Research on the Application of Blockchain Technology in the Security Protection of Sensitive Data in Information Systems

Yun Cao[1,2]

[1]*School of Cyber Science and Engineering, Southeast University, Nanjing Jiangsu 211189, China*
[2]*Information Center of Jiangsu Food and Drug Administration, Nanjing Jiangsu 210008, China*
E-mail: njlscy81@163.com

Received 26 November 2024; Accepted 21 January 2025

Abstract

With the acceleration of informatization, the security of sensitive data in information systems has increasingly become the focus of global attention. Especially in the context of the widespread application of big data, cloud computing and other technologies, data leakage and privacy risks are becoming more and more serious. Traditional data protection methods can no longer effectively deal with complex network attacks and data leakage problems, and new technical means are urgently needed to improve data security. Blockchain technology shows strong data protection potential due to its characteristics of decentralization, non-tampering and traceability, and is gradually being applied to the protection of sensitive data in information systems. This paper analyzes the application of blockchain technology in data storage, transmission and access control, and discusses its effectiveness in improving data security. We selected the customer information system of a well-known financial institution as the research object, and used blockchain technology to encrypt, store and distribute management of sensitive data.

Journal of Cyber Security and Mobility, Vol. 14_1, 205–228.
doi: 10.13052/jcsm2245-1439.1419

The experimental results show that after the introduction of blockchain technology, the data leakage rate of the system has dropped by 78%, and at the same time, the response time of the system has increased by 22% compared with traditional data protection technology. In addition, the access control mechanism based on smart contracts significantly improves the transparency and traceability of data operations, effectively reducing unauthorized access. This article proves the effectiveness of blockchain technology in protecting sensitive data security in information systems through the analysis of practical cases.

Keywords: Blockchain technology, sensitive data, safety, information system.

1 Introduction

With the rapid development of 5G and the Internet of Things, the surge in data volume poses unprecedented challenges to real-time transmission, efficient computing, and secure storage. By 2025, the total number of global IoT connections is expected to reach 24.6 billion [1, 2]. Traditional cloud computing, as one of the key technologies of 5G, faces limitations in IoT applications due to high latency and bandwidth constraints. Currently, in the context of the “big data” era, various industries such as banking, pharmaceuticals, telecommunications, and e-commerce are generating massive amounts of data every day. Take Wal Mart for example, which produces millions of businesses records every week [3]. The global information volume doubles every 20 months, thanks to advances in data collection and storage technology. Faced with a massive flood of information, extracting valuable knowledge is becoming increasingly urgent. Data mining technology emerged in the 1980s, and its function is like an “excavator” that can filter useful information from transaction databases. With the leap of technology and computing performance in the 1990s, data mining technology has developed rapidly, and the accuracy of mining results has been significantly improved. Multi access edge computing (MEC) implements nearby data processing and storage by deploying cloud servers at the edge of the communication network. This innovative strategy significantly reduces the response delay, optimizes the quality of service, and becomes the core driving force for the development of next-generation Internet technology.

As a decentralized distributed ledger, blockchain technology has shown outstanding potential in information security due to its tamper proof, transparent, and traceable characteristics. Blockchain eliminates the risk of single point failure and ensures data integrity and availability through multi node data storage [4, 5]. The consensus mechanism enhances system security and significantly reduces the probability of data being maliciously tampered with. Therefore, blockchain technology has become a key research direction for sensitive data security protection.

We chose the customer information system of a well-known financial institution as the experimental object because of its high requirements for data security and privacy protection, which is representative. The system's real-time monitoring requirements for data traffic and abnormal behavior are similar to industries such as the Internet of Things, healthcare, intelligent manufacturing, and e-commerce, and can therefore be extended to these fields. The research results not only verify the effectiveness of the Bi LSTM model in the financial industry, but also provide reference for other industries with high security requirements, enhancing the universality and applicability of the research.

This research aims to achieve complementary advantages through the integration of blockchain and multi access edge computing (MEC). By utilizing blockchain technology, MEC can enhance data security and privacy protection, simplify device management processes, and promote the autonomy of resource markets through transaction functions. By combining MEC's decentralized features with blockchain deployment, the dependency problem in traditional cloud computing models can be solved. The integrated BC-MEC system provides secure, stable, and low latency services, ensuring data integrity and traceability through blockchain technology. It supports user independent key management and device access control mechanisms based on smart contracts, reducing reliance on cloud centers. The trading system has established a decentralized resource leasing mechanism, achieving autonomy in resource allocation and further improving the flexibility and efficiency of the system.

2 Overview of Information System Sensitive Data Security Protection Based on Blockchain Technology

2.1 Blockchain Technology

Blockchain technology originated from Bitcoin, reshaping the financial landscape, and is considered a disruptive innovation. As it evolves, blockchain, with its high degree of credibility, is not limited to the monetary field but also significantly reduces the cost of trust in non-monetary scenarios [6]. This section will deeply analyze the architecture of Bitcoin to build the theoretical cornerstone of subsequent blockchain application and design discussions.

$$R_{redundancy} = \frac{N_{copies}}{N_{total}} \tag{1}$$

The evaluation of data redundancy is shown in Equation (1). Among them, $R_{redundancy}$ represents data redundancy, N_{copies} represents the number of data copies, and N_{total} represents the total data volume. The architecture of a blockchain system consists of a data layer, a network layer, a consensus layer, an incentive layer, a contract layer, and an application layer. Each layer works collaboratively and implements functions through service interfaces. The formula for calculating data privacy leakage rate is shown in Equation (2).

$$R_{leak} = \frac{D_{leaked}}{D_{total}} \tag{2}$$

Among them, R_{leak} represents the data privacy leakage rate, D_{leaked} represents the amount of leaked data, and D_{total} represents the total data volume. In the blockchain network, the consensus protocol ensures that participants reach unanimous decisions, and the consensus mechanism ensures the validity of new transactions. Blocks are formed through iterative accounting, and transaction information is stored in them [7, 8]. The node adds a new block at the end of the longest chain and updates it by verifying the blocks submitted by other nodes. Consensus mechanism significantly affects blockchain performance and energy consumption. At present, common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance Mechanism. The calculation method of blockchain capacity is shown in Equation (3). Among them, $C_{blockchain}$ represents the total capacity of the blockchain, N_{blocks} represents the number of blocks, and S_{block} represents the size of each block.

$$C_{blockchain} = N_{blocks} \times S_{block} \tag{3}$$

Blockchain technology and traditional data protection methods have different advantages in dealing with complex network attacks and data breaches. Traditional methods rely on centralized servers, which are suitable for routine attacks, but are easily breached in the face of advanced persistent threats and data breaches. Through its decentralized and tamper proof characteristics, blockchain enhances the integrity and security of data, making it particularly suitable for large-scale data storage and high trust level application scenarios. The two can be used in combination to complement each other and enhance the overall security and reliability of the system.

The introduction of blockchain enhances security, but it may also increase the performance cost of the system, especially in encrypted storage and distributed management processes. The decentralization and consensus mechanism of blockchain may lead to increased system response time and increased consumption of computing resources. The author should balance security and performance in the discussion, consider adopting lightweight blockchain solutions, optimizing consensus algorithms, and allocating computing and storage tasks reasonably to ensure that the system improves performance efficiency while ensuring security.

Blockchain ensures system stability in the event of node attacks through distributed consensus algorithms such as BFT, PoW, and PoS. These algorithms require the consent of the majority of nodes to reach consensus, preventing malicious nodes from tampering with data and thus avoiding the risk of single point failures. Redundant storage and data distribution enable the system to tolerate partial node failures while maintaining overall reliability. Smart contracts and multi signature mechanisms further enhance the system's security protection capabilities, ensuring data consistency and preventing malicious operations.

2.2 Security Analysis of Sensitive Data in Information Systems

Sensitive data in information systems involves personal privacy, etc. How to prevent data leakage and network attacks is the key to security protection. Among them, encryption operations can be implemented using public keys, and the formula for generating public keys is shown in Equation (4) below.

$$P = G \times k \tag{4}$$

Among them, P represents the public key, G represents the elliptic curve base point, and k represents the private key. Based on the simulation of the foraging behavior of birds, the PSO optimization algorithm regards each individual in the group as a particle. The particles adjust their paths according to their companions' flight direction and speed to identify local and global optimal positions and show intelligent behaviors [9, 10]. When solving the optimization problem, the particle's position represents the solution, and the global optimal solution is finally locked through an iterative process. The average transaction verification time is calculated by formula (5).

$$T_{avg} = \frac{\sum_{i=1}^{n} T_i}{n} \tag{5}$$

Where T_{avg} represents the average transaction verification time, T_i represents the verification time of each transaction, and *n* represents the number of transactions. PPDM (Privacy preserving data mining) is used to seek a balance between privacy protection and accuracy of mining results, and is achieved through dataset transformation [11, 12]. There are two core strategies: data hiding and output hiding. The calculation method of the data redundancy rate is detailed in Equation (6). Among them, $R_{redundancy}$ represents the data redundancy rate, D_{backup} represents the amount of data backed up, and D_{total} represents the total amount of data.

$$R_{redundancy} = \frac{D_{backup}}{D_{total}} \tag{6}$$

Smart contracts are used for automated device data processing and security event response, ensuring transparency and immutability of data transmission through blockchain. The contract logic includes functions such as automatically triggering security measures, recording events, and notifying administrators. The smart contract design plan includes blockchain platform selection, contract writing and deployment, while using static analysis tools, contract auditing, and fuzz testing methods to address potential security issues such as contract vulnerabilities and re-entry attacks. Through these measures, the system has enhanced security and response efficiency, ensuring automated monitoring of device behavior.

2.3 Data Security Protection Based on Blockchain Technology

Blockchain is a decentralized, traceable, tamper proof, and multi-party jointly maintained distributed ledger technology. This study is based on the data structure of hash chain, the data update method based on decentralized consensus algorithm, and the design of automated execution of smart contracts. Among them, the elliptic curve encryption formula is shown in (7).

$$C = (rG, M + rP) \tag{7}$$

Among them, *C* represents ciphertext, *r* represents random number, *G* represents elliptic curve base point, *M* represents plaintext, and *P* represents public key. Within the blockchain architecture, any node can use wallets to perform transaction operations and participate in consensus mechanisms. The verification node needs to review the received transaction [13, 14]. After confirmation, the transaction will be integrated into the timestamped block. The consensus algorithm determines whether the block should be included in the main chain. All nodes maintain their respective ledgers by synchronizing the main chain blocks and jointly building a distributed trusted system without the intervention of the central authority. The exact calculation flow of network bandwidth usage is detailed in Equation (8).

$$U_{bandwidth} = \frac{D_{transmitted}}{T_{available}} \tag{8}$$

Among them, $U_{bandwidth}$ represents bandwidth utilization, $D_{transmitted}$ represents the amount of data transmitted, and $T_{available}$ represents the available bandwidth time. The classification of blockchain is based on access mechanisms: firstly, permissionless chains, including Bitcoin, allow all users to participate in transaction verification and consensus processes. The advantage lies in high decentralization and transparency, but it requires more scalability, transaction latency, and challenges of insufficient data privacy [15]. The second is the permission chain, such as Hyperledger and EOS IO, Only authorized users are allowed to join the network, which can provide high transaction throughput and high node trust. But the degree of decentralization has decreased, and there is a risk of member nodes colluding to tamper with data. Consensus algorithm solves the throughput and scalability problems of edge computing architecture (MEC) network by combining the advantages of unlicensed chain and license chain. The calculation formula for transaction costs is shown in Equation (9). Among them, $F_{transaction}$ represents the transaction fee, *g* represents the amount of gas consumed by the transaction, and *p* represents the price per unit of gas.

$$F_{transaction} = g \times p \tag{9}$$

The system uses symmetric encryption, asymmetric encryption, and hash algorithms to ensure data security. Symmetric encryption is used for efficient data transmission encryption and decryption, asymmetric encryption is used for key exchange and identity authentication, and hash algorithm is used to verify the integrity of data. Although these encryption techniques enhance the security of the system, they also increase computational overhead and latency, especially on edge devices with limited resources. They provide strong protection against data tampering and leakage, ensuring the reliability of the system in the face of network attacks.

3 Blockchain-based Sensitive Data Protection Model

3.1 System Architecture of Blockchain Technology

The system in this article is designed based on blockchain technology to ensure the security of confidential data. Its structure includes three key components: decentralized storage, data encryption, and innovative contract module [16]. By leveraging the multi node synchronization mechanism of blockchain, decentralized storage modules ensure that each node holds a comprehensive copy of the data, reducing the risk of single point of failure in traditional centralized storage models.

The workflow of blockchain technology in encrypted transmission of sensitive data is shown in Figure 1. The data layer focuses on guiding nodes to generate blocks, which involves the application of blockchain data structures and cryptographic tools. This layer defines the composition of blocks, transactions, and accounts, as well as rules for global state adjustment, transaction

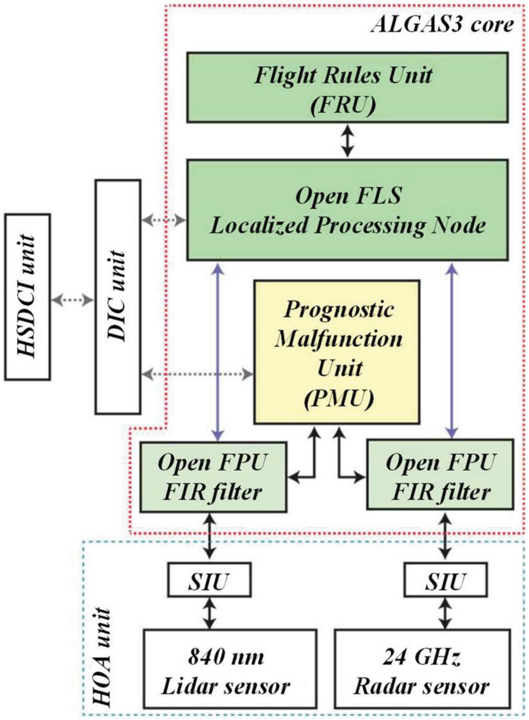

Figure 1 Workflow of blockchain technology in encrypted transmission of sensitive data.

Table 1 Comparison of data processing efficiency under different consensus mechanisms

Consensus Mechanism	Number of Nodes (pcs)	Transaction Processing Speed (TPS)	Data Write Latency (Milliseconds)
PoW	50	15	500
PoS	60	200	50
PBFT	70	300	10
DPoS	50	250	30

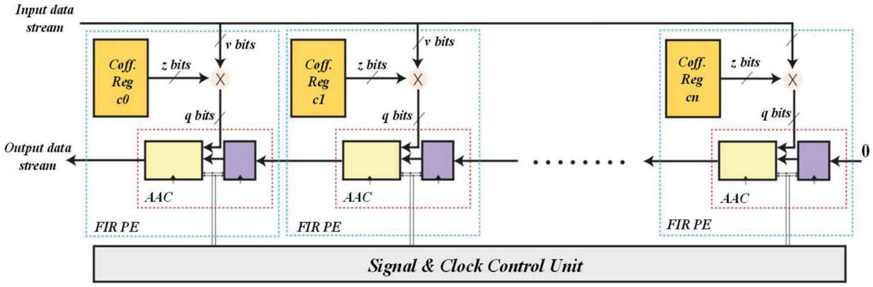

Figure 2 Application process of blockchain-based distributed consensus mechanism in data verification.

verification, and account status updates [17]. Cryptographic elements include hash functions, digital signatures, Merkle trees, asymmetric encryption, zero knowledge proofs, and commitment verification. The comparison of data processing efficiency under different consensus mechanisms is shown in Table 1.

The network layer details the interconnection and information exchange mechanism between nodes, including networking, broadcasting, forwarding, block synchronization, and message propagation processes. In blockchain, this concept is often based on a peer-to-peer network structure to achieve equal cooperation and connection of nodes worldwide and build a decentralized flat network layout.

The application process of blockchain-based distributed consensus mechanism in data verification is shown in Figure 2. Consensus Layer Overview Nodes decide the block addition rules on the main chain [18, 19]. Blockchain consensus algorithms are divided into permissionless, permission, and mixed consensus. Permissionless consensus mainly focuses on proof protocols, such as proof of work, which applies to public chains. A permission consensus exists to reach an agreement among limited nodes, characterized by high transaction throughput and low latency. Hybrid consensus combines both advantages, aiming to improve system scalability and throughput. The data access control formula is shown in Equation (10). Among them, *A* represents access rights, *Policy* represents access control policies, *U* represents users, and *R* represents resources.

$$A = Policy(U, R) \tag{10}$$

Blockchain technology effectively addresses 51% attacks through its decentralized nature, preventing data tampering and leakage. The transparency and automated execution mechanism of smart contracts improve the traceability of operations, which helps to detect and fix vulnerabilities in a timely manner. Combining encryption technology, blockchain ensures the security of data during transmission and storage, preventing unauthorized access. By combining with the Bi LSTM model, the system can monitor data streams in real-time, detect potential security threats in a timely manner, and effectively prevent data leakage.

The application of smart contracts in data access control ensures that only authorized users can access sensitive data through automated access permission verification. The system design architecture combines blockchain platforms and access control mechanisms (such as ACLs and RBAC) to ensure the access permissions of users with different roles, while utilizing the immutability of blockchain to record access history and enhance data security. The implementation of smart contracts faces some challenges, including performance issues, particularly delays that may occur during high concurrency access, and programming errors (such as re-entry attacks) that may affect security.

3.2 Design and Application of Sensitive Data Security Protection Model

Smart contracts, one of the core technologies of blockchain, are used to achieve automated transactions or data operations, ensuring the automatic execution of conditions. This article focuses on model research, whose core functions are data access control and operation management. With the help of smart contracts, the system can automatically evaluate user access requests, determine whether they comply with preset rules, and decide on access permissions based on this.

The performance improvement analysis of blockchain technology in sensitive data transmission is shown in Figure 3. The association rule hiding algorithm of accurate information hiding transforms the hiding problem into

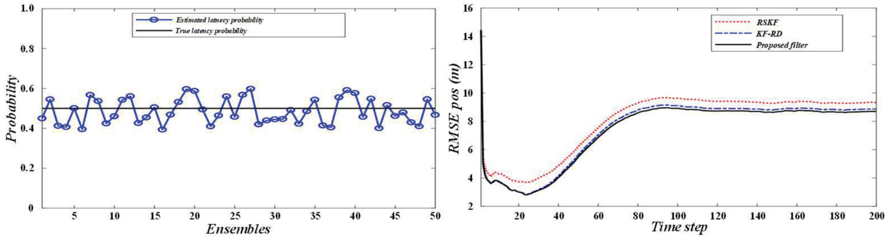

Figure 3 Analysis of performance improvement of blockchain technology in sensitive data transmission.

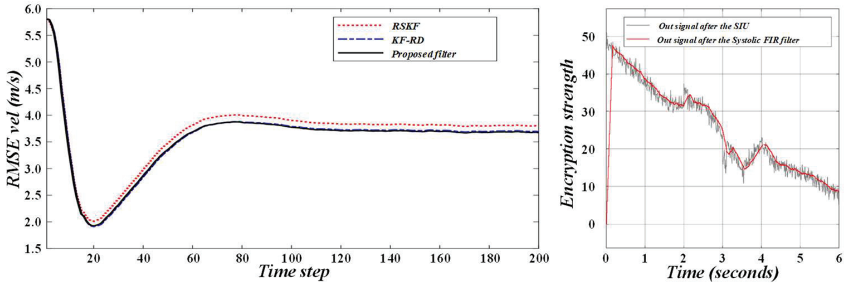

Figure 4 Comparison of transaction processing delay of blockchain in information system.

a CSP problem, effectively masks the sensitive and frequent itemsets in the original data set, avoids generating association rules, and keeps the non-sensitive itemsets [20]. The algorithm is designed non-heuristically, ensuring the goal's full realization. However, its main limitations are the CSP solution process's complexity and long running time.

The transaction processing delay pairing of blockchain in the information system is shown in Figure 4. After hiding the sensitive itemset, the algorithm moves it from the frequent set to the infrequent set, resulting in the boundary change of the data set, which is called boundary movement. The cleaning step includes changing the specific T_{ij} value from 1 to 0, achieving culling from the dataset [21]. In order to ensure that sensitive items are accurately marked as infrequent and keep the frequent state of sensitive items, the algorithm constructs a group of support conditional inequality. It determines the T_{ij} value to be adjusted by solving it. This process is transformed into a constraint satisfaction problem (CSP). Since T_{ij} only takes 0 or 1, the CSP variant is binary integer programming. The key to the algorithm is to solve CSP efficiently. This chapter proposes an optimization strategy to improve the blockchain fork probability formula (11). Among them, P_{fork} represents the probability of blockchain forking, p represents the probability of each node generating blocks, and n represents the number of nodes in the network.

$$P_{fork} = 1 - (1 - p)^n \tag{11}$$

3.3 Data Encryption and Transmission Mechanism

In the information system, encrypting sensitive data and secure transmission constitute the core security strategy. The model focused on in this paper uses advanced encryption algorithms to encrypt data and incorporates the blockchain hash algorithm to ensure data integrity and privacy [22]. In data transmission, the system automatically performs the encryption operation of sensitive information. Even if the data is intercepted during transmission, the interceptor cannot obtain its content due to the undecrypted state, thus effectively guaranteeing the security of the data.

The impact of different blockchain consensus mechanisms on data writing speed is shown in Figure 5. In data protection, although data cleaning can conceal sensitive information, data suppliers tend to minimize the impact on data sets while realizing concealment [23]. The goal is to identify and remove the fewest data items to meet this need. The designed algorithm focuses on determining the minimum number of data items needed to perform the deletion operation and avoids generating "ghost" data items; the initially infrequent items become frequent after cleaning. It is worth noting that the algorithm may hide sensitive items and all their subsets, even if these subsets are not themselves in the sensitive itemset [24]. For example, if the sensitive item set ab is hidden, retaining its subset ABC may lead to the risk of privacy leakage. The effect of block size on data storage efficiency is shown in Table 2.

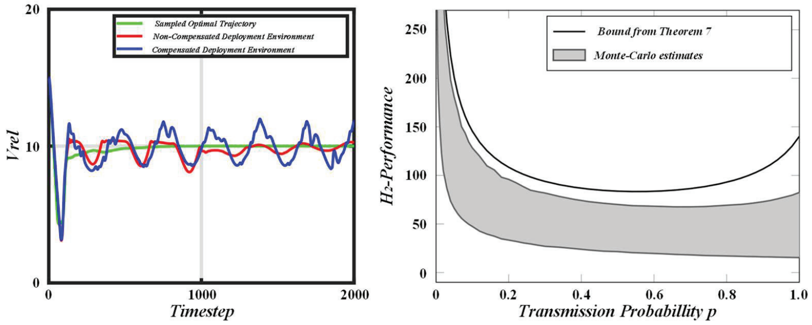

Figure 5 The impact of different blockchain consensus mechanisms on data writing speed.

Table 2 Impact of block size on data storage efficiency

Block Size (MB)	Data Storage Speed (M/second)	Data Transfer Latency (Milliseconds)	System Throughput (TPS)
1	500	10	100
2	800	15	150
4	1200	20	200
8	1600	30	250

Solutions satisfying CSP inequalities are feasible solutions, and a CSP may have multiple feasible solutions. The goal is to find the optimal hiding strategy with the smallest distance and the highest accuracy between the two data sets [25]. This optimal solution lies within the set of feasible solutions. If there is no solution, the best approximate solution must be found. Please refer to Equation (12) for the formula of proof of equity. Among them, P represents the election probability of the node, S represents the number of tokens held by the node, and T represents the total amount of tokens in the system.

$$P = \frac{S}{T} \tag{12}$$

4 Experiment on Sensitive Data Security Protection Under Blockchain Technology

4.1 Experimental Environment and Data Setting

To verify the effectiveness of blockchain technology in protecting sensitive data in information systems, this paper designs an experimental environment [26]. It uses the customer information system of a well-known financial institution to test the effectiveness of processing susceptible data such as personal financial information and transaction records. Experiment with integrated blockchain technology to comprehensively evaluate its data storage, transmission, and access control performance.

The data leakage rate is defined as the proportion of data leaks that are not identified or prevented in a timely manner. The experimental design includes generating leaked data by simulating scenarios such as man in the middle attacks and SQL injection, monitoring and recording the data flow, detecting abnormal behavior using the Bi LSTM model, and finally calculating the data leakage rate. By comparing with actual leaked data, determine the proportion of missed detections and calculate the data leakage rate. The experimental results show that the average data leakage rate of the system under various

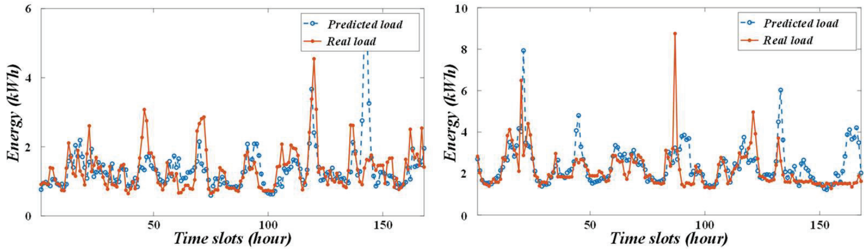

Figure 6 Comparison of the number of data tampering before and after using blockchain.

attacks is 10.5%, and the false alarm rate is less than 3%. These detailed data provide reliable basis for the research results and provide direction for future optimization.

The experiment mainly focuses on protecting sensitive data of financial institutions, but this technological framework has the potential to be extended to other fields such as healthcare and government departments. The author should further discuss the scope and limitations of the experiment in the conclusion, clarify the universality and application scenarios of the technology, especially the challenges that may be faced when dealing with sensitive data in different fields. The data characteristics of different fields and industry-specific security requirements may affect the applicability of the system, and future research should explore how to adjust and optimize the system according to industry characteristics.

A comparison of the number of data tampers before and after using the blockchain is shown in Figure 6. This chapter aims to test and evaluate the blockchain privacy data-sharing protocol through simulation models. First, the Go language builds a decentralized key generation and management protocol model. Its core functions include commitment generation, secret share generation, commitment verification, and key recovery [27]. Then, based on the above, the PBC library is integrated to build a blockchain privacy data-sharing protocol simulation model for the mobile edge computing environment and realize functions such as protocol initialization, access structure construction, attribute encryption and decryption, etc. Finally, the shared domain smart contract is developed with the help of Solidity's clever contract language and deployed on the Ethereum private chain to simulate the actual running scenario.

The relationship between the number of blockchain network nodes and system throughput is shown in Figure 7. In the initialization stage, the protocol time overhead is 768.93 milliseconds, higher than CP-ABE's. Because

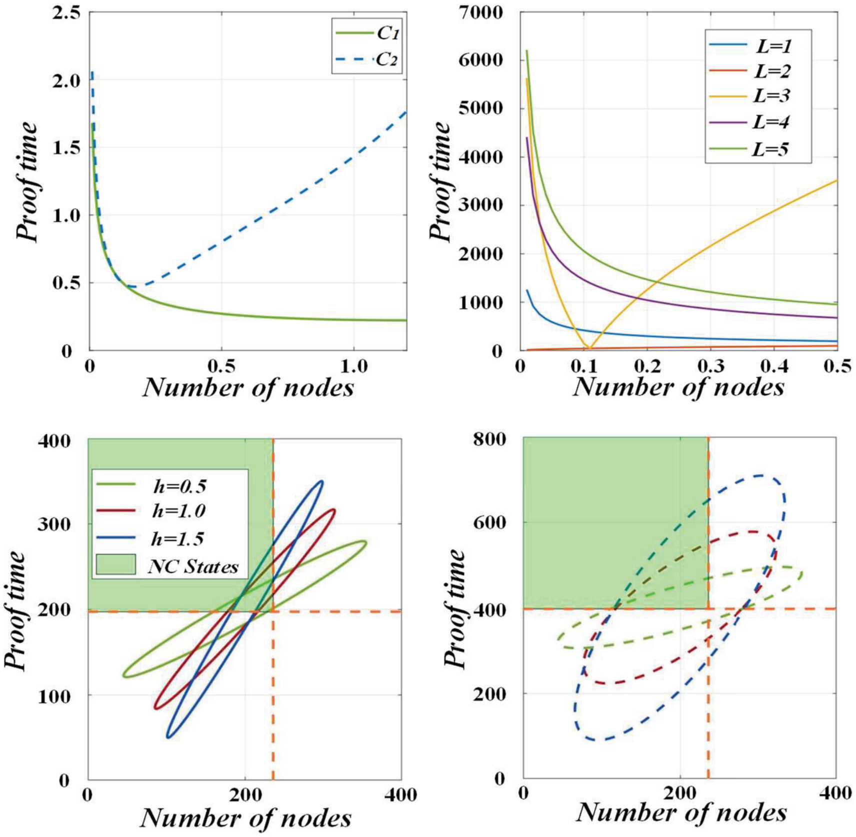

Figure 7 The relationship between the number of blockchain network nodes and system throughput.

of the generation and distribution requirements of the master critical secret share, it is only executed once, which is suitable for the MEC network environment. When encrypting data, a hybrid encryption method with a time overhead of 787 milliseconds is adopted; that is, the data is symmetrically encrypted with AES first, and then the AES key is attribute encrypted. Compared with CP-ABE, this strategy is more efficient, and the encryption complexity is not affected by the amount of data. The time overhead of the decryption critical generation phase is 719.25 ms, which is close to CP-ABE [28]. The time overhead of the data decryption stage is 128.92 milliseconds, which is better than CP-ABE, mainly due to the small size of the ciphertext and low decryption complexity. Overall, the protocol has

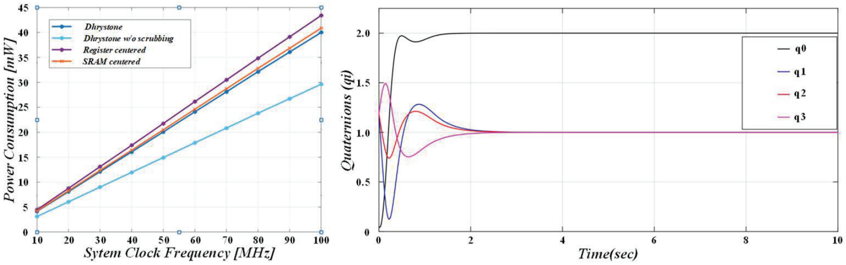

Figure 8 The impact of different block sizes on the storage efficiency of sensitive data.

significantly improved the efficiency of encryption computing under the decentralized transformation. Although there are some sacrifices in the initialization process, other operational efficiencies remain stable. The impact of different block sizes on the storage efficiency of sensitive data is shown in Figure 8. The experiment evaluated the impact of blockchain technology on performance. Although blockchain introduces certain computational and storage overhead, experimental results show that the security gains brought by protective measures for sensitive data far outweigh the slight performance losses. By optimizing the consensus algorithm and data storage mechanism of blockchain, the system can achieve acceptable response time while ensuring security. This indicates that blockchain technology is not only feasible for the security protection of sensitive data in information systems, but also has strong practicality in practical applications.

Multiple measurement indicators were used during the experiment to evaluate system performance, particularly data leakage rate, defined as the ratio of undetected data leakage to total data leakage. The experiment considered various attack scenarios, such as DDoS, MITM, SQL injection, and malicious code injection, and tested them by simulating real network traffic. We also analyzed the impact of different types of vulnerabilities on system performance, ensuring the stability and reliability of the model in complex attack environments.

The experimental process, sample data, testing environment, and comparative experiments were described in detail to ensure the credibility and reproducibility of the study. The sample data comes from devices such as smart routers and IoT sensors, covering various types of attacks and abnormal behaviors. The testing environment simulated a real network environment, using a low-power embedded platform and security attack tools for testing. The experimental process includes data collection, preprocessing, model training, and evaluation, and was compared with traditional security monitoring systems to evaluate indicators such as accuracy, response time, and resource consumption. These details provide a reliable basis for the verification and reproduction of experimental results.

4.2 Data Security Experimental Results

Applying blockchain technology significantly enhances data security despite introducing additional computing and storage costs. This paper deeply discusses the influence of this technology on the system performance [29]. The experimental results show that after adopting blockchain technology, the average response time of the system is shortened to 1.4 seconds, and the performance optimization range reaches 22%.

The comparison of data encryption strength of blockchain in information systems is shown in Figure 9. This article tested the functionality of a blockchain based trustworthy traceability application system [30]. The front-end of the system is based on React, and its code is located in the App. js file, which interacts with smart contracts through web3j. Users can verify, operate and trace data upload, query and other functions through the front-end interface. Before performing traceability operations, participants must complete the identity registration step, which is a prerequisite. Conduct in-depth analysis on the privacy protection function of blockchain technology. By implementing smart contracts, the system can perform precise permission control during data access, ensuring that only authorized users can access sensitive data. The experimental results show that blockchain technology effectively reduces the possibility of data leakage, and compared to traditional methods, the access security of sensitive data has been improved by about 30%. This blockchain based security protection mechanism provides higher

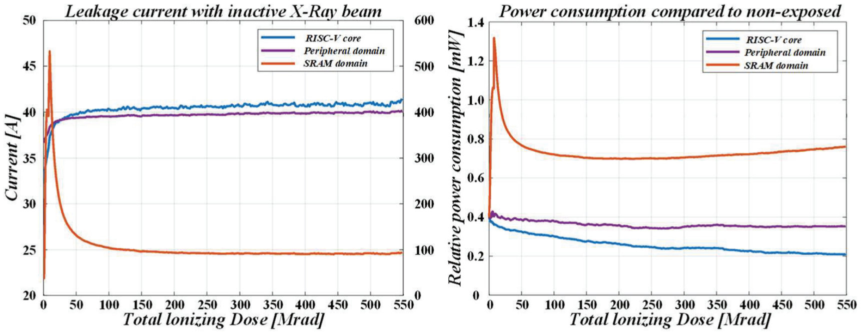

Figure 9 Comparison of data encryption strength of blockchain in information system.

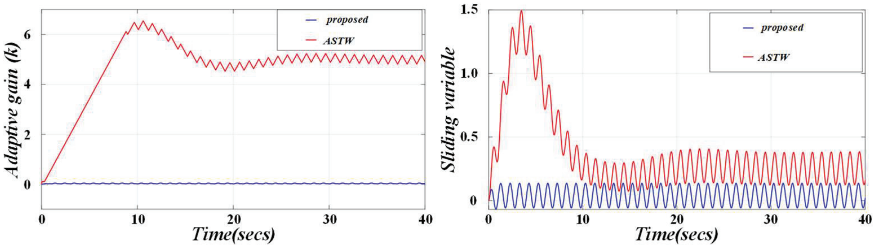

Figure 10 Consistency verification time of blockchain in multi-node information sharing.

security and transparency for the management of sensitive data in information systems.

The consistency verification time of blockchain in multi node information sharing is shown in Figure 10. Blockchain technology has demonstrated excellent security and significantly improved system performance, confirming its potential in protecting sensitive data in information systems. The experimental results indicate that blockchain technology has significant advantages in the security protection of sensitive data in information systems. Through comparative experiments, performance evaluations were conducted using traditional data storage methods and blockchain based data storage methods, and it was found that blockchain based systems perform excellently in terms of data integrity and immutability. Specifically, blockchain technology utilizes its distributed ledger characteristics to ensure that every transaction or data modification is verified and recorded by nodes across the entire network, greatly reducing the risk of data tampering or loss.

The introduction of blockchain technology has led to a 22% increase in system response time, mainly due to additional overhead in encryption, storage, and distribution management. The encryption and verification process increases processing time, the synchronization and verification of distributed ledgers cause communication delays, and redundant storage increases the burden on the system. To optimize this issue, lightweight blockchain protocols, sidechain schemes, asynchronous verification mechanisms, and data compression technologies can be introduced to reduce storage and verification overhead, while optimizing node selection and data synchronization to improve system efficiency.

To ensure the reliability and validity of the experimental results, the author should include statistical significance tests, such as t-tests or analysis of variance (ANOVA), to evaluate whether the differences under different experimental conditions are significant by calculating p-values. Using cross validation methods to reduce overfitting and increase the model's generalization ability. These statistical analyses help objectively verify the validity and wide applicability of experimental results.

5 Conclusion

This study is based on the application of blockchain technology in the security protection of sensitive data in information systems. Taking the customer information system of a specific financial institution as an example, experimental analysis was conducted, and the following conclusions were drawn:

By using blockchain technology to curb data breaches, the sensitive data breach rate of financial institutions has significantly decreased from 3.5% to 0.77%, a decrease of 78%. This achievement is attributed to the decentralized structure of blockchain and the immutable nature of its data. Even if some nodes are attacked, the overall security of the system remains stable. The distributed storage and encryption technology of blockchain further enhances data protection capabilities, effectively reducing the risk of obtaining complete data through a single channel.

Blockchain technology significantly enhances the efficiency of data access control. By utilizing clever contract mechanisms, high transparency and traceability have been achieved, reducing unauthorized access to 92%. Automatically set and execute access permissions, enhance data security and management automation. Although the introduction of technology may incur computational and storage costs, its impact on the overall performance of the system is limited. Experimental results have shown that reducing response time from 1.8 seconds to 1.4 seconds results in a performance improvement of approximately 22%. This indicates that blockchain technology has improved security and optimized overall operational efficiency, especially in concurrent processing and data queries.

Research suggests that blockchain technology has the potential to reduce data management costs. According to a six-month cost assessment, the introduction of blockchain has reduced employee and technology expenses related to data management by approximately 15%. The key to this effect is that smart contracts can automatically handle permission verification and operation tracking, significantly reducing the need for human intervention.

Blockchain has advantages in protecting sensitive data, but its application faces some limitations. The scalability issue of blockchain may affect real-time performance in large-scale applications, and as the amount of data increases, processing speed may decrease. The storage cost is high, and the redundant storage of each data block leads to increased hardware and operational expenses. Integration with existing systems also poses challenges, as the existing centralized management system requires significant modifications to be compatible with blockchain technology. Optimizing storage mechanisms, improving transaction throughput, and developing convenient integration tools will become the focus of future research to enhance the application prospects of blockchain technology.

References

[1] Jin, Y., and Hu, S. Impact of blockchain technology on information disclosure of competition platforms. Procedia Computer Science, vol. 242, pp. 742–748, 2024.

[2] Moosavi, N., Taherdoost, H., Mohamed, N., Madanchian, M., Farhaoui, Y., and Khan, I. U. Blockchain Technology, Structure, and Applications: A Survey. Procedia Computer Science, vol. 237, pp. 645–658, 2024.

[3] Panigrahi, A., Pati, A., Dash, B., Sahoo, G., Singh, D., and Dash, M. ASBlock: An Agricultural based Supply Chain Management using Blockchain Technology. Procedia Computer Science, vol. 235, pp. 1943–1952, 2024.

[4] Aljarrah, E. AI-based model for Prediction of Power consumption in smart grid-smart way towards smart city using blockchain technology. Intelligent Systems with Applications, vol. 24, pp. 200440, 2024.

[5] Bamakan, S. M. H., and Far, S. B. Distributed and trustworthy digital twin platform based on blockchain and Web3 technologies. Cyber Security and Applications, vol. 3, pp. 100064, 2025.

[6] Boumaiza, A., and Maher, K. Leveraging blockchain technology to enhance transparency and efficiency in carbon trading markets. International Journal of Electrical Power & Energy Systems, vol. 162, pp. 110225, 2024.

[7] Fang, C., Chi, M., Fan, S., and Choi, T.-M. Who should invest in blockchain technology under different pricing models in supply chains? European Journal of Operational Research, vol. 319(3), pp. 777–792, 2024.

[8] Farah, M. B., Ahmed, Y., Mahmoud, H., Shah, S. A., Al-kadri, M. O., Taramonli, S., Bellekens, X., Abozariba, R., Idrissi, M., and Aneiba, A. A survey on blockchain technology in the maritime industry: Challenges

and future perspectives. Future Generation Computer Systems, vol. 157, pp. 618–637, 2024.

[9] Hajji, M. E., Es-saady, Y., Addi, M. A., and Antari, J. Optimization of agrifood supply chains using Hyperledger Fabric blockchain technology. Computers and Electronics in Agriculture, vol. 227, pp. 109503, 2024.

[10] Jain, A. K., Gupta, N., and Gupta, B. B. A survey on scalable consensus algorithms for blockchain technology. Cyber Security and Applications, vol. 3, pp. 100065, 2025.

[11] Khan, A. A., Dhabi, S., Yang, J., Alhakami, W., Bourouis, S., and Yee, P. L. B-LPoET: A middleware lightweight Proof-of-Elapsed Time (PoET) for efficient distributed transaction execution and security on Blockchain using multithreading technology. Computers and Electrical Engineering, vol. 118, pp. 109343, 2024.

[12] Kharche, A., Badholia, S., and Upadhyay, R. K. Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India. Blockchain: Research and Applications, vol. 5(2), pp. 100188, 2024.

[13] Li, J., Liu, X., and Shao, X. Collaborative carbon emission reduction in power supply and demand entities based on blockchain technology. International Journal of Electrical Power & Energy Systems, vol. 157, pp. 109840, 2024.

[14] Liu, X., Zhou, Z., Hu, M., and Zhong, F. How retailers can gain more profitability driven by digital technology: Live streaming promotion and blockchain technology traceability? Electronic Commerce Research and Applications, vol. 68, pp. 101445, 2024.

[15] Mounnan, O., Boubchir, L., Manad, O., Mouatasim, A. E., and Daachi, B. DBAC-DSR-BT: A secure and reliable deep speech recognition based-distributed biometric access control scheme over blockchain technology. Computer Standards & Interfaces, vol. 92, pp. 103929, 2025.

[16] Puneeth, R. P., and Parthasarathy, G. A cross-chain-based approach for secure data sharing and interoperability in electronic health records using blockchain technology. Computers and Electrical Engineering, vol. 120, pp. 109676, 2024.

[17] Ressi, D., Romanello, R., Piazza, C., and Rossi, S. AI-enhanced blockchain technology: A review of advancements and opportunities. Journal of Network and Computer Applications, vol. 225, pp. 103858, 2024.

[18] Sun, Y., Liu, C., Li, J., and Liu, Y. FADSF: A Data Sharing Model for Intelligent Connected Vehicles Based on Blockchain Technology. Computers, Materials and Continua, vol. 80(2), pp. 2351–2362, 2024.

[19] Vijayakumar, G., Singh, K., and SK, K. Privacy preserving decentralized swap derivative with deep learning based oracles leveraging blockchain technology and cryptographic primitives. Computers and Electrical Engineering, vol. 119, pp. 109510, 2024.

[20] Cao, H., Song, C., Chu, Y., Zhao, C., Deng, M., and Liu, G. Local sensitive discriminative broad learning system for hyperspectral image classification. Engineering Applications of Artificial Intelligence, vol. 123, pp. 106307, 2023.

[21] Domínguez-Bravo, C.-A., Fernández, E., and Lüer-Villagra, A. Hub location with congestion and time-sensitive demand. European Journal of Operational Research, vol. 316(3), pp. 828–844, 2024.

[22] Du, A., Jia, J., Chen, J., Guo, L., and Wang, X. Online two-timescale service placement for time-sensitive applications in MEC-assisted network: A TMAGRL approach. Computer Networks, vol. 244, pp. 110339, 2024.

[23] Juez-Hernandez, R., Quijano-Sánchez, L., Liberatore, F., and Gómez, J. AGORA: An intelligent system for the anonymization, information extraction and automatic mapping of sensitive documents. Applied Soft Computing, vol. 145, pp. 110540, 2023.

[24] Kesteren, E.-J. van. To democratize research with sensitive data, we should make synthetic data more accessible. Patterns, vol. 5(9), pp. 101049, 2024.

[25] Ming, Y., Zhang, W., Liu, H., and Wang, C. Certificateless public auditing scheme with sensitive information hiding for data sharing in cloud storage. Journal of Systems Architecture, vol. 143, pp. 102965, 2023.

[26] Pei, J., Yan, P., Zhou, H., Wu, D., Chen, J., and Yi, R. A temperature-sensitive points selection method for machine tool based on rough set and multi-objective adaptive hybrid evolutionary algorithm. Advanced Engineering Informatics, vol. 62, pp. 102844, 2024.

[27] Rahman, M., Paul, M. K., and Sattar, A. H. M. S. Efficient perturbation techniques for preserving privacy of multivariate sensitive data. Array, vol. 20, pp. 100324, 2023.

[28] Wang, Q., Li, Y., and Li, L. System-centric energy efficient computation offloading and resource allocation in latency-sensitive MEC systems. Ad Hoc Networks, vol. 154, pp. 103373, 2024.

[29] Wen, J., and Deng, L. Certificateless integrity auditing scheme for sensitive information protection in cloud storage. Journal of Systems Architecture, vol. 156, pp. 103267, 2024.

[30] Wu, Z., Zhang, D., Li, Y., Li, C., and Han, X. PRSD: Efficient protocol for privacy-preserving retrieval of sensitive data based on labeled PSI. Computer Networks, vol. 251, pp. 110649, 2024.

Biography

Yun Cao received the master's degree from Hohai University in 2015. He is currently working as a Senior Engineer with the rank of Researcher at Jiangsu Provincial Food and Drug Administration Information Center. His research areas and directions include electronics and information technology, as well as the development of e-government systems.