Internet of Things Security Design Based on Blockchain and Identity Re-encryption

Lin Yang

College of Artificial Intelligence and Big Data, Zibo Vocational Institute, Zibo, 255000, China
E-mail: Y_L_8088@163.com

Received 23 November 2023; Accepted 27 December 2023;
Publication 09 April 2024

Abstract

With the development of IoT technology, IoT devices have penetrated various fields, such as smart homes, industrial automation, healthcare, etc. However, the security issues of IoT devices have always troubled people. Attackers can use various means to attack IoT devices, such as stealing data, tampering with programs, malware infection, etc. These attack methods will bring great losses to users. In response to the above issues, this study uses proxy re-encryption technology to transform data collected by IoT devices into ciphertext. Then, it stores the encrypted IoT data on the blockchain. The combination of blockchain and proxy re-encryption technologies offers a method for the secure sharing of IoT data. The experimental results show that whether the algorithm encrypts a small or large amount of data, the encryption time is relatively short, and the time consumption does not exceed 15 ms. When encrypting 8196 bytes of data, its encryption time is 50% lower

Journal of Cyber Security and Mobility, Vol. 13_3, 369–392.
doi: 10.13052/jcsm2245-1439.1332

than the Attribute-Based Encryption (ABE) algorithm. The proposed IoT data security sharing method has the advantages of high security, fast encryption speed, and good stability, which helps to improve the security performance of the IoT and provides a new approach to IoT security.

Keywords: Internet of Things, blockchain, data security, algorithm re-encryption algorithm, data sharing.

1 Introduction

With the boost and widespread application of Internet of Things (IoT) technology, IoT devices have penetrated various fields, such as smart homes, industrial automation, healthcare, etc. However, with the popularization of IoT devices, security issues are also becoming increasingly prominent. Attackers can use various means to attack IoT devices, such as stealing data, tampering with programs, and infecting malicious software, all of which can cause significant losses to users [1–4]. Blockchain technology is widely used in various fields due to its characteristics of decentralization, tamper resistance, and transparency. In the IoT security, blockchain technology could ensure the security and integrity of data through distributed ledgers. However, the transaction records on the blockchain are open to everyone, which means that sensitive information about transactions (such as personal data, transaction amounts, etc.) may be viewed or utilized by unauthorized persons [5]. This poses a significant threat to personal privacy and corporate data protection. A Blockchain and Proxy Re-encryption (BCPRE)-based secure data sharing method for IoT data is proposed based on BCPRE technology to address the above issues. This method uses proxy re-encryption technology for transforming the data collected by IoT devices into ciphertext. Then, it stores the encrypted IoT data on the blockchain. When data need to be retrieved or shared, the data owner can decrypt or re-encrypt the encrypted data through the proxy re-encryption technology authorized by the PBAA scheme. The methods proposed in the research will effectively protect the security and user privacy of IoT devices, promoting further development of the network industry. The article is divided into four sections. Section 2 contains a literature review of the domestic and international development status of IoT related technologies. Then, Section 3 proposes a BCPRE model that combines blockchain technology and proxy re encryption technology. In Section 4, the performance of the model in all aspects is evaluated and applicability testing is conducted.

2 Related Works

With the development of IoT technology, more and more researchers are embarking on research related to internet security. Tsang et al. conducted a correlation analysis on 44 highly influential articles using the system evaluation method of Co-citation Proximity Analysis (CPASR) to explore the knowledge structure issues of the integration and development of Blockchain and the Internet of Things (BIoT). The results show that the knowledge structure of BIoT is divided into 9 categories, including data privacy and security, models and applications, etc. [6].

Cruz [7] selected a multiple regression model to determine the effectiveness of a specific IoT and blockchain fusion model. The research results indicate that the hybrid model is the best fusion platform for integrating the IoT and blockchain.

Then, Sekar S et al. [8] proposed a blockchain-based autonomous trading system data security storage system to address the security issues of post-payment data storage in e-commerce applications. The experiment demonstrates that the system captures user data and effectively protects user privacy from external/bank infringement.

Next, Kumar et al. [9] designed a blockchain module for securely transmitting IoT data in response to the challenges of centralization, security, privacy protection, transparency, scalability, and verifiability in developing smart cities. Then it was applied to Component Analysis (PCA) technology to transform the original IoT information into a new form. The experimental results indicate that this framework has advantages over some recent blockchain and non-blockchain system methods.

Mothukuri et al. [10] addressed the risk of malicious attackers stealing a large amount of user data in the IoT and adopted a federated training round based on the GRU model, sharing the learned weights only on local IoT devices. Then, it maintained data integrity and privacy by sharing the learned weights. The experiment indicates that the proposed method is superior to classical/centralized machine learning methods in protecting user privacy and providing attack detection accuracy.

Deng H et al. [11] proposed a Policy-Based Broadcast Access Authorization (PBAA) scheme to address the issue of data owners being unable to share encrypted sensitive data in existing cloud storage services flexibly. This scheme combines the advantages of IBBE and KP-ABE, overcoming the limitations of PRE. The experimental results indicate that the PBAA scheme greatly improves the flexibility of data sharing for data owners while ensuring security.

He J et al. [12] presented a solution that combined Identity-Based Proxy Re-Encryption (IBPRE) and blockchain to address issues such as maintaining data security, data sharing efficiency, and single point of failure costs in cloud storage. The experiment showcases that this scheme can avoid the complexity of certificate management and improve the security and sharing efficiency of big data storage.

In [13], Zhang et al. proposed a blockchain-based multi-cloud storage data audit solution to address the challenges of reliability and data integrity in multi-cloud storage systems, as well as the credibility and dispute resolution mechanisms of existing data audit solutions. The experiment illustrates that this scheme could markedly protect the integrity of data while accurately resolving service disputes.

Karthika et al. [14] proposed a new technology called Attack Defense Shell Pay On Demand (ADS-PAYG) to address the two major issues of cloud service providers and cloud service accessibility in cloud computing. And it combined the Trust Factor method to defend against EDoS attacks. The experiment illustrates that this method can grow the quantity of authenticated users and fix the threshold, and the algorithm performs effectively in response time, accuracy, and CPU utilization.

Finally, Jiang et al. [15] presented a biometric authentication scheme for addressing the issues of information integrity, data security, and unauthorized user access in cloud computing information storage, while alleviating data redundancy and security issues. The experiment indicates that this scheme has significant advantages in computational and communication costs compared to traditional algorithms.

In summary, the application of blockchain technology and identity proxy re-encryption technology in the IoT security has duplicate theoretical and practical foundations. However, few related studies combine the two and leverage their respective strengths to solve IoT security issues jointly. Therefore, this study combines BCPRE technology to propose a secure data-sharing method for the IoT.

3 An IoT Security Model Combining Identity Re-encryption Algorithm and Blockchain

3.1 Identity Re-encryption Algorithm and Blockchain Technology

Blockchain technology is a distributed ledger technology characterized by decentralization, tamper resistance, and strong security. Its core concepts

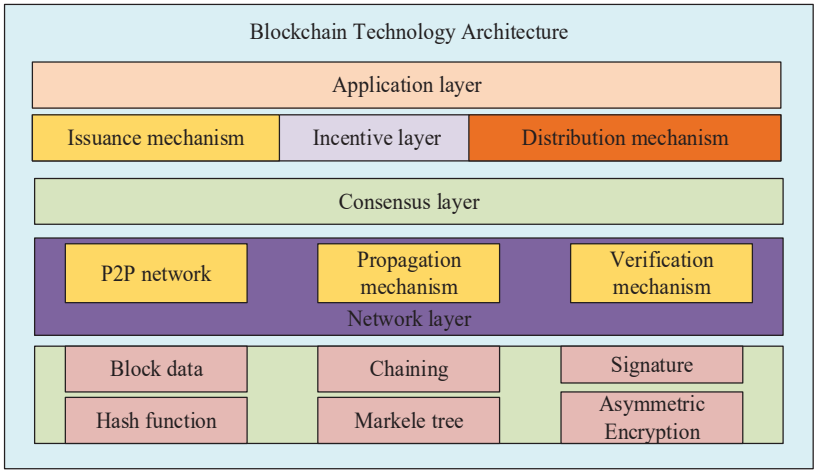

Figure 1 Schematic diagram of blockchain basic technology architecture.

include blockchain and consensus mechanisms. A block is a collection of data composed of transaction data and a unique identifier called a hash. Multiple blocks are linked to form a chain, forming a complete transaction history [16–18]. The consensus mechanism is a way for various nodes in a blockchain network to reach consensus [19]. It ensures participants' identification with new blocks and prevents malicious behavior from affecting the security of the entire system. Common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), et al. The schematic diagram of blockchain infrastructure architecture is shown in Figure 1.

IBPRE is a cryptographic algorithm used for proxy authorization and data forwarding of identities. It combines two technologies: Identity-Based Encryption (IBE) and Proxy Re-Encryption (PRE). The process of the IBPRE algorithm first involves system initialization, selecting a security parameter set, and generating a main parameter set. Then, it produces a primary private key and a corresponding primary public key. The second step is key generation, where users register and provide their identity information to authoritative authorities to obtain a user's private key. Authoritative institutions use the master private key to generate the user's private key and send it to the user. The third step is the data owner stage, where the data owner utilizes their private key for encrypting the data and generating ciphertext. The data owner sends the ciphertext to the authorized agent. The fourth step is the authorization proxy stage. After receiving the ciphertext, the authorization proxy generates a proxy private key using its private key. Its authorized agent

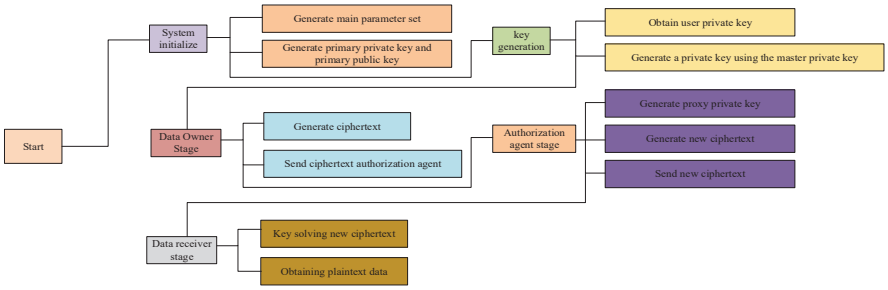

Figure 2 Schematic flowchart of IBPRE algorithm.

utilizes the proxy private key to re-encrypt the ciphertext and generate a new ciphertext. Its authorized agent sends the new ciphertext to the Data Receiver (DR). The fifth step is the DR stage, where the DR decrypts the new ciphertext sent by the authorized agent using their private key to obtain the original ciphertext. The DR decrypts the original ciphertext using their private key for obtaining plaintext data. IBPRE provides a powerful tool in IoT security for data transmission, privacy protection, access control, and device management. It can effectively address security and privacy challenges in IoT environments and provide protection and control mechanisms for various application scenarios. The flowchart of the IBPRE algorithm is shown in Figure 2.

This study proposes a method for secure data sharing in the IoT based on BCPRE technology. This model includes modules such as a gateway layer, blockchain layer, cloud service layer, and device layer. The gateway layer is an IoT device interaction module responsible for collecting raw data collected by the IoT device layer. The IBPRE algorithm participates in the entire data sharing process, which is utilized to achieve data sharing. The blockchain interaction module hashes the key information of the data involved and verifies its integrity. The purpose of the third-party cloud service interaction module is to interact with third-party cloud services and complete functions such as data storage and processing. The blockchain layer runs on multiple nodes and achieves data consistency between nodes through consensus mechanisms and P2P communication. The credit scoring algorithm improves the consensus mechanism of blockchain, improves consensus efficiency, and selects high credit nodes as proxy nodes to provide re-encrypted computing services. The cloud service layer is a cloud storage resource provided by third-party cloud service providers, which stores IoT data in ciphertext form and key data during the proxy re-encryption process, ensuring the security

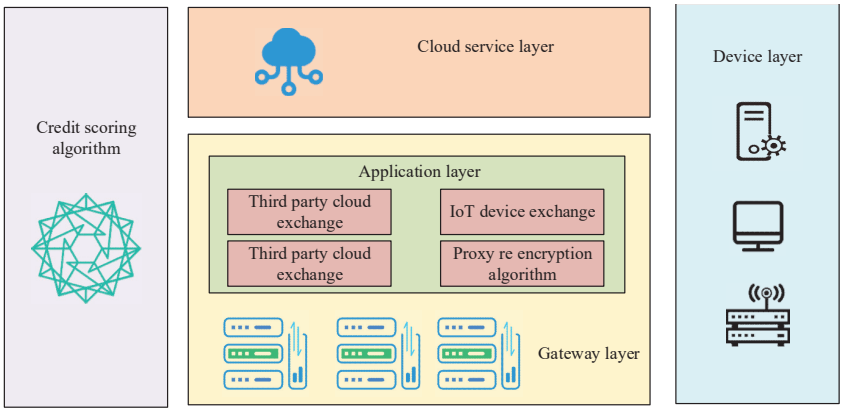

Figure 3 Schematic diagram of BCPRE model structure.

of user information. The main function of the device layer is to collect the requirement of data users. They securely transmit data to the gateway layer but do not participate in the data-sharing process. The BCPRE model structure diagram is shown in Figure 3.

The functions and relationships between each module in the BCPRE data security sharing method model are as follows. Private Key Generator (PKG), whose main responsibility is to generate and distribute private keys. Private keys are the core secrets used to encrypt and decrypt data. To ensure the security of private keys, PKG needs to take strict security measures, such as protecting the storage and transmission of keys. The private key generator PKG interacts with both the data holder and data requester, providing them with the necessary keys. The data holder is the entity that owns the data. The data requester submits the requests to the data holder through the gateway server. Proxy nodes provide re-encrypted computing services. These nodes may be semi-trusted, meaning that they may honestly follow the rules of re-encrypted computation. In the BCPRE method, proxy nodes are represented by consensus nodes in the blockchain, and they randomly select nodes to perform re-encryption operations. These nodes do not directly store data, but rather handle computational tasks related to encryption and decryption.

3.2 Design of Data Sharing and Data Encryption Technology Solutions

The blockchain network provides a decentralized data recording service, ensuring data consistency and integrity. Due to the limitations of the

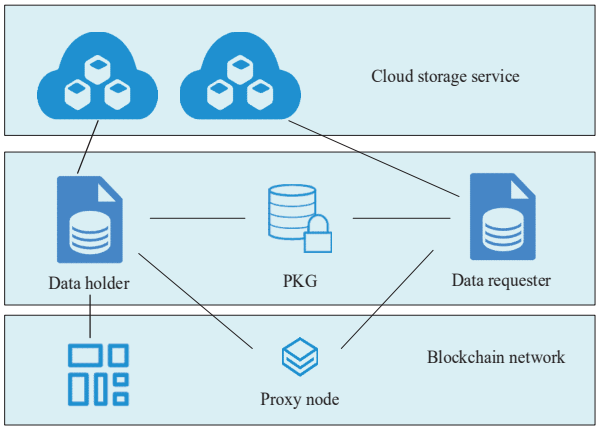

Figure 4 BCPRE data sharing model.

blockchain itself, it cannot store a large amount of file data, so it is mainly used to record summary information of shared data and verify the integrity of off-chain data [20]. Each node in the blockchain network can participate in verifying and recording data, which increases the transparency and security of the system. Cloud storage services are used to store data ciphertext and encrypted key files generated during the IBPRE process. Due to all data being stored in ciphertext format, the confidentiality of cloud data is ensured. Cloud service providers can be any third-party institution or company that meets the requirements and provides computing and storage resources to support this process. The data-sharing model is shown in Figure 4.

Firstly, BCPRE can utilize the distributed storage characteristics of blockchain to store shared data in the blockchain networks. The immutability and transparency of blockchain can ensure the integrity and credibility of data, thereby preventing data from being tampered with or forged. Secondly, BCPRE can utilize the consensus mechanism of blockchain to ensure the consistency and credibility of data. By adopting appropriate consensus algorithms, such as Proof of Work or Proof of Stake, BCPRE can achieve consensus in distributed networks and ensure the validity and reliability of data. BCPRE can leverage the cross-chain interoperability of blockchain technology to integrate and interact with other blockchain networks. This can achieve data sharing and exchange between different blockchain networks, further expanding the application scope and functions of BCPRE. The integration of smart contracts and BCPRE in blockchain technology enables automated data sharing and processing. Smart contracts can define rules and conditions

for data sharing, and it can automatically perform corresponding operations when specific conditions are met. This can reduce human intervention and errors, and improve the efficiency and reliability of the system. Each node in the blockchain network can participate in verifying and recording data, ensuring data consistency and integrity. Cloud storage services handle data storage and retrieval tasks in the background. The ID assumed of the data holder is shown in Equation (1).

$$ID_h = \text{"Factory}A \parallel \text{Data holder} \parallel Tom \tag{1}$$

In Equation (1), Tom represents the name of any IoT user, and the ID form of the IoT data requester is shown in Equation (2).

$$ID_h = \text{"Institution} \parallel \text{Data requester} \parallel \text{Allen} \tag{2}$$

In Equation (2), Allen represents the name of any IoT data requester, and the bilinear mapping process is shown in Equation (3).

$$Group_1 \times Group_1 \rightarrow Group_T \tag{3}$$

In Equation (3), $Group_1$ represents the additive cyclic group and $Group_T$ represents the multiplicative cyclic group. To resist collision attacks, two hash functions are constructed, as shown in Equation (4).

$$\begin{cases} h_0 = \{0,1\}^* \rightarrow Group_1 \\ h_1 = Group_T \rightarrow G_1 \end{cases} \tag{4}$$

Then, it selects a random number r as the main key and hands it over to the key generator for safekeeping. Then, it starts the blockchain network, and each blockchain node forms a synchronous state. Then it outputs the system's common parameters to the blockchain for re-encryption calculation of proxy nodes, as shown in Equation (5).

$$PP = \{G_1, h_0, h_1, g, g^s\} \tag{5}$$

In Equation (5), g represents a generator of an additive cyclic group. When the data holder Tom and data requester Allen register with the key generator using various IDs, the key generator will perform calculations separately, as shown in Equation (6).

$$\begin{cases} sk_T = h_0(ID_T)^S \\ sk_A = h_0(ID_A)^S \end{cases} \tag{6}$$

In Equation (6), ID_T represents the ID of the data holder, and ID_A represents the ID of the data requester. The data holder Tom encrypts the information with its own public key, and the encryption process is shown in Equation (7).

$$\begin{cases} C_1 = \mathrm{g}^r \\ C_2 = M \cdot e(g^s, h0(ID_T))^{\mathrm{r}} \\ FK = \mathrm{C}_1 || C_2 \end{cases} \tag{7}$$

In Equation (7), M represents the information that needs to be encrypted. The calculation for decryption is shown in Equation (8).

$$M = \frac{C_2}{e(C_1, FK)} \tag{8}$$

In Equation (8), FK represents ciphertext. The process of ciphertext generation stage is shown in Figure 5.

This process mainly involves three modules, namely user, blockchain, and cloud storage modules. In the user module, the key is encrypted and the encrypted data are transmitted to the cloud storage module. Then it obtains data ciphertext information from the cloud storage module and records it into the blockchain module data hash chain. Meanwhile, it performs public key and symmetric encryption on the ciphered files of the user module, and then uploads the ciphertext key to the cloud storage module. Finally, the user module obtains symmetric key ciphertext location information from the

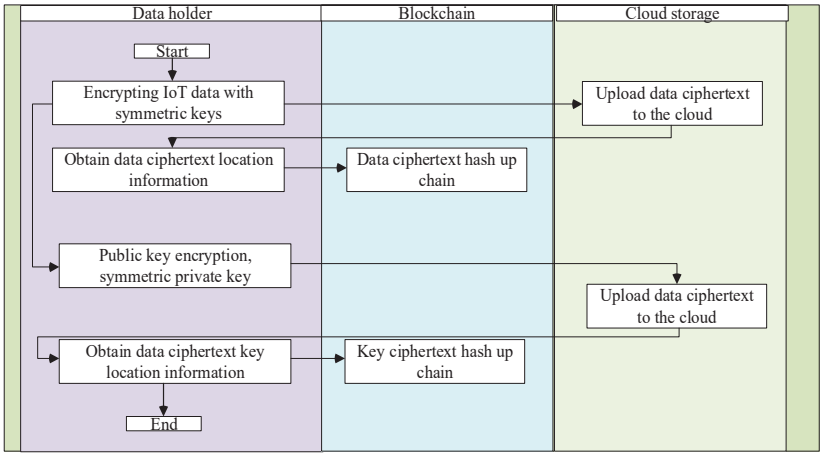

Figure 5 The process of ciphertext generation stage.

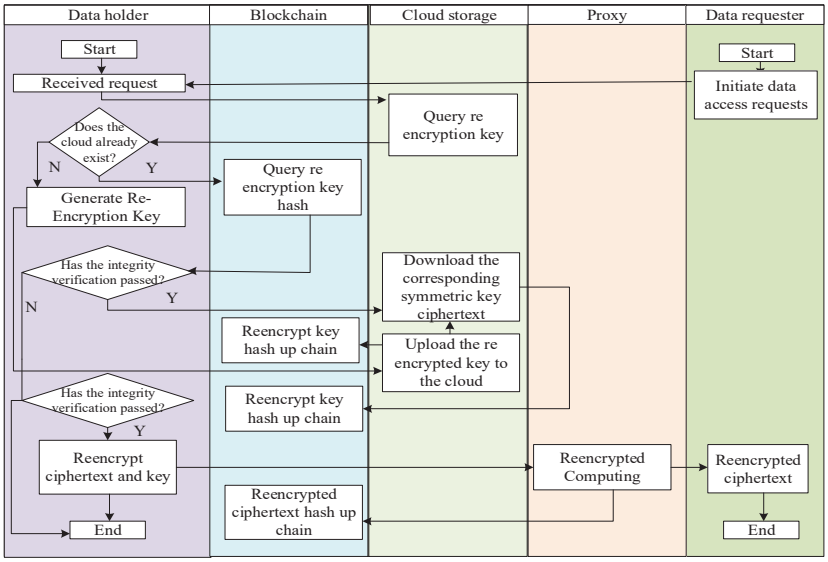

Figure 6 Re-encryption phase process.

cloud storage module and records this information onto the hash uplink in the blockchain module. Then there is the re-encryption stage, as presented in Figure 6.

This process mainly involves five modules, namely data holder, blockchain, cloud storage, proxy, and data requester. The data requester initiates a data access request, and the data holder receives the request and queries the re-encryption key from the cloud storage module. Then, it determines whether the cloud storage module has stored the re-encrypted key. If so, it queries its hash and performs integrity verification. If not, it generates the re-encrypted key. If the key can pass integrity verification, its symmetric key ciphertext is downloaded from the cloud storage module. Then, the symmetric key ciphertext hash is queried, and the integrity of the query results is verified again. If it passes, a proxy is used for re-encryption, and the re-encrypted ciphertext hash is linked and recorded in the blockchain. The data holder calculates the re-encrypted key on the ground of the data requester ID and sk_T, and the calculation process is shown in Equation (9).

$$\begin{cases} Rk_1 = g^{r2} \\ Rk_2 = X \cdot e(g^s, h_0(ID_A))^{r2} \\ Rk_3 = sk_T^{-1} h_1(X) \end{cases} \tag{9}$$

In Equation (9), X represents the random elements in the multiplication cluster and $r2$ represents a random number. After receiving the ciphertext and re-encrypting the ciphertext, the agent performs calculations, as shown in Equation (10).

$$\begin{cases} RC_1' = C_1 \\ RC_2' = C_2 \cdot e(C_1, Rk3) \\ RC_3' = Rk1 \\ RC_4' = Rk2 \end{cases} \tag{10}$$

Next, the re-encrypted key C_{rfk} is generated, and its calculation is shown in Equation (11).

$$C_{rfk} = RC_1' \parallel RC_2' \parallel RC_3' \parallel RC_4' \tag{11}$$

The data requester obtains C_{rfk} and decrypts C_{rfk} with the private key sk_A to obtain M. The decryption calculation formula is shown in Equation (12).

$$M = \frac{RC_2'}{e(RC_1', h_1(M1))} \tag{12}$$

The calculation of $M1$ in Equation (12) is shown in Equation (13).

$$M = \frac{RC_4'}{e(RC3', sk_B)} \tag{13}$$

As a decentralized solution, blockchain has significant differences from traditional centralized solutions. Traditional solutions often face performance limitations from a single-server or data center when faced with an increase in the number of devices, leading to a decrease in network performance. Blockchain, on the other hand, is not affected by single-point bottlenecks due to its distributed nature. As the amount of data increases, partitioning and indexing strategies can be adopted to disperse data across multiple blockchain or storage solutions to improve the efficiency of data retrieval and processing. This approach can effectively avoid excessive load on a single-blockchain network, thereby improving the overall performance of the network. Meanwhile, data compression and storage optimization techniques can also be implemented to reduce storage requirements and further improve network performance. In addition to improving performance, blockchain can also achieve data sharing and interaction between different networks through the cross-chain bridging technology. This technology can ensure the security of data and promote interoperability between different blockchain networks.

By achieving scalability and interoperability between networks, blockchain can better adapt to the growing demand for IoT devices and data volume. In summary, through the comprehensive application of partitioning and indexing strategies, data compression and storage optimization, and cross-chain bridging techniques, blockchain can achieve good scalability while maintaining high security.

4 Performance Testing and Application Analysis of BCPRE Technology

4.1 Performance Testing of IoT Data Security Sharing Model

The experimental evaluation was conducted on 8 servers with the same hardware configuration. The CPU of the server is Intel Xeon Processor (Skylake, IBRS) @ 2194.848MHz, with a memory size of 16GB, a disk size of 500GB, and a gigabit network card from Red Hat, Inc. Virtio network device. The operating system is Centos, and the kernel version is 3.10.0-1160.15.2. el7.x86_64. The software and related technologies used are shown in Table 1.

This experiment used a Postman tool to conduct latency testing on the BCPRE model. Postman is a commonly used API testing tool that provides an intuitive interface and powerful functions, which can be used to send requests and measure the latency of request response. The experiment tests different workloads and data scales to observe changes in system processing time. And it increases the amount of data to simulate the load situation in actual scenarios. It creates multiple requests through Postman's collection function and runs the collection to execute these requests automatically. To fully demonstrate the superiority of this algorithm, two encryption algorithms, i.e., Zero Knowledge Proof (ZKP) and Attribute-Based Encryption (ABE) [21, 22], were introduced for comparison experiments. Their encryption time is measured, and the experimental outcomes are presented in Figure 7.

Table 1 Experimental server configuration information

Entry	Parameter Value
Deploy Software	Docker
Development language	JAVA
Blockchain platform	Tendermint
Testing software	Postman
Performance testing software	JMeter

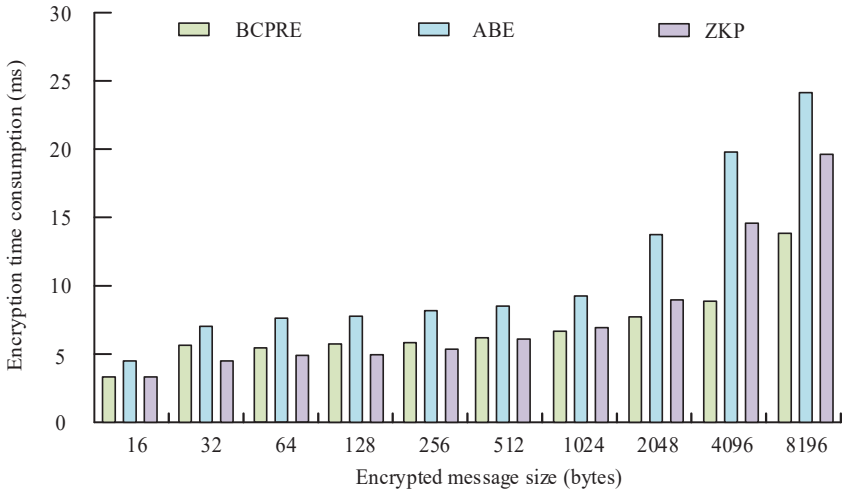

Figure 7 Statistical chart of encryption time consumption for three algorithms.

Figure 7 shows the statistical chart of encryption time for three algorithms. The graph shows that for the ZKP algorithm, it takes relatively less time to encrypt data with a relatively small amount of data. However, its encryption speed substantially increases when the data volume increases to 4096 bytes. In addition, the ABE algorithm performs the worst among the three algorithms, with relatively high encryption time for both small and large data volumes. The BCPRE algorithm proposed in the study is characterized by a relatively short encryption time, with no more than 15 ms, whether it encrypts a small or large amount of data. When encrypting 8196 bytes of data, its encryption time is 50% lower than the ABE algorithm. In addition, the experiment also records the delay situation when using these three algorithms for network transmission, including the time difference between initiating requests, recording request sending, and receiving responses. The experimental structure is illustrated in Figure 8.

Figure 8 shows the network latency during the data transmission. It clearly demonstrates that the BCPRE algorithm proposed in the study exhibits excellent performance during the data transmission process. The average network delay is only 10.1 milliseconds, much lower than the 16.9 milliseconds of the ZKP algorithm and the 26.6 milliseconds of the ABE algorithm. Furthermore, the network delay fluctuation of the BCPRE algorithm is relatively small, demonstrating its stability and reliability. On the other hand, although the average network delay of the ZKP algorithm is not

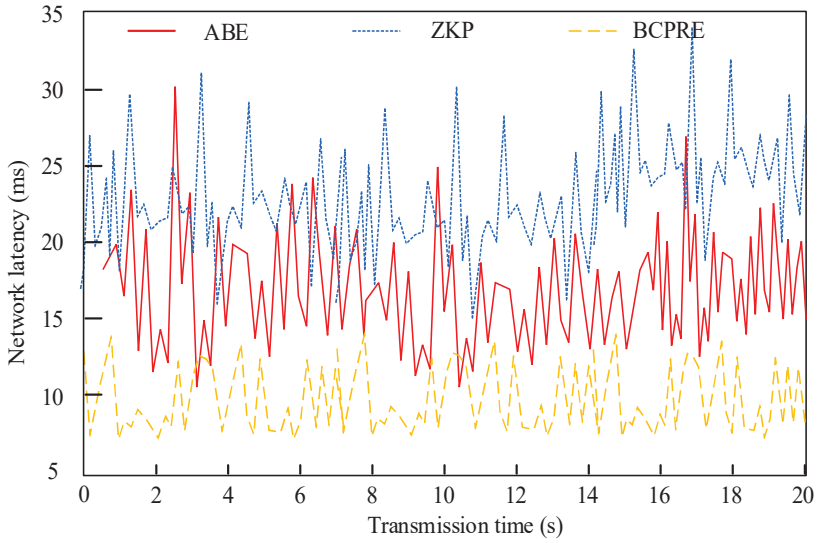

Figure 8 Network latency during data transmission using three algorithms.

significant, its fluctuation is significantly large, indicating that there may be significant delays in certain situations. The average network delay of the ABE algorithm is relatively significant, and its fluctuations are also substantial, which indicates that the algorithm's performance may fluctuate when dealing with different situations. Overall, the BCPRE algorithm performs better than the ZKP and ABE algorithms in terms of average network delay and stability.

4.2 Application Analysis of IoT Data Security Sharing Model

In the experimental scenario, the data holder collects an IoT dataset and prepares multiple devices and sensors to simulate the data provider. It ensures that the dataset contains various types of sensor data, such as temperature, humidity, lighting, etc. Meanwhile, it plans to share this data with n data requesters. To evaluate the performance of different algorithms in data transmission, 20 sets of time complexity data were recorded for four steps: user key generation, re-encryption key generation, re-encryption, and first decryption. The experimental outcomes are illustrated in Figure 9.

Figure 9 shows that during the 20 experimental processes, the re-encryption key generation takes significantly more time than the other steps, with an average encryption time of 5.1 milliseconds. Secondly, the encryption time of the re-encryption phase is the shortest, with an average encryption

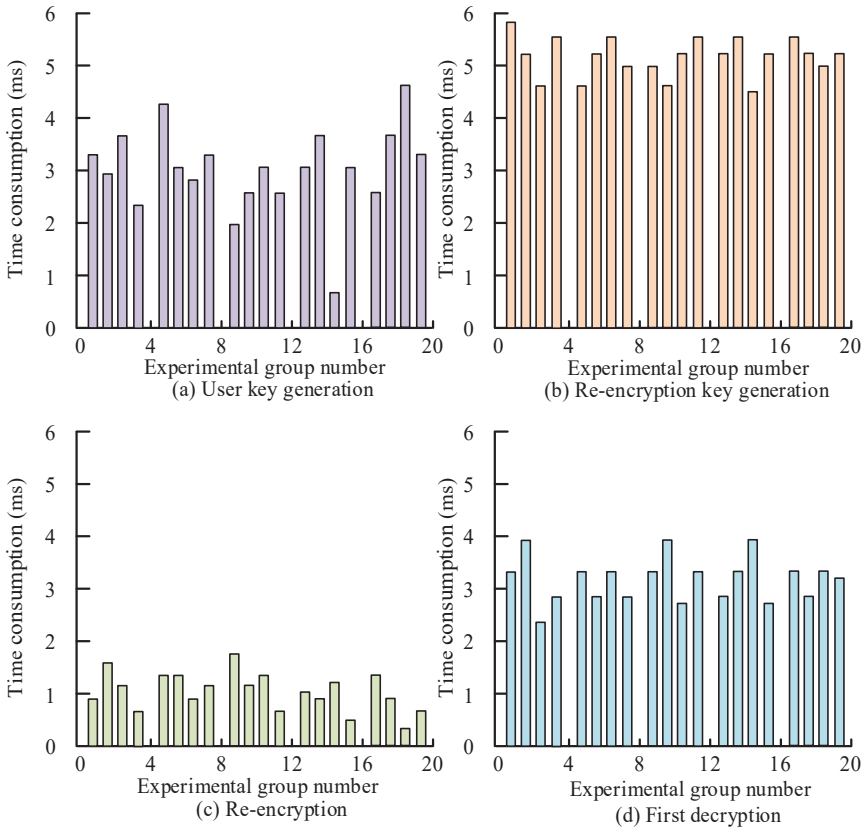

Figure 9 Performance experiments of different algorithms in data transmission.

time of 1.2 milliseconds. This may be because this stage mainly involves repeated encrypted data encryption, with relatively small computational complexity and less time consumption. In addition, the time consumption of the user key generation and first decryption steps is similar, with an average encryption time of around 3 milliseconds. This may indicate that these two steps are comparable in computational complexity and time overhead. The blockchain consensus mechanism includes various user behaviors, including normal, credit, and malicious behaviors. The experiment tested the impact of different behaviors on the network, and the relevant outcomes are presented in Figure 10.

By analyzing the data in Figure 10, the node malicious behavior has an impact on the consensus performance of blockchain networks and a

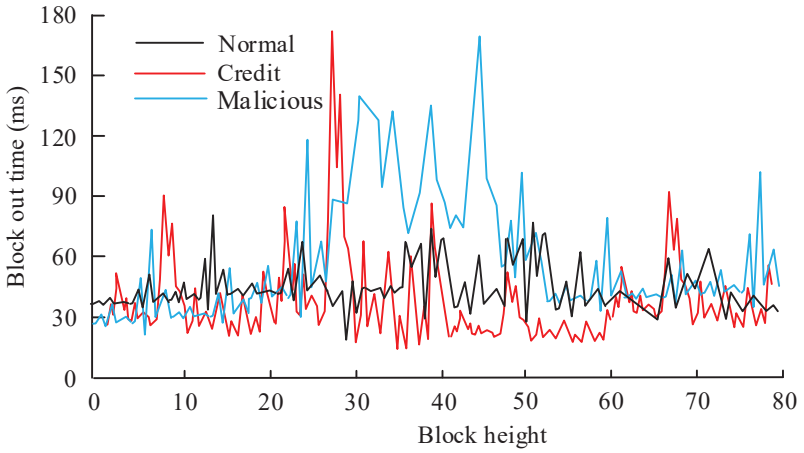

Figure 10 The impact of different user behaviors on BCPRE networks.

significant improvement in security after introducing identity re-encryption algorithms. Under normal conditions, the time for generating blocks in a blockchain network with 25 nodes is mostly maintained between 30 and 60 milliseconds, with a maximum of no more than 90 milliseconds. This time range indicates the efficiency and stability of the network during normal operation. However, when malicious attacks occur at block heights between 25 and 50, the time for generating blocks significantly increases, approximating 120 to 180 milliseconds. This significant change reveals the negative impact of malicious node behavior on the consensus process and block time, directly leading to a decrease in consensus performance. It is worth noting that after introducing the identity re encryption algorithm, although the time for nodes to generate blocks is still relatively high at the beginning, the block out time gradually decreases from the 50th block. Importantly, around the 55th block, the time for generating the block returns to the normal time range. This change not only demonstrates the recovery effect of identity re-encryption algorithm on network performance, but more importantly, verifies the high security of this method in dealing with malicious attacks. By comparing the network performance under malicious attacks and the recovery situation after introducing identity re encryption algorithms, it is clear to see the close relationship between security and network performance. The introduction of identity re-encryption algorithm not only effectively resists the impact of malicious attacks on network consensus performance, but also restores the normal operation of the network in a relatively short time.

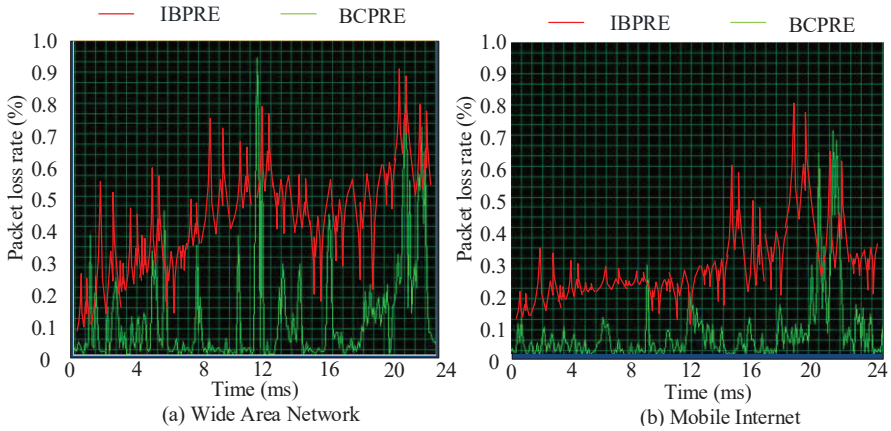

Figure 11 BCPRE algorithm security testing.

This result strongly demonstrates the effectiveness of the proposed method in ensuring blockchain network security. To comprehensively and deeply evaluate the security advantages of the BCPRE algorithm proposed in this study, a series of application experiments were conducted. These experiments were conducted in real wide area network and mobile network environments, aiming to simulate and test the performance of algorithms in various practical network conditions. During the experiment, common packet loss attacks were selected and a professional OMNeT++ simulation tool was used for attack simulation to ensure the accuracy and authenticity of the experiment. In terms of generating and transmitting test data, a certain number and size of test data packets were generated and transmitted through the network to simulate the data flow in the actual network. In addition, network performance testing tools such as iperf were utilized to record and analyze network performance data during the experimental process. Using packet loss rate as the main evaluation indicator, the experimental results are shown in Figure 11.

Through in-depth analysis of Figures 11(a) and 11(b), in real wide area network and mobile internet environments, the traditional IBPRE algorithm exhibits significant vulnerability when facing packet loss attacks. Specifically, in a wide area network environment, when using the IBPRE algorithm for simulation, the average packet loss rate is as high as 0.4%, indicating its shortcomings in dealing with network packet loss. In the mobile internet environment, the average packet loss rate of the IBPRE algorithm reaches 0.3%. This also reveals its lower resistance to packet loss attacks under mobile network conditions. In contrast, the BCPRE algorithm proposed in

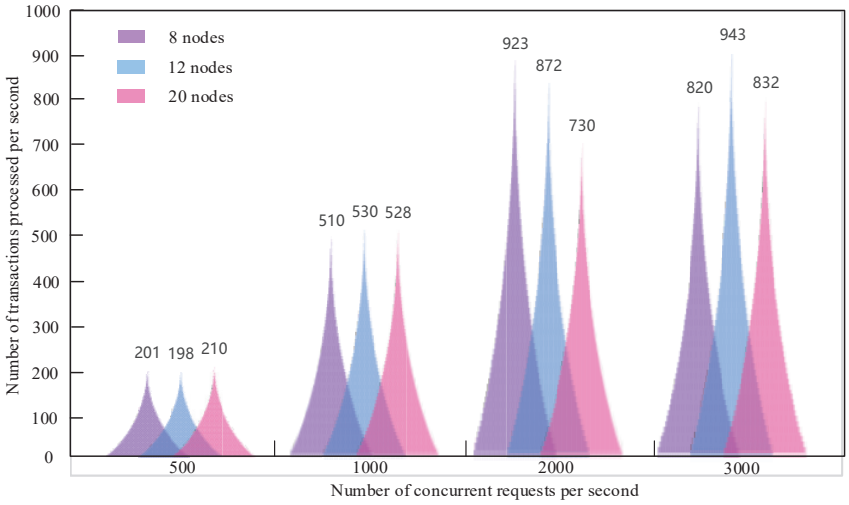

Figure 12 Read and write performance of blockchain networks with different numbers of nodes.

this study has shown significant advantages in both network environments. In wide area networks, the average packet loss rate of the BCPRE algorithm has been reduced to 0.2%, which is a 50% improvement compared to the IBPRE algorithm. In the mobile internet, the average packet loss rate of the BCPRE algorithm has been reduced to 0.15%, achieving a performance improvement of up to 50% compared to the IBPRE algorithm. These experimental results objectively demonstrate the superiority of the BCPRE algorithm in dealing with packet loss attacks, further validating the academic value and application potential of this research method. By comparing the quantitative analysis of experimental results, it clearly demonstrates the excellent defense ability of the BCPRE algorithm against packet loss attacks in real network environments. This provides strong theoretical support and practical guidance for research and application in related fields. Finally, the experiment was conducted by deploying 8, 12, and 20 node networks to test the read and write performance of the blockchain network with different numbers of nodes, and using Transaction Per Second (TPS) as the evaluation metric. The experimental structure is shown in Figure 12.

The provided chart shows that the performance of the BCPRE algorithm in transaction processing is approximately 980 TPS (transactions per second). This performance shows a significant downward trend in the face of an increase in concurrent requests. However, for the same number of

simultaneous requests, the overall performance of blockchain networks with different numbers of nodes shows a trend of increasing node numbers, leading to a decrease in TPS. For example, when the number of concurrent requests is 2000 per second, the TPS of the blockchain network from 8 nodes to 12 nodes gradually decreases, while the TPS of the 20-node network is only slightly higher than the 730 of the 20-node network. This trend is due to the inherent characteristics of the BCPRE algorithm. It is worth noting that the BCPRE algorithm performs very well in terms of query efficiency. The preliminary test results indicate that its queries can reach approximately 17500 times per second.

5 Conclusion

This study combines BCPRE technology to propose a secure data-sharing method for the IoT. The experiment demonstrates that the proposed BCPRE algorithm performs well during data transmission. The average network delay is only 10.1 milliseconds, much lower than the 16.9 milliseconds of the ZKP algorithm and the 26.6 milliseconds of the ABE algorithm. Furthermore, the network delay fluctuation of the BCPRE algorithm is relatively small, demonstrating its stability and reliability. The application experiment recorded the time spent encrypting each node. The results show that the re-encryption key generation process takes significantly longer than other steps, with an average encryption time of 5.1 milliseconds. The encryption time of the re-encryption phase is the shortest, with an average encryption time of 1.2 milliseconds. This may be because this stage mainly involves repeated encryption of encrypted data, with relatively small computational complexity and less time consumption. In addition, the time consumption of the user key generation and first decryption steps is similar, with an average encryption time of around three milliseconds. Meanwhile, the BCPRE algorithm performs very well in terms of query efficiency. The preliminary test results indicate that its queries can reach approximately 17500 times per second. In summary, the BCPRE model proposed in the study has the advantages of short encryption time, high stability, and high transmission efficiency. However, its re-encryption key generation process takes significantly more time than other steps, which is also an area that needs improvement in future research.

In the future, the algorithm can be further improved to adapt to a wider range of IoT devices and data types, enhancing its universality and adaptability. Secondly, although blockchain technology provides secure storage

and verification mechanisms for IoT data, its performance still needs to be improved. Future research can focus on optimizing the performance of blockchain, such as reducing transaction time, improving transaction speed, and reducing energy consumption, to better meet the real-time and low-power requirements of IoT devices.

References

[1] Mahmood T, Ali Z. Prioritized muirhead mean aggregation operators under the complex single-valued neutrosophic settings and their application in multi-attribute decision-making. Journal of Computational and Cognitive Engineering, 2022, 1(2): 56–73.

[2] Zhang J. Analysis of Security Access Control Systems in Fog Computing Environment. Journal of Cyber Security and Mobility, 2023: 653–674.

[3] Waziri T A, Ibrahim A. Discrete Fix Up Limit Model of a Device Unit. Journal of Computational and Cognitive Engineering, 2022, 2(2): 163–167.

[4] Hassan K M A, Madkour M A, Nouh S A E H. A Realtime Adaptive Trust Model Based on Artificial Neural Networks for Wireless Sensor Networks. Journal of Cyber Security and Mobility, 2023: 519–546.

[5] Al-Hamido R K. A new neutrosophic algebraic structures. Journal of Computational and Cognitive Engineering, 2023, 2(2): 150–154.

[6] Tsang Y P, Wu C H, Ip W H, & Shiau, W. L. Exploring the intellectual cores of the blockchain–Internet of Things (BIoT). Journal of Enterprise Information Management, 2021, 34(5): 1287–1317.

[7] Cruz A. Convergence between Blockchain and the Internet of Things. International Journal of Technology, Innovation and Management (IJTIM), 2021, 1(1): 34–53.

[8] Sekar S, Solayappan A, Srimathi J, Raja, S., Durga, S., Manoharan, P., ... and Tunze, G. B. Autonomous transaction model for e-commerce management using blockchain technology. International Journal of Information Technology and Web Engineering (IJITWE), 2022, 17(1): 1–14.

[9] Kumar P, Kumar R, Srivastava G, Gupta, G. P., Tripathi, R., Gadekallu, T. R., and Xiong, N. N. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. IEEE Transactions on Network Science and Engineering, 2021, 8(3): 2326–2341.

[10] Mothukuri V, Khare P, Parizi R M, Pouriyeh, S., Dehghantanha, A., and Srivastava, G. Federated-learning-based anomaly detection for IoT security attacks. IEEE Internet of Things Journal, 2021, 9(4): 2545–2554.
[11] Deng H, Zhang J, Qin Z, Wu, Q., Yin, H., and Castiglione, A. Policy-based broadcast access authorization for flexible data sharing in clouds. IEEE Transactions on Dependable and Secure Computing, 2021, 19(5): 3024–3037.
[12] He J, Zheng D, Guo R, Chen, Y., Li, K., and Tao, X. Efficient identity-based proxy re-encryption scheme in blockchain-assisted decentralized storage system. International Journal of Network Security, 2021, 23(5): 776–790.
[13] Zhang C, Xu Y, Hu Y, Wu, J., Ren, J., and Zhang, Y. A blockchain-based multi-cloud storage data auditing scheme to locate faults. IEEE Transactions on Cloud Computing, 2021, 10(4): 2252–2263.
[14] Karthika A, Muthukumaran N. An ADS-PAYG approach using trust factor Against economic denial of sustainability attacks in cloud storage. Wireless Personal Communications, 2022, 122(1): 69–85.
[15] Jiang T, Meng W, Yuan X, Wang, L., Ge, J., and Ma, ReliableBox: Secure and verifiable cloud storage with location-aware backup. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(12): 2996–3010.
[16] Mohan P, Sundaram M, Satpathy S, and Das, S. An efficient technique for cloud storage using secured de-duplication algorithm. Journal of Intelligent & Fuzzy Systems, 2021, 41(2): 2969–2980.
[17] Mohiyuddin A, Javed A R, Chakraborty C, Chakraborty, C., Rizwan, M., Shabbir, M., and Nebhen, J. Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system. International Journal of Fuzzy Systems, 2022, 24(2): 1203–1215.
[18] Wang F, Wang J, Shi S. Efficient data sharing with privacy preservation over lattices for secure cloud storage. IEEE Systems Journal, 2021, 16(2): 2507–2517.
[19] Elangovan P, Sumalatha M R. Weight based deduplication for minimizing data replication in public cloud storage. Journal of Scientific & Industrial Research, 2021, 80(3): 260–269.
[20] Lv Z, Lou R, Li J, Singh, A. K., and Song, H. Big data analytics for 6G-enabled massive internet of things. IEEE Internet of Things Journal, 2021, 8(7): 5350–5359.

[21] Azrour M, Mabrouki J, Guezzaz A, Guezzaz, A., and Farhaoui, Y. New enhanced authentication protocol for internet of things. Big Data Mining and Analytics, 2021, 4(1): 1–9.
[22] Lee E, Seo Y D, Oh S R, and Kim, Y. G. A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys & Tutorials, 2021, 23(2): 1020–1047.

Biography

Lin Yang graduated from Shandong University of Technology with a major in Computer Science and Technology in 2005. In 2010, he obtained a master's degree in Software Engineering from the University of Electronic Science and Technology. He is currently an associate professor at the School of Artificial Intelligence and Big Data at Zibo Vocational Institute. His technical expertises include computer communication technology, network security, Internet of Things (IoT) technology, and cryptography.