Academic Journal of Science and Technology
ISSN: 2771-3032 | Vol. 4, No. 2, 2022

Internet of Things Information Security and Preventive Measures

Minghao Niu, Hong Dai

University of Science and Technology Liaoning, Liaoning Anshan 114051, China

Abstract: The Internet of Things is the third technological revolution of modern information technology. It is a high integration of various new technologies and concepts of modern information technology. It opens up the channel between the previously unrelated technologies such as electronic technology, automation technology, communication technology, biotechnology, mechanical technology and material technology, and makes these technologies truly integrate into a whole. The communication from person to person to object, object to object expansion is realized. The Internet of Things not only drives the development of emerging technologies, but also facilitates daily education and management. However, in the environment of the Internet of Things, there are still some problems of information security, information theft, information disclosure and other problems that must be solved in the application of the Internet of Things technology. Based on the architecture, key technologies and applications of the Internet of Things, this paper explores the security problems existing in the Internet of Things environment and puts forward reasonable preventive measures.

Keywords: Internet of Things, Information security, Precautionary measure, Private protection.

1. Introduction

In recent years, Internet of Things technology has been applied to various fields of production life and work, with smart home, smart agriculture as the representative of the new line of industry has a more far-reaching impact on people's daily life production. With the development of technology, the potential safety problems are caused, especially the security issues of personal privacy. From the perspective of the future development of China, the emerging Internet of Things industry has a lot of room for development. However, it is inevitable that people with ulterior motives will take advantage of the vulnerability of IoT due to its hidden features to steal information illegally, which will greatly affect our use of IoT. Based on this, this paper explores the security problems in the IoT environment from the IoT architecture, key technologies and applications, and proposes preventive measures to protect their information security as much as possible.

2. Introduction of the Internet of Things

2.1. Concept

Internet of Things is an important part of the new generation of information technology and an important development stage in the information age.

Internet of Things (IoT) is not a new concept, it originated from the rapid development of information technology since the information revolution in the 1970s and the profound changes it brought. With the development of the Internet, the popularity of intelligent terminals and mobile devices and the maturity and perfection of the Internet of Things technology, the Internet of Things industry has become the most dynamic and promising area in the development of a new round of industrial change following the computer communications industry and the software industry, and will have a revolutionary impact on traditional industries.

2.2. Key Technologies for the IoT

2.2.1. RFID

If the object can communicate with the person, the person can know the relevant information of the item. Then RFID radio frequency recognition technology must be the key to realize. RFID electronic tag stores the most critical information of the item, through the wireless network to collect them automatically to the central information system to realize the recognition of the item. By scanning it, the corresponding information can be obtained.

2.2.2. Sensor Technology

Sensors are mainly responsible for receiving the content of the "speech" of the objects in the IOT. In the three-layer structure of IoT (as shown in Figure 1), they belong to the sensory layer, just like the sensory system of the human body. Sensor technology is a discipline that obtains information from objects and identifies, transforms and processes the information, and plays a key role in the IoT system.

2.2.3. Wireless Communication Technology

The information transmission between "things and things" and "things and people" is inevitably inseparable from wireless communication technology. Among them, short-range communication technologies such as Bluetooth, WIFI and Zigbee are suitable for information transmission in a small range. Wide area communication technologies such as 4G and 5G are suitable for scenarios with a large range and many devices, and the development of 5G creates unlimited possibilities for IoT applications.

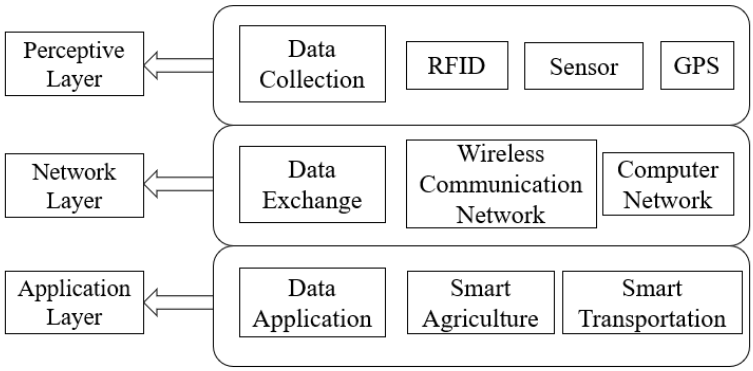

Figure 1. The three-tier structure of the Internet of Things

2.3. Application Status

2.3.1. Application in Agricultural Production

The gradual maturity of IoT technology has made agricultural IoT widely applied to the fields of crop cultivation, poultry and livestock breeding, agricultural product traceability and other typical agriculture. According to the different monitoring objects, it can be further divided into agricultural production environment monitoring Internet of Things, agricultural products quality testing and quality and safety traceability Internet of Things, etc[1].Through the application of IoT in agricultural production, the growth information of crops can be collected by using sensor devices to monitor the growth of crops more intuitively. After establishing a perfect environmental detection and control system, it is possible to intelligently adjust the light intensity and CO2 concentration of the environment at the terminal, making agricultural production more intelligent and manual operation easier and more convenient. It is also possible to trace the source of agricultural products sold in the market through IoT technology to ensure that you can buy and eat with peace of mind.

2.3.2. Application in Daily life

The application of Internet of Things in daily life is mainly reflected in the smart home, which is the deep integration of Internet of Things technology and people's daily life. We can realize the intelligent operation of the equipment at home through the terminal, including intelligent adjustment of lights, intelligent curtain switch, intelligent security, and also set many automatic operations and intelligent services of household appliances. Through IoT, we can realize the intelligent operation of the whole house, the comfort, safety and intelligence of the operation of each device of the smart home system, and realize the information exchange between things and people.

2.3.3. Applications in the field of logistics

The effective integration of technologies such as the Internet of Things, big data and cloud computing with various implementation aspects of logistics and transportation to achieve a state of wisdom is called wisdom logistics, which can improve resource utilization and productivity levels and realize logistics efficiency, informatization and scientization[2]. It is a new form of industry in the context of a new era. At present, there are already many logistics companies to achieve the robot sorting courier, which is installed on the ground sensor equipment to inform the robot delivery route, reducing the manual operation and improving the efficiency of logistics. At the same time, there are now many mature "robot courier", just need to place an order in the cell phone, enter the destination address, the robot can be intelligently delivered

2.4. IoT Development Situation

In recent years, with the continuous development and maturity of technology, the Internet of Things has been widely used in various fields such as industry, agriculture, medical, transportation, construction, etc., and gradually become the core driving force of a new round of industrial revolution. The global development of the Internet of things has entered a period of rapid development. Now developed countries have increased the construction of the Internet of things. Some well-known enterprises have also built their own Internet of things platform, which to a certain extent for the domestic Internet of things industry competitiveness has increased the difficulties[3]. In the government work reports in 2009, 2016 and 2018, the Internet of Things was written three times, including the 19th academician conference of the Chinese Academy of Sciences and the 14th academician conference of the Chinese Academy of Engineering by Xi Jinping in 2018. General secretary of the Chinese Academy of Engineering, proposed to accelerate the breakthrough in the application of a new generation of information technology represented by the Internet of Things and other information technology, which is highly concerned about the development of the Internet of Things[4].

3. Exploration of Information Security in the Internet of Things

3.1. Problems

In the Internet information era, all information is disseminated and shared through the network, which greatly facilitates our daily communication and life. With the development of mobile communication network and Internet, all kinds of data and information can be spread rapidly, and people can realize efficient communication through the network. However, in the era of IoT, although various IoT devices can be interconnected with each other, the infrastructure is weak and there are more security risks. There are many flaws and deficiencies in the network and security infrastructure, making many IoT devices targets for attack. Although the application of IoT technology in various industries has achieved good results in improving the convenience of people's life production and work, there are still many security aspects.

(1) The physical risk of the device itself. The device may

be broken inside the ring or in disrepair, resulting in information leakage.

(2) Network risk. Hackers may carry out network attacks on IoT facilities, resulting in the loss or damage of the information stored in the relevant equipment. It cannot ensure the security of private data. IoT devices through the Internet to other networks for data transmission, and other networks in the user through the device's access control, the theft of user information and privacy.

(3) Interaction risks between devices. Network security professionals may be harmed by wrong data storage and sharing behaviors.

(4) Problems in core technology. The lack of a more complete core technology system and the lack of unified technical application standards cannot ensure the effectiveness of the application of Internet of Things technology in various industries and fields, which adversely affects its long-term development and progress[5]. Outdated security solutions are one of the major issues facing the IoT era. Before the emergence of Internet and mobile communication networks, there was no effective solution to protect network information security. In the IoT era, network information security will be more important and must be paid more attention.

3.2. Analysis of security issues

The issue of information security has become increasingly prominent and its impact has spread to all aspects of society. Sensing devices and the communication network are an open communication network in the IoT. And all kinds of data can be stolen illegally. When compromised or malfunctioned, all these tiny units in sensors can be compromised. This makes the data used in IoT devices can be illegally accessed, tampered with or stolen, which causes damage to the data and threat to information security which has attracted more and more attention from users and industry players. The existence of security vulnerabilities between IoT devices and networks is a well-known fact.

4. Information Security Precautions

4.1. Building and managing secure architectures

(1) Clear security responsibilities: A clear and reasonable organizational structure should be established to regulate the information security workflow from intra-organizational to inter-organizational, and ensure that security responsibilities are implemented through clear responsibilities and authority management.

(2) Conduct comprehensive audits and inspections of all systems or information: timely rectification of non-conformities according to audit results and requirements.

(3) Conduct regular system vulnerability scans.

(4) Appropriate functional extensions should be made to application modules with problems to improve the system's own defense capability.

(5) Appropriate measures are adopted to improve the ability to resist various network attacks.

4.2. Enhance The System's Own Security Prevention Capabilities

(1) Use firewall technology to prevent hackers from launching attacks from servers through the network.

(2) Improve the monitoring capability and detection function of the intrusion detection system to ensure that intrusions are detected and stopped; issue alarm signals to remind users to take protective measures to ensure normal network operation when serious attacks occur on the network; discover and remove suspicious information in a timely manner.

(3) Adopt various means to protect data sources from being accessed or destroyed: establish reliable data transmission channels to prevent data loss, destruction or leakage due to illegal operations during transmission; use encryption technology for important data to protect information from being stolen; avoid using programs that may be damaged or affect their functions.

(4) Real-time monitoring and maintenance and management of the system: ensure that servers, terminal equipment and network connections are normal and not illegally accessed and controlled.

(5) Use a variety of methods to prevent malicious attacks: such as the organic combination of various means to use a variety of methods to prevent computer viruses, Trojan horses and other malicious programs.

4.3. Enhancing IoT System Resilience

(1) Strengthen the security management of the Internet of things, including security management personnel on user information security through certain standards required to develop, implement and implement supervision and inspection to improve network security awareness, strengthen the sense of responsibility, to ensure the safe operation of information systems.

(2) The use of various means to prevent and block the existence of attacks, to prevent the occurrence of network attacks, by strengthening the Internet of things system itself to protect the ability to effectively respond to a variety of risk attacks and sabotage activities and stop processing.

(3) To improve the anti-strike capability of IOT system by differentiating different kinds and levels of threats and implementing effective protection measures, allocating limited resources reasonably and effectively, and improving the overall anti-strike capability.

5. Conclusion

Through the above analysis, we found that the security problems of IoT are mainly concentrated in three aspects. First, there are hidden problems between infrastructure system and information system. Second, users are vulnerable to threats from network level and physical level in the process of use. Third, there are some security loopholes or hidden problems in IoT applications. In this regard, we have the following recommendations. First, the development of relevant national and industry standards, clear network, equipment, application standards, to lay the foundation for the establishment of the IofThings security system. Second, to strengthen the IoT infrastructure construction efforts to improve the quality of network access equipment, improve user awareness of information security and protection capabilities. Third, the existing equipment to upgrade or install information security protection software package to enhance Information security protection capability. Finally, we hope that the state and industry authorities can attach great importance to the IoT security issues and solutions.

References

[1] ZHENG Ji-Ye, RUAN Huai-Jun, FENG Wen-Jie, XU Shi-Wei. Agricultural IOT Architecture and Application Model Research[J]. Scientia Agricultura Sinica, 2017, 50(4): 657-668.

[2] SHI Yu-ping, WANG Jian-ping. Analysis of Problems and Countermeasures in the Development of Intelligent Logistics [J]. Logistics Engineering and Management, 2022, 44(11): 10-12.

[3] WANG Ruidong, LONG Zhenzhen. IoT's contribution to the development of the digital economy [J]. China Economist, 2022, (3):134-135.

[4] HUANG Yun-xia, DONG Zhe-yi, MENG Fan-xin. Research on Security Risks and Countermeasures in the Development of lnternet of Things [J]. Information Security and Communications Privacy, 2020, (5):78-84.

[5] MU Si. Discussing Key Technology of Internet of Things and Application of Computer Internet of Things [J]. Software, 2018,39(06):189-191+208.