

## Optimization of IoT network architecture system with security system

Zhongbo Liu<sup>1</sup>, Haixi Wang<sup>2</sup>, Wenli Chen<sup>2</sup>, Yuchen Liu<sup>3</sup>

<sup>1</sup>School of Software, Ningxia Polytechnic, Yinchuan, Ningxia, 750022, China

<sup>2</sup>Distance Education Department, Ningxia Polytechnic and Ningxia Open University, Yinchuan, Ningxia, 750022, China

<sup>3</sup>The Third Oil Transportation Department of CNPC Changqing Oilfield Branch, Yinchuan, Ningxia, 750003, China

**Keywords:** Security System; Internet of Things; Network Architecture

**Abstract:** The universally accepted concept of the Internet of Things was put forward by the International Telecommunication Union. The ubiquitous Internet of Things communication era has arrived, and various information transceiver devices are embedded through familiar articles in life. Another view of "Internet of Things Pan-Technology Theory" holds that Internet of Things technology covers all walks of life applying information technology and involves all fields of information technology research and development. The market of smart grid and airport intrusion detection system alone has hundreds of billions of dollars. At present, due to the rapid development of cloud technology, the improvement of storage capacity and processing efficiency, and the reduction of manufacturing and deployment costs, the use of the Internet of Things has grown significantly in the past few decades. Internet of things technology is still in the research and development stage. There must be some subjective speculation about the technical architecture of Internet of things at this stage. The Internet of things is an extension of the Internet. It includes the Internet and all resources on the Internet and is compatible with all applications of the Internet. But all elements of the Internet of things are personalized and privatized. Aiming at the security requirements and security problems of the Internet of things, this paper studies the system architecture of the Internet of things security, and makes an in-depth study on some key security technologies, hoping to provide a reference for establishing a reliable information security system of the Internet of things.

### 1. Introduction

The Internet of Things connects sensors, controllers, machines, people and things together in a new way by using communication technologies such as local networks or the Internet, forming a network integrating informationization, remote management control and intelligence. The universally accepted concept of the Internet of Things was put forward by the International Telecommunication Union, and the ubiquitous communication era of the Internet of Things has arrived [1]. Various information transceiving devices are embedded through familiar articles in life. People will feel different communication channels from traditional communication methods. Another view of "Internet of Things Pan-Technology Theory" holds that Internet of Things technology covers all walks of life applying information technology and involves all fields of information technology research and development [2]. According to Forester, an American market research company, by 2020, the application business of "Internet of Things" in the world will be 30 times more than that of communication between people [3]. There are hundreds of billions of dollars in the smart grid and airport intrusion detection system market alone. Due to the increase of government and enterprise investment, the Internet of things can be applied in many fields to improve economic activities and quality of life, including transportation and logistics, medical care, environmental monitoring, inventory and other applications and product management, workplace and family support, and safety and supervision [4].

At present, due to the rapid development of cloud technology, the improvement of storage

capacity and processing efficiency, and the reduction of manufacturing and deployment costs, the use of the Internet of Things has grown significantly in the past few decades. At present, the Internet of Things in all countries of the world is basically in the stage of technology research and experiment, and the United States, Japan, South Korea and the European Union are investing huge sums of money to deeply study and explore the key technologies of the Internet of Things [5]. The technology of the Internet of Things is still in the research and development stage, and there must be some subjective speculation when discussing the technical architecture of the Internet of Things at this stage. The security of the Internet of Things is based on the security of the Internet, which needs to be taken as the foundation when formulating the security strategy of the Internet of Things, and the confidentiality, integrity and availability of the security technology of the Internet of Things should also be fully considered [6]. The Internet of things is an extension of the Internet. It includes the Internet and all resources on the Internet and is compatible with all applications of the Internet. However, all elements in the Internet of things are personalized and privatized [7]. How to establish a strict and standardized information security architecture at the early stage of the establishment of the Internet of things is related to whether these systems can provide good security measures under the real Internet of things system, or upgrade the security measures to ensure the availability of the system [8].

## **2. Theoretical basis of IoT security**

### **2.1. The security requirements and characteristics of the Internet of Things**

Today, the important reason for the lack of security mechanism in Internet of Things is that the nodes in the sensing layer are limited by their ability and energy, and their self-protection ability is poor. Moreover, the standardization work of the Internet of Things has not been completed, so that the information transmission protocol in its working process can not be unified. We call the composition architecture of the Internet of Things the conceptual model of the Internet of Things, and different conceptual models of the Internet of Things can produce different technical architectures of the Internet of Things [9]. Nodes monitor various detection objects, thus providing data information transmitted by sensing devices to monitor the operation of the network system. Therefore, when we analyze the security of the Internet of Things, we divide it into three logical layers, namely, sensing layer, transport layer and processing layer. Since the sensor nodes sense independently and transmit data to the information processing system, appropriate encryption mechanism is needed to ensure the integrity of data [10]. In addition, various applications have been developed based on the Internet of things technology, such as combining the Internet of things with the existing network standards, scheduling and optimizing the model of collecting information quality, and developing an intelligent city platform as a service system based on the Internet of things hub. In the current network, more complex algorithms are used to encrypt data to protect the confidentiality and integrity of data. In the Internet of things communication environment, the data transmission volume of a single device is relatively small in most scenarios, and the use of complex algorithms will bring unnecessary delay.

### **2.2. Key technologies for IoT security**

The convergence of the Internet of Things is a particularly worth considering when we formulate security policies. It integrates the communication characteristics of several networks and also integrates the security issues of various networks. As shown in fig. 1.

In fact, some controversial issues in the research and development of the Internet of Things are caused by the complexity of the Internet of Things. In order to minimize the security risks of the Internet of Things system, the system construction and inspection should be carried out simultaneously, and both technology and management should be paid equal attention to in the process of inspection. Moreover, there are many essential differences between the Internet of Things and the infrastructure corresponding to several logical layers. The Internet of Things has been formed and developed rapidly. Internet of Things big data refers to all devices or objects

connected to the Internet, such as smart watches, smart bracelets and even home smart refrigerators. In view of this, with the continuous development and maturity of Internet of things technology, many researchers gradually began to combine Internet of things with security early warning theory to make full use of their respective advantages. It is widely used in transportation, industrial manufacturing, medical and health, disaster emergency response and other fields. In a word, when applying Internet of things security technology, we must consider all aspects of security requirements and deploy system security protection measures, so as to deal with security threats, prevent security weaknesses and carry out all-round security protection.

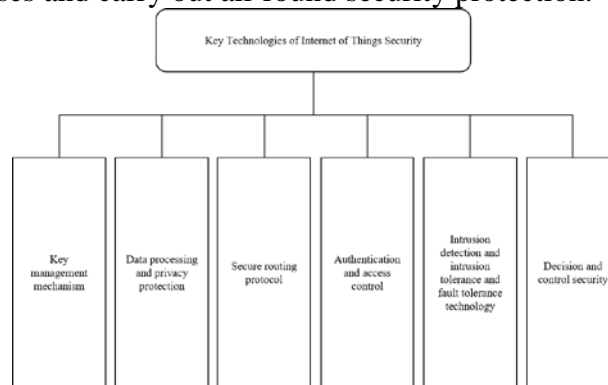


Figure 1 Key technologies of IoT security

### 3. Security architecture based on the Internet of Things structure

#### 3.1. Perception layer security of the Internet of Things

The main factor that distinguishes the Internet of Things from the Internet is the existence of the perception layer, which is at the bottom, directly facing the real environment, has a large base and different functions, and penetrates into all aspects of our daily life, so its security is particularly important. This requires that the Internet carrying the information transmission of goods should have the clock system and coordinate system associated with the physical world, which is the ability that the next generation Internet must expand. For attackers, as long as they enter the network, virus transmission through the transmission network becomes familiar, and has strong concealment, which is more difficult to defend than wired network. In view of China's development speed, many domestic cities have a lot of room to rise, and according to national policies, they will invest huge amounts of money in some living infrastructure to build on a large scale, which will also produce greater economic benefits. As shown in Figure 2.

Digital medical treatment	Modern logistics	Intelligent transportation	Satellite positioning	Space exploration
Disaster prevention and control	Internet of things application			Digital Ocean
Intelligent tourism				Safety monitoring
Digital environmental protection				Smart home
Public safety	Digital low quality	Smart grid	Digital production	Wisdom frontier

Figure 2 Application direction of the Internet of Things

At present, the Internet is consuming about 5% of the world's total energy. The final realization of the Internet of Things requires the introduction of billions of equipment around the world, and the energy consumption will definitely rise sharply. The emergence of system security engineering

means that scientific and engineering principles can be applied to identify security vulnerabilities and minimize or contain the risks associated with these vulnerabilities. Identity authentication and data encryption may be combined, but they need the cooperation of certain cryptographic algorithms.

### 3.2. Network layer security of the Internet of Things

The Internet of Things can transfer the target information quickly and accurately by using the existing communication technology provided by the network layer. Intelligent data fusion technology includes policy-based data fusion, location-based data fusion, time-based data fusion and semantic-based data fusion. Therefore, it is impossible for sensing nodes to have high-strength security measures. However, if the adversary doesn't know the shared key between the gateway node and the telematics platform, he can't tamper with the sent information, and can only prevent part or all of the information from being sent, but this is easy to be perceived by the telematics platform. Based on the organic integration and connection of various mature network technologies, we can realize the integration of the Internet of things, realize the mutual understanding and feeling between objects, people and objects, and truly reflect the intellectualization of the connection between things. At present, it is recognized that the Internet of things has a three-tier structure. As shown in Figure 3.

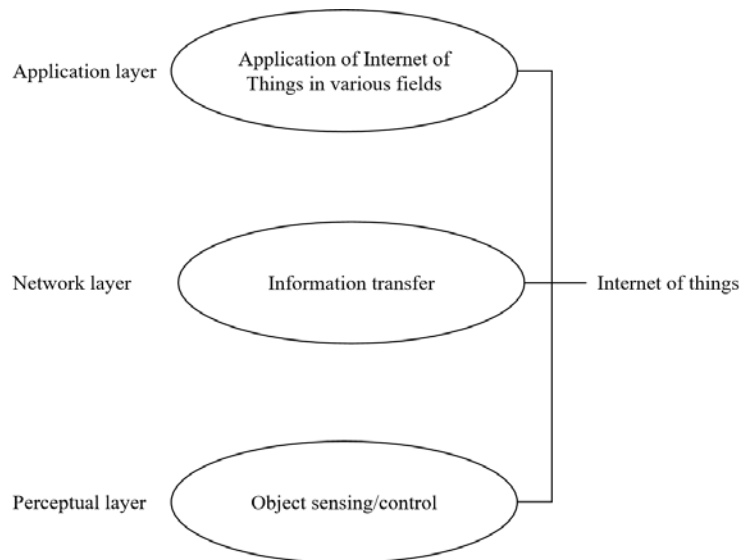


Figure 3 The currently recognized three-tier structure of the Internet of Things

In order to ensure data security, data security management and encryption/decryption algorithms, a secure database must be used. By combining various disciplines, the system suitable for the project is analyzed and designed, so that the various parts of the system can be optimized and controlled. The working principle of system engineering makes it have the characteristics of integration, integration and optimization. At present, the domestic Internet of things is in the primary stage of application, the network security standards have not been issued, and the network architecture has not been formed, but there is no doubt about the trend of network integration.

## 4. Conclusions

The proposal and development of the concept of Internet of Things will affect the information network environment in a deeper and more diversified level, facing the increasingly normal situation of non-traditional security. Aiming at the security threats, this paper studies the detection and inspection from the aspects of Internet of Things system security detection, Internet of Things system risk assessment and Internet of Things integrated security management. With the development of information age, especially the use of e-commerce platform, people have realized that information security is more widely used in commercial market. The security of the Internet of Things is not only a technical issue, but also requires the introduction of corresponding supporting

policies and regulations at the national level and the strengthening of technical standards. This paper discusses that relying solely on information item technology can not form a real Internet of things, and emphasizes that the research and development of Internet of things must pay attention to the research and development of independent network and intelligent application technology to meet the application needs of Internet of things. Therefore, the in-depth research on the security early warning system under the background of the Internet of things is of great significance to all fields of people's daily production and life, and its intelligent system, efficient management and convenient monitoring will also produce significant economic benefits.

## **Acknowledgements**

Supported by the scientific research and development fund of Ningxia polytechnic and Ningxia Open University (XJ202103)

## **References**

- [1] Li Fujuan, Wang Qun. Internet of Things Security System and Key Technologies. *Intelligent Computers and Applications*, vol. 6, no. 003, pp. 32-37, 2016.
- [2] Liu Wei, Wang Dongge. Research on the Security Architecture of the Internet of Things. *Internet of Things Technology*, vol. 6, no. 004, pp. 61-63, 2016.
- [3] Wang Huan. Research on the Security Architecture and Key Technologies of the Internet of Things. *Automation and Instrumentation*, no. 8, pp. 80-81, 2016.
- [4] Li Ruihua, Qiao Yufeng, Liu Feng. Design of Mine Safety Detection System Based on Internet of Things. *Electronic Design Engineering*, vol. 024, no. 002, pp. 135-136, 2016.
- [5] Wang Miaomiao. Research on the security system architecture of the Internet of Things based on the layered concept. *Information and Communication*, vol. 000, no. 010, pp. 86-87, 2018.
- [6] Luo Zhen, Sang Ziqin. Security access and security management platform based on the hierarchical structure of the Internet of Things. *Telecommunications Network Technology*, vol. 000, no. 002, pp. 15-19, 2016.
- [7] Liu Zhihui. Research on an Internet of Things Architecture System Based on Privacy and Security Protection. *Electronic Design Engineering*, vol. 25, no. 014, pp. 115-118, 2017.
- [8] Wu Yunwu, Li Jingliang, Tian Yaoyuan, et al. Research on Bridge Safety Monitoring System Architecture with Internet of Things. *Technician Journal*, no. 76, pp. 39-44, 2017.
- [9] Hong Jun. Analysis of Internet of Things Security System Construction Based on Intrusion Detection System. *Science and Technology Communication*, vol. 10, no. 24, pp. 161-162, 2018.
- [10] Wang Ting, Xu Xiaoquan, Tang Xiaoming, et al. Precise clock synchronization in the Industrial Internet of Things: Theoretical viewpoints of networked control. *Acta Automatica Sinica*, vol. 47, no. 7, pp. 1720-1738, 2021.