The Advance of Internet of Things Security Threats and Possible Measures

Beige He *

School of Cyberspace Security, Beijing Institute of Technology, Beijing, China

* Corresponding author: 1120202782@bit.edu.cn

Abstract. The Internet of Things (IoT) is a new stage of human informatization development after the Internet. With the IoT, physical devices can seamlessly exchange and process data with each other, further improving the human ability to process information. However, Internet of Things security research is still preliminary despite frequent data breaches and security incidents. This paper starts with the introduction of the IoT and introduces its definition, technical characteristics, and hierarchical architecture of the IoT. After that, the security threats that may be encountered at each layer are discussed, and finally, the ways to enhance the security of IoT. This paper aims to examine the security issues that arise in the IoT system and investigate the security measures that can be employed to serve as security technology guidelines for constructing secure IoT systems.

Keywords: IoT security, Security Technology, Security Measures, IoT Architecture.

1. Introduction

The origin of the IoT can be dated back to November 17, 2005, when the ITU released its Report: ITU Internet Report 2005: Internet of Things, formally establishing the concept of the IoT [1].

After more than ten years of development, IoT has been applied in many fields. Examples: wearable devices, smart homes, smart cars, telemedicine, intelligent transportation, logistics, and warehousing. According to the portal website Statista, 75 billion IoT devices will be connected to the IoT by 2025.

However, the large number of connections poses a considerable security risk. During the development of IoT, we gradually began to use typical techniques in the Internet field to protect user privacy and IoT security. Presently, the common technical deployed in the field of IoT security include public key IoT infrastructure security methods, IoT security analysis, authentication/verification of IoT devices, API security methods, IoT hardware testing, IoT security threats, and vulnerabilities analysis, and secure IoT application development.

Despite the continuous emergence of new security technologies and the improvement of existing security technologies, the current IoT security issues are still worrying. IoT security problems may bring privacy security problems and property losses to customers and may even endanger users' lives. Embedded medical devices such as insulin pumps and pacemakers on sale have the potential to be hacked remotely, causing coma, shock, and even death, according to a study.

IoT security concerns national security and social stability. In 2010, the infamous Stuxnet virus was revealed. This virus is the first in history to target real-world infrastructure. Before the Stuxnet virus was discovered, oil pipelines, national power grids, communications facilities, airports, and other infrastructure had been damaged.

The IoT threat poses a challenge to traditional Internet security. In 2016, a botnet infected with Mirai's malicious program controlled the vast physical network of devices. It launched three DDoS attacks on DNS provider Dyn, causing widespread Internet outages in the eastern United States and making many popular websites inaccessible.

Individuals and manufacturers need to establish more awareness of IoT security. According to a PEW Research Center survey, 52 percent of patients thought doctors should have shared their medical information to manage appointments and medical records, and 47 percent doubted stores could track and sell their purchases to third parties.

This paper introduces the definition, technical characteristics, and hierarchical architecture of the IoT, then gives different layers of common security threats and general measures to improve IoT security.

The paper is structured as follows: Section 2 introduces the IoT's definition, technical characteristics, and hierarchical architecture; Section 3 analyzes the security threats at different layers. The t section 4 gives the general measures to improve the security of the IoT system, and finally, section 5 concludes this paper.

2. The overview of IoT

The IoT has different definitions depending on the direction of research. The following are several representative definitions of the IoT:

Definition 1: The IoT is a network where physical objects equipped with sensors, software, and other technologies are connected through specific communication protocols to achieve one or more functions over the Internet [2].

Definition 2: The IoT is an innovative group of technologies that creates an overall system where linked devices and services gather, exchange, and manage data to adjust dynamically. It is closely linked with cyber-physical systems and plays a crucial role in improving the quality of service for Smart Infrastructures [3].

Definition 3: The IoT is a network of intelligent objects that are open and all-encompassing, capable of self-organization and information sharing. They can react and respond to environmental situations and changes by sharing resources and data [4].

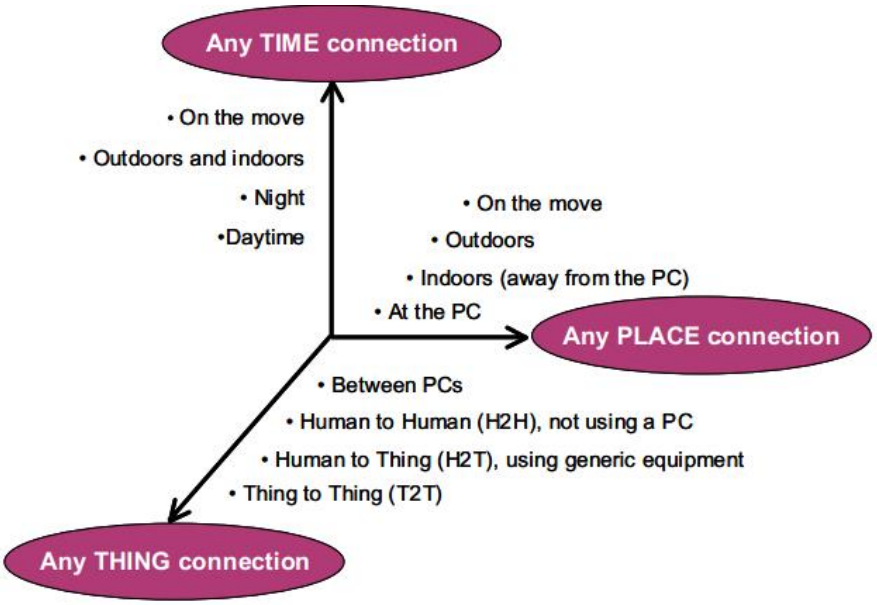

Figure 1. Connecting dimensions in IoT [1].

Three vectors are in a qualified IoT system, as shown in Figure 1. The paper posits that the IoT pertains to the network that has abilities to connect objects to achieve intelligent object identification and management. The IoT integrates the physical and information spaces, as depicted in Figure 2, enabling effective communication among objects, between people and objects, and between people and the environment. It is a high-level embodiment of informatization in human society.

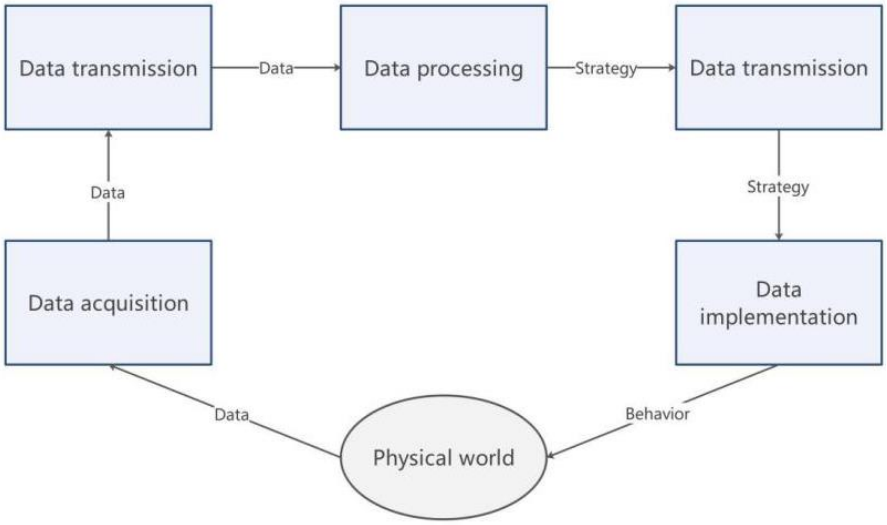

Figure 2. The Information Function Model of the IoT

2.1. Technical characteristics of IoT

Looking at it from the viewpoint of communication objects, the IoT denotes exchanging information among objects, individuals, and things. The fundamental characteristics of the IoT can be encapsulated as follows:

Comprehensive perception: Utilizing methods such as RFID, locators, sensors, QR codes, and others to gather information about objects at any time and place. Perception involves obtaining sensor information, collaborative processing, smart networking, and even information services to enable control and command.

Reliable transmission: Through integrating various telecommunication networks and the Internet, the perception information received can be transmitted remotely in real-time, information interaction and sharing can be realized, and all kinds of effective processing can be carried out.

Intelligent processing: Employing intelligent technologies like cloud computing and fuzzy recognition to analyze and handle the vast data and information collected in real time across various places. This improves the understanding of the physical world, ultimately leading to intelligent decision-making and control.

2.2. Architecture of the IoT

There needs to be a unified architecture definition for the IoT. According to previous research, the IoT can be summarized as a four-layer structure, as shown in Figure 3:

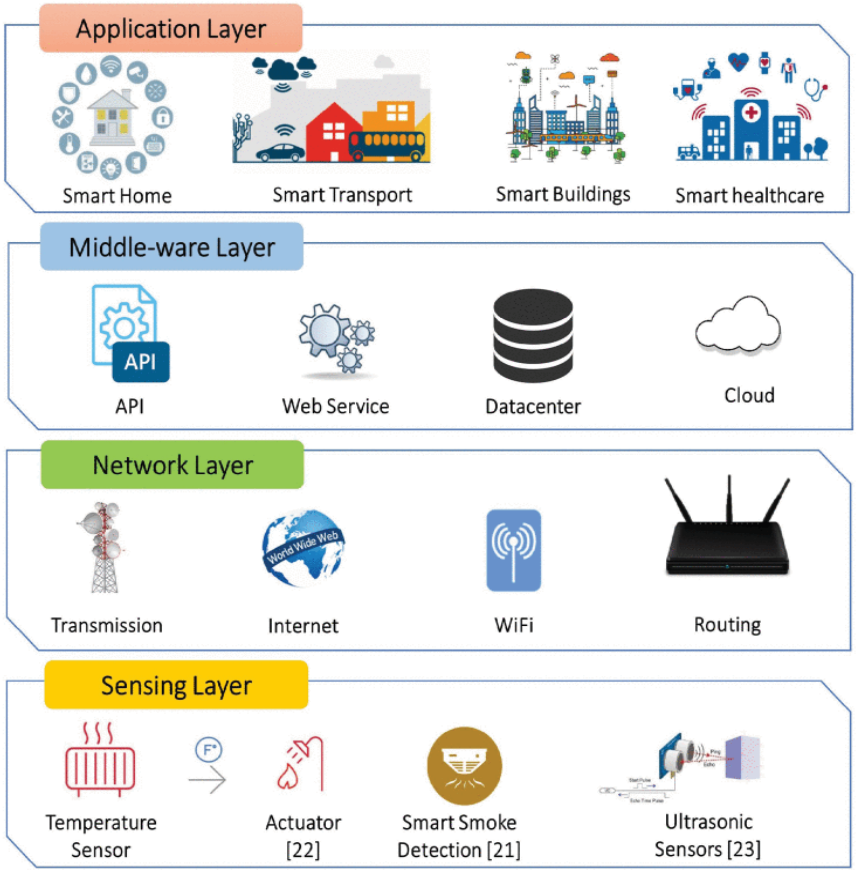

Figure 3. Four layers of IoT [5].

Sensing layer. The sensing layer refers to various physical devices, sensors, and actuators in the IoT. They obtain data by collecting environmental information and monitoring device status, and transmitting it to the application layer for processing and analysis via the network layer. The sensing layer is the primary and fundamental component responsible for collecting data in the IoT.

Network layer. The IoT's network layer involves the technology and protocols used to transmit the data gathered by the sensing layer over the network to the application layer for analysis and processing. It is responsible for achieving secure and reliable data transmission and connectivity, making it the key component in data transmission within the IoT. In the IoT, the network layer includes various network technologies and protocols, such as wireless communication technologies (Wi-Fi, Bluetooth.), Wired communication technologies (Ethernet, RS485.), Internet protocols (TCP/IP, HTTP, MQTT.), IoT-specific protocols (CoAP, AMQP.)

Middleware layer. The middleware layer of the IoT serves as a mediator connecting the sensing layer and the application layer., providing data processing, management, and communication services to facilitate the interaction between the two layers. It is responsible for integrating the various devices and sensors in the sensing layer, processing and analyzing the data collected by them, and providing the results to the application layer. The middleware layer comprises various software components and services, including data processing and management, communication and protocol translation, security and privacy, and service discovery and management.

Application layer. The application layer in IoT is the topmost layer of the IoT architecture. It is responsible for providing services and applications that enable users to interact with the devices and data collected by the lower layers. The application layer is where the end-users and their devices, such as smartphones and computers, access and utilize the data collected by the IoT devices in the sensing layer.

3. Security threats to the IoT

3.1. General security threats

Lack of authentication and authorization: IoT devices and applications can be vulnerable to unauthorized access if they lack proper authentication and authorization measures, such as weak passwords or insufficient access controls. Lack of authentication and authorization can allow attackers to intercept and manipulate data or gain access to critical Systems. Insufficient encryption and insecure data transmission: Every moment, a large amount of IoT-generated data often flows through or is stored in third parties or untrusted devices. These data usually contain user privacy or business secrets. Transmitting or storing data in an unencrypted manner is extremely insecure, which could lead to data leakage and thus pose a systemic risk to the IoT.

Lack of update and patch management: Historically, software updates and patches for industrial control software have primarily focused on enhancing system stability and functionality, with less emphasis on security. As mentioned in IEC 62443-2-1-2010, patch management is essential in improving network security policies. As shown in Figure 4, devices and applications can be vulnerable to known vulnerabilities and exploits without proper update and patch management, making them an easy target for attackers.

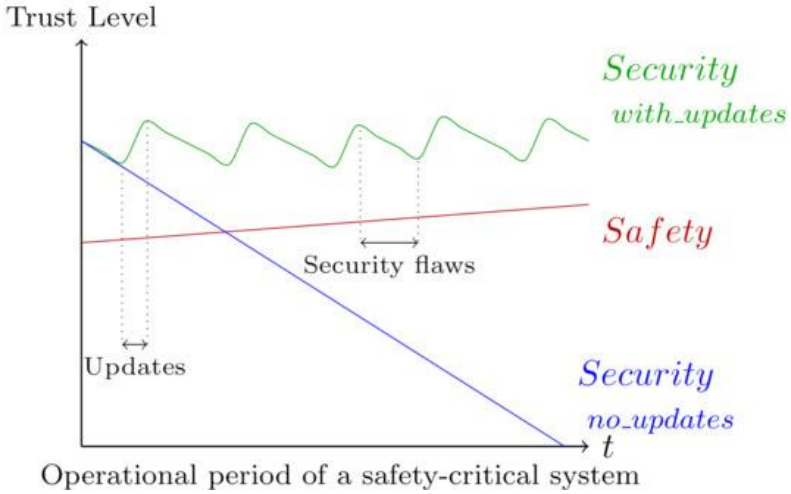

Figure 4. Safety and security trust levels [6].

Insider threats and human error: An individual who has been authorized to access an organization's network, system, or data and uses that access in a way that harms the confidentiality, integrity, or availability of the organization's information or information systems is known as an insider threat [7]. This person can be a current or former employee, contractor, or business partner. The misuse of access may be intentional or unintentional. Several cases have shown that internal personnel data leakage and public inscription data will pose a serious threat to system security. Mistakes by employees or other authorized users, such as misconfigurations or insufficient security measures, can also pose a significant security threat to the IoT network.

Supply chain attacks: A Supply Chain Attack refers to a deliberate and malicious act that involves inserting, modifying, or substituting information and communication technology (ICT) - hardware, software, or firmware - at any stage within the supply chain. The ultimate aim is to exploit a vulnerability in the ICT system and disrupt or monitor a mission using cyber resources. Regarding supply chain attacks, software-based attacks involve injecting harmful code into an application that can infect all app users. On the other hand, hardware-based attacks compromise the physical components of a system. IoT devices can be vulnerable to supply chain attacks, where attackers infiltrate the manufacturing process and introduce malware or other vulnerabilities into the devices before they are shipped to customers.

3.2. Attacks in sensing layer

The sensing layer primarily handles the data gathered by various sensors and actuators. Sensors automatically sense what is happening in the physical world. For the sensing layer, common security threats include the following:

Malware and hacking attacks: Due to power consumption and usage environment limitations, sensing layer devices are usually deployed in resource-constrained environments. The lack of security measures makes it easier for attackers to hack into sensing layer devices using malware. Malware and hacking attacks can exploit vulnerabilities in IoT devices and sensors, allowing unauthorized access to sensitive data or control of the devices themselves.

Node capturing: The sensing layer comprises multiple low-power nodes comprising various sensors and actuators, and these nodes are susceptible to attack within the environment. An attacker may attempt to capture a legitimate node or replace a legitimate node with one controlled by the attacker. Attackers can use these nodes to inject fake data into the system or rely on nodes to access other system parts.

Physical tampering: Physical tampering is an attack that requires exposing and attacking a target device through physical methods. Because most physical attacks are invasive, such attacks can permanently alter some of the properties of the target. Physical access to IoT devices can allow attackers to tamper with the sensors, leading to the collection of inaccurate data or the disruption of critical services.

Data privacy and confidentiality: IoT sensors can collect a vast amount of sensitive data. Without proper encryption and security measures, unauthorized parties can intercept or steal this data.

Lack of standardization and regulation: The lack of standardization and regulation in the IoT industry can lead to insecure and poorly designed devices, making them vulnerable to various security threats.

3.3. Attacks in network layer

The network layer connects IoT devices and sensors to the internet and other devices. The network layer's primary role is to forward the data gathered by the sensing layer to the subsequent layer. For the network layer, common security threats include the following:

Man-in-the-middle (MITM) attacks: MITM attack is a standard method of internet attack. The attacker occupies the communication channel of both sides and can eavesdrop, intercept, and even modify the communication content of both sides, as shown in Figure 5. During a MITM attack, a perpetrator intercepts and alters data exchanged between two devices on a network., potentially allowing them to steal sensitive information or alter critical system commands.

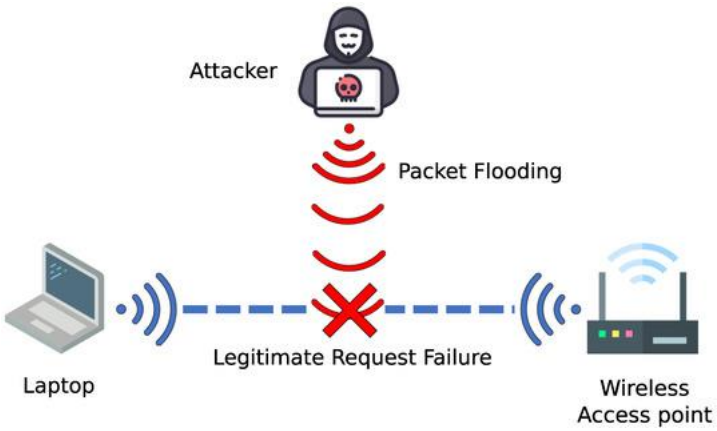

Figure 5. An example of MITM attacks [8].

Distributed Denial of Service (DDoS) attacks: Launching DDoS attacks is simple, while defending against them can be challenging. These attacks are designed to consume bandwidth or allocatable

resources of devices to deny legitimate users access to services [9]. IoT devices can be hijacked and used to launch DDoS attacks, which can overwhelm targeted networks and servers.

Advanced persistent threat (APT): Advanced persistent threat is a highly targeted and sophisticated cyber-attack. An APT attack targets a network in several stages and sustains ongoing access to the target. By deploying APT malware, attackers can take remote control of a targeted device and extract sensitive data. Since IoT devices receive and send sensitive data all the time, they are easy target for APT attacks.

3.4. Attacks in middleware layer

The middleware layer aims to offer an intermediate layer between the network and application layer, providing abstraction while providing powerful computing and storage capabilities. For the middleware layer, common security threats include the following:

SQL injection attacks: The middleware layer often involves using a database to store and manage data from IoT devices. SQL injection occurs when an attacker injects malicious code into a database query through input fields or other vulnerable areas of an application [10]. If the middleware layer is not properly secured, attackers can exploit vulnerabilities to insert unauthorized or malicious data into the database or extract sensitive data.

Data manipulation and injection: Attackers can exploit vulnerabilities in middleware to manipulate or inject data into the system, leading to inaccurate data or control of critical systems. API vulnerabilities: In the middleware layer, the middleware opens various APIs to the user to implement the functions required by the user. However, the APIs are not securely designed. In that case, they can be vulnerable to injection, DoS/DDoS attacks, and cross-site scripting, leading to data leakage or unauthorized access.

3.5. Attacks in application layer

The application layer provides a direct interface for users to interact with the IoT. For the application layer, common security threats include the following:

Data theft: IoT applications process sensitive and private data all the time. These data stored within IoT applications can be vulnerable to theft or manipulation if improperly encrypted or protected.

Malware and viruses: IoT applications can be vulnerable to malware that can infect the devices and systems they interact with, leading to data loss or system compromise.

Malicious code injection attacks: This attack operates by inserting meticulously crafted malicious code into a web application, inducing an error in the application that enables the malicious code to be interpreted and executed. In the case of XSS, this attack can inject malicious scripts into a website, which can cause data leakage, system malfunction, or even system crashes [11].

Sniff attacks: Sniffing attacks involve the unauthorized interception and monitoring of data transmitted over a network. Attackers use specialized software and hardware to capture and analyze network traffic, including sensitive data such as login credentials, personal information, or device commands.

4. Security improvements of the IoT

Addressing security concerns related to the IoT necessitates a comprehensive approach involving technical and non-technical strategies. The following lists several technology or methods to improve the existing IoT security.

4.1. Implement strong access controls

IoT devices and systems should have strong authentication and authorization measures. Access controls are crucial in restricting access to confidential information and actions within an IoT system, ensuring that only authorized users or devices are allowed. Organizations can minimize the risk of

data breaches, unauthorized modifications, and other security threats by limiting access to sensitive information. The following lists some access control methods to enhance IoT security:

Use strong authentication: Authentication measures such as strong passwords, biometric scans, or two-factor authentication should be used to verify user or device identities.

Choose the proper access control model: Choose the appropriate access control method according to the specific usage scenario. Static access control methods comprise Access Control List (ACL), Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC). On the other hand, dynamic access control methods include Risk-Based Access Control, Trust-Based Access Control, and a combination of Risk-Based and Trust-Based Access Control.

Monitor access logs: Access logs should be monitored for suspicious activity, such as multiple failed logins attempts or access from unauthorized devices.

Regularly review and update access policies: It is important to regularly review and update access policies to ensure that they are current and able to address security threats effectively.

4.2. Data encryption

As the number of IoT devices and the volume of data transmitted continue to rise, encryption becomes crucial in safeguarding confidential information and upholding users' privacy. All sensitive data transmitted through IoT devices and layers should be encrypted to prevent interception and theft by unauthorized parties. The following lists some encryption methods to enhance IoT security:

Use robust encryption algorithms: Strong encryption algorithms, such as AES or RSA, should be used to ensure the data is properly protected. Insecure encryption schemes, such as MD5, should no longer be used.

Secure key management: Encryption keys should be stored securely and only accessible to authorized users or devices. New technologies, such as blockchain, can be used for key management.

Periodically change encryption parameters and keys: Changing encryption parameters and keys regularly increases the difficulty of adversary attacks, thus enhancing system security.

4.3. Network segmentation

From the point of view of convenient management and security, we often cut the real-life network into segments, each of which is isolated from the others. Each segment is protected by its security measures, such as firewalls, access controls, and intrusion detection systems. IoT networks should be segmented to limit the impact of security breaches and prevent attackers from moving laterally within the network. The following lists some network segmentation methods to enhance IoT security:

Identify IoT devices: Separated devices based on their physical or logical addresses and importance. Set up monitoring devices and firewalls between different sub-networks. Also, administrators should configure appropriate security policies based on the attributes and levels of sub-networks.

Use access controls and identity authentication: Deploy access controls and identity authentication to prevent exceeding authority or unauthorized access, as well as disguised malicious networks from accessing other sub-networks.

Monitor network traffic: Set up dynamic traffic and access monitoring mechanisms to prevent malicious data and code from circulating in the network and causing widespread damage.

4.4. Regularly update and patch systems

System updates and patches are designed to fix vulnerabilities and bugs in software or firmware that attackers can exploit. Regular updates and patches should be applied to all IoT devices and systems to address known vulnerabilities and exploits. The following lists some update and patch methods to enhance IoT security:

Develop an update and patch management plan: Create a plan that outlines the process for updating and patching IoT devices, including how often updates will be applied and how they will be tested.

Test updates and patches before deployment: Before deploying updates and patches, test them in a controlled environment to ensure they do not cause any issues with device functionality or compatibility.

Prioritize critical updates: Prioritize updates and patches that fix critical vulnerabilities, such as those that can be exploited remotely or allow attackers to access sensitive data.

Automate update and patch management: Automate the update and patch management process wherever possible to ensure updates are applied consistently and on time.

4.5. Monitor for suspicious activity

By monitoring for any suspicious behavior, organizations can detect potential security threats early, allowing them to take action to prevent or minimize the impact. All IoT devices and systems should be continuously monitored for suspicious activity, such as unusual data transfers or unexpected device behavior. The following lists some network segmentation methods to enhance IoT security:

Define security monitoring policies: Define policies for security monitoring, including what types of activity will be monitored and how often monitoring will occur.

Use automated monitoring tools: new technologies, such as artificial intelligence, can increase the efficiency of monitoring abnormal data and operations to achieve the effect of automated monitoring networks.

Monitor logs and alerts: Monitor logs and alerts to identify suspicious activity. Properly save monitoring data for analysis. When an exception, such as unusual login attempts or unauthorized access attempts, occurs, the system should be able to notify the administrator promptly.

Respond quickly: When a security incident is identified, respond quickly to prevent or mitigate the damage.

4.6. Non-technical methods

Educate employees and users. As security technology advances, the IoT is becoming increasingly secure at a technical level. However, it is worth our attention that human factors are becoming a significant weak link in information system security. A report shows a positive correlation between human factors and multiple information breaches [12]. The following measures can be taken to mitigate the impact of human factors on system security: 1) Provide regular security training: Regular training on security best practices ensures that employees and users are up-to-date on the latest security threats and best responses. 2) Emphasize the importance of security: Emphasize the importance of security to employees and users and how their actions can impact the organization's security. 3) Use real-world examples: Provide tangible instances of security breaches to demonstrate to employees and users the significance of security measures and how their behaviors can either prevent or alleviate potential security risks.

Use secure development practices. Security is not a factor for many IoT companies, which prefer efficient development for greater competitive potential. As a result, many engineers and programmers at IoT companies need more experience with security development. This undoubtedly poses a huge challenge to the security of IoT devices and applications. To achieve secure development, the following measures can be taken: 1) Conduct threat modeling: Conduct threat modeling to identify potential security threats and vulnerabilities and address them during development. 2) Follow secure coding practices: Follow secure coding practices, such as avoiding buffer overflows, validating input, and implementing proper error handling. 3) Use secure software development tools, such as static analysis tools and vulnerability scanners, to identify and address security vulnerabilities. 4) Conduct security testing: Perform security testing, such as penetration testing or vulnerability scanning, to detect and rectify any security weaknesses.

Develop and follow standards and regulations. Security standards and security controls are the best security practices that can be implemented in the IoT environment. Infosys reports that 89% of manufacturing departments know the importance of data standards, but only 11% deploy security

controls and standards [13]. Standards and regulations should be developed and followed to ensure IoT devices and systems meet minimum security requirements.

5. Conclusion

This paper introduces the definition, technical characteristics, and system architecture of the IoT, then explores the security threats that may be encountered at different layers by system level, and finally gives several general suggestions to improve the security of the IoT system. The IoT is the web of the future, and as efficiency and scale continue to grow, designers and engineers should make security an important consideration. Only by constantly developing the security of the IoT can we resist the increasingly severe IoT attacks so that the public can enjoy the convenience brought by the development of the IoT at ease.

References

[1] ITU Strategy and Policy Unit (SPU). ITU Internet Reports 2005: The Internet of Things [R]. Geneva: International Telecommunication Union (ITU), 2005.

[2] What is IoT? [Online]. Available: https://www.oracle.com/internet-of-things/what-is-iot/.

[3] Internet of Things (IoT). [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastuctures/iot.

[4] Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 03, 164 - 173. doi: 10.4236/jcc.2015.35021, 2015.

[5] 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," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[6] I. Mugarza, J. L. Flores, and J. L. Montero, “Security Issues and Software Updates Management in the Industrial Internet of Things (IIoT) Era,” Sensors, vol. 20, no. 24, p. 7160, Dec. 2020, doi: 10.3390/s20247160.

[7] A. Kim, J. Oh, J. Ryu and K. Lee, "A Review of Insider Threat Detection Approaches with IoT Perspective," in IEEE Access, vol. 8, pp. 78847-78867, 2020, doi: 10.1109/ACCESS.2020.2990195.

[8] E. Staddon, V. Loscri, and N. Mitton, “Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey,” Applied Sciences, vol. 11, no. 16, p. 7228, Aug. 2021, doi: 10.3390/app11167228.

[9] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, “Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey,” Sensors, vol. 22, no. 3, p. 1094, Jan. 2022, doi: 10.3390/s22031094.

[10] Chen, Ding, et al. "Sql injection attack detection and prevention techniques using deep learning." Journal of Physics: Conference Series. Vol. 1757. No. 1. IOP Publishing, 2021.

[11] M. Liu, B. Zhang, W. Chen and X. Zhang, "A Survey of Exploitation and Detection Methods of XSS Vulnerabilities," in IEEE Access, vol. 7, pp. 182004-182016, 2019, doi: 10.1109/ACCESS.2019.2960449.

[12] Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon, 7 (3), e06522.

[13] L. L. Dhirani, E. Armstrong, and T. Newe, “Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap,” Sensors, vol. 21, no. 11, p. 3901, Jun. 2021, doi: 10.3390/s21113901.