International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Survey of Secure IoT using Machine Learning Approach

Asst. Prof. Monali Suthar, Dr. Satvik Khara,

Computer Engineering Department & Silver Oak College of Engineering and Technology, Silver Oak University
Computer Engineering Department & Silver Oak College of Engineering and Technology, Silver Oak University

---

Abstract – The future Internet of Things (IoT) will have a deep economical, commercial and social impact on our lives.[1] The participating nodes in IoT networks are usually resource constrained, which makes them luring targets for cyber-attacks [1]. Internet of Things security is attracting a growing attention from both academic and industry communities. Indeed, IoT devices are prone to various security attacks varying from Denial of Service (DoS) to network intrusion and data leakage [2]. The disruptive acceleration of Internet of Things (IoT)is drastically modifying the current ICT landscape with a massive number of cellular IoT devices expected to be deployed in the next few years. IoT devices are taking over a variety of aspects of our current lives, such as health care, transportation, and home environments [2].

***Key Words*:** IOT, Machine Learning, Cyber Security, Security Attacks, Security, data privacy

1.INTRODUCTION

IoT is considered as an interconnected and distributed network of embedded systems communicating through wired or wireless communication technologies. IOT defined as a network of physical object or things empowered with limited computation, storage and communication capabilities as well as embedded with electronics, software and network connectivity that enable these devices to collect, sometimes process, and exchange data. Things in IOT are the smart object from daily life [6]. There are a plethora of applications and services offered by the IoT ranging from critical infrastructure to agriculture, military, home appliances, and personal health-care [7] . The huge scale of IoT networks brings new challenges such as management of these devices, sheer amount of data, storage, communication, computation, and security and privacy [1]. However, the cornerstone of the commercialization of IoT technology is the security and privacy guarantee as well as consumer satisfaction. The fact that IoT uses enabling technologies such as Software-Defined Networking (SDN), Cloud Computing (CC), and fog computing, also increases the landscape of threats for the attackers[8].

IoT devices generate amount of data and process it and therefore , some traditional techniques for data collection , processing and communication may not work. These collected and processed data will able to use detect some patterns, behaviors and predictions. Machine Learning will be consider as a most suitable option to process on data collected and processed by IoT devices to provide the intelligence to the IoT network devices.

Machine Learning will provide the automation and will also help to detect the pattern or knowledge form the IoT devices. Machine Learning regression , classification and deep learning algorithms will be used in various IoT applications like health care, agriculture , home appliances and military. In this paper we will focus on the application of ML to provide security and privacy in IoT. We will discuss various ML techniques for securing IoT.

The rest of the paper is structured as follows: Section II presents a brief background and motivation while Section III explains the current IoT threat detection research advances. The IoT challenges are discussed in Section IV followed by the future research directions in Section V. Finally, conclusions are given in Section VI.

1. Background and Motivation

2.1 Three Layer IoT Architecture

The abstract level of IoT model contains various physical devices, or sensors i.e. controllable sensors, RFID (Radio Frequency Identifications), IoT getaways, web servers as depicted in Figure 1.

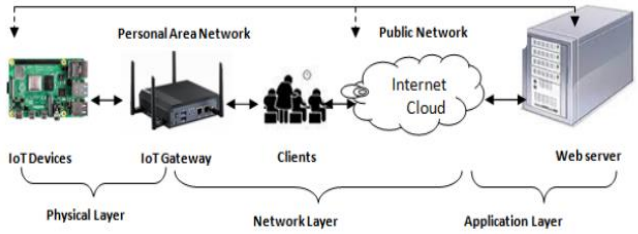

Figure 1 : IoT Layered Architecture

The general IoT architecture divides in 3 layers i)Physical Layer ii) Network Layer iii) Application layer. Physical layer also known as perception layer. The perception layer takes care of the IoT devices or sensors [10]. Network layer work as an intermediate layer between physical layer and application layer. Application layer stands for the end application which uses IoT technologies.

It is predicted that, the number of connected Internet of Things (IoT) devices will rise to 38.6 billion by 2025 and an estimated 50 billion by 2030 [4]. The increased deployment of IoT devices into diverse areas of our life has provided us with significant benefits such as improved quality of life and task automation[4]. However, each time a new IoT device is deployed, new and unique security threats emerge or are introduced into the environment under which the device must operate.

The IoT security is a fervent research area which attracts a rising amount of attention from the research community. Different techniques can address a variety of IoT attacks [3]. Cyber security is the set of technologies and processes designed to protect computers, networks, programs, and data from attack, unauthorized access, change, or destruction. Cyber security system is composed of network security and host(device) security. Cyber security collect the set of techniques to protect network devices, network, process and data from various attacks, unauthorized access. Firewall and antivirus are basic solution form cyber-attack.

2.2 Security Issues on IoT

In IoT many sensor devices and smart peoples are connected with each other through Internet to provide services at anytime, anywhere, and any types of services. IoT owing to the wide range of impact on daily life, all the sensor devices are connected through Internet and all are also vulnerable to all privacy and security issues like authenticity, confidentiality and integrity.[9]

Secure Network Requirements :

Data/Device Authentication : Data collected and communicated from secured and authenticated devices. Devices must followed some protocols for the same.

Client Privacy : At the client application processed and computed data must be secured and safe. Only authenticated devices can be communicate data from client application.

Access Control : Application devices and data must be protected by the other user. Every user device need to follow authentication methods like username and password.

Resilience to attacks : During the process and transmission of data any device fails , data of device must be recoverable.

There are major two IoT security and privacy issues, data security and monitoring and tracing of fraudulent activities.[11] Data are include in IoT application on large scale and when it is about data privacy and security of data are always concerned. IoT applications suffers due to response time during data communication and scalability of devices. IoT application faces security challenge and issue because of Insecure network services, Insufficient authentication or authorization, Poor physical security[12].

Security challenges:

Data Privacy : Collected data by devices and communicated data between various devices must be secured.

Lack of Security Standard : IoT application use many devices connected and communicate with each other. Each application use various security standard. Proper security standard is necessary for the application.

System/Application vulnerability : IoT application security is combination of device security and network security. To secure IoT application we require to secure application device and network for communication with various devices.

Security attacks:

IoT architecture use different devices and technology for communication not bounded with IPv6, Zigbee, 6LoWPAN, Bluetooth, Z-Wave, WiFi, and Near Field

Communications (NFC), RFID. All the IoT devices and technology have their own limitations from the performance and security point of view. Deployment of large number of devices in network increases the chances of security attacks. IoT application suffers from security attacks in all architecture layers. Security attacks in IoT can be abstractly divided into physical, network, transport, application, and encryption attacks. [1]

Physical Layer Attacks : In the physical layers attacker have direct access to the devices. Device cloning and eavesdropping are the attacks possible in physical layers. [13] By having physical access of device attackers can modify the working of devices or they can change the device with malicious devices to impact the communication of application.

Network Layer: IoT combines various communication technologies at the lower layers of TCP/IP protocol stack and thus-forth provides a complex heterogeneous network.[1] Yang et al.[14] has mentioned the security issues in IoT layers in details. At the link layer, different security requirements such as confidentiality, data authenticity and integrity, semantic security and security against different attacks such as replay attacks, and access control are supported by the IEEE 802.15.4. AES, cipher block chaining (CBC) or any mode of AES can be useful providing confidentiality if data during the communication.

2. Existing Surveys

IoT has a rich literature , many surveys have been published that cover different aspects of the IoT security. In this section of paper we will discuss the existing surveys and compare them with each others.

To the best of our knowledge, most of the surveys in the literature do not focus on the ML techniques used in IoT. Various studies utilizing static, dynamic, hybrid, and memory analysis methods have been conducted to analyze how malware works and how code flows prior to its detection. Most of the methods checks overall the security aspect of the architecture.

Mario Frustaci et al. [17] describe the order on IoT security in the different layers of IoT. The authors taxonomically analyze the three key layers of IoT system model i.e perception (Physical layer), transportation (Network layer) and application levels (Application layer). Their approach represents a fertile ground to overcome the cyber threats. Due to limited resources of IoT architecture this generic policy fails to address all the security aspects of IoT.

Other ways to analyze the security aspects in different layers of IoT application architecture. the IoT. Shivang vashi et. al. [15] and Kiwoony Kwon et al. [16] deals with some security issues in different layers. These two authors mainly focused on illegal authorization, also focus on malicious code injection, DoS, Spear phishing, and Sniffing etc.

Other than Security attacks services of application like storage service, information or data privacy, access control , data communication , authentication of devices and durability of IoT devices during the various operations are also important aspect while design the security architecture of IoT application. V. Kherechenko et al. [18] focused on the security in SBC application. In this author is focused on the reliability of the application and security at different layers.

IoT application security depends on architecture and application domains and end application user devices like mobile app, smart energy, smart home and road transportation ,smart agricultures and many more. describe in their survey, about the new threats for the security issues at different levels of IoT architecture.

3. Conclusion

IoT applications are basically depends on architectures and end devices. Security and privacy also differs from architectures and protocols. All IoT layers have their own security issues. Physical layer of IoT architecture suffer from device authentication, device cloning and eavesdropping. Network layers have data security issues which can be solve using AES,DES or any security algorithm. Machine learning approach can be

apply on every level of architectures and various security issues.

In future we can focus on deep learning approaches from Machine Learning to analyze various security and privacy issues like malicious code injection, DoS, Spear phishing, and Sniffing and instruction detection in IoT architecture of various application domain.

REFERENCES

1. Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain "Machine Learning in IoT Security: Current Solutions and Future Challenges" IEEE April 2020.
2. miloud bagaa, tarik taleb, jorge bernal bernabe and antonio skarmeta "A Machine Learning Security Framework for IoT Systems" IEEE Access IEEE 2020
3. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2020.
4. Nickson M. Karie, Nor Masri Sahri, Paul Haskell-Dowland "IoT Threat Detection Advances, Challenges and Future Directions.", May 27,2020 ,IEEE.
5. Arunan Sivanathan , Hassan Habibi Gharakheili , and Vijay Sivarama "Managing IoT Cyber-Security Using Programmable Telemetry and Machine Learning" Ieee Transactions On Network And Service Management, Vol. 17, No. 1, March 2020
6. O. Novo, N. Beijar, and M. Ocak, "Capillary Networks - Bridging the Cellular and loT Worlds ," IEEE World Forum on Internet of Things (WF-IoT), vol. 1, pp. 571–578, December 2015.
7. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol. 17, pp. 2347–2376, Fourthquarter 2015.
8. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging sdn and nfv security mechanisms for iot systems," IEEE Communications Surveys Tutorials, vol. 21, pp. 812–837, Firstquarter 2019
9. Debabrata Singh, Pushparaj, Manish Kumar Mishra, Anil Lamba, Sharabanee Swagatika, "Security Issues In Different Layers Of IoT And Their Possible Mitigation" International Journal Of Scientific & Technology Research Volume 9, Issue 04, April 2020.
10. Burhan,M., Rehman,R.A., Khan, B. and Kim, BS.,(2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors 2018, 18, 2796; doi:10.3390/s18092796
11. Chandrika Sai Priya.Integrated Framework for Multi-User Encrypted Query Operations on Cloud Database Services, International Journal of Cloud-Computing and Super-Computing, Vol. 3, No. 2. Dec. 2016, pp:1-6.
12. Frustaci, Mario, P. A. C. E. Pasquale, A. L. O. I. Gianluca, and Giancarlo FORTINO., "Evaluating critical security issues of the IoT world: Present and Future challenges", IEEE Internet of Things Journal (2017).
13. S. Benzarti, B. Triki, and O. Korbaa, "A survey on attacks in internet of things based networks," in 2017 International Conference on Engineering MIS (ICEMIS), pp. 1–7, May 2017.
14. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," IEEE Internet of Things Journal, vol. 4, pp. 1250–1258, Oct 2017.
15. Vashi, Shivangi, Jyotsnamayee Ram, Janit Modi, Saurav Verma, and Chetana Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues", In I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference on, pp. 492-496, IEEE, 2017
16. Kwon, Kiwoong, Dongsoo Kim, and Daeyoung Kim, "Oliot-Discovery Service: Dealing with Performance and Security Issues from Intra-DS Aspect for IoT", In Global Communications Conference (GLOBECOM), 2016 IEEE, pp. 1-6, 2016.
17. Kharchenko, Vyacheslav, Maryna Kolisnyk, Iryna Piskachova, and Nikolaos Bardis, "Reliability and Security Issues for IoT-based Smart Business Center: Architecture and Markov Model", In Mathematics and Computers in Sciences and in Industry (MCSI), 2016 Third International Conference on, pp. 313-318, IEEE, 2016.
18. D. Kozlov, J. Veijalainen, and Y. Ali, "Security and Privacy Threats in IoT Architectures," in Proceedings of the 7th International Conferenceon Body Area Networks,ICST, Brussels, Belgium, pp. 256–262, 2020