Analysis of Using Blockchain Technology to Solve the Security Problem of the Internet of Things

Weijun Lei

School of Information Engineering, Xi'an University, Xi'an, Shaanxi, China

Keywords: Internet of Things, blockchain, security issues, architecture.

Abstract: In recent years, the Internet of Things technology has developed rapidly, and the Internet of Things applications are rapidly expanding. Due to the problems of Internet of Things security, privacy, reliability, etc., Internet of Things applications have been limited. This paper starts with the three-tier architecture of the Internet of Things and analyzes the main security issues facing each level. Based on the analysis, the characteristics of decentralization, trust mechanism, data encryption and time series of blockchain technology are used to explore and solve the security problems of the Internet of Things, and enrich the Internet of Things security method to improve the security of the Internet of Things.

1. Introduction

The Internet of Things (IoT) is an information industry chain that integrates information and communication technologies such as networks, sensors, cloud computing, and big data. For example, smart home, smart transportation, smart medical care, etc. are the specific applications of the IoT.The IoT generally has three major characteristics, namely, comprehensive perception, reliable transmission, and intelligent processing .

Due to the openness, ubiquity and multi-source heterogeneity of the IoT, the IoT faces serious security problems such as private disclosure. How to use emerging technology to solve the problems of security, privacy and reliability in the development of the IoT has become a real problem that needs to be solved urgently. For example, blockchain technology can solve some of the security issues of the IoT.

2. The Main Security Issues in the IoT

The IoT is an open architecture. Currently, the three-tier architecture of the IoT is generally recognized. The structure adopts a bottom-up hierarchical architecture, which is mainly divided into: a sensing control layer, a network interconnection layer and an application layer, as shown in Fig.1 .In order to more clearly describe the security issues of the IoT, this paper starts with the three-tier architecture of the IoT, and analyzes the security issues faced by the IoT.

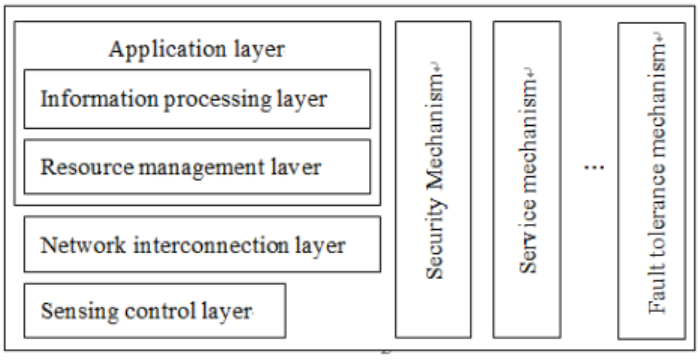

Fig. 1 Three-tier architecture of the IoT

2.1 IoT Perceived Control Layer Security Risks.

The perceptual control layer is the foundation of the IoT architecture. Its main function is to

  DOI: 10.25236/systca.18.005

collect, identify and control information. This function is composed of sensing devices and gateways. Due to the wide variety of perceived objects, the perceived nodes exhibit multi-source heterogeneity, and generally lack comprehensive and effective monitoring. And because most of the terminal nodes are exposed, it is more vulnerable and faces more security threats.

Signal leakage and interference

The attacker intercepts, falsifies, falsifies, replays, and so on the data and signaling transmitted in the sensor network, and obtains user sensitive information or causes information transmission errors, resulting in the failure of the service to proceed normally.

Forgery or spoofing

The attacker can also use the security flaws of the IoT terminal to obtain the identity and password information of the node, and the fake identity communicates with other nodes to perform illegal actions or malicious attacks.

Tag embedding threat

When the IoT collects data from the sensing control layer, its information transmission method is mainly wireless network transmission. This kind of signal method may embed the label in the IoT perception control layer into any substance, which means the item or even the user itself. Being in a monitored state directly leads to the information contained in the embedded tag that poses a potential threat to the privacy of the individual. May pose a huge threat to trade secrets and public safety.

2.2 Network Interconnection Layer Security Risk.

This layer implements access to the sensing control layer information and transmits the data obtained from the sensing layer to the IoT service platform. The network interconnection layer mainly realizes communication through network infrastructure such as mobile communication network, internet, satellite network,etc. Since the collected information needs to be integrated through various networks, the transmission path will go through various networks, and the IoT is a multi-network overlay. The open network, so security issues will also overlap.

Transmission data destruction

Because the amount of data transmitted by devices in the IoT is small, complex encryption algorithms are generally not used to protect data, which may result in theft, tampering, attack, and destruction of data during transmission.

Heterogeneous network convergence

The IoT is an open network that is superimposed by multiple networks. As the network continues to merge, the network structure becomes increasingly complex, and network communication protocols in the network layer continue to increase. When data is transferred from one network to another, it involves many issues such as identity authentication, key agreement, data confidentiality and integrity protection, and the security threats will increase greatly.

2.3 Application Layer Security Risk.

The application layer is an interface between the IoT system and the user, providing users with personalized services, identity authentication, privacy protection, and providing user operation instructions to the processing layer. Since the application layer is directly facing the outside world, it is the most sensitive and risky part.

Data Security. The IoT application layer stores a large amount of user data, how to effectively store data, avoid data loss or damage, how to avoid data service blocking, and the rapid recovery of data after a failure is a security issue that the application layer needs to consider.

Authentication and access control. The authentication method adopted by the application layer of the IoT is the message verification code when the sender and the receiver determine the communication. However, during the communication process, the authentication code is static and easy to be used by others, resulting in false authentication success, which leads to security problems. Therefore, there are still a large number of security issues in the process of access control.

2.4 IoT System Architecture Security Risk.

The current operating environment of IoT devices is a traditional centralized system that requires a trusted third party to manage the identity information of all devices. However, there are many devices in the IoT environment, which will put a lot of pressure on trusted third parties. The IoT requires a decentralized operating environment, and a new trust mechanism needs to be established to maintain consensus among devices and ensure the overall operation of the system.

3. New Ideas for Solving the Problem of IoT Security by Using Blockchain Technology

Most of the solutions to the IoT security problem are not only complicated but also costly. There is a need for a lightweight technology and mechanism to address the security issues of the IoT. The blockchain provides security-related technologies for the IoT and improves the problems of the IoT system architecture without delay.

This article will introduce blockchain technology and its architecture to provide lightweight and decentralized security and privacy protection for the IoT. Blockchain technology is actually a distributed database technology [1].In a blockchain, information or records are placed in blocks, and then cryptographically signed "chain" Go to the next block, as shown in Fig. 2.These blockchains have complete copies on every node of the system, and all information is time stamped and can be traced back. Therefore, the blockchain implements a brand-new credit system, which is a system that does not require trust. The blockchain system is not affected by users at the same time, and cannot be destroyed at the same time.

Through the security risk analysis of the IoT three-tier architecture and the overall architecture of the system, its security issues are mainly reflected in data security, privacy leakage and authentication, access control and system centralization. Security issues are addressed from the technologies and mechanisms included in the following five blockchains[2].

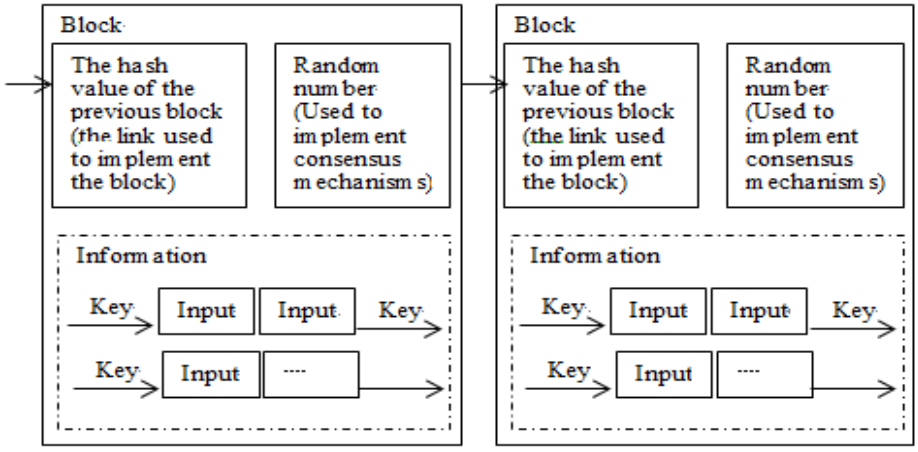

Fig. 2 Link model of blockchain

3.1 Data Encryption and Digital Signature in Blockchain Technology.

There is an asymmetric encryption algorithm called elliptic curve encryption algorithm in blockchain technology. The principle is a pair of mathematically related keys, data information encrypted using one of the keys, and the information can only be decrypted using another key. A valid transmission above the blockchain has a digital signature that is valid for transmitting the initiator private key signature, and the signature of the transmission can be verified by using the public key of the transmission initiator. The public key can be calculated from the private key by an algorithm, but the private key cannot be pushed out of the public key. The principle of asymmetric cryptography is used to sign the data transmission process so that the signal cannot be forged. At the same time, the hash algorithm is used to ensure that the data in the transmission cannot be easily falsified. It can effectively solve the security problems such as signal leakage or forgery of the IoT awareness layer, spoofing attacks, data protection of the network interconnection layer, and ensure

the normal operation of the application layer authentication and access mechanism.

3.2 Distributed Database in Blockchain.

The block in the blockchain is similar to a notepad, recording all the transmission information on the blockchain, and the information of each user's transmission content is permanently embedded in the data block for others to verify the query. The data information in these data blocks is stored in each user's client node, and all of these nodes constitute a distributed database system. Therefore, the destruction of data of any one node will not affect the normal operation of the entire database, because the complete database is stored in other healthy nodes [3]. The blockchain distributed database structure can creatively store data efficiently to avoid data loss or corruption.

3.3 Using Timestamps and Non-defective Modification of Blockchains.

A timestamp is usually a sequence of characters that uniquely identifies a moment. In the blockchain, the node that obtains the transmission right needs to stamp a time stamp in the block header when linking the block, and is used to record the write time of the current block data. The timestamp in each subsequent block enhances the previous timestamp to form a time-increasing chain [4]. Applying timestamps in blockchain technology is a major innovation. Timestamps add a time dimension to future IoT and big data based on blockchain, making data easier to trace, and timestamps can be used as important parameters for proof of existence. It can confirm that certain data must exist at a certain moment, which ensures that the blockchain database is not tamperable and unforgeable. Time series is used to ensure the security of IoT data, preventing attackers from injecting a lot of dirty data into the data platform to prevent data services from being blocked. The block structure is shown in Figure 3[2].

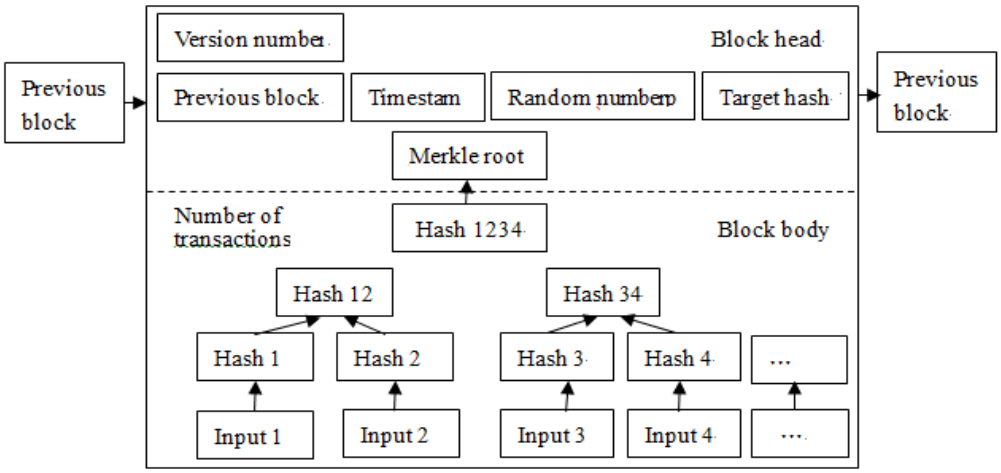

Fig. 3 Block structure

3.4 Consensus Mechanism Using Blockchain Systems.

The blockchain system uses the address linked to the user's public key to make the user's identity. By running a consensus algorithm on the entire network node, the consensus of the honest nodes in the network to the state of the whole network is established, and the trust between the nodes is indirectly established. Users only need to open the address, do not need to disclose the real identity, and the same user can constantly change the address. Therefore, the transmission on the blockchain is not linked to the user's real identity, but is linked to the user's address, which protects the user's privacy and has anonymity. Therefore, the consensus algorithm and mechanism can be applied to protect the privacy of users in the physical network [5].

3.5 Decentralization Using Blockchain Technology.

Decentralization is the most prominent feature of blockchain technology. The process of storing, transmitting, and verifying blockchain data is based on a distributed system structure [6], and there is no management mechanism between each node. As a deployment model of the blockchain, all

participating nodes in the public chain network can have the same rights and obligations. When data is transmitted from one node to another, the receiving node first verifies the identity information of the node, and if successful, broadcasts the received information throughout the network. The decentralized features can improve the centralized state of the existing IoT and prevent the entire IoT system from being damaged due to the destruction of the central node.

4. IoT Application Blockchain Technology Security Example

The core strengths of blockchain technology are decentralization and consensus mechanisms. By using hash algorithm, digital signature, time stamp, distributed consensus, etc., credit is established in distributed systems where nodes do not need to trust each other, and point-to-point transmission and cooperation are realized, which is insecure in the centralized structure of physical network system. And the problem of privacy and easy disclosure reveals a better solution. The following is an example of using the blockchain technology to improve the security of the Internet of Vehicles.

Internet of Vehicles is a typical application of IoT technology in the field of transportation systems. The entire system network is based on the in-vehicle network, the inter-vehicle network and the in-vehicle mobile Internet. In accordance with the agreed communication protocols and data interaction standards, wireless communication and information transmission and exchange are carried out between vehicles, roads, pedestrians and the Internet. With the gradual popularization of the Internet of Vehicles technology, in-vehicle systems have become more and more popular, but the security risks of the Internet of Vehicles have been exposed, and some systems have been invaded and interfered. For example, the Tesla Model S was invaded, and the network security expert opened the door and opened the loop through the vulnerability of the Model S. At the same time, it could send a "suicide" command to the Model S to suddenly shut down the system engine while the vehicle was running normally. Therefore, system intrusion, data transmission and signal interception or interference in the Internet of Vehicles are the biggest hidden dangers of safe driving. The asymmetric encryption technology and digital signature technology in the blockchain are used to realize that the signals in the transmission are not easily intercepted. At the same time, the hash algorithm is used to ensure that the data in the transmission cannot be easily falsified, and the security of the signal transmission process is ensured. At the same time, the timestamp technology in the blockchain ensures that the physical network database is not tamperable and unforgeable, preventing the attacker from threatening the security of the car network system by changing the data in the database [7].

5. Conclusion

With the development of the IoT and blockchain technology, the consensus mechanism and decentralized architecture of the blockchain will provide a more secure environment for the IoT, realizing a truly distributed database and system architecture. The time stamping technology, encryption technology, signature technology and blockchain database are not tamperable and unforgeable, which ensures the security of data transmitted by the IoT. Blockchain technology provides better technical support for IoT security.

Acknowledgements

This study is supported by the Xi'an Social Science Plan project (16WL12).

References

[1] Z.J.Yao, J.G.Ge.A Summary of the Theory and Application of BlockChain.e-Science Technology & Application, 2017 (2):3-17.

[2] Y.N.Jiao,Y.H.Chen. Research on Blockchain Technology in the Security Field of IoT,Computer Engineering & Software,2018,39(2):88-92.

[3] Y.D.Li,Z.Yang,etc. Technology Architecture of IoT Security. Journal of Information Security Research, 2016, 2 (5) :417-423.

[4] N.Zhang,Y. Wang, etc. Blockchain Technique in the Energy Internet. Proceedings of the CSEE, 2016, 36 (15):4011-4023.

[5] H.Fan,H.Shao,etc. Research on Security Technology Architecture of EPC global Network. Netinfo Security,2011(9):5-8.

[6] Z.Q.Wu,Y.W.Zhou,etc. A Security Transmission Model for Internet of Things. Chinese Journal of Computers,2011,34 (8) :1351-1364.

[7] P.He,Y.Ge,etc.Survey on Blockchain Technology and Its Application Prospect. Computer Science,2017,44 (4):1-7+15.