ISSN 2706-655X Vol.5, Issue 2: 46-49, DOI: 10.25236/IJFET.2023.050208

A Brief Analysis of Internet of Things Security

Yundi He*

North China University of Technology, Beijing, 100144, China
**Corresponding author*

Abstract: *With the rapid development of the Internet of Things, it has brought serious security threats. IoT security technology can guarantee the sustainable and healthy development of IoT. First, this paper analyzes the concept and principle of the IoT; then, builds the architecture of the IoT security based on the security technology of each component of IoT, and analyzes the role of each component and its security protection technology; finally, analyzes the current status of IoT security, and looks forward to next working.*

Keywords: *IoT security, security technology, architecture, emerging technology*

1. Introduction

The Internet of Things is known as the third wave of world information, and it is accelerating towards the great blueprint of the Internet of Everything. In recent years, with the rapid development of emerging technologies such as big data, artificial intelligence, and cloud computing, and their integration into the IoT, IoT technology has continued to mature. At present, IoT is widely used in many fields, such as the Industrial IoT, smart transportation, smart cities,and smart agriculture, which has well promoted development of society, economy, and production. By 2025, the potential value of IoT will reach 1.1 trillion US dollars, accounting for about 11% of the world's total economic volume [1]. However, while applying IoT is increasing rapidly, it brings various security threats. Only by doing a good job in IoT security can we develop IoT sustainably and healthily. Therefore, it is of great significance to study IoT security.

2. Internet of Things

The word “Internet of Things (IoT)” was first proposed by Bill Gates in his book "The Road to the Future". In 1999, Professor Ashton [2] of EPC Global's Auto-ID Center first proposed the concept of IoT, saying that IoT is objects that are connected to the Internet through radio frequency identification and other sensing devices, aiming to realize automatic identification of objects and information that can be interconnected and shared. In 2005, the International Telecommunication Union (ITU) [3] elaborated the concept of IoT in more detail and vividly depict the scene of IoT communication era.

This paper gives an understanding of IoT. Internet realizes information exchange and communication between people. While IoT is the expansion of Internet, it can be realized between people and objects, and objects and objects. Specifically, objects are embedded with various sensors, which sense and collect various data with massive and heterogeneous characteristics, and these data are transmitted to the platform through the network, and the platform will aggregate the data, Intelligent processing and analysis, and then make corresponding decisions according to the needs of users / application industries.

For the architecture of IoT, many researchers divide it into three layers, namely the perception layer, the transport layer, and the application layer. Each layer structure of the IoT has corresponding functions.

3. Architecture of IoT Security

Based on constituent elements of IoT, this paper proposes the classification of IoT security, and then builds the architecture of IoT security. According to the above-mentioned architecture of IoT and relevant international influential standards, such as GB/T 37044-2018 "Internet of Things Security Reference Model and General Requirements", GB/T 37025-2018 "Technical Requirements for Internet

ISSN 2706-655X Vol.5, Issue 2: 46-49, DOI: 10.25236/IJFET.2023.050208

of Things Data Transmission Security", etc., IoT security is divided into perception security, transmission security, and application security. Then, further analyze the security technology involved in each component. At last, the architecture of IoT security were formed, as shown in Figure 1.

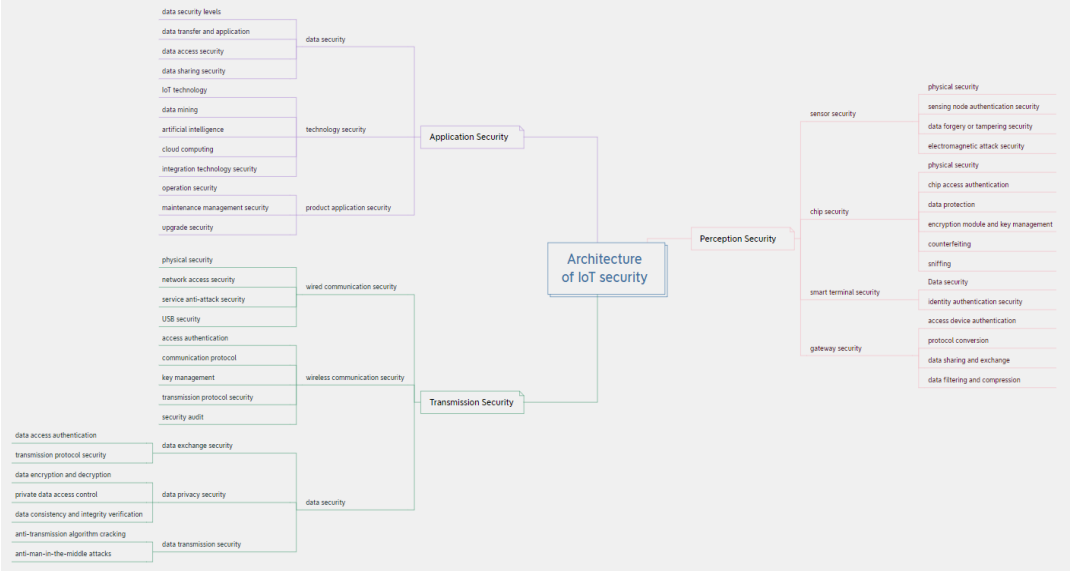

Figure 1: Architecture of IoT Security

3.1 Perception Security

In IoT, perception security includes various sensor security, chip security, smart terminal security, gateway security, etc. Among them, sensors are devices that perceives and detects things. Sensor security includes physical security, sensing node authentication security, data forgery or tampering security, electromagnetic attack security, etc. Chip mainly completes the tasks of data calculation, processing, and storage. Chip security usually includes physical security, access authentication, sniffing, counterfeiting, data security, encryption management and other security content. Smart terminals have certain computing and storage capabilities, and their security includes data security, identity authentication security, etc. Gateway is located at the junction between the perception layer and the transmission layer (near the edge of the object), combined with emerging edge computing technology, it can directly process, store and apply data at the edge, greatly improving working efficiency. Meantime, gateway is a place that upload data and feedback command. Gateway security includes access device authentication, data filtering, data compression, data exchange, protocol conversion, etc.

3.2 Transmission Security

Transmission security includes wired communication security, wireless communication security, data security,etc. Among them, wired communication is that uses physical medium (e.g. metal wires) to transmit information. Images text, sound, etc can be transmitted through optical or electrical signals. Wired communication security includes physical security, network access security, service anti-attack security, USB security, etc. Wireless communication is that uses electromagnetic wave signals to exchange information. Because electromagnetic waves do not need any medium to conduct, people call it wireless communication. Wireless communication includes Bluetooth, 6LoWPAN, Lora, NarrowBand-IoT, Wi-Fi, etc. Wireless communication security includes access authentication, communication protocol, key management, and security audit. Data security at the network layer involves data privacy security, data exchange and transmission security, etc. Specifically, data exchange security includes data access authentication, transmission protocol security, private data access control, etc. Data privacy security includes data encryption and decryption, data consistency and integrity verification, etc. Data transmission generally needs to go through different types of network, which poses more serious security threats than a single network. Data transmission security includes transmission protocol security, anti-man-in-the-middle attacks, etc.

ISSN 2706-655X Vol.5, Issue 2: 46-49, DOI: 10.25236/IJFET.2023.050208

3.3 Application Security

Application security is mainly for designers, developers and users of IoT, including data security, technology security and product application security. In addition to data-related security at the network layer, data security at application layer also includes data security levels, data transfer and application, data access security, and data sharing security,etc. The technology at application layer includes IoT technology and data mining, cloud computing, artificial intelligence, and blockchain, as well as their mutual integration technologies. Technology security includes the security of emerging technologies themselves. In addition, it also includes the security generated by the integration of these emerging technologies and IoT, such as integrated access security, data interaction security, communication transmission security, management control security, etc. Product application security refers to the security of the entire life cycle of a product from being put into use to being eliminated, including operation security, maintenance management security, upgrade security, etc.

4. Current Status and Prospect of IoT Security

4.1 Current Status of IoT Security about Theory

In the current research of IoT security, there are relatively many research about objects identification security and sensory terminal security [4], but there are relatively large gaps in IoT security risk assessment, gateway and edge computing security, data privacy security, etc. It's very weak in research of integration security of new IoT chips and new technology of protocols, Beidou, 5G/6G, edge computing, AI, etc [5].

4.2 Current Status of IoT Security about Application

At present, IoT is applied in many fields, such as industry, transportation, medical treatment, military and so on. However, each field is very different, and the level of security protection is also different [5]. In addition, IoT vendors ignore or pay insufficient attention to the security of IoT products. A survey by MPI Group's 2017 found that [6], amazing 14% of IoT manufacturers didn't considered security issues, respectively 18% and 21% of IoT manufacturers Security issues didn't considered until the quality management stage and the production stage, less than 50% of IoT manufacturers considered security issues at the design stage.

4.3 Prospect of IoT Security

According to the current situation of IoT security, the future work is preliminarily prospected.

1) For research, relevant scientist should increase research on the weak parts of IoT security. For example, 5G/6G, Beidou, blockchain security, data privacy protection, edge computing security, artificial intelligence security, etc. At the same time, researchers could combine the characteristics of each field, integrate emerging security technologies, and provide differentiated IoT security services to each field.

2) For the industry, IoT manufacturers should increase security awareness, take security into consideration in products as early as possible, and run through the entire process of product design, development, and application, so as to avoid security issues.

5. Conclusion

IoT is deeply affecting the world. Security will surely become an essential attribute for IoT, which is beneficial to develop IoT sustainably and healthily. This paper analyzed IoT and constructed architecture of IoT security, and preliminarily studies the current situations and prospects of IoT security. Only by facing up to security threats and addressing them with IoT security technologies can we move towards a secure and connected world.

References

[1] S. J. Mohammad, P.K. Jessica and S. Michael (2019). The Internet of things promises new benefits

ISSN 2706-655X Vol.5, Issue 2: 46-49, DOI: 10.25236/IJFET.2023.050208

and risks: A systematic analysis of adoption dynamics of IoT products. IEEE Security & Privacy, vol. 17, no. 2, p. 39-48.
[2] K. Ashton (2009). That'Internet of Things'Thing.
[3] International telecommunication union. ITU internet reports 2005: The internet of things. (2005). http://www.itu.int/osg/spu/publications/internetofthings/.
[4] L.S. Zhou, Y.P. Kong, G. Lu (2017). Interpretation of Internet of Things Security Policy and Summary of Technical Standards. Guangdong Communication Technology, vol.37, no.12, p.39-41.
[5] F. Li, L. Chen and K. Li (2022). Research on the framework of the security standard system of the Internet of Things. Application of Electronic Technique, vol. 48, no.7, p.8-12.
[6] The MPI Internet of Things Study (2017). https://www.bdo.com/getattachment/9adeb668-5c54-47b7-9108-08ad37fe6fd3/attachment.aspx.