ROOTINDEXING
JOURNAL ABSTRACTING AND INDEXING SERVICE
INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
January-June 2023, Submitted in March 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

The Role of Machine Learning in Enhancing Intrusion Prevention Systems for Iot

Bharath GG, Research Scholar, Department of Computer Science, SunRise University, Alwar
Dr. Kamal Kumar Srivastava, Professor, Computer Science, School of Computer Science, SunRise University, Alwar

Abstract

The large and interconnected nature of IoT devices has made maintaining strong security a serious problem as the Internet of Things (IoT) has proliferated. This research investigates how Artificial Neural Networks (ANNs), a kind of machine learning, might improve Intrusion Prevention Systems (IPS) designed for Internet of Things contexts. Conventional IPS techniques are unable to provide sufficient security for Internet of Things devices due to their limitations, including limited battery life and processing power. In order to efficiently identify and stop malicious activity, this research suggests an IPS architecture that is based on machine learning and is able to handle and analyze massive amounts of data provided by Internet of Things devices. An ANN with several hidden layers is used to ensure a dynamic and robust defense mechanism by allowing the system to learn and adapt to new threats. The better capabilities of machine learning models in tackling the particular security concerns of IoT networks are highlighted by the comparative examination of different IPS systems. By using this strategy, the study hopes to show how machine learning can be successfully integrated into IPS to strengthen IoT security against changing cyberthreats.

Keywords: Machine Learning, Intrusion Prevention Systems, Internet of Things (IoT), Artificial Neural Networks (Anns), Intrusion Prevention System (IPS) Technologies.

1. INTRODUCTION

The term "Internet of Things" describes a system of networked devices and goods that are connected to one another through the internet and various methods of computerized communication. It is also possible to think of it as an organization that detects devices connected to the cloud and managed by devices placed within the organization. When one considers how extensive the Internet of Things (IoT) is, it becomes evident how difficult it is to maintain security at each sensor hub. This is especially evident when one has limited knowledge of tools and organizational capabilities.

The term "Internet of Things" (IoT) refers to a network of networked devices and other real objects that may be managed remotely. Different things, such as cars, buildings, and other objects, are included into the framework using equipment, software, sensors, and an organization. It enables data sharing and communication between various devices. Through an association's already-built network base, the Internet of Things paves the door for remote item identification and control. This facilitates the synchronization of this current reality with digital frameworks, leading to increased effectiveness, accuracy, and financial gain.

Every component that is necessary to form the Internet of Things is shown in Figure 1. The device itself, the gateway, the research, the user interface, and the cloud are the components that make up the Internet of Things. A completely new phase in the data innovation sector is being ushered in by the Internet of Things (IoT). When it comes to information mechanization, the PC waiter rack, work stations, and adaptable advanced aids are just the tip of the iceberg. It is now moving in the direction of every nearby item. Most of the items that we use on a regular basis are either linked right now or will be linked soon. They would be able to identify and convey facts about luxury with the aid of the intelligent apps they may interact with. Media, information, and apps are playing a bigger role in the lives of those who are growing more and more connected. It ultimately turns out to be an enhanced net, or skin, for our bodies thanks to technological innovation. We envision a computerized future in our minds, and it's amazing to consider that we may even say, "No Net, No Planet."

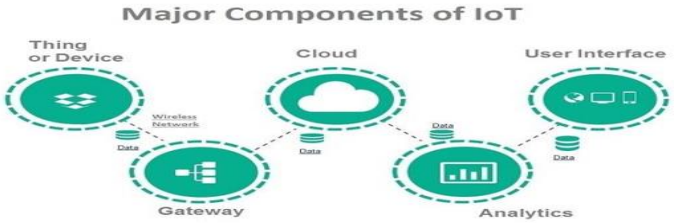

Figure 1: Principal Elements of IOT

2. LITERATURE REVIEW

Mosenia, A., & Jha, N. K. (2016) The Internet of Things (IoT), sometimes known as the Internet of Items, may be a promising way to deliver a variety of services. Smart little devices are key to the Internet of Things. They vary greatly in use, size, energy limit, and computing power. Connecting these smart devices to the Internet raises security issues. This is because most Internet breakthroughs and communication standards did not enable the Internet of Things. Commercialization of the Internet of Things has raised concerns about open security, including individual protection, cyberattacks, and coordinated misbehavior. This paper covers flaws and countermeasures on the edge-side layer of the Internet of Things (IoT), which has three levels: edge hubs, communication, and edge figuring. This overview gives anyone interested in investigating IoT security and improving it a rule. We will briefly describe three major Internet of Things reference models before defining IoT security. We discuss the Internet of Things (IoT)'s potential uses and the minds of those who embrace this new vision. The final section discusses several assaults and hazards. The fourth section discusses opponent of assault tactics. Overall, we discuss two novel security concerns that have been extensively covered in the current collection of work.

Pal, S., Hitchens, et.al., (2020) The number of smart devices and their uses (such as smart sensors, wearable devices, PDAs, smart automobiles, etc.) in our daily lives has grown significantly. Another link between the advanced and real realms is the Internet of Things. This changes the paradigm so that everything can be related via communication. To prevent unauthorized access to assets like apps and services, these systems need advanced security measures. Building secure Internet of Things (IoT) systems requires a deep understanding of their requirements. Current craftsmanship lacks a detailed evaluation of Internet of Things security demands. This article provides a methodical approach to understanding the security demands of the Internet of Things (IoT) to help develop safe IoT systems for the future. We describe these safeguards using several Internet of Things scenarios and associated dangers and threats. After reviewing the Internet of Things (IoT)'s features, we divided the dangers and assaults into five categories: specialized, gadgets and services, users, flexibility, and asset combinations. We then examine the Internet of Things (IoT) security needs in the writing and discuss our approach to meeting them. Our contention is that if the guidelines are followed, an Internet of Things framework can be built safely, delivering a large portion of the guaranteed benefits of versatility, convenience, association, and adaptability in a reasonable and exhaustive manner.

Henze, M., Hermerschmidt, L., et.al., (2016) It is predicted that the Internet of Things will soon permeate every part of the real world, including public and municipal spaces. Combining distributed computing with the Internet of Things (IoT) is the most compelling option because it makes it possible to handle the massive quantity of data that can be collected and to organize services based on that data. However, the genuine security concerns of individual users impede the broader recognition of this appealing concept. This is particularly true for application areas including assisted living, unavoidable medical services, and smart urban communities. Therefore, a key component of turning this idea become reality is how the consumers respond to it. We provide an all-inclusive approach to safety in this envisioned environment to address this pressing element and, consequently, complete the cloud-based Internet of Things for a broad range of diverse application domains. We enable users to enforce all of their security requirements before any sensitive data is moved to the

cloud, we make it feasible for cloud service providers to integrate security features into the most popular method of constructing cloud services, and we provide users with an intuitive and adaptable interface for managing their security requirements.

Ahemd, M. M., et.al.,(2017, April) The Internet of Things, or "IoT" for short, is arguably the most significant advancement in the field of information and communication technology (ICT). Over fifty billion devices are predicted to be connected to the Internet of Things (IoT) in the next years. The first priority should be to confirm the security of the organization that the Internet of Things uses. In this analysis, we examine the security features that were accessible in the four Internet of Things design layers between 2010 and 2016, along with the solutions we propose to address those challenges. Similarly, the context of the Internet of Things also involves the investigation of incredibly fundamental security breakthroughs such as encryption. Overall, we highlight the possibility of future focus on the Internet of Things' architecture and investigate plausible fixes for the security flaws that have been launched against the network's several tiers.

Burhan, M., et.al., (2018) Owing to the increasing number of people using the Internet these days, a new industry that makes use of the Internet has emerged: the Internet of Things (IoT). As a result, it facilitates communication, information gathering, and coordination between the machines and protestors. This breakthrough makes possible knowledge related to many basic components of the modern world, such as houses, clinics, buildings, transportation components, and metropolitan regions. Security and protection are likely the top concerns when it comes to the growing use of the Internet of Things. As a result, these problems hinder the Internet of Things from being extensively adopted. The purpose of this article is to provide an overview of the many layered architectures of the Internet of Things (IoT) and security threats from a layer perspective. In addition, an overview of the elements that address these questions is provided, along with a discussion of the limitations of these cycles. To alleviate these difficulties further, we have put out an extra secure layered architecture for the Internet of Things.

3. INTRUSION PREVENTION USING ARTIFICIAL NEURAL NETWORK IN MACHINE LEARNING

The intrusion prevention system functions in all three of the levels that comprise an Internet of Things ecosystem: perception, network, and application. The thesis materials' previous chapters provide a more thorough discussion of these levels. An intrusion system designed for an Internet of Things network should be built to use minimal computational resources, such as random-access memory (RAM), processing power, and power, in order to provide a quick reaction and extensive data handling capabilities. With their massive computing power and low energy consumption, today's devices have created an Internet of Things environment that is unsuitable for an intrusion prevention system (IPS) that employs traditional preventative tactics. An in-depth study of IoT frameworks, as well as the available security solutions and vulnerabilities, is necessary to assure the security of the Internet of Things (IoT), a crucial and continuous endeavor. A system that is intended to identify security issues on an Internet of Things network is able to read, examine, and analyze the data. Furthermore, the packets can be gradually divided by the system according to the levels and stack. Monitoring the data generated by the devices in the Internet of Things ecosystem on a regular basis is one of the most crucial ways to identify any form of attack. Applications of fine-tuned machine learning techniques and algorithms are necessary for reading and analysing such a large amount of data. Furthermore, in order to provide adequate access to many websites, the data collected from the various phases of the transaction can be processed on cloud computing infrastructure.

4. INTRUSION PREVENTION SYSTEM

The term "intrusion detection and prevention system" is another name for the intrusion prevention system. It is a network security tool that keeps an eye out for potentially harmful activity on networks or systems. The identification of harmful behavior, the gathering of

information about it, reporting of it, and attempts to block or stop it are the main duties of intrusion prevention systems.

Because both intrusion prevention systems (IPS) and intrusion detection systems (IDS) monitor network traffic and system operations for malicious behavior, they are often thought of as an addition to IDS.

IPS usually create reports, alert security administrators to significant observed occurrences, and record information about observed events. In addition, a lot of IPS can try to stop a danger before it ever gets a chance to succeed. They employ a variety of reaction strategies, such as having the IPS halt the assault directly, altering the security setting, or modifying the attack's content.

4.1.Comparison of Intrusion Prevention System (IPS) Technologies

The Table that follows lists the many IPS Technology types:

Table 1: Comparison of Intrusion Prevention System (IPS) Technologies

Type of IPS Technology	Kinds of Malevolent Behavior Found	Range for Each Sensor	Advantages
Network-Oriented	TCP/IP layer activity at the network, transport, and application levels	Several host groups and network subnets	The only tool that can examine the greatest variety of application protocols is IDPS;
Without a cord	Unauthorized usage of wireless local area networks (WLANs); wireless protocol activities	Several WLANs and wireless client groups	Wireless Protocol Activity Prediction is Only Possible with IDPS
NBA	Application, Transport, and Network Activity at the TCP/IP layer that results in unusual network flows	Several host groups and network subnets	Usually superior to the others at recognizing DoS assaults and reconnaissance scans, as well as in reconstructing large malware infections
Web-Based	Network, transport, and application TCP/IP layer activity; host application and operating system (OS) activity	lone host	able to examine data sent during end-to-end encrypted conversations

5. MACHINE LEARNING IN IPS

As was covered in the literature research part, there are several ways to use machine learning in real-world scenarios. An artificial neural network was selected for this investigation in order to train the preexisting dataset. The trained dataset is used to identify potentially dangerous devices and block them from accessing network resources. We have illustrated our training procedure in Figure 2. The training dataset for an artificial neural network (ANN) should have one input, one output, and at least one hidden layer. Consequently, multiple hidden layer architecture is used in the training process. Along with showing that there are three input parameters and one output parameter, the image also shows that there are several hidden layers. The neurons and training functions were changed with each iteration in compliance with the technique used to train the dataset. The minimum, maximum, and average bandwidth of Internet of Things devices are used as input for the training of the dataset, depending on which dataset is used.

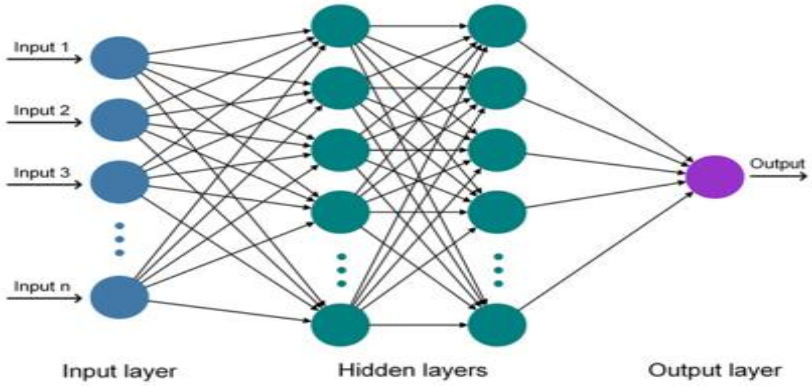

Figure 2:A schematic illustration of an artificial neural network (ANN)

6. CONCLUSION

Intrusion Prevention Systems (IPS) inside the Internet of Things (IoT) ecosystem are much more successful when machine learning is incorporated, particularly with the usage of Artificial Neural Networks (ANNs). The study shows that conventional IPS techniques are insufficient for the particular limitations and specifications of Internet of Things (IoT) devices, which frequently have constrained processing capabilities. The suggested IPS architecture can effectively collect and analyze enormous volumes of data produced by IoT devices, detecting and blocking malicious activity with high accuracy by utilizing the adaptive and dynamic characteristics of ANNs. This methodology not only tackles extant security issues but also offers a scalable resolution that may progress in tandem with the growing intricacy and expansion of Internet of Things networks. For this reason, in the ever-expanding IoT world, implementing machine learning-based IPS is crucial to provide strong and resilient security.

REFERENCES

1. Ahemd, M. M., Shah, M. A., & Wahid, A. (2017, April). IoT security: A layered approach for attacks &defenses. In 2017 international conference on Communication Technologies (ComTech) (pp. 104-110). IEEE.
2. Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. sensors, 18(9), 2796.
3. Chetan, R., &Shahabadkar, R. (2018). A comprehensive survey on exiting solution approaches towards security and privacy requirements of IoT. International Journal of Electrical and Computer Engineering, 8(4), 2319.
4. Dahiya, A., Gupta, B. B., Alhalabi, W., &Ulrichd, K. (2022). A comprehensive analysis of blockchain and its applications in intelligent systems based on IoT, cloud and social media. International Journal of Intelligent Systems, 37(12), 11037-11077.
5. Dhanda, S. S., Singh, B., & Jindal, P. (2020). IoT security: A comprehensive view. Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm, 467-494.
6. Dhar, S., & Bose, I. (2021). Securing IoT devices using zero trust and blockchain. Journal of Organizational Computing and Electronic Commerce, 31(1), 18-34.
7. Gopinath, V., Rao, K. V., & Rao, S. K. (2022). A comprehensive analysis of IoT security towards providing a cost-effective solution: a layered approach. International Journal of Information Technology, 15(7), 3813-3826.
8. Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294.
9. Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., &Wehrle, K. (2016). A comprehensive approach to privacy in the cloud-based Internet of Things. Future generation computer systems, 56, 701-718.
10. Johnson, D., &Ketel, M. (2019). IoT: application protocols and security. International Journal of Computer Network and Information Security, 11(4),.

11. Karmakar, K. K., Varadharajan, V., Nepal, S., &Tupakula, U. (2020). SDN-enabled secure IoT architecture. IEEE Internet of Things Journal, 8(8), 6549-6564.

12. Li, C., Wang, J., Wang, S., & Zhang, Y. (2022). A review of IoT applications in healthcare. Neurocomputing, 127017.

13. Lone, A. H., &Naaz, R. (2021). Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review. Computer Science Review, 39, 100360.

14. Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing, 5(4), 586-602.

15. Pal, S., Hitchens, M., Rabehaja, T., &Mukhopadhyay, S. (2020). Security requirements for the internet of things: A systematic approach. Sensors, 20(20), 5897.