A SURVEY ON IoT ATTACKS

Anu V Jacob
Research Scholar, APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala, India

Niyah Meriyam Mathew
Mar Athanasius College of Engineering, Kothamangalam, Kerala, India
niyahmeriyam@gmail.com

Dr. Elizabeth Issac
Mar Athanasius College of Engineering, Kothamangalam, Kerala, India

Abstract- *Over the past ten years, the Internet of Things (IoT) has paved the way for society's ongoing digitalization in a number of ways. The IoT is a vast network of intelligent devices exchanging data online. Since the Internet of Things may involve safety-critical processes and the online storage of sensitive data, its security component is essential given its quick development as a new technological paradigm. Regretfully, the biggest obstacle to using Internet of Things (IoT) technologies is security. Therefore, enhancing the security of IoT devices has become a primary goal for manufacturers and researchers. Many problems and potential solutions are covered in the extensive amount of literature on the topic. Nevertheless, the majority of current research falls short in providing a thorough understanding of IoT assaults. So, the purpose of this survey is to provide valuable insights for researchers to fortify the resilience of IoT systems in an increasing interconnected world. It utilizes the four-layer IoT architecture as a reference to identify security issues with corresponding solutions. A comprehensive analysis of the countermeasures offered in academic literature.*

Key words – *Internet of Things (IoT) Security, Privacy, Issues Networks.*

1. Introduction

The concept of the Internet of Things has been introduced by Kevin Ashton in 1999. IoT aims to link anything at anytime in anyplace [1]. Physical devices ranging in size from minuscule to massive machines that ideally connect with one another over the Internet without the need for human intervention are included in the Internet of Things [2]. The IoT devices are provided with sensors to capture data and actuators to autonomously and intelligently perform actions [3]. Last few years, the IoT has gained significant attention since it brings potentially enormous benefits to the human. The primary objective of the IoT is merging of these numerous diverse application domains under the same umbrella referred as smart life [4]. Shortly, billions of devices expected to be linked to the Internet [5]. Hence, an increasingly huge amount of data will flow within the Internet [6]. This data can face several security attacks such as eavesdropping and altering. Consequently, the user's privacy will be threatened [7].

But the extensive use of IoT devices has also revealed serious security flaws that endanger system integrity, data privacy, and network resilience as a whole. This article explores the complex world of IoT security threats and difficulties while highlighting the promise of IoT to spur innovation and improve social services. IoT ecosystems face a variety of intricate security threats, ranging from malevolent cyberattacks that target IoT devices to the exploitation of flaws in network protocols and data transmission systems. Through a comprehensive examination of existing security frameworks, emerging technologies, and best practices, we seek to provide valuable insights and practical solutions for enhancing the security posture of IoT deployments.

Architecture of IOT

The architecture of IoT is divided into 4 different layers i.e. Sensing Layer, Network Layer, Data processing Layer, and Application Layer.

- **Sensing Layer:** The sensing layer is the first layer of the Internet of Things architecture and is responsible for collecting data from different sources. This layer includes sensors and actuators that are placed in the environment to gather information about temperature, humidity, light, sound, and other

physical parameters. Wired or wireless communication protocols connect these devices to the network layer.

- **Network Layer:** The network layer of an IoT architecture is responsible for providing communication and connectivity between devices in the IoT system. It includes protocols and technologies that enable devices to connect and communicate with each other and with the wider internet. Examples of network technologies that are commonly used in IoT include WIFI, Bluetooth, Zigbee, and cellular networks such as 4G and 5G technology. Additionally, the network layer may include gateways and routers that act as intermediaries between devices and the wider internet, and may also include security features such as encryption and authentication to protect against unauthorized access.

- **Data processing Layer:** The data processing layer of IoT architecture refers to the software and hardware components that are responsible for collecting, analyzing, and interpreting data from IoT devices. This layer is responsible for receiving raw data from the devices, processing it, and making it available for further analysis or action. The data processing layer includes a variety of technologies and tools, such as data management systems, analytics platforms, and machine learning algorithms. These tools are used to extract meaningful insights from the data and make decisions based on that data. Example of a technology used in the data processing layer is a data lake, which is a centralized repository for storing raw data from IoT devices.

- **Application Layer:** The application layer of IoT architecture is the topmost layer that interacts directly with the end-user. It is responsible for providing user-friendly interfaces and functionalities that enable users to access and control IoT devices. This layer includes various software and applications such as mobile apps, web portals, and other user interfaces that are designed to interact with the underlying IoT infrastructure. It also includes middleware services that allow different IoT devices and systems to communicate and share data seamlessly. The application layer also includes analytics and processing capabilities that allow data to be analyzed and transformed into meaningful insights. This can include machine learning algorithms, data visualization tools, and other advanced analytics capabilities[11].

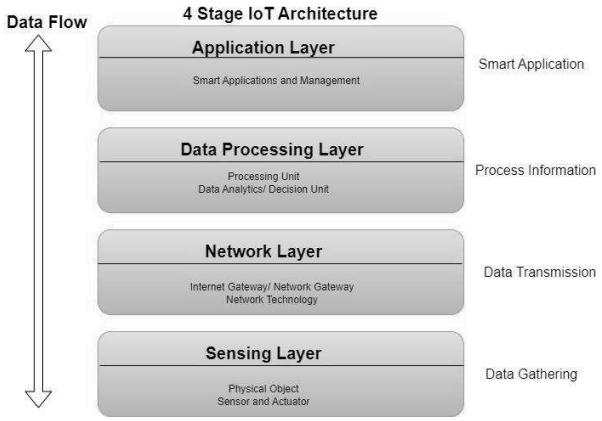

Fig. 1: Architecture of IoT

2. Methodology

Smart devices have different functions or hardware capabilities and therefore, different threat models. While some devices are connected to the network and wait for instructions, others are actively sending out data. Consequently, the attacks against these devices and their intended outcome vary.

Security Issues

The goal of IoT security is to defend against cyberattacks on the devices, networks, and business processes they enable. As the number of IoT devices continues to rise, IoT security is becoming increasingly important. As the number of devices with internet access increases along with their importance in both personal and professional lives, fraudsters have more potential ports of entry.

Numerous complex security risks affect IoT networks. It's possible that the Internet of Things' extensive network of interconnected gadgets is too complicated for conventional cybersecurity methods and tools to manage. One of the biggest challenges is protecting IoT devices, which often lack basic security features and are incompatible with modern security technology. Moreover, IoT security must protect the networks.

IOT Security Concerns and Challenges

1. Weak Authentication and Authorization

Weak authorization mechanisms can also pose a security risk. Many IoT devices come with default usernames and passwords that are often easy for attackers to guess. If an attacker gains access to a device, they may be able to perform unauthorized actions or access sensitive data [8].

2. Memory and Processing Power Limitations

IoT devices often have limited memory and processing power. This can make it challenging to implement robust security measures, as these often require significant computational resources. There are ways to enhance the security of IoT devices with limited resources. This could involve using lightweight encryption algorithms, employing secure coding practices, and leveraging dedicated on-device security solutions [9].

3. Insecure Communications Protocols and Channels

If the data transmitted between devices and the network is not properly secured, it can be intercepted and manipulated by attackers. This could lead to data breaches, device malfunction, or even network-wide attacks. IoT devices commonly use proprietary communication protocols, many of them are insecure, making them susceptible to man in the middle (MitM) attacks [11].

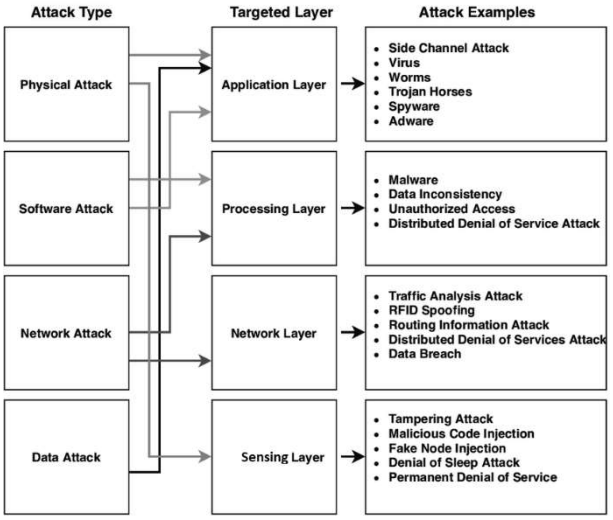

Fig. 2: Different layers of Attacks

3. Results and Discussions

IOT Incidents in 2023

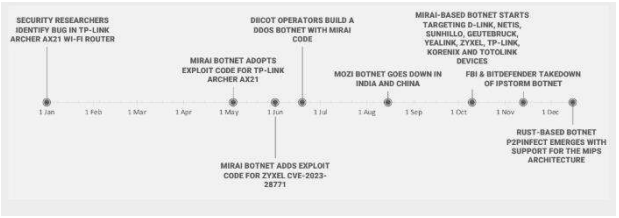

Fig. 3: Different Iot Incidents in 2023

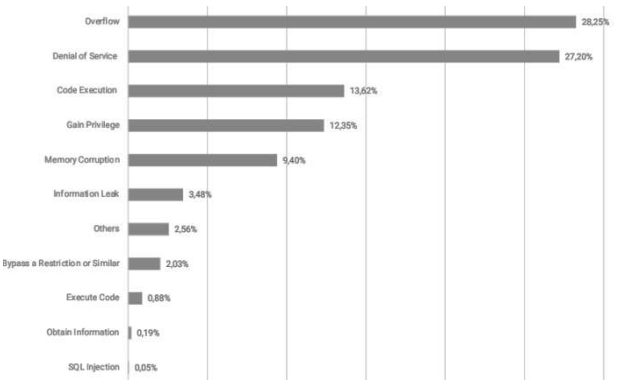

Fig. 4: Vulnerabilities by targeted outcome

4. Conclusion

The explosion of Internet of Things (IoT) devices has brought about a plethora of security and privacy challenges. Vulnerabilities in popular IoT frameworks that connect devices to their clouds can expose tens of millions of users to privacy risks. These vulnerabilities highlight the pervasive risks associated with IoT devices, which often suffer from inadequate security measures and slow

patching cycles. As the number of connected devices continues to proliferate across various industries and sectors, as well as at home, we can expect to see a significant increase in regulatory efforts aimed at establishing comprehensive IoT security standards and guidelines [12].

References

[1] Gubbi, j., buyya, r., marusic, s., & palaniswami, m. (2013). Internet of things (iot): a vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645.

[2] Yan, z., zhang, p., & vasilakos, a. V. (2014). A survey on trust management for internet of things. Journal of network and computer applications, 42, 120.

[3] Saif, i., peasley, s., & perinkolam, a. (2015). Safeguarding the internet of things: being secure, vigilant, and reilient in the connected age. Deloitte review, 17. https://www2.deloitte.com/ insights /us/en/ deloitte review/issue-17/internet-ofthings-datasecu rity-and-privacy.html.

[4] Vermesan, o., & friess, p. (2013). Internet of things: converging technologies for smart environments and integrated ecosystems. Aalborg: river publishers.

[5] Singh.S, & Singh.N. (2015). In 2015 international conference on green computing and internet of things. Ieee.

[6] Borgohain, t., kumar, u., & sanyal, s. (2015). Survey of security and privacy issues of internet of things. Arxiv preprint arxiv:1501.02211.

[7] Jing, q., vasilakos, a. V., wan, j., lu, j., & qiu, d. (2014). Security of the internet of things: perspectives and challenges. Wireless networks, 20(8), 2481.

[8] Internet of things security: challenges and key issues M Azrour, J Mabrouki, A Guezzaz - Security, 2021 - Wiley Online Library.

[9] Security challenges and limitations in IoT environments SI Al-Sharekh, KHA Al-Shqeerat - Int. J. Comput. Sci. Netw. Secur, 2019 - academia.edu

[10] New security architecture for IoT network F Olivier, G Carlos, N Florent - Procedia Computer Science, 2015 – Elsevie.

[11] A feature exploration approach for IoT attack type classification M Erfani, F Shoeleh, S Dadkhah, B Kaur… - 2021 IEEE Intl Conf …, 2021 - ieeexplore.ieee.org

[12] SPF: An SDN-based middleware solution to mitigate the IoT information explosion M Tortonesi, J Michaelis, A Morelli, IEEE Symposium, 2016 - ieeexplore.ieee.org

