A STUDY OF NETWORK SECURITY WITH INTRUSION PREVENTION SYSTEM IN DIFFERENT ENVIRONMENT

P. K. Anoos Babu, N. Thangarasu*

Abstract

The global use of the internet has increased significantly in recent years. Attacks on computer security are on the rise at the same time as new developing tactics and technologies. The connected devices in the networks were experiencing security problems brought on by malicious content or other hacker activities. The two systems utilised for the detection and prevention of these malicious softwares are the intrusion detection system (IDS) and intrusion prevention system (IPS), respectively. This essay examines the security principles and methods that are employed in intrusion prevention systems to stop assaults caused by malicious software. Additionally, it describes how various platforms' Intrusion Prevention Systems operate.

Keywords: Intrusion detection System, Intrusion Pretension System, Internet of Things, Hybrid Computing, MANET, Two-level classification, Security, Machine Learning

I. INTRODUCTION

The ability to use the internet has emerged as a necessary component of society. The security of every computer network is compromised. The ability to use the internet has emerged as a necessary component of society. The security of every computer network is compromised. Every computer network system on the planet is insecure and vulnerable to attack from any direction. We have two systems for the detection and prevention of these compute network challenges. both an intrusion detection system and an intrusion prevention system to stop malicious stuff from entering the network. In this study, we discussed the security-related technologies used in intrusion prevention systems.

II. LITERATURE STUDIES

The intrusion prevention system is used to stop attacks in computer networks that have been flagged by intrusion detection systems. To stop malicious content from entering the network, intrusion prevention systems use a variety of different tactics and precautions. The measures and technologies utilised in intrusion prevention systems in various environments will be detailed in the information that follows.

1. Android Platform

Android platform security concerns related to wireless assaults cannot be disregarded. Only relatively straightforward attack scenarios can be prevented using the conventional intrusion

The most frequent assaults on the Android platform are wireless cracking and phishing. In this area, a novel intrusion prevention system was developed that uses TcpDump and VPNService as data sources to collect traffic. Real-time intrusion is carried out by the single-step attack rule in conjunction with the attack chain signature database and the signature database. In order to determine the detection, penetration intent and output alerts are combined with these detections [1].

2. Cloud Computing

Traditional intrusion detection and prevention systems (IDPS) are mainly ineffective to implement in a cloud computing environment. The open and distributed architecture of cloud computing and services makes them an appealing target for possible cyberattacks by outsiders. IDPS and alarm management were both built using thorough taxonomy methodologies. The primary characteristics of

[1]Department of Computer Science
[2]Department of Computer Applications
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

IDPS and cloud computing systems identify a set of needs, and the most pertinent concepts—self-management, ontology, risk management, and fuzzy theory—are discovered to satisfy these requirements [2].

3. Mobile ad-hoc Network MANET

Computer networks can be secured in a number of ways using encryption, firewalls, DMZs, and other techniques. An intrusion detection system is used to find and report the attacks. Additionally, the intrusion protection system will protect the system from these additional attacks. There is a combined system for these two types of systems known as an intrusion detection and prevention system (IDPS). This IDPS can identify and stop harmful activities simultaneously. a MANET vulnerability not present in a wired network. Artificial neural networks are one type of architecture that can be used to construct hardware circuits for detecting and blocking attacks [4]. The standard wired network cannot withstand certain types of attacks that MANET needs to deal with, such the selfish attack, black hole attack, sleep deprivation attack, and others [3]. It is challenging to execute this architecture on a little wireless device because it calls for a lot of resources.

4. IoT Environment

IoT security refers to the process of protecting networks and IoT devices. In this study, intrusion detection systems (IDS) and network-based intrusion prevention systems (NBIPSs) are developed with the purpose of protecting Network systems from unauthorised access to cloud servers and IoT systems [5]. To secure top-level engineers, a network-based intrusion prevention system was put in place. This NBIPS operates behind a firewall and offers an interactive layer of inquiry that picks out dangerous substances negatively. It is possible to install NBIPS sensors to keep an eye on any passing traffic. utilising IoT signature-based technology Sensors are installed to intercept traffic and thwart attacks. It will limit obligations to violate copyright. If the attack has a recognised attack signature, NBIPS can thwart any network-based attack based on malicious traffic. [5][6].

5. Deep Learning on IoV

Traffic updates and other information about road safety will be transmitted via internet of vehicles, which is utilised to lessen traffic accidents. Sometimes, any misleading information that some attackers may have gotten will stop this IoVs. In its initial state, the network will pre-process data using an auto encoder to remove unwanted information. Deep learning techniques are used to distinguish between legitimate and malicious communication packets (packets). The first step in the procedure is to create a training dataset using the free and open-source KDD99 and CICIDS 2018 datasets. 1,20,223 network packets with 41 characteristics were present in it [8]. To remove undesirable data early on, the one-dimensional network data is pre-processed using an auto-encoder. One-dimensional data is pre-processed using an auto encoder in the initial stage to remove unnecessary data. after which the Softmax classifier and the Relu activation function were integrated. The specific Intrusion Prevention System model is tested using Google Collab, a cloud service that runs on an open platform, and TensorFlow. This prevention system was validated in Twerk Simulation, with a 99.57% accuracy rating [7].

6. Rreal Time Network And Hybrid Machine Leaning

Different types of network attacks are developing. Two main strategies—signature-based and anomaly detection—exist to combat such attacks or threads. Risky is signature-based detection. Variant assaults cannot be detected with anomaly detection, but real-time data traffic can. a two-level classifier that can accomplish high performance and real-time classy classification at the same time [10]. Internally, it employs classifiers at levels 1 and 2. Initial Actual-Moderate accuracy time for incoming data flow is carried out by a level 1 classifier. If the classifier cannot sort the data by a higher priority, it will likely wait classifying the data until traffic is at its peak. Classifier at

Level 2 gathers data on traffic flow statistics to carry out precise classification. The suggested two-level classification system can perform better in terms of accuracy and detection time when compared to existing strategies [9].

The two stages of the intrusion detection strategy that allows for great detection precision in real-time processing. It makes use of flow- and packet-based classifiers. to make up for accuracy and performance. Level One The classifier takes out from the packet a few chosen features. In order to enhance quicker classification Attack detection, real-time is first realised. Only Level 2 classifiers deal with flows. Not classified by level 1 classifier, hence machine learning-based classifier. Traffic is little enough to be processed quickly. Such a distinctive building Both classification speed and precision can be offered by a two-level classifier. We can attest that it works. Extensive performance evaluation is advantageous for this strategy. We want to construct real-time IPS that effectively addresses the security flaws in contemporary networks [9].

7. Real Time Network Incremental Feature Generation

The proposed method's machine studies were designed and investigated to efficiently identify different network threats. These are not only passive methods that are helpless against network attacks; they also catch them after the session has ended. The suggested classifier structure has two levels. Real-time classification is supported by the first-stage classifier. Furthermore, accurate classification is supported by the second-stage classifier [11]. Even in areas with high traffic, this was once utilised to confirm whether an attack took place. This technique has a high rate of real-time detection because it is quick and light.

8. Intelligent IPS on Snort

It is a new generation of intrusion detection and firewall technology for information security. It is also a safe solution that shields the system and network against attacks in real-time and is currently the focus of research in the field of network security. Support vector machine (SVM) applied to the Snort intrusion detection system is the major emphasis of this, which then develops a small-scale intelligent intrusion prevention system by fusing the Snort intrusion detection system and firewall [13][14].

9. IoT Based Machine Learning

The three key obstacles provided by machine learning are code, IoT devices, and sensors. In general, idea drift and high dimensionality are IDSs for the Internet of Things (IoT), and computational complexity is the third IDS [14]. a set of three distinct datasets, KDD99, NSL, and Kyoto. The three elements of idea drift-high-dimensional awareness, computational awareness, and the conclusion of this article are symmetrical in their effects and ought to be addressed in A neural network (NN) based model for an IDS in IoT [14].

10. Hardware Platform

The analysis of intrusion detection should be outsourced to network node IDS (NNIDS) executing in hardware on end hosts. A Network Node IDS (NNIDS) can inspect traffic to and from the host implicitly. The network interface is built in hardware and can run independently of the host operating system to give better protection with less overhead software implementations. Intel leverages COTS components such as IXP networking processors and Xilinx Virtex FPGAs to map these operations to a hardware platform. The NNIDS is capable of achieving high performance pipelines and careful assignment of processing steps to the most appropriate hardware resources [15].

III. SUMMERY AND CONCLUSION

The internet with security systems is a very complicated thing as it deals secure connection. To secure the network devices, it must overcome numerous obstacles. Malware intrusion can be extremely destructive to both the network and the network devices. These malwares can be found using the intrusion detection system, and these types of attacks can be stopped using the intrusion prevention system. The actual preventive system operates significantly differently on various platforms. Every platform makes use of its own algorithm, methodologies, equations, and fresh approaches. Malware is now more prevalent on these platforms, whether they are made of hardware or software, including ones like the Internet of Things. The introduction prevention system worked as intended regardless of the study's context (Cloud, IoT, Machine Learning, Android MANET). It includes appropriate techniques, algorithms, and tools. All of the platforms this paper covers make this clear. In the near future, a setting can be picked and new approaches and methods can be specified for it. Malware may be becoming more potent concurrently. It is advantageous to have in-depth research in this field. The society will then be able to use the Internet without feeling too nervous.

REFERENCES

[1]. Guanlin Chen; Kunlong Zhou; Yubo Peng; Liang Zhou; Yong Zhang "A novel network intrusion prevention system based on Android platform" International Journal of Internet Protocol Technology (IJIPT), Vol. 14, No. 2, 2021
____Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari

[2]. Joaquim Celestino JúNior "Review: An intrusion detection and prevention system in cloud computing: A systematic review" Journal of Network and Computer Applications Vol. 36, No. 1

[3]. Abhishek Kundu, Tamal Kumar Kundu, I Mukhopadhyay "Survey on Intrusion Detection and Prevention System: A MANET Perspective" International Journal of Scientific & Engineering Research Volume 3, Issue 9, September-2012 1 ISSN 2229-5518

[4]. Monika Dorji,Bhusan Trivedi,"Survey of Intrusion and Prevention System in MANET based on data gathering Techniques", doi: 10.5120/ijais12-450153

[5]. Ajay Kumar, K. Abhishek, M.R. Ghalib, A. Shankar, X. Cheng "Intrusion detection and prevention system for an IoT environment" Digital Communications and Networks 2022

[6]. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, P. Faruki, Network intrusion detection for iot security based on learning techniques, IEEE Commun. Surv. Tutorials 21 (3) (2019) 2671–2701.

[7]. Vipparthy Praneeth*, Kontham Raja Kumar, Nagarjuna Karyemsetty "Security: Intrusion Prevention System Using Deep Learning on the Internet of Vehicles"International Journal of Safety and Security Engineering (Vol. 11, No. 3, June, 2021, pp. 231-237)

[8]. Deep Learning basics. https://www.deeplearning.ai/program/deep-learning-specialization/, accessed on January 12, 2021

[9]. WOOSEOK SEO, WOOGUIL PAK "Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning" IEEE Access March 17, 2021

[10]. N. Wattanapongsakorn, S. Srakaew, E. Wonghirunsombat, C. Sribavonmongkol, T. Junhom, P. Jongsubsook, and C. Charnsripinyo, ``A practical network-based intrusion detection and prevention system," in Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun., Jun. 2012, pp. 209_214

[11]. Yeongje Uhm and Wooguil Pak "Real-Time Network Intrusion Prevention System Using Incremental Feature Generation" Computers,Materials & Continua Vol 70 No.1 May 2021

[12]. I. Ahmad, M. Basheri, M. J. Iqbal and A. Rahim, "Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection," IEEE Access, vol. 6, pp. 33789–33795, 2018.

[13]. Hui Li and Dihua Liu "Research on intelligent intrusion prevention system based on Snort" International Conference on Computer, Mechatronics, Control and Electronic Engineering, 2010, pp. 251-253, doi: 10.1109/CMCE.2010.5610483

[14]. Ahmed Adnan, Abdullah Muhammed, Abdul Azim Abd Ghani, Azizol Abdullah and Fahrul Hakim "An Intrusion Detection System for the Internet of Things Based on Machine Learning: Review and Challenges" Symmetry 2021 Volume 13 DO-10.3390/sym13061011

[15]. Chris Clark, Wenke Lee, David Schimmel, Didier Contis, Mohamed Koné, Ashley Thomas "A Hardware Platform for Network Intrusion Detection and Prevention" Center for Experimental Research in Computer Systems (CERCS)

[16]. Amjad Abdallah Abdelkarim, Hebah H. O. Nasereddin "Intrusion Prevention System" International Journal Of Academic Research Vol. 3. No.1. January, 2011, Part II

[17]. Karen Scarfone Peter Mell " Guide to Intrusion Detection and Prevention Systems (IDPS)" Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

[18]. Kanika "Intrusion Detection System and Intrusion Prevention System – A Review Study" International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013 ISSN 2229-5518

[19]. Indraneel Mukhopadhyay, Mohuya Chakraborty, Satyajit Chakrabarti "A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems" Journal of Information Security > Vol.2 No.1, January 2011

[20]. M.Azhagiri, Dr A.Rajesh, Dr S.Karthik "TRUSION DETECTION AND PREVENTION SYSTEM : TECHNOLOGIES AND CHALLENGES" rnational Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.87 (2015)

[21]. Yousef Farhaoui "Design and Implementation of an Intrusion Prevention System" International Journal of Network Security, Vol.19, No.5, PP.675-683, Sept. 2017