Raj Kumar Yaduwanshi, 2022, 10:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

A Survey on Network Intrusion Detection System Types and Features

M.Tech. Scholar Raj Kumar Yaduwanshi, Prof. Manorama Malviya
Department of Computer Science and Engineering
Technocrats Institute of Technology (Main)
Bhopal,MP,India

Abstract- Digital computer network reduces the load of communication and increase the dependcy of many individual, organization, nation, etc. This network uses attracts the intruders to do unfair activities, hence detection of such action is an important security issue. In this paper network intrusion detection systems were introduced with its requirement and application. Paper has summarized different types of attacks used by intruders for doing unethical activity. Many of scholars has done lot of work in this research area and proposed many models for intrusion detection. This paper has brief few of proposed models with techniques of intrusion detection. Paper has detailed a dataset UNSW-15 in the paper for understanding of intrusion relation features.

Keywords- Intrusion detection, Network Security, Feature reduction.

I. INTRODUCTION

One of the leading technical progressions of computing is "Internet of Things" (IoT). The IoT carries in numerous services, promising individuals' personal lives obtained from the reliable process. It is forecasted that by 2022 trillion IP objects (addresses) will be associated with the internet. Low accessibility and obscurity of many devices in the massive heterogeneous network makes it problematic to observe the flow of data.

However, to protect networks, the intruders who are unauthorized should be identified within the limitations of each kind of device before distributing the system information [3]. The concept of IoT is rapidly increasing into different industrial areas comprising automotive, logistics and health care. IoT environment attains enormous prominence for ensuring security and safety of both connectivity and information [4].

Contemporarily, the security of data is maintained via authenticating and encrypting mechanism. Nevertheless, the tools which are used for security cannot guarantee the complete protection in contrast to malevolent intruders. Consequently, an efficient and appropriate Intrusion detection system (IDS) is obligatory for ensuring the security in the IoT. There are lightweight encryption techniques that have been regarded as the main technology for building IoT's security mechanism.

However, taking into consideration the rapid rise in the computation capacity of the hackers, which generally include the application of Distributed Computing, Cloud Computing, and Quantum computation among others, light weight cryptography techniques will stop being used in the coming years. The other types of security enforcement techniques like the use of systems for detecting intrusion ought to be used to ensure that IoT networks are protected in the right manner [5-6].

"Intrusion Detection" is a hardware or software that is capable of detecting unauthorized user behavior in computer system. A standard IDS sensor facilitator, a reporting system, and an analytics engine; In addition, sensors are placed in different network areas or hosts, and their primary task is to collect data.

Additionally, the collected data is supplied to the analytics engine responsible for data collection and intrusion detection. The reporting system creates a caution for the network administrator, out of the chance that an intrusion can be detected by the output engine.

The object of the paper that is to discuss the different kinds of attacks, which have been tended to within the IDS guidelines for IoT. Along these rows, motivating IoT solution involves a system of a few standards, facilities, and innovations, each with its privacy and security needs.

Considering this, it is prudent to assume that the IoT model, which has at any rate a similar security issues as a mobile communication network (i.e., WSN), the Internet, and cloud services. Sherasiya and Upadhyay, (2016) concentrated on the traditional attack and also surveyed the display of their IDS with the standard assault situations which contained inside tunnelling, worm propagation, directory traversal assaults, and SQL code injection.

II. RELATED WORK

Yulong Fu et. al. in [7] analyzed the intrusion detection requirements of IoT networks and then proposed a uniform intrusion detection method for the vast heterogeneous IoT networks based on an automata model. The proposed method can detect and report the possible IoT attacks with three types: jam-attack, false-attack, and reply-attack automatically.

Sai Kiran et. al. in [8] proposed amodel of machine learning to identify attacks in IoT network. To build a model, normal and attack data needs to be generated from the IoT environment. A test bed is build to simulate the IoT environment using Node MCU ESP8266, DHT11 sensor and wireless router.

An adversarial system is build using a laptop system which performs actions of sniffing and poisoning attacks. Data captured from the sensors were temperature, humidity and due-point which are transmitted to Think Speak platform using wireless gateway.

In the normal phase, sensor values is captured by Node MCU and transmitted to Think Speak server which are stored and labeled as normal data. In the attacking phase, from an adversarial system, the attacker secretly intercepts the data, modifies the data when it is transmitted between the Node MCU and Think Speak server. In the attacking phase, Man in the Middle attack is performed in the network using ARP Poisoning and the data captured is labeled as attack data.

Bacem Mbarek et. al. in [9] proposed a new NIDS protocol with an efficient replica detection algorithm to increase the utility and performance of existing NIDS, where a number of replica test nodes are intentionally inserted into the network to test the reliability and response of witness nodes. The proposed protocol, Enhanced NIDS, can address the vulnerability of NIDS and improve IoT network security to detect severe compromise attacks such as clone attacks.

Sstla, V. et. al. in [10] evaluated the performance of two supervised machine learning algorithms such as SVM and Deep Neural Networks on Network Intrusion Detection Systems. Now-a-days, all the services are available on internet and malicious users can attack client or server machines through this internet and avoid such attack request IDS. IDS will monitor request data, and then check if it contains a normal or attack signature; if it contains the attack signature, then the request will be dropped.

We have constructed Network Intrusion Detection System using SVM and DCNN and evaluated the performance using different types of kernels and different types of activation functions. The performance of the proposed method is evaluated on the NSL-KDD dataset. From the experimentation, higher accuracy achieved with DCNN compared to SVM.

Nomaan Jaweed Mohammed in [11] proposed IDS solution utilizes Fish Schooling Genetic Algorithm and an error back propagation neural network. The genetic algorithm has been used for detecting the good feature set from the training dataset and the selected good features train the neural network. This combination of genetic algorithm and Neural network increases the detection accuracy of intrusion with a lesser number of training features, and the reduction of the feature set increases the learning accuracy of neural networks for intrusion detection.

III. TYPES OF INTRUSION

This section brief intrusion types intruder use for attack on networks [12]:

1. Cross Site Scripting Attack:
XSS uses the HTML for the attack in which malicious code is injected into the data by using the Flash, JavaScript or others.

International Journal of Science, Engineering and Technology

An Open Access Journal

2. SQL Injection Attack:
In this attack the attacker uses the input field of the database of the user. The most common example for such types of attacks is the attack occurred on the Sony play station in the year 2008 website.

3. Command Injection Attack:
The name of this attack is given as per its role, because it injects the command and those commands are run according to the runtime environment or may create shell.

4. Abuse and Nefarious use of Cloud Services:
The main difference in this attack than the insider is the attacker's background, otherwise all is in common. In the insider attack the attacker is the authorized user of the data while in this attacker is the hacker which attacks the less secured database or poor clouds. As due to this no need of using expensive DoS and did brute forced attacks on the target.

5. Denial of Service Attack:
This type of attacks is mainly done by the flooded networks having many packets like TCP, UDP, ICMP or their combinations. Due to the risk of the intruder attack on the distributed services of the computer, some of them are not even available to the authorized users also.

As this attack overloads all the systems, due to which legal users are unable to used them. These types of attacks prove very dangerous for the single cloud data and servers as many users depend on that cloud.

6. Side Channel Attack:
This type of attack done with the cryptographic algorithm of the system. For this they used the special VMM service which is virtual machine manger which guides the user attack for the creation of virtualization layer. They placed a physical virtual machine on the targeted system, while VMM helps other users and supervises known as hypervisor.

7. User to Root Attack:
In this attack, the attacker uses the sniffing password for the authentication of the targeted user's system. So, by combining traditional various methods for the raising of the privileges to the super user access acceptance. An example of such escalation technique is the smashing stack, in which a packet of the set-UID- root program that corrupts the address space, so that returning information from the instruction to sub shell space.

8. A remote to Local Attack:
In this attacker takes the advantages of the targeted user local privileges. This attack is also known as remote to user attack. In this attacker sends packets to the user host and close the exposures of the access of asxlock, guest, xnsnoop, phf and send mail.

9. Scanning Attacks:
A scanning attack [13] is an attack that attempts to send packets of information to a network system to gather information about the topology. It involves looking for ports which are either open or closed, what type of traffic is permitted and not permitted, which hosts are active or even the type of hardware running on different devices. For instance, a type of attack that finds weak points in a network is Blind SQL injection attacks. A Blind SQL injection attack is an attempt to ask a database questions that make it respond by a Boolean value to find vulnerabilities. These types of attacks often attempt to find open ports to be exploited by injecting malicious code or malware.

10. Asymmetric Routing:
When packets take a specific route to the destination and a different route back to the source, this behavior is called asymmetric routing [13]. This behavior is normal in general, but it is unwanted. The reason behind that is adversaries can benefit from asymmetric routing by sending malicious data through particular parts of the network to bypass security systems, depending on firewalls configuration. If the network is allowed to perform asymmetric routing, then it is exposed to attacks such as SYN flood attacks.

An SYN flood attack is an attack that attempts to open many connections without closing them (half-open attack), which leads to a total consumption of system or server resources so that it becomes unresponsive. This attack is a DDoS attack type, and one reason to deactivate asymmetric routing in the network.

11. Buffer Overflow:
Attacks Buffer overflow [13] attacks attempt to replace normal data with malicious data in penetrated memory parts, such that a malicious code

gets executed later on. In generic terms, a buffer overflow attack writes more data in the memory's buffer than it can handle; performing this action results in making the data overflow into the neighboring memory.

IV. TYPES OF INTRUSION DETECTION SYSTEM

1. Network based Intrusion Detection System:
Network intrusion detection system monitors and analyzes network traffic by reading individual packets through network layer and transport layer. It searches for any suspicious activity or network based attack such as Denial of Service (DoS) attack, port scans etc. Once an abnormal behavior in network traffic is identified, alert can be sent to system administrator. Most of the commercial IDSs are based on the NIDS such as Snort, Tcpdump and Natural flight [14]. These are well known for general sized networks and convenient for implementation to detect intrusions. The main issues of Snort IDS when integrating with distributed computing environment.

To overcome the issues, they introduced new approach for handling these issues. For virtual network systems, multi phase distributed vulnerability detection and measurement technique has been proposed to detect DDoS attack. It has detected attacks based on attack graph by analyzing network traffic flowing through virtual machines. It has significantly improved attack detection and mitigates attack consequences.

2. Host based Intrusion Detection System:
Host based intrusion detection system monitors the individual host or device on the network by analyzing any change in the activity performed by host and events occurring within that host. It looks at every activity of host by checking application logs, system calls, and file-system modifications, inbound and outbound packets to and from host.

If any suspicious activity is found, an alert is generated and sent to administrator to protect the system from malicious attack. Since majority of sectors prefer HIDS also after NIDS which are mainly based on the log file analysis of system. A model of HIDS has been developed based on log file analysis of Microsoft Windows XP operating system. It detects intrusions by matching predefined pattern with the logs of operating system [15].

3. Distributed based Intrusion Detection System:
Distributed IDS (DIDS) also known as hybrid IDS, consists of two or more detection methods or systems i.e., NIDS, HIDS etc [16]. This type of system is deployed over large distributed network like cloud computing so as all entities can communicate with each other and with network monitor such as central server In this way, all hosts deployed over network collect system information and send it to central server by converting it into standard format.

4. VMM/Hypervisor based Intrusion Detection System:
Hypervisor provides a platform for communication among VMs. Hypervisor based IDSs is deployed at the hypervisor layer. It helps in analysis of available information for detection of anomalous activities [17]. The information is based on communication at various levels like communication between VM and hypervisor, between VMs and communication within the hypervisor based virtual network.

V. FEATURE OF DATASET

UNSW-NB15 was created using a commercial penetration tool in the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS). This tool can generate hybrid synthetically modern normal activities and contemporary attack behaviors from network traffic. They collected tcpdump traces for a total duration of 31 h.

From these network traces, they extracted 49 features categorized into five groups: flow features, basic features, content features, time features, and additional generated features. Feature and statistical analyses are the most common methods used in several published papers employing UNSW-NB15 [18].

Id	Feature Name	Description
1	dur	Record total duration
2	sbytes	Source to destination bytes
3	dbytes	Destination to source bytes
4	rate	Number of packets per second
5	sttl	Source to destination time to live

6	dttl	Destination to source time to live
7	sloss	Source packets retransmitted or dropped
8	dloss	Destination packets retransmitted or dropped
9	sload	Source bits per second
10	dload	Destination bits per second
11	spkts	Source to destination packet count
12	dpkts	Destination to source packet count
13	swin	Source TCP window advertisement value
14	dwin	Destination TCP window advertisement value
15	Stcpb	Source TCP base sequence number
16	dtcpb	Destination TCP base sequence number
17	smeansz	Mean of the packet size transmitted by the srcip
18	dmeansz	Mean of the packet size transmitted by the dstip
19	trans_depth	The connection of http request/response transaction
20	response_body_len	The content size of the data transferred from http
21	sjit	Source jitter (mSec)
22	djit	Destination jitter (mSec)
23	sinpkt	Source inter-packet arrival time
24	dinpkt	Destination inter-packet arrival time
25	tcprtt	Setup round-trip time, the sum of 'synack' and 'ackdat'
26	synack	The time between the SYN and the SYN_ACK packets
27	ackdat	The time between the SYN_ACK and the ACK packets
28	is_sm_ips_ports	If srcip = dstip and sport = dsport, assign 1 else 0
29	ct_state_ttl	No. of each state according to values of sttl and dttl
30	ct_flw_http_mthd	No. of methods such as Get and Post in http service
31	is_ftp_login	If the ftp session is accessed by user and password then 1 else 0
32	ct_ftp_cmd	No of flows that has a command in ftp session
33	ct_srv_src	No. of rows of the same service and srcip in 100 rows
34	ct_srv_dst	No. of rows of the same service and dstip in 100 rows
35	ct_dst_ltm	No. of rows of the same dstip in 100 rows
36	ct_src_ltm	No. of rows of the srcip in 100 rows
37	ct_src_dport_ltm	No of rows of the same srcip and the dsport in 100 rows
38	ct_dst_sport_ltm	No of rows of the same dstip and the sport in 100 rows
39	ct_dst_src_ltm	No of rows of the same srcip and the dstip in 100 records

VI. CONCLUSION

Vulnerability on network functionality leads to loss of important information of individual, organization, community, nation, etc. Network dependency increases the chance of attack from various mediums. So security measures were taken in form of trust based node working, but malicious program still need to be checked.

This paper has found that reducing the dimension of session dataset increases the detection accuracy. It was found that because of dynamic nature of network vulnerability increases and this directly raise the chance of attacks. It was found from the survey that machine learning approach was mostly used by scholar to detect the intrusion on the cloud. In future scholar can develop a less false alarm generator algorithm.

REFERENCES

[1] Okan CAN, Ozgur Koray SAHINGOZ,"A Survey of Intrusion Detection Systems in Wireless Sensor Networks", 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), 2015.

[2] Abdur Rahaman Sardar, Rashmi Ranjan Sahoo, Moutushi Singh, Souvik Sarkar, Jamuna Kanta Singh, and Koushik Ma- jumder, "Intelligent Intrusion Detection System in Wireless Sensor Network", Proc. Of the 3rd Int. Conf. on Front. Of Intell. Comput. (FICTA), 2014 Vol. 2, Advances in

Intelligent Systems and Computing 328, Springer DOI: 10.1007/978-3- 319-12012-6 78.

[3] P. Gokul Sai Sreeram, Chandra Mohan Reddy Sivappagari," Development of Industrial Intrusion Detection and Monitoring Using Internet of Things", International Journal of Technical Research and Applications, 2015

[4] A. Anand, B. Patel, "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols", International Journal of Advanced Re- search in Computer Science and Software Engineering, vol.2, no. 8, 2012.

[5] A. Sen and P. Jain," Technique of intrusion detection based on Neural Network- A review", 2014 Conference on IT in Business, Industry and Government (CSIBIG), 2014.

[6] Sherasiya, T. and Upadhyay, H., 2016. "Intrusion detection system for internet of things". Int. J. Adv. Res. Innov. Ideas Educ.(IJARIIE), 2(3).

[7] Yulong Fu, Zheng Yan, Jin Cao, Ousmane Koné, Xuefei Cao, "An Automata Based Intrusion Detection Method for Internet of Things", Mobile Information Systems, vol. 2017, Article ID 1750637, 13 pages, 2017.

[8] Sai Kiran, K.V.V.N.L. R.N. Kamakshi Devisetty, N. Pavan Kalyan, K. Mukundini, R. Karthi. "Building a Intrusion Detection System for IoT Environment using Machine Learning Techniques". Procedia Computer Science, Volume 171, 2020, Pages 2372-2379.

[9] Bacem Mbarek, Mouzhi Ge, and Tomás Pitner. 2020. Enhanced network intrusion detection system protocol for internet of things. In Proceedings of the 35th Annual ACM Symposium on Applied Computing (SAC '20). Association for Computing Machinery, New York, NY, USA, 1156–1163.

[10] Sstla, V., Kolli, V.K.K., Voggu, L.K., Bhavanam, R., Vallabhasoyula, S. (2020). Predictive model for network intrusion detection system using deep learning. Revue d'Intelligence Artificielle, Vol. 34, No. 3, pp. 323-330.

[11] Nomaan Jaweed Mohammed. Neural Network Training by Selected Fish Schooling Genetic Algorithm Feature for Intrusion Detection. International Journal of Computer Applications 175(30):7-11, November 2020.

[12] M. A. F. Pimentel, D. A. Clifton, L. Clifton, and L. Tarassenko, "A review of novelty detection," Signal processing, 02-Jan-2014.

[13] "What Is an Intrusion Detection System? Definition, Types, and Tools," DNSstuff, 18-Oct-2019.

[14] E. K. Subramanian, Lathatamilselvan. "A Focus On Future Cloud: Machine Learning-Based Cloud Security". Service Oriented Computing And Applications, 12 August 2019.

[15] M. Ahmed, R. Pal, M. M. Hossain, M. A. N. Bikas and M. K. Hasan, "NIDS: A Network Based Approach To Intrusion Detection And Prevention," 2009 International Association Of Computer Science And Information Technology - Spring Conference, Singapore, 2009

[16] Zegzhda P., Kort S. (2007) Host-Based Intrusion Detection System: Model And Design Features. In: Gorodetsky V., Kotenko I., Skormin V.A. (Eds) Computer Network Security. MMM-ACNS 2007. Communications In Computer And Information Science, Vol 1. Springer, Berlin, Heidelberg.

[17] Y. -J. Ou, Y. Lin, Y. Zhang and Y. -J. Ou, "The Design and Implementation Of Host-Based Intrusion Detection System," 2010 Third International Symposium On Intelligent Information Technology And Security Informatics, Jian, China, 2010.

[18] Nour M, Slay J (2015) UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: Military communications and information systems conference (MilCIS). IEEE.