Research and Application of Security and Privacy in Industrial Internet of Things Based on Fingerprint Encryption

Cong Xie(✉) and Shu-Ting Deng

School of Information Engineering, Guangxi University of Foreign Languages, Nanning 530222, China
ningjianfeng123@126.com

Abstract. Industrial Internet of things is developing with a high speed, but it also faces the threat from all sides. In order to deal with the security applications of industrial Internet of things, this paper summarizes the security and privacy issues of industrial Internet of Things, then analyzes the common security threats and attacks, and draws on several kinds of fluent security measures, putting forward the security program of Fingerprint encryption. The program combines the fingerprint identification technology, PDF417 code and RC4 encryption method, matching through the fingerprint data to be decoded out. Because the fingerprint information is unique, whether the success of the match can determine whether the operation is by itself, and then decides the next step, protects the user's security and privacy in a great degree.

Keywords: Industrial Internet of Things · Fingerprint technology · PDF417 code · RC4 encryption

1 The Development of Industrial Internet of Things

With the development of industrial technology and intensify of market competition, in order to improve efficiency and product quality, making full use of resources, reducing labor intensity, meeting the needs of mass production, industrial automation came into being. Then, with the development of information technology, industrial automation broke through the limitations of LAN, enterprise information system will be extended to the Internet, achieving the fifth generation of Internet-based industrial automation technology–industrial networking technology.

Industrial Internet of things is related to the traditional things for a few different things: the Internet of Things architecture has a perception layer, transport layer and application layer, but industrial Internet of Things applications are closed-loop, while the other is open-loop; Internet of Things is not so strict to the real-time of the network, but industrial networking has strict requirements of the time synchronization and stable communication; Internet of things is not demanding on the equipment working environment, but industrial Internet of Things is not only in a high temperature, humidity

F. Chen and Y. Luo (Eds.): Industrial IoT 2017, LNICST 202, pp. 102–110, 2017.
DOI: 10.1007/978-3-319-60753-5_11

and vibration and other harsh environment, but also maintaining smooth in complex network interference.

At present, the industrial Internet of Things is still at the early stage of development, but because of its broad application prospects and huge revenue potential, many large multinational corporations, governments and international organizations have invested heavily in industrial Internet of Things. Such as the second Internet of Things Forum Cisco hosted, Cisco exhibited more than 250 industrial applications case; in 2014, General Electric achieves 1 billion in revenue increase for its global customers through industrial Internet of Things technology and services; Huawei is the acquisition of Neul which is a company of industrial Internet of Things British startups. At the national level, the Chinese and German governments have had a high-level dialogue about jointly promoting the development of "Industrial 4.0", developing two strategy that major manufacturing countries deepen cooperation in the Internet of things and cloud computing and other related technologies.

In addition, international organizations such as Industrial Internet Consortium (IIC), AllSeen Alliance and Open Interconnect Consortium (OIC) 6 have been set up in the world.

According to Accenture research report, the global industrial Internet of Things market size in 2012 reached 20 billion US dollars, expected in 2020 will be more than 500 billion US dollars in recent years will have a high growth. At the same time, based on the current level of input, by 2030, industrial Internet of things is expected to bring at least $10 trillion to the world economy, while investment based on sustained increases suggests that by 2030, Reaching 14 trillion dollars.

At present, Chinese industrial Internet of things is in the initial formation of the industrial chain, which's main gainers of industrial profits, are the equipment manufacturers and system integrators. As the industry matures, the market demand for services will become stronger, network operators and platform providers will rapidly rise in profits, and will become the industry's main profit earners. With the implementation of 《Made in China 2025》 , the next decade, Chinese manufacturing industry will greatly enhance the overall level of information technology, manufacturing digital, network, intelligent will make significant progress. Digital Research and development design tools, key processes manufacturing equipment NC will be used as the basis of industrial Internet of Things and in the above-scale enterprises will be widely used also.

Industrial Internet of Things develops in China fast, but the overall level is not as good as abroad. The development of industrial Internet of Things in China basically has the following characteristics: small-scale enterprises, low level of technology Research and development; technical standards behind the application development; the number of application level is low; lack of industry talent, industrial development environment needs to be further improved, the industry management system to be improved. Therefore, at present, foreign enterprises have monopolized the industrial Internet of things in China. Although technology import substitution has promoted the development of local enterprises, foreign enterprises have monopolized industries such as smart grid, railway, oil and gas, etc. It has a large potential threats to information security, which requires us to make breakthroughs in the field of industrial Internet of Things. With

Chinese enterprises to gradually replace foreign enterprises, it also greatly promote the development of domestic industrial Internet of Things.

2 The Security and Privacy of Industrial Internet of Things

Enterprise users and individual users in the enjoyment of industrial Internet of things personalized service, at the same time, will also face their own privacy information which may be leaked because of "ubiquitous" network environment and "get in by every opening" hackers. In addition, the industrial Internet of things project is completed by a number of network nodes, collaborative data output during the node will also cause privacy leaks. Therefore, how to protect the privacy of users is an urgent problem to be solved.

From the industrial Internet of things point of view, the perception layer is mainly based on the sensor field devices; at present, the specific potential attacking against the industrial Internet of things are mainly the following:

(1) Attacks on the node. Mainly on the node control and node capture. Node control is due to the network attacker access to the network node within the Shared secret or gateway nodes and remote information processing platform between the Shared secret leaked; Node capture not involves the secrets of network nodes, but can block nodes to compromise network connectivity, or to obtain network privacy by identifying the type of sensor and inferring the mode of operation of the network.
(2) Attacks on RFID systems. RFID, also known as radio frequency identification, is a communications technology that allows radio signals to identify specific targets which can read and write related data without establishing a mechanical or optical contact between the system and a specific target. Companies prevent theft, improve inventory management, easy inventory of stores and warehouses. Besides, the use of RFID technology, which can greatly reduce consumer waiting time in front of the checkout counter. However, with the development of RFID technology and the increasing popularity of RFID tags, security issues, especially user privacy, are becoming more and more serious. If a user uses a product with an insecure label, which is read by a nearby reader without the user's perception, thereby disclosing personal sensitive information such as money, drugs (associated with a particular disease), a book (Which may contain personal preferences), etc., in particular, may expose the user's location privacy, so that users are being tracked.

In addition, due to the introduction of industrial control systems of the industrial network, there are some forms of attack that are not available in other fields, such as resonance attacks: In the implementation of this attack, the network attacker will force the existing physical system to produce resonance near the specific frequency through the illegal control of the sensor or controller, which will destroy the normal operation of the system. Clock synchronization attack: for strict industrial control system, it belongs to the timing system, the network attacker can spread the false clock message to destroy the unified system clock, so as to achieve the purpose of attack; Control system

attacks. In this attack, the network attacker will influence the correct evaluation of the current network state through the interference control system, and forge or replay the control command to implement the forgery attack, the tampering attack of the sensing data and the control network DOS attack.

3 Industrial Internet of Things System Security and Privacy Solutions

At current protection technologies and measures, mostly concentrated in the industrial application of things level, the application of technology are: data dissemination, data mining and wireless sensor networks. Specific privacy protection methods are:

(1) Anonymization method: it is the most important one kind of technical means of privacy protection in data mining. It protects privacy by blurring sensitive information.
(2) Encryption method: this method is the original plaintext file or data by an algorithm to deal with, making it unreadable code, usually referred to as "ciphertext", so that it can only be entered after the corresponding key to show the original content, in such a way to achieve the protection of data from unauthorized persons to steal, the purpose of reading. The reverse process of this process is decryption, that is, the process of converting the encoded information into its original data.
(3) Routing protocol method: This method is generally used for wireless sensor network node location privacy protection, generally based on random routing strategy, that is not every packet transmission from the source node to the convergence layer, a certain probability of the packet away from the convergence layer in the direction of transmission, while the transmission path will change. Each data packet transmission path will be randomly generated, which makes the attacker to obtain accurate location information on the node becomes difficult, so as to achieve the purpose of security.

In summary, to the current level of industrial networking, a lot of industrial networking security system is built on the existing mobile network based on the industrial sensing network and industrial application platform integration, gathered together. In addition, in the traditional network architecture, the network layer and the business layer are separated from each other in the security and protection level and independent, while the industrial Internet is due to constitute the specific way and specificity. At the same time, although the industrial Internet of things referred to the Internet information network model, the industrial Internet of things for industrial production, reliability, data integrity, real-time and security requirements are high. Therefore, the security mechanism needs to be supplemented and adjusted according to its characteristics.

4 Fingerprint Recognition Overview

Biometrics is the combination of computer and optical, acoustic, biosensor and biostatistics principles, using the inherent physiological characteristics of the human body

(such as fingerprints, face images, iris, etc.) and behavioral characteristics (such as handwriting, Voice, gait, etc.) for personal identification. According to the IBG (International Biometric Group) statistics, the market has a variety of applications for different physiological characteristics and behavioral characteristics. Among them, the highest share is the fingerprint identification. Fingerprint recognition is currently the most widely used one. Fingerprinting technology to a person with his fingerprints, by comparing his fingerprints and pre-stored fingerprints to compare, you can verify his true identity. Each person (including the fingerprints) is different in pattern, breakpoint, and intersection point, that is, unique, and remains unchanged.

Two fingerprints often have the same general characteristics, but the details are not exactly the same. Fingerprint lines are not continuous, smooth straight, but often interrupted, fork or transition. These breakpoints, bifurcation points and turning points are called "feature points".

The feature points provide the fingerprint identification information, the most typical is the end point and bifurcation point, the other also includes bifurcation point, isolated point, ring point, short lines etc. The parameters of feature points (including the direction of node can toward a certain direction) and curvature (description of pattern direction change speed), position (the position of the node is described by x/y coordinates can be absolute, can also be compared to the triangulation points or feature points). The typical fingerprint feature points are shown (Fig. 1):

（a）End point （b）Bifurcation point

Fig. 1. Typical fingerprint feature points

Fingerprint identification to achieve a variety of ways. Some of which are modeled after traditional methods used by the public security department to compare local details of fingerprints; some are identified directly by all features; and others are more unique, such as corrugated edge patterns of fingerprints and ultrasound. Some devices can instantly measure finger fingerprints, while others do not.

5 The Concrete Application of PDF417 Two-Dimensional Code

PDF417 two-dimensional bar code is a stacked two-dimensional bar code, currently the most widely used. PDF417 bar code is invented by the US company SYMBOL, PDF (Portable Data File) means "portable data files". Each bar code composed of bar code by the four and four empty 17 modules, it is called PDF417 bar code. PDF417 bar code need to have 417 decoding function of the bar code reader to identify. PDF417 bar code biggest advantage lies in its huge data capacity and strong error correction capability. The following Fig. 2 shows the PDF417 two-dimensional code:

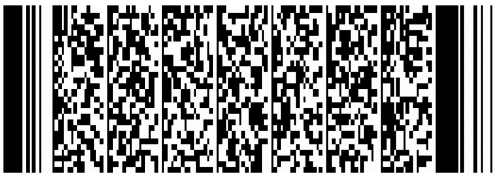

Fig. 2. PDF417 two-dimensional code

Because fingerprints are the key to identity recognition, fingerprint encryption provides a strong fence for user security and privacy. Fingerprint information is encrypted to generate PDF417 bar code. It Can effectively protect the user's security and privacy. In addition, the fingerprint can also be encrypted to prevent forgery of fingerprints to enhance the security of identification.

The workflow of a typical fingerprint identification system is as follows (Fig. 3):

(1) Acquisition of the required fingerprint image through the fingerprint acquisition device.
(2) The collected fingerprint images are processed as follows:
   - Image quality judgment
   - image enhancement
   - Fingerprint region detection
   - Fingerprint pattern and frequency estimation
   - Image two value (the gray value of each pixel in the fingerprint image is set to 0 or 255)
   - Image thinning
(3) From the preprocessed image, the ridge line data of the fingerprint is obtained.
(4) The required feature points of the fingerprint identification are extracted from the ridge data of the fingerprint.
(5) The extraction of fingerprint features (feature points) in the database and the preservation of the fingerprint feature matching one by one, to determine whether the same fingerprint.
(6) After the completion of the fingerprint matching process, the output of the fingerprint identification processing results.

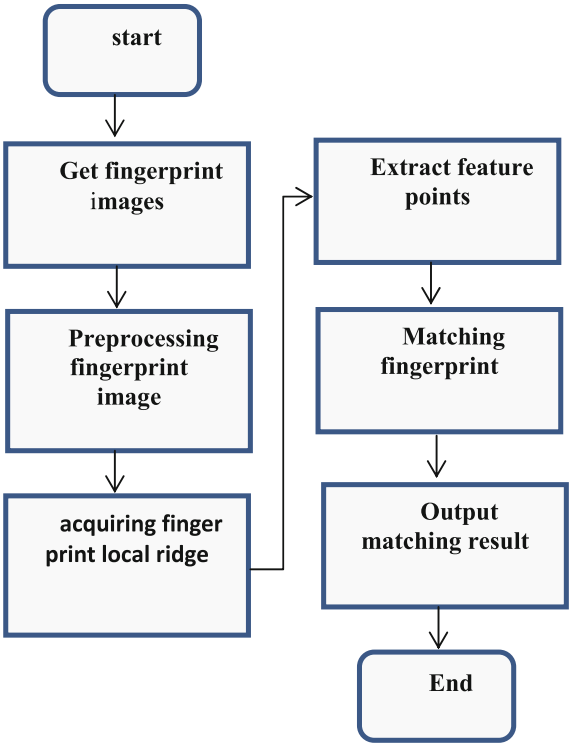

Fig. 3. Fingerprint identification process

Through the above process of fingerprint identification can be seen, the fingerprint identification system does not take the form of encryption, which makes criminals easily illegal access to fingerprint information, which has a negative effect on the security and privacy of users, thereby undermining the production safety. The structure of the current fingerprint identification system is shown in the following Table 1:

Table 1. Structure of fingerprint identification system

Upper application system		
Fingerprint classification	Recognition and Matching	Fingerprint compression
Fingerprint acquisition device		

In this paper, the use of RC4 algorithm for encryption and decryption. RC4 algorithm is a kind of electronic information in the field of encryption technology, for wireless communication network, is an electronic password, only authorized (to pay the corresponding fee) users can enjoy the service. RC4 algorithm characterized by the algorithm is simple, fast, and the key length is variable, variable range of 1–256 bytes (8–2048 bits), in today's technology support, when the key length is 128 bits, it is not feasible to use the violent method to search for the key. Therefore, it is expected that the key range

of RC4 can still resist the attack of violent search key for a long time. The structure of the data encryption system is shown in the following Fig. 4:

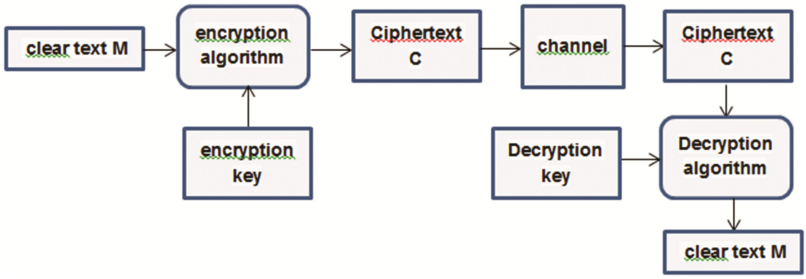

Fig. 4. Structure of data encryption system

In fact, there is no effective attack method for RC4 encryption algorithm with 128 bit key length.

6 Concluding Remarks

Industrial Internet of things in the traditional Internet of things based on the integration of the Internet, WSN and field bus network and other related technologies, and then have the environmental awareness of various types of terminals, cloud computing model, mobile communications, real-time communication into industrial production Link network, in today's industrial environment, the application prospects are very good.

In order to adapt to the security applications of industrial Internet of things, this paper mainly studies the industrial objects networking to strengthen the protection of users' security and privacy through the combination of fingerprint identification technology, PDF417 code and RC4 encryption methods, to promote the industrial networking and industrial networking security. The reference role. Industrial Internet of Things technology is rapid progress in all directions, but in the long run, industrial production and management of the demand continues to increase, the requirements of security technology also continue to put forward new challenges.

References

1. Yang, Y.: Ning executive loop. Research on the security and protection technology of industrial object networking. Intell. Process. Appl. 65–66 (2015)
2. Liu, D.: Fingerprint encryption two-dimensional code in the file management system application research. Zhejiang University of Technology, Zhejiang (2015)
3. Chen, H.: Entropy analysis based on fingerprint identification and encryption algorithm application research. Xidian University, Xi'an (2012)
4. Liang, T.: PDF417 two-dimensional code of the fingerprint encryption and identification. Liaoning University of Science and Technology, Liaoning (2015)

5. Wang, H., Li, Y., Mi, M., Wang, P.: A method of data fusion based on supervisory mechanism for industrial Internet of Things Safety. J. Instrum. Instrum. 817–824 (2013)
6. Ji, J.: Industrial Internet of Things security technology. Jiangnan University, Wuxi (2012)