Research on Security Verification Mechanism of Perception Layer Terminal of Power Internet of Things Based on Device Operation Fingerprint

Siyao Liu*, Ye Yu, Anle Guo, ZhongYing Zhao, ZongHou Wu, Yi Zhou
State Grid NingXia Electric Power Information & Communication Company, NingXia YinChuan 750001

*Corresponding author: siyao_liu@sgcc.com.cn

Abstract. Integrating the Internet of things technology into the power grid is a major development trend in the future, which can effectively improve the overall performance of the existing power grid. However, due to the traditional Internet of things mainly uses the form of digital password for security protection, due to the low security problems, there are great hidden dangers to the operation of the equipment. For this reason, this paper proposes a security verification mechanism for the perception layer terminal of the power Internet of things based on the device operation fingerprint. In this paper, the biometric fingerprint identification technology and Internet of things architecture are deeply studied, and the fingerprint identification algorithm process and steps are analyzed in detail, and the processing time of each step is compared. In order to improve the comprehensive performance of the security verification of the perception layer terminal of the Internet of things, according to the actual security requirements of the power Internet of things, combined with the biometric fingerprint identification technology, a new security verification system is established. In this paper, the security mechanism of RFID system is adopted, and the performance of fingerprint image filtering is improved by optimizing calculation method and simplifying algorithm. By improving the identity authentication mode and optimizing the data encryption transmission mechanism, the security protection performance of the perception layer of the power Internet of things is further improved. In the simulation test, the system identification accuracy rate of this paper reaches 99.75%, and the software implementation efficiency test results are good, which shows that the system in this paper has high security protection performance, and can meet the current security protection needs of the power Internet of things.

1. Introduction
The Internet of things has been widely used in China's intelligent AC grid, intelligent rail transit and other fields. In the near future, the Internet of things will truly realize interconnection. Interconnection may occur at anytime and anywhere, and then transmit a large amount of information to be exposed in the perception layer [1-3]. If we don't have effective privacy protection measures, the personal information exposed at will in some public places is easy to be monitored, stolen and maliciously interfered by illegal elements. Especially in the current stage of the development of the Internet of things,
if these widely existing sensor devices are illegally damaged or manipulated, it will pose a new threat to the national and personal information security [4-6].

The main types of traditional data recognition and analysis technology include data recognition and analysis technology based on physical objects and data recognition and analysis technology based on text knowledge. However, these two kinds of electronic identity information authentication communication technologies also have some major defects: electronic identity information authentication technology methods based on different physical authentication objects are easy to be lost or forged [7-8]. In knowledge-based authentication method, complex information is not easy to remember and simple information is not reliable. In biometric identification technology, fingerprint identification technology has the advantages of easy collection; high security, high cost performance, and has developed rapidly in recent years. At present, fingerprint identification technology is divided into two categories: PC based fingerprint identification technology and embedded fingerprint identification technology [9-10].

This paper deeply studies the security verification mechanism of the power Internet of things in our country in the aspect of perception layer, and understands that the physical verification method is mainly used for security protection. Due to its low security performance, easy to be attacked, weak protection ability and other major problems, it has brought serious hidden dangers to the safe operation of the power Internet of things. Therefore, this paper puts forward the research on the security verification mechanism of the perception layer terminal of the power Internet of things based on the device running fingerprint, hoping to improve the overall security protection performance of the power Internet of things in China through the biometric fingerprint identification technology and the reconstruction of the security protection mechanism. In this paper, the authentication mechanism of RFID is proposed, including the improvement of the security mechanism of the system. In the corresponding simulation test, the system in this paper has achieved good results in recognition accuracy and recognition efficiency. The analysis shows that the security of the perception layer of the power Internet of things is related to the security of the whole power Internet of things system. Therefore, it is necessary to strengthen the security verification mechanism of the perception layer. The research in this paper has achieved ideal results and made a contribution to the research in this field.

2. Internet of Things and Fingerprint Identification Technology

2.1. Brief Introduction of Fingerprint Identification Technology
In operation, fingerprint identification technology can be divided into four modules: (1) fingerprint collection; (2) fingerprint preprocessing; (3) feature extraction; (4) fingerprint matching. The principle of fingerprint input collection is to generate the data distribution of fingerprint image lines by inputting fingerprints of related electronic devices; fingerprint preprocessing is to process the fingerprint texture image data obtained after fingerprint acquisition by fingerprint segmentation and two-dimensional numerical processing; Fingerprint feature extraction is to extract the key texture features of fingerprint based on the prediction and processing of fingerprint image data; fingerprint image matching is used to determine whether the fingerprint image comes from the same or two people. Fingerprint identification is one of the most reliable identification application technologies, which has a long history. At present, there are a large number of automatic fingerprint identification products in various fields.

2.2. Internet of Things Architecture
The system structure of the Internet of things can be divided into three layers: perception layer, network layer and function layer. The key technologies of each link are wireless sensor network technology, intelligent network information processing system technology and wireless network data transmission technology. Sensor recognition technology refers to the acquisition of sensing technology through laser sensors, RFID and other multimedia devices to achieve accurate perception and visual recognition of the external real world. Intelligent information processing and cooperation technology is to realize information collaborative processing by building intelligent application system middleware such as data
processing and storage, data mining, information processing and display. Network information transmission technology through a variety of wired and wireless network transmission technology, to achieve high-speed and security of network information wireless transmission. The role of the perception layer is equivalent to the original information collector, which is often the most easy to control and destroy. For the Internet of things, security management and control is particularly important, in which the security of big data and information will become an important basis for the information security of the entire industrial Internet of things system.

3. Analysis of Fingerprint Identification Algorithm Process and Steps

The efficiency of fingerprint recognition algorithm determines the accuracy and accuracy of fingerprint identification. Fingerprint recognition has two standards: false acceptance rate and false rejection rate. The first error acceptance rate is the ratio of the number of identical fingerprints in the database to the total number of comparisons. The second false rejection rate is the ratio of the number of times correct fingerprints are excluded from the database after comparison to the total number of comparisons.

In order to improve the reliability of fingerprint image, it is necessary to segment and evaluate fingerprint image. In the fingerprint identification algorithm, due to the complexity of each process, the operation time is different, but the time proportion of each step, whether embedded system or PC, should be similar. Therefore, we can carry on the corresponding simulation on the PC, and use the simulation effect to evaluate the embedded system. As can be seen from Table 1, there are several projects that require the most time in different parts. At present, some excellent fingerprint processing algorithms can achieve high performance, but the operation time is also very long, which is not conducive to the application of embedded system.

| Algorithm                         | Time |
|-----------------------------------|------|
| Fingerprint segmentation, pattern calculation, filtering and enhancement | 68%  |
| Binarization                      | 4%   |
| Refine                            | 8%   |
| Remove the fake                   | 5%   |
| Feature point extraction          | 7%   |
| Fingerprint matching              | 8%   |
| Total                             | 100% |

4. Discussion

4.1. Test Results and Analysis

The algorithm is simulated on PC with MATLAB 7.0. Taking the fingerprint database of public data set as the test object, there are 10 groups of fingerprint images in each database, each group has 10 different collected same fingerprint images, a total of 10 databases, 1000 fingerprint images. The database is relatively complete, including various types of fingerprints. 15000 automatic matching experiments have been carried out on 10 fingerprint databases, and the test results are shown in Figure 1. According to the test results in Figure 1, the number of correct matching is 14963, the number of false rejections is 24, and the number of error recognition is 13. The recognition accuracy is 99.75%, the false recognition rate is 0.16%, and the false recognition rate is 0.09%. Experimental results show that the algorithm has high recognition rate and strong anti-noise ability.
On this platform, two algorithms are implemented by C language programming. Their software implementation efficiency is shown in Figure 2. Compared with the results in Figure 2, the efficiency of the improved algorithm is significantly higher than that of the clefia-128 algorithm. It should be noted that lightweight cryptographic algorithm is mainly used for hardware implementation, so the software implementation efficiency under 64-bit platform is not high compared with other commonly used cryptographic algorithms.
4.2. Security Mechanism of RFID System in Internet of Things
At present, there are two solutions to the security and privacy problems of RFID system in the Internet of things: physical method and logical method diagram. Physical methods include active interference, blocking tags, etc. The logic method mainly refers to the logical encryption method based on cryptography technology, which uses authentication and encryption means to ensure the security of communication information between reader and tag. So far, experts at home and abroad have proposed a variety of RFID system security authentication protocols, but these protocols have their own defects, it is difficult to meet the security requirements of the Internet of things RFID system. Although some people have proposed encryption security system based on chaotic algorithm, the label is strictly restricted. Due to the need to put a large number of tags on the Internet, it is difficult to support complex and high-cost encryption system to ensure the communication between security tags and readers. Therefore, it is necessary to improve the security mechanism of RFID in the application of the Internet of things and improve the security of the security mechanism.

4.3. Fingerprint Image Filtering and Enhancement
The fingerprint image is divided into 20 * 20 size, and its direction is taken as the direction of window \( l \times w \) with point \((i, j)\) as the center, and it \( w \) is consistent with the direction of the block. \( l \times w \) in this paper, \( l = 32 \), \( w = 16 \) calculate the average gray value of 32 pixels. The details are as follows:

\[
X[k] = \frac{1}{w} \sum_{u=0}^{w-1} G(u,v), k = 0,1\ldots l-1
\]  

(1)

\[
u = i + \left( d - \frac{w}{2} \right) \cos o(i, j) + \left( k - \frac{1}{2} \right) \sin o(i, j)
\]  

(2)

\[
v = j + \left( d - \frac{w}{2} \right) \sin o(i, j) + \left( k - \frac{1}{2} \right) \cos o(i, j)
\]  

(3)

If there is no singular point in the direction, \( X[k] \) forms a sine wave with the same frequency as the ridge frequency of the local fingerprint, so \( X[k] \) obtains the ridge frequency from it.

4.4. Identity Authentication
The C4.5 algorithm of decision tree is used to train the decision tree by using the past situation factors of user app or DTU equipment, and the latest situation factors are classified. Through the data set, the situation factor fingerprint of fingerprint table in database is summarized, and the optimal feature of C4.5 algorithm is selected. Finally, the classification results are output in the form of text. At the same time, the latest fingerprint matching classification results can reflect whether the fingerprint information is successfully matched. Through the authentication management module, the matching results are analyzed. The task of authentication management is to judge the result of identity authentication, and pass it to the corresponding step module in turn to complete the matching work or open the authentication problem for subsequent processing. If the fingerprint information of Mirai matches under certain conditions, there will be a corresponding warning prompt to prevent the corresponding authentication access.

4.5. Data Encryption Transmission Mechanism
The identification information collected by the sensor on the node needs to be transmitted to the server through the network. In order to prevent the attacker from using the data transmission channel to obtain the valid data of the node, the node must be encrypted. This paper uses trusted chip to encrypt data transmission.
(1) The hardware data encryption control module corresponding to the node can execute nonce instruction, and the hardware data encryption control module can generate 32-byte unique random function RN.

(2) The node sends data to the encryption module. The data is encrypted to the chip, and the information authentication code mac is generated to verify the integrity of the message and decrypt the data.

(3) The node sends the obtained authorization certificate token and encrypted data to the server.

(4) After the server receives the data and checks the token, it sends the data to the server encrypted chip for decryption, and finally saves it in the database for future use.

(5) When the server sends data to a node, it exchanges encrypted and decrypted objects.

5. Conclusions
In this paper, the security verification mechanism of the perception layer terminal of the power Internet of things based on the device operation fingerprint is studied in depth. The analysis shows that the overall performance is not high due to the backward security verification technology in the perception layer of the power Internet of things. The perception layer is the main application in the whole Internet of things, and its security is particularly important. Therefore, it is necessary to further improve the security mechanism. The proposed security verification mechanism based on biometric fingerprint identification technology, to a certain extent, makes up for the shortcomings of the traditional verification mechanism, and plays a positive role in improving the security protection ability of the perception layer. Through the optimization and improvement of the security system in this paper, the overall security performance of the power Internet of things is further improved. In the related simulation test process, the recognition accuracy and recognition efficiency are greatly improved compared with the traditional security system. The analysis shows that the power Internet of things has a broad development prospect, and it is also a new requirement of the times for the development of electric power. However, the backward security verification mechanism greatly limits the development speed. And the research in this paper has achieved ideal results, which plays an important role in the research and development of this field.

References
[1] Bera, S., Misra, S., & Rodrigues, J. J. P. C. (2015). Cloud computing applications for smart grid: a survey. Parallel & Distributed Systems IEEE Transactions on, 26(5), 1477-1494.
[2] Erol-Kantarci, M., & Mouftah, H. T. (2015). Energy-efficient information and communication infrastructures in the smart grid: a survey on interactions and open issues. Communications Surveys & Tutorials IEEE, 17(1), 179-197.
[3] Nadeem, J., Sakeena, J., Wadood, A., Imran, A., Ahmad, A., & Atif, A., et al. (2017). A hybrid genetic wind driven heuristic optimization algorithm for demand side management in smart grid. Energies, 10(3), 1-27.
[4] Chang, S. F., Chen, C. F., Wen, J. H., Liu, J. H., Weng, J. H., & Dong, J. L. (2015). Role of internet of things in the smart grid technology. Journal of Power & Energy Engineering, 03(4), 356-361.
[5] Wang, X. F., Mu, Y., & Chen, R. M. (2016). An efficient privacy-preserving aggregation and billing protocol for smart grid. Security and Communication Networks, 9(17), 4536-4547.
[6] Sha, K., Alatrash, N., & Wang, Z. (2017). A secure and efficient framework to read isolated smart grid devices. IEEE Transactions on Smart Grid, 8(6), 2519-2531.
[7] Lin Chuqiao, Tong Hui, Yu Wenfang, Xin Yechun, & Zhang Rufeng. (2019). Distribution grid intelligent state monitoring and fault handling platform based on ubiquitous power internet of things. Journal of Northeast Dianli University, 039 (004), 1-4.
[8] Song, F., Zhu, M., Zhou, Y., You, I., & Zhang, H. (2020). Smart collaborative tracking for ubiquitous power iot in edge-cloud interplay domain. IEEE Internet of Things Journal, 7(7), 6046-6055.
[9] Bayram, S., Sencar, H. T., & Memon, N. (2015). Sensor fingerprint identification through
composite fingerprints and group testing. Information Forensics & Security IEEE Transactions on, 10(3), 597-612.

[10] Kumar, A., & Kwong, C. (2015). Towards contactless, low-cost and accurate 3d fingerprint identification. Pattern Analysis & Machine Intelligence IEEE Transactions on, 37(3), 681-696.