Network security of IoT devices

Zhengtao Wang

Abstract—**As a hot research topic, the Internet of Things has always been valued by scientists and entrepreneurs. The Internet of Things interconnects devices and networks, improves the interaction between people and devices, and greatly improves the efficiency of office and society. The development of the Internet of Things has enabled billions of Internet of Things devices to be used. So many devices and the huge amount of data they generate make us worry about the network security of Internet of Things devices, especially in the field of privacy and security. This article will briefly explain the operating mechanism of the Internet of Things, summarize the current methods of protecting the network security of Internet of Things devices, and provide some open source resources for your reference.**

Keywords—**Data, Devices, Internet of Things, Network security**

I. Introduction

The Internet of Things is used in all aspects of our lives. Personally, our smart homes, smart appliances, even smart wearable devices and some medical devices are closely connected to the Internet to form part of the Internet of Things. For companies, smart buildings, smart logistics, and smart control systems are all helping companies improve efficiency and reduce costs. As far as society is concerned, the development and popularization of the concept of smart cities have made the lives of residents more convenient and energy-saving, and made our society more sustainable. Therefore, the further popularization and development of the Internet of Things will bring about tremendous changes to our lives. But what is worrying is that the Internet of Things equipment and network security is something that researchers and users need to pay attention to, because the popularity of the Internet of Things will make it easier to expose the data of our devices to Internet hacker attacks. . In a security research report on the Internet of Things, only seven percent of business executives interviewed believed that Internet of Things devices were safe, and only three percent thought they were very safe. Therefore, the development of network security for Internet of Things devices will be one of the focuses of the next development of the Internet of Things.

II. What is IoT?

The Internet of Things is a network system that interacts between physical devices and physical devices or systems. It provides mutual communication and contact between people, people and things, and things. According to the research of researchers Somayya Madakam, R. Ramaswamy and Siddharth Tripathi, the Internet of Things can be best defined as: " An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment".

In the Internet of Things, users use the network to connect physical entities so that users can control items and obtain real-time feedback and status of items. The Internet of Things integrates technologies such as sensors, automation, embedded systems, wireless transmission, and network computing, and the large amount of data and control systems it generates are also closely related to data analysis and artificial intelligence.

III. How IoT Works?

The International Telecommunication Union (ITU) defines architecture of IoT as five layers. They are the sensing layer, the access layer, the network layer, the middleware layer and the application layer. But most of the researchers would use three layers to define the architecture of IoT: the perception layer, the network layer and the application layer.

The perception layer includes data collection equipment such as sensors, including the sensor network before the data is connected to the gateway. The perception layer is the foundation of the development and application of the Internet of Things. RFID technology, sensing and control technology, and short-range wireless communication technology are the main technologies involved in the perception layer.

The network layer is responsible for using the Internet of Things, the Internet and communication networks to transmit data. It includes the storage and analysis of sensor network data, as well as theories and technologies based on perception data for decision-making and behavior. The network layer transfers the information collected by the perception layer to the data processing center, and transfers the commands of the data center to the application layer.

The application layer of the Internet of Things uses analyzed and processed data to provide users with specific services. The application layer is the purpose of the development of the Internet of Things. Software development and intelligent control technology will provide users with a variety of applications.

There are several important technologies used in IoT related to network security.

1.Radio Frequency Identification (RFID) is a system to identify an object wirelessly by radio signals.

2.Wireless Fidelity (Wi-Fi) is a technology to make devices communicate wireless.

3.Bluetooth is a wireless technology used in short-range situation.

4.Wireless Sensor Network (WSN) is a wireless network using sensors or automatic devices to monitor the environment or physical status.

IV. How to protect the IoT devices from cyber attack?

According to the architecture of IoT, we could have some plans to protect the network security. For the perception layer and application layer, the company must have a full understanding and management of the IoT devices it uses, such as the number, model, and function of the IoT devices. And always update and maintain the Internet of Things equipment. If there are vulnerabilities in IoT devices and systems, they need to be patched and updated in time. Enterprises also need to monitor devices at all times so that they can respond in a timely manner after they are attacked.

What ' s more, the company can set the password for the Internet of Things devices it uses to enhance its security. Many IoT devices have simple passwords when they are used for the first time. Enterprises can reset their passwords for more secure protection.

For the network layer, enterprises can apply network segmentation to enhance security defenses. Network segmentation can reduce the scope of network attacks, and can achieve more refined network control. Even if a part of the network is attacked, the impact of large-scale attacks will be reduced to a greater extent. Network segmentation can also be combined with more powerful firewalls, which can better separate physical devices and networks to avoid greater losses.

According to the IoT technology, we can have other ways to improve the devices' network safety.

A. RFID-Based

RFID is widely used in the information identification of objects, so if it is deliberately attacked and destroyed in the process of identity verification, it will have a huge impact on the Internet of Things system. In order to improve the security of RFID, access control and data encryption can be used. For example, RFID signals are encrypted through algorithms to prevent privacy leakage.

B. WSN-Based

In improving the security of WSN technology, we can start with preventing hackers from attacking data transmission. For example, for key management, the construction algorithm continuously updates the key. Or use authentication and access control to increase the security of data transmission and sharing. It is also possible to design a safer node design and antenna design to enhance the stability of its work.

V. Open source resources

There are many open source resources for IoT devices ' network security.

A. ThingsBoard

This platform is for Internet of Things developers to analyze and process data, and it can issue alarms for abnormal device activities. Users can visualize the data obtained from the Internet of Things devices, and these data will be stored in the database for safekeeping

B. Kaa IoT Platform

This open source platform can promote cross-device operability, and can control and monitor connected IoT devices in real time. When the system is abnormal, it can provide customers with alerts. And the number of sensor devices that the platform can manage is unlimited.

References

[1] Y. Lu and L. D. Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2103-2115, April 2019, doi: 10.1109/JIOT.2018.2869847.

[2] Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises[J]. Business Horizons, 2015, 58(4): 431-440.

[3] Madakam S, Lake V, Lake V, et al. Internet of Things (IoT): A literature review[J]. Journal of Computer and Communications, 2015, 3(05): 164.

[4] https://www.paloaltonetworks.com/cyberpedia/how-to-secure-iot-devices-in-the-enterprise

[5] https://internetofthingsagenda.techtarget.com/definition/IoT-device

[6] https://www.opensourceforu.com/2020/02/how-open-source-technologies-can-add-security-to-iot/