Security Transmission and Storage of Internet of Things Information Based on Blockchain

Nana Liang*
Henan Industry and Information Technology Professional College, Henan, Jiaozuo, 454000

*Corresponding author e-mail: liang-na@163.com

Abstract. The Internet of Things is developing rapidly. Many devices around us are connected through the Internet, and humans have entered the era of the Internet of Things. However, while many devices are connected to the Internet, it also provides more attack surfaces for hackers, so the security issues of the Internet of Things are becoming increasingly prominent. This paper uses asymmetric encryption algorithms and blockchain technology to build a key-based security architecture. In terms of information security transmission, this article uses ECC (Elliptic Curves Cryptography, Elliptic Curve Cryptography) and DH (Diffie-Heilman key exchange, Diffie-Heilman key exchange) as encryption tools for the entire architecture, not just for encrypted communication between IoT devices is also used for encrypted communication between IoT Internet of Things (IoT) devices and Raft service clusters, thereby ensuring the privacy of sensitive information and the efficiency of data communication. In terms of information security storage, this article uses the blockchain data structure and consensus algorithm to achieve reliable storage. Considering the real-time nature of the Internet of Things, the Raft consensus algorithm is adopted. This consensus algorithm has strong consistency in the existing blockchain consensus algorithms, which is more in line with the requirements of the final consensus consensus algorithm of public chains such as POW. The blockchain data structure is used to store the public key data content submitted by each IoT device. The hash pointer in the blockchain data structure guarantees the integrity and difficulty of change of the stored data.

Keywords: Block Chain, Internet of Things, ECC Asymmetric Encryption, D-H Key Exchange Protocol

1. Introduction
The word "Internet of things" has been widely recognized at home and abroad. It was first proposed by Professor Ashton in 1999 when he was studying RFID (radio frequency identification). Since its development, it has been widely used in transportation, intelligent manufacturing, health care, finance, petrochemical and other commercial and national infrastructure industries, so the information security and privacy issues of the Internet of things are related to the national economy and people's livelihood,
and the research on the information security protection technology of the Internet of things is imminent [3-4]. Compared with the traditional Internet, if intruders successfully invade and attack the Internet of things system, they will gain more interests or social attention, which also leads to more and more illegal people trying to invade the Internet of things system in all walks of life [5]. Intruders use a variety of attack methods, such as DDoS (distributed denial of service) attack, data disclosure, control terminal control and hijacking [6].

In recent years, we have seen the explosive growth of IOT devices. From smart watches to smart homes, people began to mass produce and purchase these devices with network functions [7]. According to the forecast, there will be more than 21 million Internet of things devices in the world by 2020 [8]. Whether it is health monitoring system or remote control home thermostat, IOT equipment makes people's life more and more comfortable and convenient [9]. However, with more and more IOT devices connected to the Internet, the possibility of these devices being attacked is also growing, especially the sensors that send important data of users or the IOT devices that perform certain actions according to the command should do a good job in security defense [10]. Relevant researchers of the Internet of things system found that the distrust, transparency and security mechanism of blockchain technology can guarantee the communication security of the Internet of things, and can verify the identity of the Internet of things devices by establishing a decentralized consensus mechanism, so as to improve the privacy of the Internet of things [11]. The introduction of blockchain technology can improve the current situation of the lack of security of the Internet of things. Taking blockchain technology as the support technology for the security of the Internet of things can provide better security for the Internet of things, thus promoting the development of the Internet of animals and reducing the cost of the application of the Internet of things [12]. It is also proposed that blockchain technology is the foundation of the Internet of things era, so it is of great significance to study how to use blockchain technology to improve the information security of the Internet of things system.

This paper first uses the super ledger fabric of the open source blockchain project to build a simple, private, Internet of things platform running on the blockchain network. On the basis of this experimental platform, the information security technology is designed and intrusion tolerance test is carried out for all levels of the Internet of things by using relevant blockchain technology. In this paper, PBFT (Practical Byzantine fault tolerance) algorithm is studied deeply, and a general information security transmission technology of Internet of things is designed and implemented based on the algorithm. Under the security technology designed in this paper, the transmission message is encapsulated by an envelope structure to achieve the compatibility of different Internet of things transmission protocols. Each data transmission between nodes will no longer pass a single central server, but will pass a consensus module deployed by multiple nodes through a cluster. Multiple nodes in the module will verify the transmission information, including information transmission The identity of the party and the authenticity of the message content. In this paper, the distributed storage method is used to design the block suitable for the data of the Internet of things, and the block chain storage structure is used to store the key location information in the Internet of things system safely, so as to ensure that the data cannot be tampered with or stolen.

2. Method

2.1 PBFT Consensus Algorithm
In the blockchain network system, consensus is a process in which multiple participants reach an agreement on whether a transaction is submitted to the ledger and the order of submission. Consensus and consistency problems are often discussed together, but in fact, they are not the same, and consensus algorithms tend to solve more extensive problems. In the blockchain network system, consensus algorithm is used to reach an agreement on a proposal, including endorsement strategy, transaction sequencing, whether to include transactions in the account book and other transaction processes involving consensus algorithm.

According to FLP impossibility theory, there is no consensus algorithm that can solve the problem
of consistency. Therefore, consensus algorithm should be selected according to the requirements of the distributed system and the use scenarios, but this does not mean that the research on consensus algorithm is meaningless. According to cap principle, the system can do better in consensus problem at a certain price. Cap principle means that distributed system cannot guarantee consistency, availability and partition tolerance at the same time. Therefore, for specific distributed application scenarios, you can choose to weaken one of the characteristics of the system, and in blockchain network, you can choose to weaken availability or weaken partition tolerance to improve the feasibility of consensus algorithm. Therefore, a consensus algorithm appears a variety of excellent consensus algorithms.

PBFT uses services as state machine to model, which is a replication algorithm of state machine. Each replica saves the state of the service, and represents the total set of nodes in the network as N, while I represents each node replica. Assuming that the number of malicious nodes in the network is f, through the analysis of Byzantine problem in the previous section, we know that there must be at least 2F + 1 normal nodes in the network, that is, the total number of service nodes in the whole network must be at least \( n = 3F + 1 \).

The replication node performs an operation when the view configuration is successful. In the traditional PBFT algorithm, one node is selected as the primary node of the view and the rest is selected as the backup node. The view is an integer with consecutive numbers. When the primary node fails, the view modification process begins. The primary node is generally calculated by formula (1), where \( V \) represents the view number, \( M \) represents the replica node number in the network, and \( R \) represents the number of nodes in the network.

\[
M = V \mod R
\]  

(1)

3. Experiment
Step 1: Firstly, the research status of blockchain technology at home and abroad and the information security research status of the Internet of things industry are summarized and analyzed, and the security requirements and threats of all levels of the Internet of things system are analyzed. Through the research of super ledger fabric blockchain project, further research on blockchain related technologies are conducted, and the application prospect and feasibility of blockchain technology in the security of the Internet of things are analyzed. Secondly, the paper proposes a scheme of using the block chain consensus algorithm to design an Internet of things transmission information security technology and using the block structure to store the Internet of things network data securely.

Step 2: Design and implementation of Internet of things transmission information security technology based on PBFT algorithm. Combined with the relevant components of the blockchain platform, the transmission information security technology suitable for the Internet of things is designed and implemented. It mainly includes the design and implementation of IOT node management module, transmission message structure design, transmission information encryption and identity authentication module and PBFT consensus module. Finally, taking the industrial Internet of things data monitoring system as the test platform, the paper tests the protection against three kinds of attack threats in the process of data transmission, and tests the robustness of the Internet of things network system after using the security transmission technology, and compares the security effect with the traditional security technology.

Step 3: Secure data storage technology of Internet of things based on block structure. Combined with the data characteristics of the Internet of things system, firstly, the total structure of the Internet of things data storage technology is designed, including block structure design and implementation, block file manager design and implementation. Then, the security performance and storage efficiency of secure storage technology are tested and analyzed. The research work of Internet of things information security technology based on blockchain is summarized and analyzed, and the significance of the research results and the further research direction in the future are described.

4. Discuss


4.1 Implementation Result Analysis

Compared with the traditional IoT, the security system combines the blockchain technology, which has significantly improved the security of the whole network. The specific security comparison is shown in Table 1. With the characteristics of blockchain technology decentralization, information openness and transparency, secure communication, hard to tamper with after writing blocks and multi-party consensus, it ensures the safe storage of information records of IOT devices. In the security system, the information records of the modification needs to go through half, and the confirmation of the node on increases the difficulty of the attacker to tamper with the records, and ensures the integrity of the information records. The authority management and consensus algorithm for identity can help the system effectively identify the receiver of the illegal node, and the chain structure of the block chain can facilitate the construction of effective electronic storage card for the illegal node. The security comparison between traditional IOT and security system is shown in Table 1.

Table 1. Security comparison of traditional IoT and security systems

|                      | Information integrity | Privacy protection | Secure storage | Reliance on trusted third parties |
|----------------------|-----------------------|--------------------|----------------|-----------------------------------|
| Traditional IoT      | Incomplete            | √                  | √              | ×                                 |
| Security system      | Complete              | √                  | √              | √                                 |

In the front, the functional test of the modules under the secure transmission technology is carried out, and the performance of the secure transmission technology needs to be tested and analyzed, that is, whether the system throughput and response time have changed greatly before and after the PBFT based secure transmission technology is adopted. The throughput changes are shown in Figure 1.

Figure 1. Data acquisition time comparison between not started and started

Through comparison, we can see that the average throughput is 33.484mbps before enabling secure transmission technology, and 32.531mbps after enabling secure transmission technology, a decrease of about 2.93%.

4.2 Experiment Summary

The use of blockchain structure can only increase the characteristics that can not be reduced, so that any data operation in the Internet of things network will be completely recorded, providing data traceability, which ensures that malicious operations of any illegal elements will be exposed, and improves the security of data storage. In data storage, digital signature and encryption technology are used to ensure the privacy of data. At the same time, with the increase of the amount of data in the Internet of things network, the block structure using Merkel tree and hash technology can guarantee the storage efficiency, so it can greatly improve the storage security of the Internet of things data without losing the storage efficiency.

4
The above tests the encryption and decryption of communication data and the blockchain of stored data of the whole security architecture. Among them, the asymmetric encryption and decryption test is carried out to submit IOT public key data and obtain the public key data of the other side of IOT communication, and the expected effect is achieved; the generation of symmetric session key between IOT devices is also tested, and the session symmetric key generated by both sides of IOT communication is the same; for the blockchain storage of data, the consensus process of raft cluster and the query of blockchain data are mainly tested.

In general, the above experimental tests basically meet the requirements of security architecture in data communication encryption and data storage reliability. However, the setting of the random period value of raft cluster heartbeat detection needs to be further improved in the future practice. When the performance of physical equipment allows, the random period value should be reduced as much as possible, which is more in line with the real-time nature of the Internet of things communication.

5. Conclusion

With the arrival of the era of IOT intelligence, more and more IOT devices come into people's production and life, but at the same time provide more attack surfaces for attackers. This paper studies and tests the key security architecture of the Internet of things based on blockchain and other technologies to realize the secure communication between IOT devices and service center, and the efficient secure communication between IOT devices. At the same time, because the public key data corresponding to each IOT device is saved through the blockchain data structure, it is not only difficult to tamper with, but also for the later group permission setting of each IOT device It provides convenience.

References

[1] David Yermack. Corporate Governance and Blockchains[J]. Social Science Electronic Publishing, 2017, 21(1):7-31.
[2] Suveen Angraal, Harlan M. Krumholz, Wade L. Schulz. Blockchain Technology: Applications in Health Care[J]. Circ Cardiovasc Qual Outcomes, 2017, 10(9):e003800.
[3] Jiawen Kang, Rong Yu, Xumin Huang. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains[J]. IEEE Transactions on Industrial Informatics, 2017, PP(99):1-1.
[4] Esther Mengelkamp. A blockchain-based smart grid: towards sustainable local energy markets[J]. Computer Science - Research and Development, 2018, 33(1-2):207-214.
[5] Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang. Untangling Blockchain: A Data Processing View of Blockchain Systems[J]. IEEE Transactions on Knowledge & Data Engineering, 2017, PP(99):1-1.
[6] M.A. Razzaque, Marija Milojevic-Jevric, Andrei Palade. Middleware for Internet of Things: a Survey [J]. IEEE Internet of Things Journal, 2017, 3(1):70-95.
[7] Andrei Palade, Christian Cabrera, Fan Li. Middleware for internet of things: an evaluation in a small-scale IoT environment[J]. Journal of Reliable Intelligent Environments, 2018(4):1-21.
[8] Edwin Cartlidge. The Internet of Things: From Hype to Reality[J]. Optics & Photonics News, 2017, 28(9):26.
[9] Jeffrey M. Perkel. The Internet of Things comes to the lab[J]. Nature, 2017, 542(7639):125-126.
[10] JAN F. TESCH, ANNE-SOPHIE BRILLINGER, DOMINIK BILGERI. Internet of Things Business Model Innovation and the Stage-Gate Process: An Exploratory Analysis[J]. International Journal of Innovation Management, 2017(5):1740002.
[11] Godfrey Akpakw, Bruno Silva, Gerhard P. Hancke. A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges[J]. IEEE Access, 2017, 5(12):3619-3647.
[12] Orlando Arias, Jacob Wurm, Khoa Hoang. Privacy and Security in Internet of Things and Wearable Devices [J]. IEEE Transactions on Multi-Scale Computing Systems, 2017,
1(2):99-109.