Internet of Things Applications and Security in Communication Engineering

Zijun Ma

Beijing-Dublin International College at BJUT, Beijing University of Technology, Beijing, China
Zijun.ma@ucdconnect.ie

Abstract. The Internet of Things (IoT) is a technology that connects everything. It builds an intelligent network of items through radio frequency identification, global positioning, and other technologies so that items can be closely connected. The emergence of the Internet of Things has expanded the boundaries of the Internet and promoted the innovation of the information technology industry, which has become the general trend of current development. The rapid development of the IoT also brings new challenges and security issues. This paper investigates the applicability of a sample-enhanced palm print model in software improvement for large-scale application scenarios by analyzing the two ways of installing hardware security modules on sensors and using sample enhanced fingerprint model to solve data security problems. The method of installing a hardware security module on the sensor is more suitable for smaller application scenarios with higher requirements for data security.

Keywords: IoT, Security, Hardware, Model.

1 Introduction

The Internet of Things (IoT) is a technology that connects everything by embedding software and other components that enable various devices to transmit data and communicate over the Internet [1]. By connecting various items with the network, it realizes the information exchange and communication between objects. The Internet of Things uses a variety of sensing technologies, such as radio frequency identification and global positioning, to build an intelligent item network, so that items can be identified, located, tracked, monitored, and managed. IoT devices enable physical objects to store and exchange data without human intervention, enabling automatic communication between machines [2]. The emergence of the Internet of Things not only expands the boundaries of the Internet but also promotes the innovation of the information technology industry. By integrating the physical world with the digital world, it provides a broader space for innovation in all walks of life [3].

The concept of the Internet of Things originated in 1999 by the Massachusetts Institute of Technology professors and graduate students, and then the International

Y. Yue (ed.), *Proceedings of the 2024 International Conference on Mechanics, Electronics Engineering and Automation (ICMEEA 2024)*, Advances in Engineering Research 240,
https://doi.org/10.2991/978-94-6463-518-8_47

Organization for Standardization in 2003 established the Internet of Things Research Group, laying the foundation for the development of relevant standards for IoT. With the rapid development of technology, technologies such as radio frequency identification and wireless sensor networks have promoted the progress of the IoT, while the popularity of smartphones and 5G technology has further promoted the Internet of Things to enter a new stage. From the initial concept of the Internet of Things to its wide application today, IoT technology has experienced rapid development, and its historical process is full of innovation and practice. With the deep integration of wireless communication, cloud computing, big data, and other technologies, the IoT continues to break through technical bottlenecks and gradually build a stable and reliable system architecture. As a technology and concept, the Internet of Things has great potential and value, which can bring more convenience and intelligent applications to society.

With the rapid development of science and technology, IoT technology has penetrated all aspects of people's lives, from the smart bracelet and watch worn in People's Daily lives to the traffic lights in the city, the IoT not only provides convenience and comfort for people in daily life, with the blessing of the Internet of Things, but people's lives have also become safer and more reliable. As an important part of communication engineering, the application of IoT technology has injected new vitality into the development of the communication industry, but it also brings new challenges, namely, security issues [4]. Security is very important because it can almost determine whether a technology can be widely used [5]. This paper will focus on the analysis of the application of the Internet of Things in sensors and biometrics technology to discuss the application of the Internet of Things in communication engineering and its security issues.

2 Install a Hardware Security Module on the Sensor to Solve the Physical Intrusion

2.1 Physical Intrusion of the Sensor

Over the past decade, driven by the industry, the demand for sensors and drivers has increased dramatically, thus rapidly building the IoT ecosystem [6], and under the general trend, the choice of sensors is often suitable for the Internet of Things, in the wide application of sensors, physical threats have become a key part of solving security problems. However, providing different solutions for different physical threats often leads to excessive security maintenance costs, such as security maintenance costs higher than the value of the sensor itself, which is very unreasonable. However, if it is not regulated, it is likely to lead to core data and information leakage, causing serious security problems.

2.2 Physical Security Module Design of IoT Sensor

Based on the development of the IoT ecosystem, the security of sensors is particularly critical. As an important node of information collection and transmission, the

sensitive information stored in the sensor will pose a serious threat to the whole system once it is illegally accessed or tampered with. To this end, a physical security module is designed for IoT sensors, aiming to ensure the security of sensors through the improvement of hardware level [6,7]. The biggest feature of this solution is its low cost and high efficiency because it is based on existing hardware and encryption technology, without investing a lot of research and development costs, to achieve effective protection of sensor systems.

Specifically, this approach is to add a security module to the sensor that not only has strong encryption capabilities but also can sense and respond to physical intrusions. When users need physical access to the sensor, they can communicate with the security module through a mobile phone application using an NFC or BLE communication interface [8]. In this process, the security module verifies the user's identity to ensure that only authorized personnel can perform operations. Crucially, when someone tries to open the lid of the sensor without authorization, the security module immediately activates the preset security mechanism. These mechanisms may include deleting cryptographic keys stored in the module or blocking access to those keys. Since cryptographic keys are necessary to access system services, once they are removed or inaccessible, compromised sensors will no longer be able to connect to the system's shared services. In this way, our solution effectively eliminates the potential risks that can arise from unauthorized physical intrusions. Even if the sensor is unlawfully turned on, attackers cannot exploit the sensitive information inside it, as the loss or lack of access to the cryptographic key prevents them from gaining further access or compromising other parts of the system.

While protecting the sensor from physical intrusion, how to avoid the data loss problem caused by the security module when triggering security measures is equally important. The deletion or loss of cryptographic keys can be solved to a certain extent by using encryption modules, spare batteries, detection devices, and other devices [9]. In this way, when the sensor is faced with physical intrusion, it can not only avoid the threat of data theft or data tampering caused by physical intrusion but also solve the problem of data loss when the security module protects itself from intrusion to a certain extent.

2.3 Evaluation

The use of encryption modules, spare batteries, detection devices, and other devices to protect the deletion or loss of keys can protect the sensor from physical intrusion to a large extent, but this method has the problem that the current technology is not perfect, and there may be unknown problems caused by imperfect technology. Another problem lies in the use of encryption modules, spare batteries, and detection devices. The cost of the security module itself is nearly double, and the application of the sensor with a small cost often leads to the problem of high-security maintenance costs, which leads to the limitations of this method.

If the data loss caused by key loss or deletion is ignored, then the score situation is discussed. If the data loss has little impact on the overall data, it is necessary to repair or replace each sensor with data loss, but this will generate additional work, and also increase the security maintenance cost of small-cost sensors to a certain extent, and

there are certain limitations. If the loss of data has a significant impact on the overall data, it can be a serious problem.

3 Improve Security with a Sample Enhanced Fingerprint Model

3.1 Development and Problems of Biometric Technology

In the past decade, with the development of the Internet of Things, biometric identification technology has been widely used. People use biometric technologies such as fingerprint recognition and facial recognition in their daily lives to replace traditional physical locks and password authentication. Biometric technology is a technology for identity authentication through human biometrics, fingerprint locks that people see in daily life, and face verification are the application of biometric technology.

Biometric can be seen as a biometric lock with biometric information as the key, which refers to the technology of verifying identity through measurable physical or behavioral biometrics. At present, many security companies, such as Hikvision, Icis, and other world-renowned security companies, have invested a lot of money in the field of biometric technology. Biometric technology is widely used in the field of the Internet of Things due to its excellent performance in identity authentication and security protection, because biometric technology is based on the unique physiological or behavioral characteristics of the human body for identity verification, and these characteristics have a high degree of uniqueness, scalability, and stability. The technology can accurately and reliably identify individual identities and effectively prevent identity fraud and illegal access, which makes biometrics an important means to ensure information security in the Internet of Things. In contrast to traditional authentication methods, biometrics do not need to carry additional equipment or remember complex passwords, and users can complete authentication through their biometrics. This convenience makes biometrics even more advantageous in IoT applications, especially in areas such as mobile devices and wearables.

Although IoT technology has gained widespread attention and application in recent years, IoT devices and associated data are extremely vulnerable to multiple security threats if not properly handled. According to SonicWALL, in 2018 alone, the number of malware attacks faced by the IoT surged by 215.7% [10]. This data fully shows that the security of the Internet of Things can not be ignored, and people need to take effective measures to strengthen the security of the Internet of Things. Since each person's biometric information is unique and difficult to imitate by others, biometrics, as a high-security authentication method, can prevent unauthorized access and malicious attacks to a large extent. However, the current biometrics technology is not perfect, and the biggest problem facing biometrics technology is security.

3.2 Analysis of Existing Biometric Technologies

Existing biometrics can be roughly divided into two categories, namely Behavioral and Physiological, Behavioral can be divided into two categories: signature, voice, Physiological, face, iris, hand geometry, and fingerprint, as shown in Fig. 1.

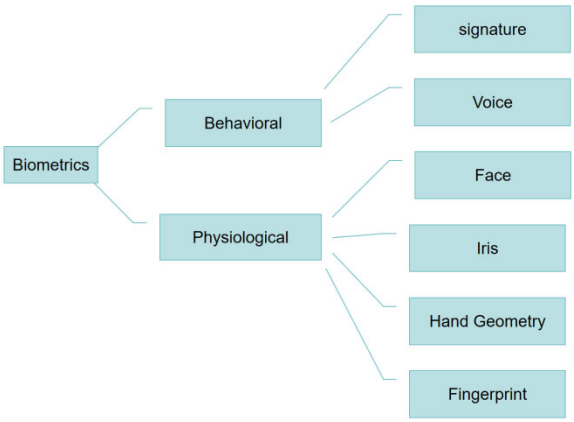

Fig. 1. Existing biometric technology classification.

Face recognition technology is a technology that identifies people by analyzing their facial features. It uses computer vision and image processing technology to extract facial features from images or videos and compare them against known facial databases to verify or identify individuals. Face recognition technology has high efficiency and convenience. Compared with traditional authentication methods, such as passwords or ID cards, face recognition technology can quickly and automatically complete the authentication process, improving the user experience. However, due to the similarity of facial features, changes in expression, occlusions, or facial injuries, the recognition may be inaccurate.

Iris recognition technology is a biometric authentication technology based on the unique features of the human eye iris. The iris, the colored part around the pupil, has a unique pattern that makes it different for everyone, thus improving the reliability of iris recognition patterns. However, the iris recognition model suffers from moderate accuracy and insufficient data, which limits its use in some iris recognition-based applications.

Hand geometry recognition verifies an individual's identity by the width, height, thickness, and circumference of the palm, and the area covered by the fingers. However, due to its limited accuracy, it is usually only suitable for 1:1 classification, and it is difficult to extend to 1: N classification, which has limitations of use. Among them, 1:1 classification refers to the comparison between the sample to be verified and a known sample in the process of identity authentication or identification, which has the characteristics of high accuracy. 1: N classification refers to comparing the sample to be verified with multiple samples in the database in the process of identity

authentication or identification to find a match. This classification method is usually used to find items that match the sample to be verified in a large number of samples.

Fingerprint recognition technology is a kind of identity verification technology based on the unique pattern characteristics of each person's finger skin surface. This fingerprint-based recognition model has made significant progress in the field of personal identification and authentication in recent years, and the technology is relatively mature, and its application has expanded to many fields such as Internet of Things security. The reason why this technology can be widely used is mainly because each person's fingerprint pattern is unique, which can effectively avoid the risk of fraudulent use. However, because fingerprint information is easy to obtain, there are also certain security risks, and fingerprint damage due to burns and other reasons will also lead to inaccurate identification.

Signature recognition technology is a technology that performs identity verification by analyzing the unique behaviors and characteristics of an individual's signature process and is often used in daily business transactions. Although relevant research is ongoing, signature-based recognition models have not yet been generalized. Although the signature is commonly used, it is vulnerable to threats such as forgery and the security level is low, so this identification method is relatively limited in use.

Voice recognition technology is a technology that performs authentication by analyzing the unique characteristics of an individual's voice. This technique uses acoustic properties such as frequency, pitch and timbre of sound to distinguish between different individuals. However, such systems are vulnerable to threats such as voice imitation, and users can easily alter the voice due to physical factors, resulting in inaccurate recognition.

3.3 Sample Enhanced Fingerprint Recognition Model

Compared with the existing biometrics technology, it can be found that fingerprint recognition technology in the existing biometrics technology, in the accuracy of recognition, the convenience of implementation, and also has a certain advantage in cost, indicating that fingerprint recognition has a broader prospect of use. The working principle of a fingerprint recognition model is shown in Fig. 2 [9].

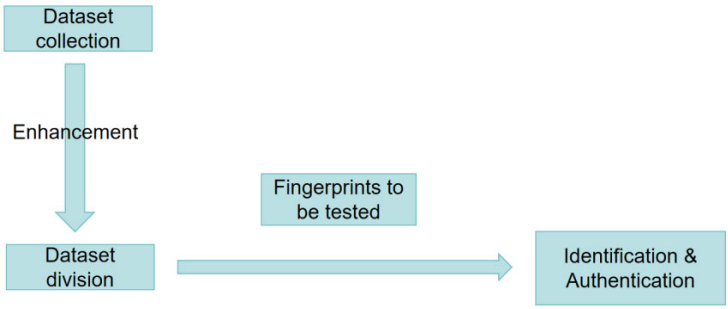

Fig. 2. Fingerprint recognition model principle.

This model first collects the data set and then enhances the collected data. The enhancement process includes three parts: enhancement library processing, enhancement of fingerprint details, conversion to gray level, and enhancement using a directional Gabor filter [9]. The use of the enhancement library can help eliminate the blur of the fingerprint part, and the problem of noise, and make the fingerprint image clearer. The main features of the fingerprint, such as ridges and valleys, are independent of color. Converting the image to a gray level can simplify the processing process and reduce the amount of calculation. The feature of a fingerprint can be extracted by using a Gabor filter. The enhanced dataset is classified by features, and the detected fingerprint sample is first matched with the key part of the data in the dataset utilizing rotation, etc. The 1: N classification algorithm is adopted, and the detected fingerprint sample is searched in the database. Then, for the identity authentication 1:1 classification, the fingerprint sample is matched with each sample image in the database, and the matching rate is greater than 83.33%. Through experimental verification, this method has about 90% accuracy.

3.4 Evaluation

Through an in-depth analysis of various biometric technologies, this fingerprint-based identification technology does show its advantages in many aspects, including feasibility, accuracy, ease of implementation, and subsequent maintenance. Moreover, this sample-enhanced fingerprint recognition model also improves the security of fingerprint recognition to a certain extent through higher accuracy.

4 Contrastive Analysis

Installing hardware security modules on sensors and using sample-enhanced fingerprint models are both applications of IoT in communications engineering, both

of which can protect data security to a certain extent. Both of these methods are protected from the access end of the data. Installing a hardware security module on the sensor can prevent the data in the sensor from being accessed by unauthorized people to protect the data security, while adopting a sample-enhanced fingerprint model protects the data security by improving the accuracy of fingerprint identification and further reducing the security risks caused by fingerprint imitation.

In terms of the protection effect, the security of installing hardware security modules on the sensor is to a large extent better than the sample-enhanced fingerprint model, even if the sensor is acquired by the attacker, it will be unable to obtain the data because of the loss of the key or damage, if the fingerprint system is cracked, the data in the device is likely to be lost. In terms of cost, the cost of sample sample-enhanced fingerprint model may be lower than that of installing hardware security modules on the sensor, especially in scenarios with large requirements for the number of sensors. Installing such hardware modules for each sensor, but also unified management, may require high security maintenance costs. If the application scenario requires a backup battery, the cost of a security module that can protect data in the event of an attack is even higher. However, in application scenarios with high data security requirements, such as military and financial fields, it is necessary to provide special protection for each data. In this case, installing advanced hardware security modules on the sensor is better than the sample-enhanced fingerprint model. In terms of realizability, it is more feasible to adopt the sample-enhanced fingerprint model in application scenarios with large samples, and it is feasible to install hardware security modules on the sensor and adopt the sample-enhanced fingerprint model in application scenarios where the sample size is relatively small and the samples need to be protected separately.

5 Conclusion

The Internet of Things is a hot topic and development trend of the current era, in this situation, security issues have become an urgent problem to be solved. By comparing the two methods of installing a hardware security module on the sensor and using sample enhanced fingerprint model to solve data security problems, this sample-enhanced palm print model on the improvement of software is more suitable for large-scale application scenarios. The method of installing a hardware security module on the sensor is more suitable for smaller application scenarios with higher requirements for data security.

References

1. Kaur, K., Gandhi, V.: Internet Of Things: A Study on Protocols, Security Challenges and Healthcare Applications. 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) 2022, Greater Noida, India, pp. 1206-1210 (2022).

2. Duangphasuk, S., Duangphasuk, P., Thammarat, C.: Review of Internet of Things (IoT): Security Issue and Solution. 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) 2020, Phuket, Thailand, pp. 559-562 (2020).
3. Gupta, A. K., Johari, R.: IOT based Electrical Device Surveillance and Control System. 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) 2019, Ghaziabad, India, pp. 1-5 (2019).
4. Kumar, J., Ramesh, P. R.: Low Cost Energy Efficient Smart Security System with Information Stamping for IoT Networks. 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU) 2018, Bhimtal, India, pp. 1-5 (2018).
5. Sai, G. H., Tyagi, A. K., Tyagi, N.: Biometric Security in Internet of Things Based System against Identity Theft Attacks. International Conference on Computer Communication and Informatics (ICCCI) 2023, Coimbatore, India, pp. 1-7 (2023).
6. Mozny, R., Ilgner, P., Dzurenda, P., Cika, P.: Design of Physical Security for Constrained End Devices within the IoT Ecosystem. 14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) 2022, Valencia, Spain, pp. 85-89 (2022).
7. Suciu, G., Ijaz, H., Pastea, D. V.: The IoT Devices and Secured Communication Architecture and Use Cases. 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) 2019, Dublin, Ireland, pp. 1-5 (2019).
8. Hajn´y, J., Dzurenda, P., Casanova Marqu´es, R., Malina, L.: Cryptographic protocols for confidentiality, authenticity and privacy on constrained devices. 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) 2020, pp. 1–6 (2022).
9. Hu, W., Chang, C.-H., Sengupta, A., Bhunia, S., Kastner, R., Li, H.: An overview of hardware security and trust: Threats, countermeasures, and design tools. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2021, vol. 40, no. 6, pp. 1010–1038 (2021).
10. Ding, C., Xu, C., Tao, D.: Multi-Task Pose-Invariant Face Recognition. IEEE Transactions on Image Processing 2015, vol. 24, no. 3, pp. 980-993 (2015).