Design of Security Control System Based on Internet of Things

Mu Chang

Shaanxi Polytechnic Institute, Xianyang, Shaanxi, 712000, China

Email: Mcsky@163.com

Keywords: Internet of Things, Internet, Security Control, Public Safety

Abstract: the Security of the Internet of Things Can Be Used as an Extension and Extension of the Current Security of the Internet Technology. the Security Risks of the Internet Directly Affect the Security of the Internet of Things. This Paper First Analyzes the Research Significance of the Security of the Internet of Things. According to the Research Focus of the Internet of Things, It Constructs Two Security Model Systems and Describes the Differences in Detail. Because the Public Safety System is Especially Important for Human Production and Life, the Emergency System is Designed. the Introduction of Pdrr Technology into the Security Model Has a Far-Reaching Impact on the Realization of the Iot Security Control System.

1. Introduction

The Internet of Things [1] is in the Early Stage of Development. People's Research on Internet of Things Security [2] Only Focuses on Personal Privacy Protection. But the Internet of Things (Iot) is Called “Internet of Things Connected”. It Often Uses Information Sensing Devices to Exchange Information and Communicate. Usually, the Equipment Used is Radio Frequency Identification, Global Positioning System, Infrared Sensors and So on. It Uses the Agreed Security Protocol, and Then Achieves the Purpose of Intelligent Identification. Despite the Rapid Development of Internet of Things [3], Everything Has Its Two Sides. Usually, on the One Hand, It Brings Comfort and Convenience to Our Life, But on the Other Hand, It Also Has Many Security Risks.

The Internet is the Main Component of the Internet of Things. the Security of the Internet Will Threaten the Security of the Internet of Things. Because the Internet of Things Puts Real Objects on the Internet, the Hidden Dangers of the Internet Will Not Only Bring Us Inconvenience, But Also Threaten Our Property Security Sometimes. Therefore, We Must Pay Attention to the Research of Internet Security [5]. the Vulnerability of Internet Security Has Caused the Instability of Internet of Things [6] from the Beginning. the Internet Has Many Security Risks [7], and There Are Even Many Security Defects. the Internet Needs Tcp/Ip Protocol as Its Support, But There Are Also Big Hidden Dangers. If the Foundation is Not Reliable, There Will Be More Loopholes in the Security Aspect [8], and More Loopholes in the Internet of Things. This Paper Mainly Studies Its Security Architecture.

2. Security Architecture

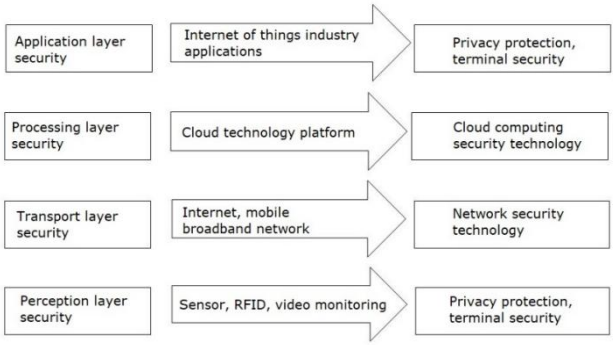

Fig.1 Security Architecture Diagram

  DOI: 10.25236/ISMHI.2019.051

The core focus of the Internet of Things has three aspects, including the perception layer, the processing application layer and the transport layer [9]. But in general, the Internet of Things (IOT) system obtains raw data from the perception layer [10]. In the transport layer, the original data is placed on a remote platform and processed separately. The main object of application layer is small perception nodes, which are usually processed. But because data processing and data application are usually different in process or method, if we want to better describe its architecture, we can list its processing application layer into two parts, such as application layer and processing layer. As a result, it can be transformed into a four-tier structure, which can be shown in Figure 1. But in essence, the principle is the same, and the difference lies in the different boundaries of the logical layer.

Of course, there is another way to distinguish the architecture of the Internet of Things system. Usually, the number of terminals in the Internet of Things is very large, which can be divided into the architecture of Figure 2, such as cloud, network, mass sensor structure. In this structure, the terminal equipment will call the infrastructure network facilities “network”. At this time, this “network” is relatively small and single, so we can call this kind of equipment “sea”. For the data of the Internet of Things, it needs a strong processing capability. But users only need to understand the relationship between processing platforms, do not need to know which computer their data is processed on, do not need to know where to store data, just care about getting data and processing results. At this time, the center of data processing is called “cloud”, and then the structure can be formed.

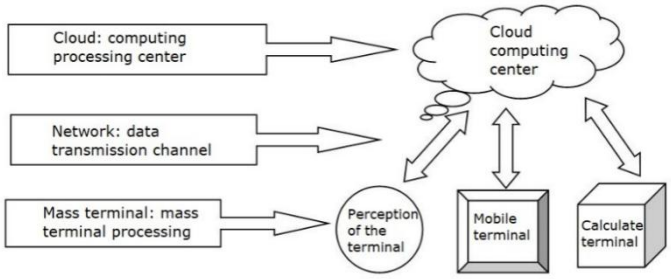

Fig.2 Cloud, Net and Sea Architecture

Because there are two kinds of terminals in the Internet of Things. Usually one kind is used to collect data, this kind is the perception terminal, which is represented by class A terminal. It has a small processing capacity and a large number; the other is the user mobile terminal, usually including mobile phones and tablets. This kind of terminal mainly acquires data or wants to acquire processing results, usually it can control class A terminal. At this time, it can be called class B terminal. In the above three-tier architecture, the perception layer is usually in class A, while the class B terminal is usually in the processing application layer. In the four-tier architecture, class A terminal is in the perception layer, and class B terminal is in the application layer. However, for the structure of Figure 2, whether class A or class B plenary will be displayed in the “sea” position, at this time, it can indicate that the boundary of division is different.

For the security system, RFID technology can scan the equipment information quickly in the security system, and then manage each device. Depending on this technology, we can realize the identification and perception of underlying devices, and provide a basis for future applications and development. The application of security system is very extensive. Taking public security system as an example, this paper designs an emergency system for public security in Internet of Things. Public security system is usually built to maintain public security and reduce emergencies.

3. Internet of Things Emergency System

The platforms of emergency system mostly depend on Internet structure, and usually adopt B/S mode and C/S mode combined system structure. Figure 3 shows the system, which consists of the following five parts:

First, the emergency command and dispatch system, which can use C/S structure to complete

data processing, command and dispatch work. This emergency system can be used as a comprehensive integrated system to process data in time and record data in real time. According to the graph, there are three subsystems in the mobile command system. Usually its subsystems issue dispatching commands, acquire relevant information, then transmit through the network to control the car, and receive information at the same time. At this time, communication is mainly responsible for data processing.

Secondly, information management and maintenance system, mainly some equipment maintenance modules. These modules can provide powerful equipment support for information maintenance.

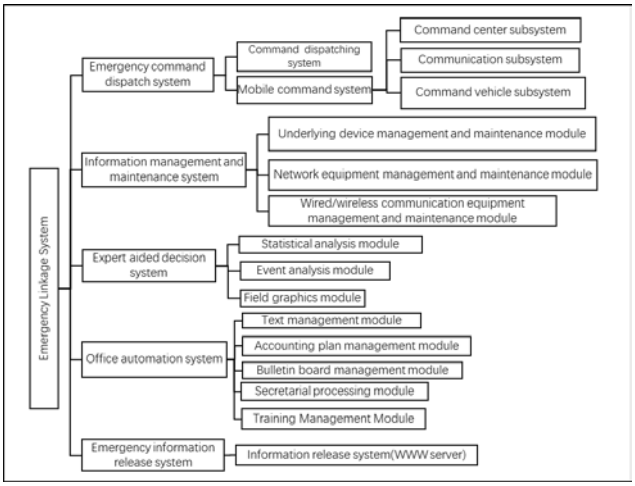

Fig.3 Internet of Things Emergency System

Thirdly, expert-assisted decision-making system. This kind of assistant decision-making mainly relies on the system to analyze the events, describe the situation on the spot, count and analyze the current situation, which can provide timely help for everyone.

Fourth, office system. The office system includes some management modules, relying on its office facilities, to better describe the current situation, for people to describe this event more clearly and specifically, to provide a strong guarantee for everyone's safety.

Finally, emergency information dissemination system. We can access through browsers to convey certain information, so that you can get the latest information in time.

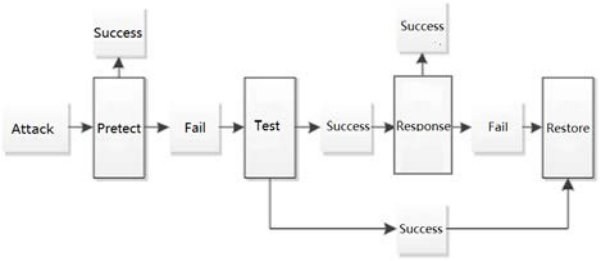

Fig.4 Pdrr Model

The security of the Internet of Things is similar to some aspects of human health. They all need common protection and autoimmunity, but external factors are more important. Therefore, in the security model of the Internet of Things, we should introduce PDRR into the security model, which is particularly important. Figure 4 shows the security model structure. There are four parts in PDRR: protection, detection, response and recovery. Its main security objectives are to increase protection time, reduce detection and response time. When the system is destroyed, it can make the system recover better and faster, and reduce the system risk exposure time. At the technical level, the security of the system can be controlled by some software, and it can also rely on its firewall, or even network monitoring, to carry out multiple security scans. However, a single security component can only temporarily provide local security functions for some locations. If a security component is missing, there will be a security vulnerability in the system. So, whenever we use

various technical means, we often need to strengthen the network protection system. We need to consider security policy first. In order to better adapt to the rapid response mechanism, we need overall control. Security is dynamic, but its concept is relative. Basically, every system has potential hazards, and the degree of security changes over time. Especially in a specific time, under the environment of its security policy, the system is relatively safe. With the change of time and the progress of the times, new network vulnerabilities will emerge and new system insecurity will emerge. This requires us to constantly adapt to the environment and adjust the corresponding programs to ensure safety.

4. Conclusion

With the development of communication technology, we have new requirements for the security of the Internet and stricter requirements for the development of the Internet of Things. Human beings have a clearer requirement for information security acquisition. This paper designs the security control system of the Internet of Things, hoping to provide a reference for the future development of the Internet of Things.

References

[1] Sun Chunzhi, Hu Xiaolin, Wang Xuechuang. Design of Intelligent Kitchen Security System Based on Internet of Things [J]. Internet of Things Technology, 2018, 8 (10): 70-73.

[2] Chen Lin. Design of secure communication system based on multi-channel transmission Internet of Things [J]. Information Communication, 2017 (08): 168-169.

[3] Mayanan. Design optimization and key technology research and application of Internet of Things security monitoring system [D]. North China Institute of Science and Technology, 2017.

[4] Fu Longtian, Yu Yumei. Design of Public Place Security System Based on Internet of Things [J]. Computer Knowledge and Technology, 2017,13(05): 21-22+24.

[5] Anyabin. Design of security monitoring and control system based on Internet of Things [J]. Fujian Computer, 2016,32 (06): 120-121.

[6] Xia Hongxing, Wang Nannan, Zheng Qinghua, Wu Shengwen. Design and implementation of security risk detection terminal system based on Internet of Things [J]. China Public Security (Academic Edition), 2015 (02): 18-21.

[7] Jiang Shuai, Wu Qisheng, Wang Weizhi. Design of Intelligent Home Security System Based on Internet of Things [J]. Microcomputer and Application, 2013, 32 (23): 55-57.

[8] Zhou Xia, Xue Xiaolei. Design of fire safety system based on Internet of Things [J]. Digital technology and application, 2010 (10): 11.

[9] Zhang Wenjun. Design and Implementation of Intranet Secure Transmission System of the People's Bank of China [D]. University of Electronic Science and Technology, 2006.

[10] Xiao Dan. Design of security and secrecy system for special line interconnection [J]. Mass Science and Technology, 2005 (10): 77-78.