Eng Int Syst (2025) 3: 239–248

Engineering
Intelligent Systems

Construction of Internet of Things Resource-Sharing Platform Based on Intelligent Information Processing from the Perspective of Network Security

Bin Wang[a] **and Yumin Ye**[b]*

Library, Guangdong Polytechnic of Industry and Commerce, Guangzhou 510510, Guangdong, China

The Internet of Things (IoT) technology has become part of the daily life of many people, with its advanced concept, convenience and practicality, and has played a huge role in many aspects. The application of the IoT technology can establish a sound intelligent service system that plays a positive role in the productivity of enterprises and the lives of individuals. Taking into account the characteristics and needs of the current various types of large-scale IoT businesses, this paper designs a set of cross-domain business management solutions, unified modeling, unified identification and unified representation, thus enhancing the scalability of applications. Open industrial services provide a bridge for different industries and achieve cross-industry and cross-field service cooperation. The application of the IoT in many fields, through data sharing and resource sharing, enables systems in various sub regions to be connected to each other for the purpose of exchanging and sharing information. In this study, a data-based, fine-grained access control mechanism is designed, which uses three layers of access control permissions to ensure that access to data legally authorized during the data exchange process, and to prevent data leakage and illegal access. Hence, this paper proposes a secure resource sharing system based on the IoT, with a minimum energy consumption of 28 milliseconds. The method proposed in this paper effectively prevents a collusion attack by malicious members, thereby improving the control of access to resources and confirming that this protocol performs well in terms of ensuring the security of data.

Keywords: IoT Resource Sharing Platform, Network Security, Intelligent Information Processing, IoT Services

1. INTRODUCTION

At present, the IoT has been widely used in transportation, logistics, industrial control, medical and health industries, and smart homes. Especially in high-risk fields such as disaster early warning and disaster relief, the application of the IoT is unparalleled. With the development of IoT technology, data sharing and interaction have become more efficient. IoT devices can generate and exchange massive amounts of data, facilitating the sharing of information and strengthening harmonious business cooperation. Therefore, how to ensure the safe sharing of user data, avoid the leakage of sensitive information, and protect the privacy of users are important issues at present. Access control technology is key to security and reliability, and has been widely used to ensure data security. However, access control still has problems

*Corresponding author. Email: [a]wangbin@gdgm.edu.cn, [b]yeyumin@gdgm.edu.cn

associated with security issues such as privacy disclosure, fixed access rights, system vulnerabilities, etc.

The security of the IoT is the problem causing the most concern. Lee believes that in the IoT environment, security and interoperability may be important obstacles to the implementation of the IoT in the real world [1]. Amiruddin maintains that the IoT has become a new paradigm of current communication technology and needs a more in-depth overview to describe its application fields, advantages and disadvantages [2]. Magaia found that the significant development of the IoT has enabled the development of many devices, which can improve many aspects in various fields of smart cities. He also discussed the security challenges facing this emerging field [3]. Sfar discovered that communication entities (objects or things) in the IoT environment play an active role in human activities, systems and processes. He discussed security issues related to privacy, trust, identity, and access control. He also investigated and discussed current standardization measures taken intended to ensure the security of IoT components and applications [4]. Jurcut found that the interconnection of "things" and devices in the form of wearable devices, sensors, mobile phones, computers, instruments and even vehicles, is an important requirement of the current era. The security of the IoT plays a central role, and there is no room for error. He conducted a survey on IoT security, aiming to highlight the most important security-related issues in the IoT ecosystem [5]. Because the solutions to the IoT security problems proposed by these scholars are not very effective, this paper discusses network security in depth.

Network security concerns the privacy security of computers. Fernandes found that in recent years, the application of the IoT has been rapidly developed and deployed in various fields. He gave an overview of IoT security attacks and classified them based on application fields and underlying system architecture. He also discussed several key features of the IoT that make it difficult to develop a robust security architecture for IoT applications [6]. Alrawais discussed the security and privacy issues in the IoT environment, and proposed a mechanism that uses fog computing to improve the distribution of certificate revocation information among IoT devices to enhance security [7]. Aydos explained the vulnerabilities of the IoT, classifying the types of attacks that threaten the physical layer, network layer, data processing layer and application layer. In addition, he proposed a risk-based security model by examining the vulnerabilities and threats of intelligent objects that generate the IoT. The proposed IoT model is an overall security model that assesses the vulnerabilities and threats at each layer of the IoT based on the risk level method [8]. Banerjee discovered that IoT devices were increasingly appearing in civil and military environments, from smart cities and smart grids to medical IoT, Internet of Vehicles, military IoT, battlefield IoT, etc. He investigated articles on IoT security solutions, including the lack of publicly available IoT data sets for research and practitioner communities [9]. Bertino believed that the recent distributed denial-of-service attacks indicate the high vulnerability of IoT systems and devices. To solve this challenge, it is necessary to provide solutions for scalable security of the optimization of the IoT ecosystem [10]. However, the network security issues raised by these researchers have not been addressed successfully.

In order to ensure the security of the data when sharing it via the IoT, it is necessary to encrypt the data and set the threshold function to give access rights to users. Due to the complexity of the IoT access environment, the disclosure or malicious attack on users' personal privacy and shared resources has become problematic. Therefore, appropriate measures should be taken to ensure the safety and reliability of information resources. This paper presents an access control protocol based on authorization, and also gives the specific implementation method and results obtained for this protocol. In order to prevent the leakage of information resources and ensure the security of information resources, all users' shared information resources must be encrypted before being uploaded to the cloud server. When accessing data resources, terminal members are accessed and graded according to the attributes giving them the right to access information with different levels of sensitivity, which prevents the leakage of sensitive information and improves the flexibility and efficiency of access. Finally, the accuracy, security and performance of the proposed protocol are analyzed. The scheme can be used to access resources in resource-constrained platforms. After the model is initiated, the usage of heap memory fluctuates regularly between 88.35Mb and 289.59Mb.

2. METHODS FOR CONSTRUCTION OF IOT RESOURCE SHARING PLATFORM

2.1 Secure Sharing of IoT Data

In the IoT, information resource sharing faces both internal and external threats. Due to the complexity of the network environment, the privacy and shared resources of users in the network can be leaked or maliciously attacked. In order to ensure their security and reliability, corresponding countermeasures must be taken. This paper proposes an access control protocol based on permission, and explains the implementation and research methods of the protocol in detail. To ensure their security and prevent their disclosure, shared information resources need to be encrypted before they are uploaded to the ECS. When accessing data resources, users can be classified according to their attributes to achieve access to information with different levels of sensitivity, effectively preventing users' privacy disclosure, and improving the flexibility and efficiency of access. This paper analyzes the correctness, security and performance of the system.

An encryption algorithm is used to improve the security of the IoT. Ordered attribute set [11]:

$$a_m = \{ai1\ , ai2\ , ..., aik\ , ..., aim\} \tag{1}$$

When terminal members share their data resources, they first obtain the corresponding network attribute parametersaccording to the attribute serial number corresponding

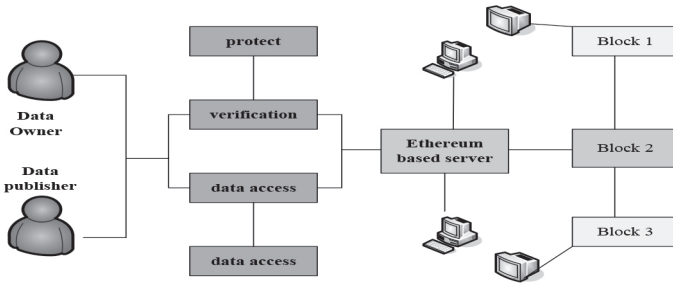

Figure 1 Data security sharing of the IoT.

to their own attribute set, and then apply their own attribute permission parameters to calculate the following formula:

$$x_i = t_{i,j} \tag{2}$$

IoT security test [12]:

$$x_i = \left(y \sum T \cdot \frac{P}{P_V} \right) / P_Y \tag{3}$$

$$Q = q_1 \times q_2 \times \cdots \times q_r = \prod q \tag{4}$$

$$G = Y \cdot \frac{P}{P_V} \tag{5}$$

The security index of IoT information sharing x_g, namely [13]:

$$x_g = Y \sum TM \tag{6}$$

The main information flow ranges from publishing to encrypting, decrypting, accessing and finally receiving data. On the traditional data-sharing platform, there are problems such as information openness and security. In order to enable the sharing of all kinds of data on the IoT, a reliable, safe, transparent and decentralized security sharing mode must be established so as to facilitate the flow of information. It can effectively integrate information and provide users with safe and reliable data-sharing services. The secure data-sharing process of the IoT is shown in Figure 1.

(1) Before data exchange, there needs to be a secure way of ensuring that data will not be stolen.

(2) During the data-sharing process, due to the data characteristics of the IoT, it is necessary to ensure that the user's control granularity is fine and extensible, and the authorization process must be transparent and open. This can ensure the credibility of the data, and also ensure that only authorized users can access and use this information.

(3) After the sharing of data, a reliable and tamper proof technology should be applied to ensure the integrity of the shared IoT data.

Industrial IoT security [14]:

$$J_M = (TYP + 1)/P_V \tag{7}$$

The shared resources are calculated with:

$$mc_{k,m} = H2(x_j) \tag{8}$$

From the perspective of security and efficiency of the IoT, a unique solution X_j can be calculated according to the standard Chinese remainder theorem [15]:

$$X_j = \left(TY + \frac{p}{p_v} \right) / P_m \tag{9}$$

The security of the IoT faces many challenges [16]. The network attribute parameter x_i corresponding to the attribute set is calculated as follows:

$$x_i = T_{i,j}\ (b/p_r) \tag{10}$$

For secure transmission of the IoT data, it is necessary to obtain public and private key pairs (SKA, PKA), where [17]:

$$PKA = b * SKA \tag{11}$$

The load of distributed clusters is unbalanced. Therefore, in order to ensure the load balance of the cluster, the HBase (Hadoop Database) load balancing algorithm based on the IoT must be adopted. The function of the HBase load balancing algorithm is to calculate the matching between HRegion and HRegionServer by means of table load balancing, server load balancing, local storage and other factors, so that HRegion can be managed by HRegionServer.

2.2 Construction of IoT Resource Sharing Platform

The platform architecture proposed in this paper is based on SOA (service-oriented architecture), which completes data exchange and sharing through collaboration with corresponding businesses. Its main functions are: 1) real-time loading, adjustment, extraction, conversion and encapsulation; and 2) data transmission that includes instruction identification, message routing, data access, data transmission, message format adjustment, etc. In the data sharing and exchange system, a unified data identification specification can be used for the sharing and exchange of data among systems, networks and fields through unified encapsulation, identification and representation.

The architecture of the data sharing and exchange system is shown in Figure 2. The architecture comprises a data layer, network layer, service layer and application layer. It is characterized by cross-domain management, cross-domain data sharing, cross-domain services, and cross-system application connectivity. This system structure breaks

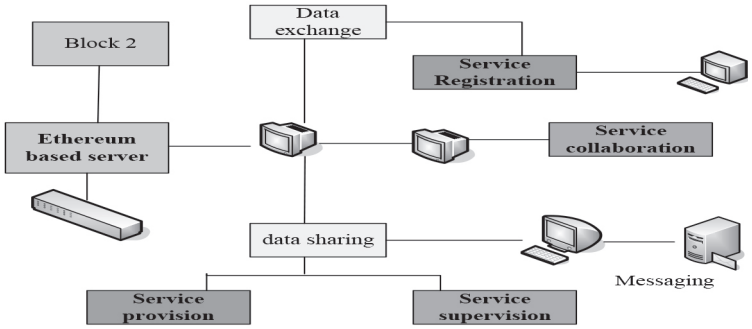

Figure 2 Data sharing exchange architecture.

through the "island" phenomenon caused by the independent operation of various fields, making the resources of the whole region interconnected, open and shared, especially in terms of cross-domain services and cross-domain cooperation.

Data sharing across domains: The sub-domain system is independent, and sub-domains are divided according to regions, management scopes, and trust scopes. According to different sub domain structures, different standards, and different security levels, it can use information sharing and exchange platforms to connect various domains for unified management and support cross-domain data exchange.

Cross-domain services: IoT business data is massive and diverse. The data-sharing and trading platform has unified modeling, identification, description and business representation. This not only reduces the difficulty of application development, but also increases the scalability. On the other hand, it also provides various services to all walks of life, connects different industries, and facilitates cross-industry and cross-field collaboration.

Cross-system application connection: The IoT application system operates independently. Due to its closed architecture and different standards, the data sharing ability between systems is low, and it is difficult to achieve cross-system collaboration. The data-sharing and trading platform connects one system to another system, models and encapsulates the system services, and they interact with each other in accordance with unified specifications so as to achieve system collaboration and interaction.

In this system, IoT sensing devices, cloud service devices, application systems and the data generated by them are all part of a complete identification system. The recognition system produces a unique recognition pattern in the data exchange system, which supports the interconnection between entities.

R-order polynomial is constructed by using the elements in the ordered network attribute set $B = \{B_1, B2, ..., B_R\}$ [18]:

$$\begin{aligned} f(x) &= (x-B_R)(x-B_{R-1})\cdots(x-B_1) \\ &= ax_R + ax_{R-1} + \cdots + ax_0 \end{aligned} \tag{12}$$

CA of certification center is calculated as follows:

$$f(a) = \gamma b_0 g_1 + \gamma b_1 g_2 + \gamma b_2 g_3 + \cdots + \gamma b_n g_{n+1} \tag{13}$$

This means that any terminal member uj obtains the permission parameter T_m from the registered member information and then calculates T_p using the following formula:

$$T_p = T_m = uj\gamma g \tag{14}$$

The relationship between blockchain and IoT security is inseparable [19]. An R-1 order polynomial is built with:

$$f(x) = mk + mkx + M_j \tag{15}$$

The demand of the IoT for the Internet is not only the demand of the network layer, but also requires that the network layer be able to transmit data without obstacles, with strong reliability and high security. Therefore, the combination of traditional network connection technology, sensor network, mobile communication technology and other technologies brings more security problems. In order to ensure the confidentiality and integrity of data in the network layer, relevant cryptographic techniques are usually used to encrypt it before transmission.

At present, the available security technologies include redundant backup, reliable message verification and key management, security audit, network attack, intrusion detection, virus detection, etc. On the whole, the IoT needs decentralized and trusted information security technology. In order to reduce investment costs, it should not include any additional security measures, but start from the residual computing power of physical network nodes to improve the robustness and counterattack capability of the network. The blockchain technology has this feature. Its distributed design makes it a decentralized network maintained by multiple people. Its unique consistency mechanism can conduct security authentication through the redundant operations of nodes. Therefore, this paper discusses the design and implementation of IoT information security technology using blockchain technology.

Terminal members construct a polynomial according to information and Lagrange interpolation theorem:

$$f(x) = y_m \sum (\log_2 x w) \tag{16}$$

The constant term is calculated with:

$$M_j = y \sum \left(\frac{w}{w_i - w_j} \right) \tag{17}$$

In IoT security, p_u, p_j are used as the decryption key. Similarly, terminal member p_u can obtain the encryption key from the registered member information:

$$PK = y\,(p_u, p_m) = k\left(p_u, p_j\right) \tag{18}$$

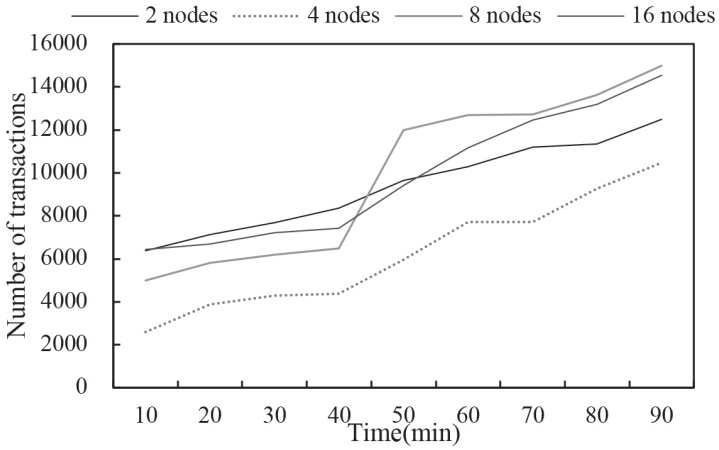

Figure 3 Mining details of miner nodes.

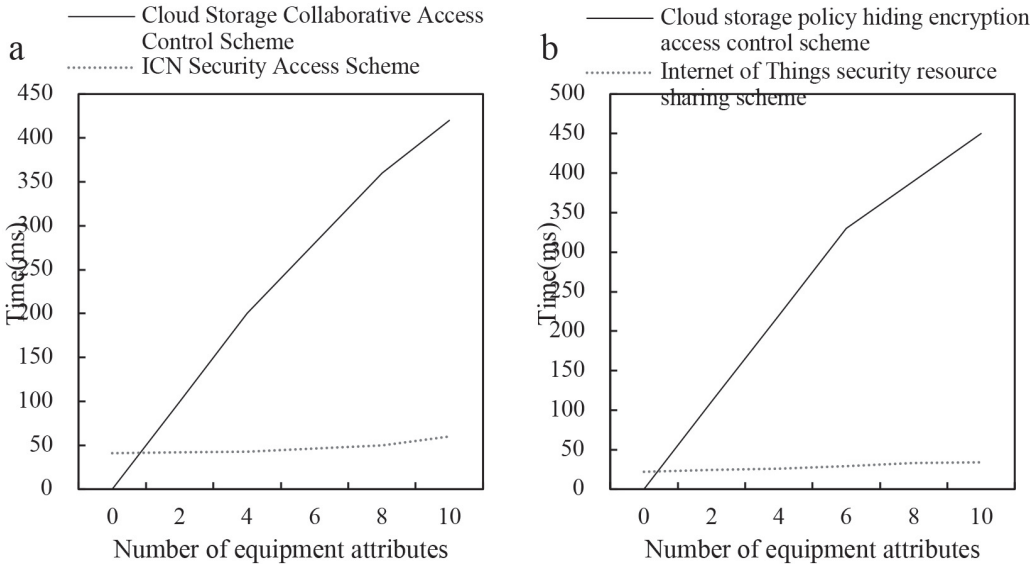

Figure 4 Results of registration phase comparison.

The decryption algorithm takes the attribute decryption private key SG of the data consumer as the input:

$$C_P = S_M * C_1 = SG + T\left(\sum KG\right) \tag{19}$$

In the IoT security vulnerability repair, the probability that the attacker guessed β correctly is [20]:

$$M_U = P_r\left[\beta\left(G, G_1, G_2, Z = abG\right)\right] \tag{20}$$

The advantages of simulator β_U to solve this security problem are:

$$\beta_U = \frac{1}{2} P_r\left[\beta\left(G, G_a, G_b, Z = MCG\right)\right] \tag{21}$$

3. RESULTS OF THE CONSTRUCTION OF THE IOT RESOURCE SHARING PLATFORM

A virtual machine environment is used for this test, and blockchain nodes are built for implementation. It controls 2, 4, 8 and 16 nodes of the network for experimental simulation. In this study, the transactions that take place every ten minutes are counted. The mining details of the miner node are displayed in Figure 3. At the same time, the speed with which new blocks are mined by a different number of nodes does not change much, and the number of transactions is not affected by the number of nodes in the blockchain network.

The computating time required by the security resource sharing scheme for the networking of cultural relics is compared with the other three protocols [21]. The results of the registration phase comparison are displayed in Figure 4. Figure 4a shows the cloud storage cooperative access control scheme and ICN security access scheme. Figure 4b shows the cloud storage policy hidden encryption access control scheme and the cultural relics networking security resource sharing scheme. In addition to this networking security resource sharing scheme for cultural relics, in the other three protocols, the public cloud storage collaborative access control scheme and ICN (Information Centric Networking) security access scheme require relatively little computing time.

In general, the IoT has three layers: the perception layer, the transmission layer and the application layer. The IoT

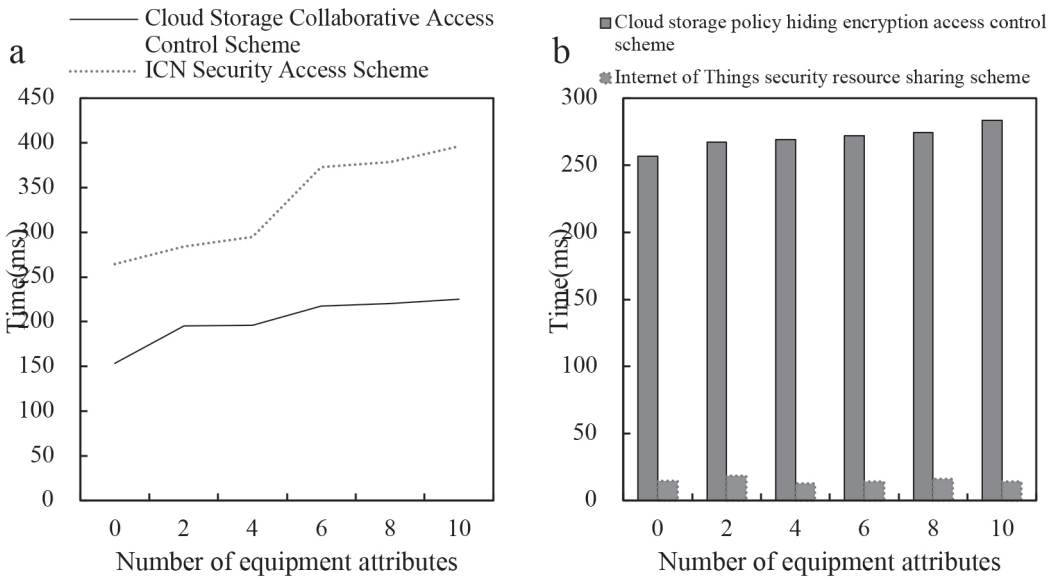

Figure 5 Comparison results of time consumption in the group key calculation phase.

Table 1 View the cluster load status through the web page.

Client	Write data	Time (ms)
1	10000	20
2	15000	25
3	20000	30
4	25000	35
5	30000	40

gateway uses sensor nodes to collect the sensing data deployed in the transport layer of the IoT. However, since the traditional wireless sensor network adopts a self-organized structure and cannot achieve long-distance communication, the IoT gateway between the sensor network and Ethernet is essential.

The time consumption during the group key calculation phase are displayed in Figure 5 for comparison. Figure 5a shows the time consumption of the cloud storage cooperative access control scheme and the time consumption of the ICN security access scheme. Figure 5b indicates the time consumption of the cloud storage policy hidden encryption access control scheme and the time consumption of the cultural relics networking security resource sharing scheme. The cultural relics networking security resource sharing scheme requires the least amount of computing time. The computing consumption of the cloud storage policy hidden encryption access control scheme and the public cloud storage cooperative access control scheme are relatively small, and the computing consumption of the ICN security access scheme is the largest.

The system can use commands to write data, simulate five clients, that is, five threads, and divide them into 100 HRegions. For the load balancing algorithm, three groups of tests were conducted, and 10000, 15000, 20000, 25000 and 30000 data were written for each thread. Table 1 shows the cluster load status on the web page.

The comparison results of the time consumption in the encryption phase are displayed in Figure 6. The time consumption of the networking security resource sharing scheme of this cultural relic is the minimum, with an average time of 28ms.

The two load balancing algorithms were tested, and the reading times are shown in Figure 7. As indicated, the time consumption of the load balancing algorithm of HBase for the IoT is less than that of the load balancing algorithm of HBase itself, and with the increase of the amount of data read, the advantages are more obvious. The load balancing algorithm proposed in this paper can improve the read speed of the HBase [22].

An examination of the whole running state of the program shows that the usage of heap memory is relatively stable. When the resource-sharing platform of the IoT is not operating, the average usage of heap memory is about 44 Mb, and the peak is 75 Mb. After the model is started, the usage of heap memory increases and fluctuates regularly between 88.35Mb and 289.59Mb. The change in heap memory usage is shown in Figure 8.

The recall rate and time performance of intelligent information processing model and general information processing model are displayed in Figure 9. The recall rate is shown in Figure 9 (a), and the time performance is shown in Figure 9 (b). The performance of the resource matching algorithm based on the intelligent information processing model is better than that of the ordinary information processing model. Because the model proposed in this paper has a well-defined hierarchy in each dimension, the structural similarity algorithm can obtain greater accuracy.

When a resource instance is added to the test set to test the time performance, the resource allocation structure does not change, and the new resource instances are dominated

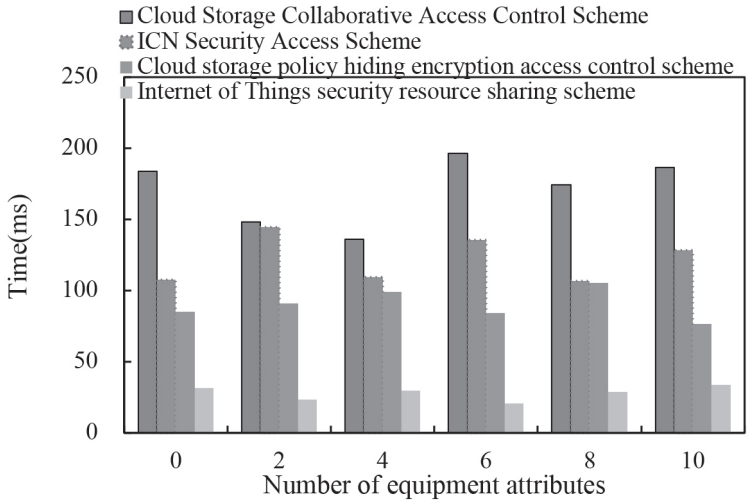

Figure 6 Comparison results of time consumption in the encryption phase.

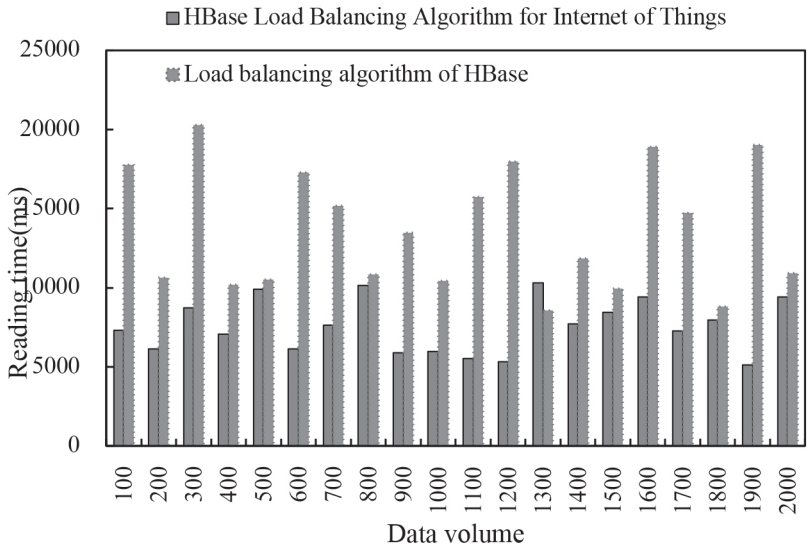

Figure 7 Reading time comparison.

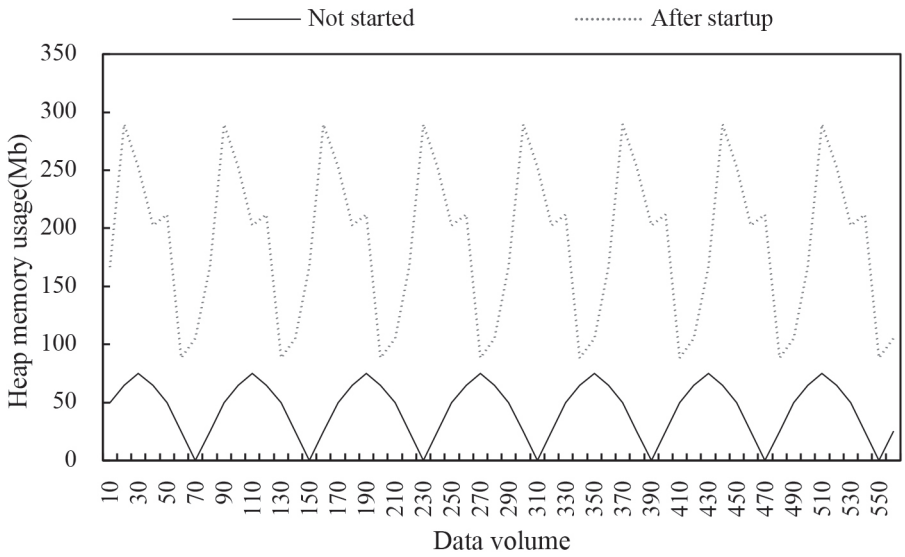

Figure 8 Changes in heap memory usage.

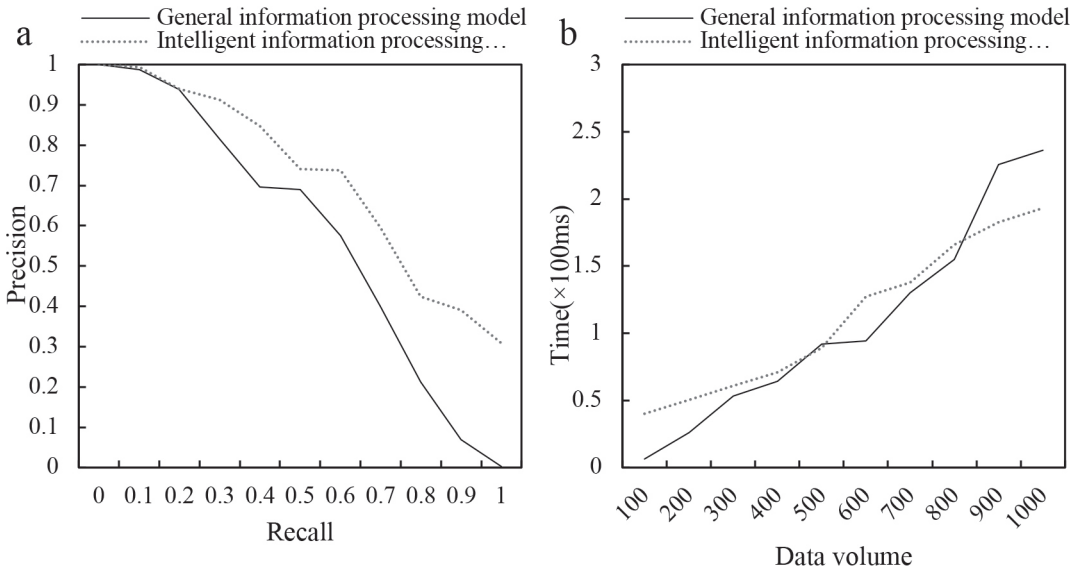

Figure 9 Recall rate and time performance of intelligent information processing model and general information processing model.

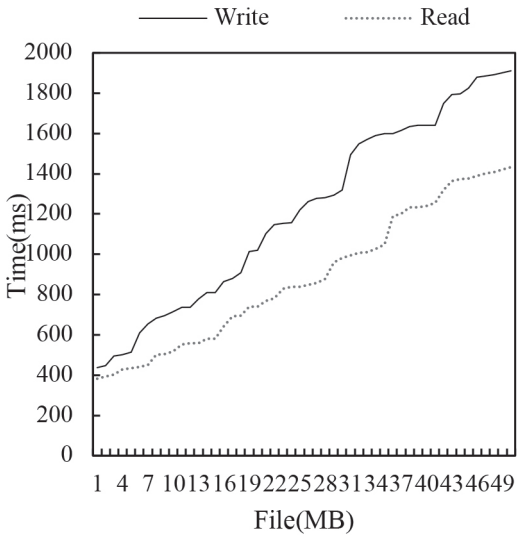

Figure 10 File size read/write performance.

Table 2 Comparison of each blockchain.

Project	Transaction speed (times/second)	Read/write speed (times/second)
Public chain	30	2000
Alliance chain	1000	3000
Private chain	1500	3500

by interference. The fractal dimension method can calculate the similarity of each dimension at the same time, so the calculation time used in these dimensions is the time required for the longest dimension.

As the file size increases, the read/write time increases. In the same network environment, it takes longer to write to the network than to download and read. This is because when using the IPFS (InterPlanetary File System) for file storage, more time is needed to partition and hash the data, while downloading and reading do not require these operations. The read-write performance of the file size is shown in Figure 10.

There are three types of blockchain: public, federated and private. For comparison, each blockchain is shown in Table 2. Given the requirements of the IoT, this paper takes into account the storage requirements of images, sounds, etc., as well as the storage capacity of the blockchain itself. Therefore, a method of linking external databases is proposed to store IoT data in an interstellar archive system and store the data on the blockchain.

The database E-R diagram user table includes user ID, user login name, user display name, password, email, contact mobile phone, status, creator ID, creation time,

Table 3 Partial Information.

Serial Number	Field Name	Length
1	full name	5
2	native place	20
3	age	15
4	time	25

Table 4 Information of IoT network cards.

Serial Number	IoT network card ID	Length
1	Card No	4
2	SIM No	8
3	Agent ID	16
4	Creation time	12

last modification time, gender, birthday, avatar, residential address, province, city, region, type, WeChat, WeChat name, Alipay, Alipay name and other fields, corresponding to user management functions. Some information is shown in Table 3.

The IoT network card table includes IoT network card ID, card number, SIM number, agent ID, use package, status, creation time, activation time, number and other fields, corresponding to the IoT network card management function. Table 4 shows the information of some IoT network cards.

The IoT (IoT) is a communication channel between human beings, entities and virtual worlds, and an important part of today's information society. The IoT is widely used in many fields, especially in military, transportation, agriculture, medical and other domains. However, with the continuous development of the IoT technology, the management of massive data is also facing severe challenges. Many data in the IoT involve personal privacy or other important information, which requires high security and integrity of both individual users and public platforms. Because the IoT has a large degree of randomness in terms of all users and devices, it is difficult to distinguish them from hardware and software. Information on the network can be lost or attacked and tampered with, while the sensing network nodes on the network are vulnerable to attack. Therefore, at the perception level of the IoT, there are many security issues, including physical capture, brute force cracking, node cloning, identity forgery, routing attacks, denial of service attacks, and node privacy leaks. This not only leads to the instability of data transmission in the network, but also brings great challenges to the information security transmission of network nodes. The core of the IoT is data. Only by allowing these data to flow in the network can they be utilized fully. The IoT technology can be used to shorten the distance between people and things. However, with the increase of data volume and network complexity, data security needs to be further improved.

This paper introduces a method that uses the characteristics of blockchain to access and manage billions of resource-constrained devices in the network. The system is distributed and scalable, which can effectively overcome users' distrust of the system and improve its robustness. It can recognize a new transaction, which records a proxy for attribute authorization. The IoT device in this solution would not be added to the negotiation process of the blockchain network, thereby greatly reducing the computing and communication burden of the device. In addition, the proposed scheme is also implemented in a modular manner. Some of the components, such as consistent algorithm, authentication and key negotiation, can be replaced by the same method, which improves the flexibility of the system and facilitates future system maintenance and upgrading.

IoT devices are responsible for collecting, processing and sharing information. The data user does not confirm transactions; only the blockchain is read. To ensure the legal access to and security of data, data users must obtain access permission from the data holder before they can share data. The data user uses the properties approved by the property authority to prove that the data holder has the necessary permissions. A data user can access data only if the properties held by the data user meet the requirements of the access policy set by the data holder. Because data users do not comply with the access strategy established for data ownership, driven by self-interest, data users may collude with each other, even try to maliciously modify data on the blockchain, or affect the consensus of the attribute authorizer.

4. CONCLUSIONS

Today, with the rapid development of information technology, information materials have become an important means to increase productivity, and are the core of various application systems and services. With the continuous emergence of IoT products, people can use various network application services and access various types of information anytime and anywhere. However, there are many security and privacy issues associated with the use of data. The leakage of data during storage and transmission, distrust of data providers, the robustness of data, fixed access rights and other issues are important factors that hinder the efficient and secure use of data. Therefore, this paper focuses on how to effectively use these data while ensuring the privacy of terminal equipment and user data, and discusses these issues in depth. The security resource sharing protocol proposed in this paper uses the blockchain encryption method to store data. The encrypted

data is stored on the blockchain database, and the index information of terminal devices and ciphertext resources are saved in the data block.

FUNDING

This work was supported by the Guangzhou Science and Technology Planning Project.

REFERENCES

1. Lee, Euijong. "A Survey on Standards for Interoperability and Security in the IoT". IEEE Communications Surveys & Tutorials 23.2 (2021): 1020–1047.
2. Amiruddin, Amiruddin, Anak Agung Putri Ratna, and Riri Fitri Sari. "Systematic review of internet of things security". International Journal of Communication Networks and Information Security 11.2 (2019): 248–255.
3. Magaia, Naercio. "Industrial internet-of-things security enhanced with deep learning approaches for smart cities". IEEE IoT Journal 8.8 (2020): 6393–6405.
4. Sfar, Arbia Riahi. "A roadmap for security challenges in the IoT". Digital Communications and Networks 4.2 (2018): 118–137.
5. Jurcut, Anca. "Security considerations for IoT: A survey". SN Computer Science 1.4 (2020): 1–19.
6. Fernandes, Earlence. "Internet of things security research: A rehash of old ideas or new intellectual challenges?" IEEE Security & Privacy 15.4 (2017): 79–84.
7. Alrawais, Arwa. "Fog computing for the internet of things: Security and privacy issues". IEEE Internet Computing 21.2 (2017): 34–42.
8. Aydos, Murat, Yılmaz Vural, and Adem Tekerek. "Assessing risks and threats with layered approach to IoT security". Measurement and Control 52.5–6 (2019): 338–353.
9. Banerjee, Mandrita, Junghee Lee, and Kim-Kwang Raymond Choo. "A blockchain future for internet of things security: a position paper". Digital Communications and Networks 4.3 (2018): 149–160.
10. Bertino, Elisa, and Nayeem Islam. "Botnets and internet of things security". Computer 50.2 (2017): 76–79.
11. Safi, Amirhossein. "Improving the security of internet of things using encryption algorithms". International Journal of Computer and Information Engineering 11.5 (2017): 558–561.
12. Siboni, Shachar. "Security testbed for Internet-of-Things devices". IEEE transactions on reliability 68.1 (2019): 23–44.
13. Mendez Mena, Diego, Ioannis Papapanagiotou, and Baijian Yang. "Internet of things: Survey on security". Information Security Journal: A Global Perspective 27.3 (2018): 162–182.
14. Tange, Koen. "A systematic survey of industrial IoT security: Requirements and fog computing opportunities". IEEE Communications Surveys & Tutorials 22.4 (2020): 2489–2520.
15. Ni, Jianbing, Xiaodong Lin, and Xuemin Sherman Shen. "Toward edge-assisted IoT: From security and efficiency perspectives". IEEE Network 33.2 (2019): 50–57.
16. Moon, Seo Yeon, Jin Ho Park, and Jong Hyuk Park. "Authentications for internet of things security: threats, challenges and studies". Journal of Internet Technology 19.2 (2018): 349–358.
17. Liu, Yanbing. "SDN-based data transfer security for IoT". IEEE IoT Journal 5.1 (2017): 257–268.
18. Ferrag, Mohamed Amine, Lei Shu, and Kim-Kwang Raymond Choo. "Fighting COVID-19 and future pandemics with the IoT: Security and privacy perspectives". IEEE/CAA Journal of Automatica Sinica 8.9 (2021): 1477–1499.
19. Atlam, Hany F. "Blockchain with internet of things: Benefits, challenges, and future directions". International Journal of Intelligent Systems and Applications 10.6 (2018): 40–48.
20. Ling, Zhen. "Security vulnerabilities of internet of things: A case study of the smart plug system". IEEE IoT Journal 4.6 (2017): 1899–1909.
21. Hao Pan. Application of 5G wireless communication and BIM technology in management of construction projects. Engineering Intelligent Systems, Vol 32 No 3, 2024.
22. Tao Zhang. Design of virtual reality visualization display system based on big data technology. Engineering Intelligent Systems, Vol 32 No 3, 2024.

Bin Wang was born in Yangchun, Guangdong, P.R. China, in 1972. He received the Master degree from South China University of Technology, P.R. China.He works Library, Guangdong Polytechnic of Industry and Commerce. His research interests include educational technology, computer technology applications, cloud computing, and big data technology.
E-mail: wangbin@gdgm.edu.cn

Yumin Ye was born in Guangdong, P.R. China, in 1980. She received the Bachelor degree from South China Normal University, P.R. China. She works in the Library of the Guangdong Polytechnic of Industry and Commerce. Her research interests include image and text information retrieval, and literature classification.
E-mail: yeyumin@gdgm.edu.cn