Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 10 Issue: 06 | June-2024

SMART DEFENSES: MACHINE LEARNING-BASED PROACTIVE CYBER ATTACK DETECTION IN IOT SYSTEMS

N.R.Vikram[1] ,K.Divya[2], P.Prakash[3] , S.Keerthika[4],R.Manoj Kumar[5]

[12,3,4.5]Assistant Professor, Department of Computer Science & Engineering, Paavai College of Engineering,Namakkal

---***---

Abstract - One quickly developing technology is the Internet of Things (IoT). Billions of smart objects (called "Things") have the ability to gather information about their surroundings and themselves because of a multitude of sensors. Thus, they could enhance commercial services and activities or control and oversee industrial services. But today more than ever, the Internet of Things is susceptible. The field of machine learning (ML) has made great strides, opening up new research directions to address present and future Internet of Things problems. However, machine learning is a useful technique for spotting danger in networks and intelligent devices. This study will evaluate multiple machine learning algorithms for threat detection and the various security measures related to machine learning techniques after a comprehensive literature review on machine learning methods and the need for IoT security.

Key Words:IoT, IoT Threats and attacks, Machine Learning, Artificial Networks.

1. INTRODUCTION

Internet of Things connects electrical devices to a server and disperses data without requiring human assistance [1-4] [5,6]. Computers can be remotely operated by users from anywhere making them vulnerable to several kinds of attacks. As an as a result, the growing quantity of smart devices available today poses security problems for the IoT system, as the gadgets preserve sensitive and confidential user data [1, 4, 6]. Kevin The term "internet of things" was first used by Ashton in a 1999 presentation of research. IoT has been applied to several connection protocols to create a connection between individuals and the virtual world via smart gadgets and related offerings. [7,8]. For instance, information about the buyer's position, contact details, health, and other details is provided by smart homes and portable gadgets; all of this information needs to be kept private and confidential [9]. Due to resource constraints on the majority of IoT devices (such as limited batteries,

adaptable and sophisticated algorithm-based security solutions are not available [10–12].Systems for image analysis, recommendation, and intrusion detection have incorporated a variety of IoT and machine learning techniques, including as classifiers and deep learning [13, 14].IoT projects can be kept dependable by using machine learning (ML) techniques.

2. RELATED WORKS

The use of ML and DL to improve IoT security based on each tier of the IoT architecture was a critical area that this study added. Numerous vulnerabilities affect IoT devices, people, systems, and apps that could be exploited by an attacker. AI technology connects low computational complexity and high security levels because of the restricted resources of IoT devices. Lately, a lot of innovative solutions have emerged to increase the security of IoT systems, and ML and DL technologies have been utilized more frequently to improve the security of IoT environments.

IoT vulnerability detection has been the subject of numerous previous surveys, with a particular emphasis on firmware and IDS. A summary of the most pertinent ones encourages us to move forward with our contributions in this paper. Neshenko et al. addressed the dynamic nature of IoT vulnerabilities and provided an explanation of a thorough method for classifying state-of-the-art surveys in [12]. Furthermore, although [15] detailed the popular IoT communication protocols and how they implemented certain security procedures to make a comparison of the taken into consideration IoT technologies, [13, 14] and [15] concentrated only on discovering vulnerabilities in IoT firmware. On the other hand, a publication evaluated the most recent research and discussed IoT vulnerabilities, but it didn't delve further into the ML and DL methods that are employed to increase IoT security [16]

3. IoT LAYERS & ATTACKS

The network of physical objects, or "things," that have sensors, software, or other technologies installed in order to connect and exchange data via the internet is referred to as "the Internet of Things" (IoT). Both in the office and at home, a lot of these devices are common. Nowadays, anything from a tablet to an airplane may be integrated into the Internet of Things [19–22] because of the advancement of affordable computer processors and widespread wireless networks. By connecting and adding sensors, artificial intelligence can be applied to normally inanimate objects so that they can transmit real-time data without the assistance of a human.

Our civilization will get more intelligent and adaptable thanks to the Internet of Things (IoT) [18, 23–25]. In order to create a connection and improve IoT services at each entryway, the IoT architecture serves as a gateway to several hardware applications [16]. Numerous networking protocols, including Bluetooth, Wi-Fi, RFID, narrow and broadband, ZigBee, and LPWAN, are utilized to deliver and receive data from various IoT architecture levels [13, 17].The majority of an IoT architecture is composed of the physical, network, and application layers [18, 19]. Internet of Things device security has been a popular topic in the twenty-first century. IoT, on the one hand, links and draws people worldwide closer together. However, it also provides multiple ports of entry for various kinds of attacks. [10–12].Devices are made more user-friendly by IoT applications, which are used for a range of purposes across an open network [23]. The Internet of Things makes human existence more difficult and technically more submissive, but it also puts it at risk due to innumerable threats and attacks. [24, 15].

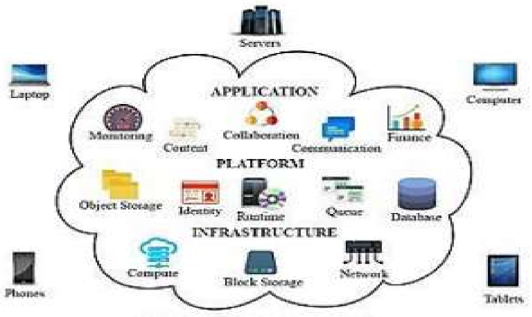

Figure 1: Application Layer devices in IoT

Maintaining information private means keeping it hidden from outsiders. For example, while handling sensitive military data, sensitive sensors require secrecy. The Wireless Sensor Network (WSN) capability is one of the most often requested features. If a WSN's reports can be fabricated to the enemy's advantage, forces could be duped. Equal importance is given to confidentiality in crucial industrial and social applications [19].

The communication receiver must ensure that messages received during transmission or delivery have not been changed in order to preserve the integrity of IoT data. Data integrity guarantees that the provided information is not altered or interfered with. It is particularly crucial because if compromised nodes tamper with the data they send, the network might not work correctly even if attackers are prevented from accessing the data. In fact, data can be changed without the help of an outsider if the communication link is faulty. Integrity management makes sure that message alterations, whether deliberate or inadvertent, are identified [19]. The authentication process confirms whether a communication comes from the person who is supposed to receive it. It is proclaimed or asserted to be the truth. The sensor nodes bear the responsibility of ascertaining the legitimacy and identity of the peer node with which they are establishing communication.
Authenticity ensures that the communication is sincere. A piece of data called the Communication Authentication Code (MAC) is utilized to confirm the validity and integrity of a message [19, 20].

4. IoT ATTACKS AND THEIR EFFECTS

In recent years, there have been various attacks on the Internet of Things (IoT), which has increased the vigilance of both IoT makers and consumers. This section covers effects, attacks, and IoT surfaces. The two main types of IoT assaults are cyber and physical. Cyberattacks can be either passive or aggressive, as shown in Figure 2. The user's data on a wireless network could be lost, altered, stolen, or destroyed by a cyber-attack threat that targets a lot of wearable technology. On the other hand, human assaults could cause physical harm to IoT devices. This kind of device attack doesn't require a network connection.

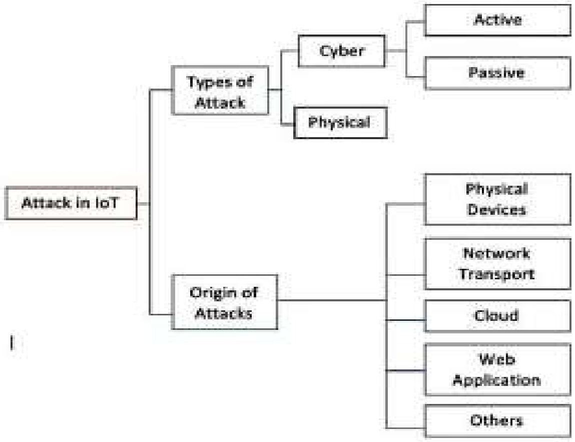

Figure 2: IoT Attacks

Active IoT Attacks

An active assault occurs whenever a hacker takes over a computer network and stops providing necessary services. Attackers may employ a variety of techniques to undermine IoT device security, including interventions, disruptions, and modifications to current attacks.

Denial of service attacks

As may be observed, the most common cause of system outages is disruptions in system services, or denial-of-service (DoS) attacks. Stated differently, the IoT gadget prevents the user from making well-informed decisions. Because IoT devices are used constantly, DoS attacks shorten their battery life[16–18]. The goal of "distributed denial of service" (DDoS) assaults is to overwhelm servers with too many requests. As a result, it is hard to distinguish between harmful and lawful transmissions.

Spoofing Attacks

Sybil and spoofing attacks are commonly used to gain unauthorized access to Internet of Things (IoT) systems. Because TCP/IP does not have a full security protocol, IoT devices are particularly vulnerable to spoofing attacks. These two attacks initiate denial of service attacks as well as man-in-the-middle attacks.

They were jamming attacks: as demonstrated, constantly busy due to undesired signals being transmitted to IoTT devices, which maintains continuous wireless network connectivity. This kind of assault makes matters worse by using more memory, bandwidth, and other resources in IoT systems [10].

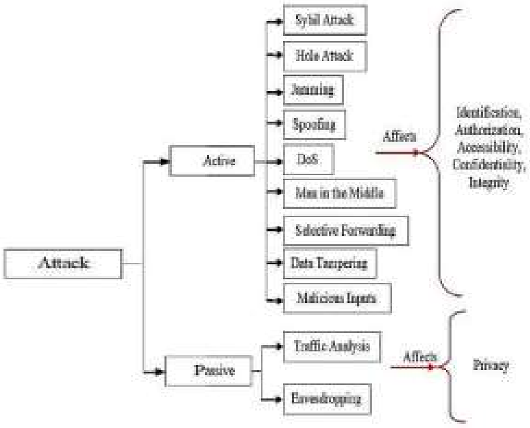

Figure 3: Active & Passive Attacks with their effects

Man in the Middle attack

Attacks known as "man-in-the-middle" are executed by network users who have a direct connection to a different user interface. Therefore, tampering with the original data with erroneous or fraudulent information is a simple method to obstruct communication.

5. MACHINE LEARNING APPLICATIONS IN IOT ATTACK DETECTION

ML uses a variety of techniques to train machines, allowing them to pick up new skills by experience rather than explicit programming [16]. Large networks, complex mathematical procedures, or human input are not required for machine learning [25]. There have been notable advancements recently in machine learning (ML) for IoT security. As a result, ML techniques may be able to identify unique IoT attacks by analyzing system behavior in advance. Furthermore, combining various ML algorithms could provide suitable solutions for Internet of Things devices with constrained resources. This section is divided into two subsections: ML Techniques and ML-based IoT Security Technologies [16].

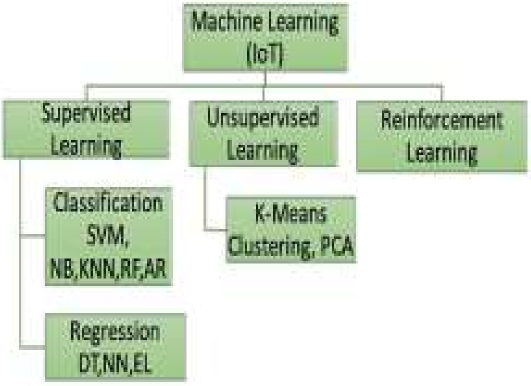

Figure 4: Machine learning Techniques

ML techniques including reinforcement learning, unsupervised techniques, and supervised techniques can be used to secure IoT devices. Figure 3 shows a range of machine-learning methods for IoT device security.Supervised learning, which uses an algorithm to assess the output in accordance with the input, is the most widely used machine learning technique. Regression and classification are two categories of supervised learning. For these input variables, there are no output data in unsupervised learning. Most of the data is kept unlabeled since the algorithm looks for patterns in the information it gathers. These clusters consist of different classes.

6. CONCLUSION

The Internet of Things will revolutionize the world in the future by giving us access to global themes. Users of IoT smart services will therefore be able to share and save data virtually anywhere they have internet access. IoT gadgets connect us to the virtual world and make our lives faster, easier, and more straightforward, yet their security raises concerns. This article examines a wide range of security concerns, algorithms, and solutions for the Internet of Things utilizing machine learning (ML) (IoT) in-depth based on a thorough assessment of the literature. With an emphasis on embedded machine learning methods, this study offers a broad review of various Internet of Things hazards and their consequences. In order to assist future researchers in outlining their ultimate goals and objectives, scholars have also examined machine learning algorithms.

REFERENCES

[1] Khan MA, Salah K. "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems. 2018;82:395-411.

[2] Farooq M. Supervised learning techniques for intrusion detection system based on multi-layer classification approach. International Journal of Advanced Computer Science and Applications. 2022;13(3).

[3] Lu Y, Da Xu L. "Internet of Things (IoT) cybersecurity research: A review of current research topics," IEEE Internet of Things Journal. 2018;6:2103-2115.

[4] Singh RP, Javaid M, Haleem A, Suman R. "Internet of things (IoT) applications to fight against COVID-19 pandemic," Diabetes & Metabolic Syndrome: Clinical Research and Reviews. 2020;14:521-524.

[5] Farooq M, Hassan M. IoT smart homes security challenges and solution. International Journal of Security and Networks. 2021;16(4):235-43.

[6] Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. "A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues," IEEE Communications Surveys & Tutorials. 2020;22:1191-1221.

[7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," IEEE Access. 2019;7:82721-82743.

[8] Farooq M. Genetic algorithm technique in hybrid intelligent systems for pattern recognition. International Journal of Innovative Research in Science, Engineering and Technology. 2015;4(04):1891-8.

[9] Adat V, Gupta B. "Security in Internet of Things: Issues, challenges, taxonomy and architecture," Telecommunication Systems. 2018;67:423-441.

[10] Fawzi LM, Alqarawi SM, Ameen SY, Dawood SA. "Two Levels Alert Verification Technique for Smart Oil Pipeline Surveillance System (SOPSS)," International Journal of Computing and Digital Systems. 2019;8:115-124.

[11] Al-Sultan MR, Ameen SY, Abduallah WM. "Real Time Implementation of Stegofirewall System,"

[12] International Journal of Computing and Digital Systems. 2019;8:498-504.

[13] Farooq M, Khan MH. Artificial Intelligence-Based Approach on Cybersecurity Challenges and Opportunities in The Internet of Things & Edge Computing Devices. International Journal of Engineering and Computer Science. 2023 Jul;12(07):25763-8.

[14] Ammar M, Russello G, Crispo B. "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications. 2018;38:8- 27.

[15] Chernyshev M, Baig Z, Bello O, Zeadally S. "Internet of things (iot): Research, simulators, and testbeds," IEEE Internet of Things Journal. 2017;5:1637-1647.

[16] Farooq M, Khan MH. Signature-Based Intrusion Detection System in Wireless 6G IoT Networks. Journal on Internet of Things. 2022 Jul 1;4(3).

[17] Vashi S, Ram J, Modi J, Verma S, Prakash C. "Internet of Things (IoT): A vision, architectural elements, and security issues," in 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). 2017;492- 496.

[18] Sharma B, Sharma L, Lal C. "Anomaly Detection Techniques using Deep Learning in IoT: A Survey," in 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). 2019;146-149.

[19] Farooq M. Application of genetic algorithm & morphological operations for image segmentation. International Journal of Advanced Research in Computer and Communication Engineering. 2015 Mar;4(3):195-9.

[20] Costa KA. da, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," Computer Networks. 2019;151:147-157.

[21] Hussain F, Hussain R, Hassan SA, Hossain E. "Machine learning in IoT security: Current solutions and future challenges," IEEE Communications Surveys & Tutorials. 2020;22:1686- 1721,

[22] Farooq M, Khan R, Khan MH. Stout Implementation of Firewall and Network Segmentation for Securing IoT Devices. Indian Journal of Science and Technology. 2023 Sep;16(33):2609-21.

[23] Othman A, Ameen SY, Al-Rizzo H. "Dynamic Switching of Scheduling Algorithm for," International Journal of Computing and Network Technology. 2018;6.

[24] Arko AR, Khan SH, A. Preety, M. H. Biswas, "Anomaly detection In IoT using machine learning algorithms," Brac University; 2019.

[25] Farooq M. Optimizing pattern recognition scheme using genetic algorithms in computer image processing. International Journal of Advanced Research in Computer Engineering & Technology. 2015 Mar;4(3):834-6.

[26] Hassan RJ, S. R. Zeebaree, S. Y. Ameen, S. F. Kak, M. A. Sadeeq, Z. S. Ageed, et al., "State of Art Survey for IoT Effects on Smart City Technology: Challenges, Opportunities, and Solutions," Asian Journal of Research in Computer Science. 2021;32-48.