatively. One of the surveys from [5] suggests that there are processing delays in large scale of network there in our system, the intruders are detected in real time and also provides a list of intruders and their activities and comparatively to the survey [4], it is less time consuming, So, when designing a new IDS, these characteristics can be used in real time system to detect the internal intruders and their malicious behaviours. This will be a valid IDS which will identify the internal intruder's accurately in real time and can be used by several firms, MNC's for protecting their valuable data.

ACKNOWLEDGEMENT

We are mainly thanks to our guide Prof. R.S.Shishupal who has provided guidance, expertise, encouragement. Thanks to all those who helped me in the completion of this work knowingly or unknowingly.

REFERENCE

[1] Lazarevic, Aleksander, Yipin Kumar and Jaideep Srivastava, "Intrusion Detection: A Survey", managing cyber Threats, Springer US, 2005, pp 19-78, 2005.

[2] Mohammed Anbar, Rosni Abdulah, Izan H. Hasbullah, Yung-Wey Chong; Omar E. Elejla, "Comparative Performance Analysis of classification algorithm for Internal Intrusion Detection ", 2016 14th Annual Conference on Privacy Security and Trust (PCT), Dec 12-14,2016, Penang, Malaysia.

[3] Weiwei Chen, Fangang Kong, Feng Mei, GuiginYuan, Bo Li, "a novel unsupervised Anamoly detection Approach for Intrusion Detection System", 2017 IEEE 3rd International Conference on big data security on cloud, May 16-18,2017, Zhejiang, China.

[4] Anna L. Buczak, Erha n Guven, "A Survey of Data Mining and Machine Learning methods for cybersecurity intrusion detection", IEEE communication surveys and tutorials, vol. 18, Issue 2,2016.

[5] Manoj s. Koli, Manik K. Chavan, "An Advanced method for detection of botnet traffic using Internal Intrusion Detection", 2017 International Conference on (ICICCT), March 10-11, 2017, Sangli, India.

[6] Thabet Kacem, Duminda Wijesekera, Paulo Costa, Alexander Barreto, "An ADS-B Intrusion Detection System", 2016 IEEE on ISPA, 2016, Fairfax, Virginia.

[7] Shengyi Pan, Thomas Morris, Uttam Adhikari, "Developing a Hybrid Intrusion Detection System using Data Mining for power system", IEEE Transactions on, vol. 6, issues. 6, Nov. 2015.

[8] Mehdi Ezzarii, Hamid Elghazi, Hassan El Ghazi, Tayeb Sadiki, "Epigenetic Algorithm for performing Intrusion Detection System",2016 International Conference on ACOSIS, Oct17-19,2016, Rabat, Morocco.

[9] Panagiotis I. Radogloa-Grammatikis; Panagiotis G. Sarigannidis, "Flow anamoly based Intrusion Detection System for Android Mobile Devices", 2017 6th International Conference on MOCAST, May 4-6, 2017, Kazani, Greece.

[10] Trae Hurley, Jorge E. Perdomo, Alexander Perez-pons, "HMM-Based Intrusion Detection System for software-defined networking", 2016 15th IEEE Conference on Machine Learning and Application, Dec 18-20, 2016, Miami, Florida.

[11] Mariem Belhor, Farah Jemili, "Intrusion Detection based on genetic fuzzy classification system", 2016 IEEE 13th International Conference on Computer Systems and Application (AICCSA), Nov 29 2016-Dec 2, 2016, Sousse, Tunisia.

[12] Sharad Awatade, Shweta Joshi. "Improved EAACK: Develop Secure Intrusion Detection System for MANETS using hybrid cryptography", 2016 International Conference on computing communication control and automation (ICCUBEA), Aug 12-13, 2016, Maharashtra, India.

[13] Mayank Agarwal, Sanketh Purwar, Santosh Biswas, Sukumar Nandi, "Internal Detection System for PS-Poll DOS attack in 802.11 networks using real-time discrete event system",IEEE,vol.4,issue4,2017.

[14] Md Zahangir Alom, Tarek m. Taha, "Network Intrusion Detection for cybersecurity on neuromorphic computing system", 2017 International Joint Conference on Neural Networks (IJCNN), May 14-15,2017, USA.