Research on Blockchain-based Security Sharing Algorithm of Social Assistance Data in Internet of Things

Xiuli Yang* and Xinyuan Wang

Public Management and Law School, Northeast Agricultural University, No. 600 Changjiang Road, Xiangfang District, Harbin 150300, Heilongjiang, China
E-mail: yangxiuli73@126.com
**Corresponding Author*

Received 19 May 2025; Accepted 28 June 2025

Abstract

With the in-depth application of Internet of Things technology in the field of social assistance, the security issue of data sharing has become increasingly prominent. In order to solve the risks of data leakage and tampering in traditional centralized management, this paper proposes a security sharing algorithm for IoT social assistance data based on blockchain and smart contracts. By evaluating different blockchain types in simulation experiments, the results show that private chains perform best in terms of data transmission time and processing power, alliance chains have the highest security score, and hybrid chains achieve a balance between performance and security. Further experiments show that smart contracts significantly improve the efficiency of data sharing, with an intermediary cost saving rate of more than 50% and a maximum contract execution efficiency of more than 20 times per second. In terms of data encryption algorithms, AES has the shortest processing time, RSA has the most stable performance under high

Journal of Cyber Security and Mobility, Vol. 14_3, 747–776.
doi: 10.13052/jcsm2245-1439.14310

security levels, and SM2 consumes more than 65% of CPU in high data volume scenarios, which is costly. In terms of safety score, SHA-256 has the highest score, with an anomaly detection rate of 95%. This study verifies the feasibility and superiority of blockchain combined with smart contracts in ensuring the safe sharing of social assistance data in the Internet of Things, and provides theoretical and practical support for the intelligent and credible construction of social assistance systems in the future.

Keywords: Blockchain, Internet of Things, social assistance, data security, smart contracts.

1 Introduction

With the continuous development of information technology, the Internet of Things (IoT) has become an important part of global digital transformation [1]. Through the deep integration of intelligent devices, sensors, etc., with the Internet, the Internet of Things has greatly changed human lifestyle and social operation mode, especially in social assistance. The application of the Internet of Things significantly enhances the operational efficiency and transparency of social assistance systems by enabling real-time data collection and analysis [2]. However, in this process, data security issues have become increasingly prominent. Many sensitive data from IoT devices must be transmitted and stored in a complex network environment. Without effective security mechanisms, risks such as data leakage and tampering may be faced, thus affecting the normal progress of social assistance work. Therefore, how to ensure the security, sharing and transparency of social assistance data in the Internet of Things system has become a key problem to be solved urgently.

Traditional social assistance data management usually relies on a centralized database system. Although this centralized management mode is convenient for data storage and processing, it is easy to become the target of attacks when facing the distributed Internet of Things environment, and it isn't easy to share and trace data [3]. With the continuous development of network attack methods, especially the increasingly complex attack forms aimed at data integrity and privacy protection, how to ensure that the rescue data is not illegally tampered with or leaked in the process of transmission has become an important research topic in the field of network security. In addition, the credibility and sharing of data are also difficulties in the current social assistance system. In many cases, the social assistance data involved

by different departments and agencies in the rescue process must be shared. However, due to the lack of an effective sharing mechanism, all parties have concerns about the security and privacy of data, resulting in obstacles to data sharing still exist.

The emergence of blockchain technology provides new ideas for solving this problem [4]. As a decentralized distributed ledger technology, blockchain has its unique non-tampering and transparency, which provides an effective means to ensure the safe sharing of social assistance data in the Internet of Things environment [5]. Through blockchain technology, the decentralized storage and management of social assistance data can be realized, avoiding the security risks a single data center may face. Because its data cannot be tampered with, it can ensure the authenticity and integrity of assistance data in the sharing process. In addition, blockchain technology can realize an automated trust mechanism through smart contracts, allowing participants to exchange trusted data without intermediaries, thereby improving the efficiency and security of data sharing.

However, although blockchain technology has shown great potential in the secure sharing of social assistance data, its application in the IoT environment still faces some challenges. First of all, since the transaction confirmation process of blockchain technology consumes a lot of computing resources and time, improving the processing efficiency and response speed of the blockchain system is an urgent problem to be solved in the case of a huge number of IoT devices. Secondly, the blockchain itself has limited data storage and processing capabilities. Future research focuses on how to design a more efficient consensus mechanism and data storage scheme to ensure efficient data processing while ensuring security. In addition, with the continuous development of blockchain technology, its integration with other technologies, such as the Internet of Things and cloud computing, will become an important direction to promote the safe sharing of social assistance data.

Firstly, this article introduces the importance of protecting social assistance data in the IoT environment and emphasizes the challenges brought by centralized data management systems. Next, it reviews the theoretical foundation of blockchain technology and its potential to address these challenges. The core contribution of this article is the proposal of a blockchain based secure sharing algorithm, which has been validated through a series of experiments involving different blockchain architectures and data encryption algorithms. This article further explores the use of smart contracts to automate data access control and sharing, improve efficiency, and reduce costs. Finally,

this article discusses the results of simulations and practical applications, demonstrating the effectiveness of the proposed algorithm in ensuring secure and efficient data sharing in IoT based social assistance systems.

The innovation of this study lies in combining blockchain technology with the Internet of Things to ensure secure data sharing in the field of social assistance. Firstly, this article proposes a new hybrid blockchain architecture that combines private, consortium, and public blockchains, balancing data security, processing power, and cost. Secondly, the use of smart contracts automates data access control and sharing processes, eliminates intermediaries, and reduces transaction costs by over 50%. Thirdly, the study investigated and compared various encryption algorithms of blockchain, such as AES, RSA, and SM2, to ensure effective data protection while minimizing resource consumption. Finally, the proposed model provides secure, transparent, and traceable data sharing through decentralized management, supports multi-party collaboration scenarios, and significantly improves the efficiency and credibility of the social assistance system. To address these challenges, this article explores the potential of blockchain technology, which has unique advantages in data security and sharing. In the next section, this article will provide an overview of blockchain technology and its fundamental role in ensuring the security of social assistance data in the Internet of Things environment.

2 Theoretical Basis and Related Research

2.1 Overview of Blockchain Technology

Since it was first proposed, blockchain technology has quickly become an important innovation in information technology. As a decentralized distributed ledger technology, blockchain realizes transparent, non-tampering, and untrusted data management by removing intermediaries [6, 7]. Each block contains a set of encrypted data, which are chained in chronological order to form a continuous, unchangeable record. In the blockchain network, each node can participate in the verification and storage of data, which makes the blockchain have high security and anti-tamper capabilities, especially when facing the threat of network attacks and data tampering, it can effectively guarantee Data integrity and reliability. Therefore, blockchain has unique advantages in improving data security and transparency and is especially suitable for application scenarios that need to guarantee data security, privacy, and trust.

One of the core advantages of blockchain is its decentralized nature. In traditional database systems, all data storage and verification depend on a centralized server or database, which makes the system vulnerable to attacks and tampering [8]. In contrast, the decentralized structure of blockchain validates and stores data through a network of distributed nodes, each of which holds a copy of the blockchain and jointly maintains the system's security [9]. This structure not only improves the anti-attack ability but also avoids the single point of failure problem and ensures the high availability and robustness of the system. In addition, the consensus algorithms adopted by blockchain, such as proof of work and proof of stake, ensure the reliability and consistency of data through calculation and verification mechanisms, greatly reducing the risk of data tampering.

In network security, blockchain technology further improves data security through its built-in encryption algorithm. A hash algorithm encrypts the data in each block, and any modification of the data will cause the block's hash value to change, which will be detected by other nodes in the network [10]. This non-tamperable feature gives blockchain a natural advantage in protecting sensitive data. In the Internet of Things environment, the data generated by devices usually has the characteristics of high frequency and massive volume, and blockchain can provide an efficient and secure storage and management method for these data. For example, in managing social assistance data of the Internet of Things, blockchain can ensure the authenticity of each assistance record and avoid data deviations caused by human error or malicious tampering, thereby enhancing the credibility of assistance data.

However, although blockchain has significant advantages in data security, it still faces some challenges in practical applications. First, the blockchain scalability problem has not been fully solved. When dealing with large-scale data, blockchain storage, and transaction verification, capabilities may be limited, resulting in longer response times for the system [11]. In addition, the energy consumption of the blockchain network is also an issue that cannot be ignored, especially when using the proof of work mechanism; the consumption of computing resources is very large. Therefore, how to improve the processing efficiency and reduce the energy consumption of blockchain while ensuring data security is still a hot topic in current technology research. In addition, when blockchain technology is applied to the Internet of Things, it is also necessary to solve the interoperability and protocol compatibility issues between different devices to ensure smooth transmission and efficient data sharing.

2.2 Current Status of IoT Social Assistance Based on Blockchain

With the rapid development of Internet of Things technology, social assistance has gradually begun on Internet of Things devices for data collection, transmission, and management. Through smart sensors, smart devices, and data collection platforms, the Internet of Things can obtain all kinds of social assistance information in real-time, such as basic information about people experiencing poverty, assistance needs, and distribution of assistance materials [12, 13]. This kind of real-time collection and analysis of information provides more accurate data support for social assistance work and can improve social assistance's efficiency and response speed. However, with the increasing amount of data and the acceleration of informatization, ensuring the security, privacy, and integrity of these sensitive data has become an important issue in the field of social assistance of the Internet of Things.

Although the Internet of Things has brought significant improvements to the field of social assistance, due to the open and distributed characteristics of the Internet of Things system itself, its security issues cannot be ignored [14]. IoT devices usually transmit data through wireless networks, which makes them vulnerable to security threats such as man-in-the-middle attacks, data tampering, and theft [15]. Especially in social assistance, a field related to people's livelihood, the assistance data involved often contains much personal privacy information. If these data are leaked or tampered with, it will greatly affect the fairness and transparency of the assistance work and may even bring social instability. Therefore, establishing a system that can realize data sharing and ensure data security has become a core issue in the current social assistance Internet of Things application.

The emergence of blockchain technology provides new solutions for the secure sharing of social assistance data in the Internet of Things. With decentralization, non-tampering, openness, and transparency, blockchain technology can achieve efficient data sharing while ensuring data security [16, 17]. In the IoT environment, blockchain can be used as an underlying architecture to ensure the authenticity and consistency of data through smart contracts and consensus mechanisms [18]. Specifically, blockchain can provide a secure storage method for social assistance data, avoiding the risks of hacker attacks and data loss that traditional centralized storage methods may encounter. At the same time, the transparency of blockchain enables all parties to trace the source and change of data in real-time, effectively improving the fairness and trust of social assistance work.

However, blockchain application in the IoT social assistance field still faces some challenges. First of all, the popularity of IoT devices has generated massive data, which puts forward higher requirements for the storage capacity and processing efficiency of blockchain [19, 20]. The storage and verification process of blockchain may face performance bottlenecks when processing large amounts of data. Improving the scalability and response speed of blockchain has become an urgent problem to solve. Secondly, the heterogeneity of IoT devices makes data exchange and protocol compatibility between different devices a technical problem. Uniform standards and protocols need to be developed to ensure that IoT devices can interact efficiently and securely with blockchain systems. In addition, the high energy consumption of blockchain is also an issue that must be considered in IoT applications. Researchers still focus on how to reduce the energy consumption of blockchain and improve its sustainability in the large-scale Internet of Things environment. While blockchain technology offers significant potential in securing data, its application in the Internet of Things for social assistance still faces several hurdles. The following section examines the current status of IoT-based social assistance systems and how blockchain can address key challenges in data security and sharing.

3 Establishment of a Real-time Encryption Anomaly Detection Model for 5G Communication Data Integrating AES-GCM and LSTM

3.1 Overall Model Framework and Process

Given the allocation of a large amount of sensitive personal data and public resources in the social assistance system of the Internet of Things, this study points out the problems of ensuring privacy protection, integrity, and sharing security of data during transmission. To meet this challenge, this study proposes an algorithm model for the security sharing of the Internet of Things social assistance data based on blockchain [21]. This model provides an efficient, secure, and transparent solution for data sharing in the field of social assistance by combining blockchain technology with smart contracts.

The core framework of the system consists of two main modules: the first module is a blockchain-based data storage and management module, and the second is a smart contract-based data access control and sharing module [22]. As a decentralized distributed ledger technology, blockchain has the advantages of non-tampering, transparency and distributed storage,

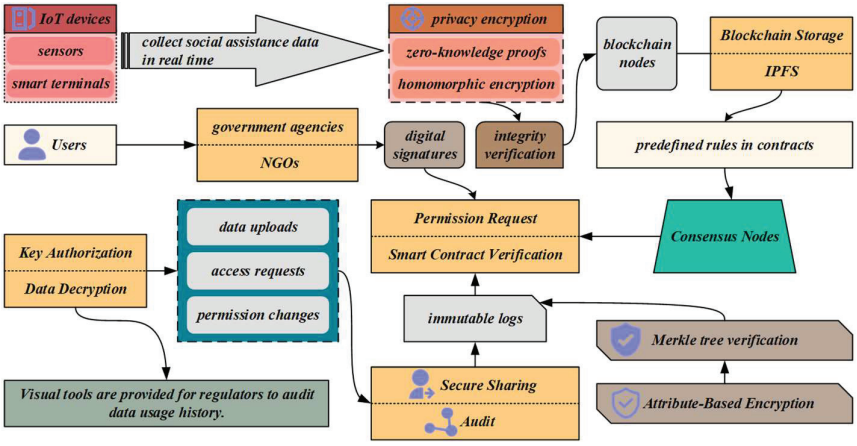

Figure 1 Flowchart of social assistance data security sharing based on blockchain and smart contract.

and can effectively guarantee the security of social assistance data. Smart contracts achieve precise control of data access rights through automated contract execution, ensuring that data is shared under legal authorization. The flow chart of social assistance data security sharing based on blockchain and smart contracts is shown in Figure 1.

As can be seen from the figure, the data ensures the security of sensitive information through privacy encryption, zero-knowledge proof and homomorphic encryption, and then the blockchain node requests and verifies permissions according to the preset rules in the smart contract. After the consensus node confirms, the data is stored in the blockchain and IPFS, and a non-tamperable log is generated simultaneously. Visitors can access, decrypt, and modify their permissions after being authorized by the key. The system also supports Merkle tree verification and attribute-based encryption to strengthen security control. The process supports regulatory auditing and visualization tools to track data flow records, realizing safe, efficient, and controllable data sharing in multi-party collaboration scenarios.

The innovation of this model lies in the combination of blockchain and the Internet of Things, and using the decentralized characteristics of blockchain and the automatic execution of smart contracts to solve the potential security hazards existing in the social assistance data sharing of the Internet of Things [23]. Traditional data-sharing models often rely on centralized servers or intermediaries, and there are risks such as single point of failure and data tampering. However, blockchain technology solves these problems through

decentralized mechanisms, ensuring the security and transparency of the data-sharing process. At the same time, through smart contract technology, the data-sharing process can be automatically executed without intermediary intervention, improving efficiency. The data data-sharing security coefficient formula is shown in (1).

$$S = \frac{l - P_f}{l + R_m} \tag{1}$$

Among them, S represents the security coefficient of data sharing, P_f represents the probability of single point failure of the system, and R_m represents the risk coefficient of data tampering. The formula of contract execution efficiency is shown in (2).

$$E = \frac{N_t}{T_e} \tag{2}$$

Among them, E represents the contract execution efficiency, N_t represents the number of smart contracts successfully executed per unit time, and T_e represents the total execution time.

Suppose a natural disaster occurs in a certain place, and relief agencies must quickly mobilize social assistance resources and distribute aid funds to the affected people. In the traditional model, the centralized system may affect data transmission and resource allocation, causing delays or information leakage [24]. The blockchain-based system automatically executes the distribution of rescue funds through smart contracts, and all transactions and data-sharing processes are recorded on the blockchain, ensuring that the whereabouts and usage of each fund are transparent and traceable, preventing data tampering and corruption. By organically combining blockchain and smart contract technology, the model proposed in this study ensures the security of social assistance data of the Internet of Things, improves the efficiency and transparency of data sharing, and has high innovation value.

3.2 Blockchain Data Storage and Management Module

In the Internet of Things social assistance system, data storage and management is the key link to ensure information security and efficient sharing. Traditional data management models often rely on centralized servers for data storage and management, susceptible to problems such as data tampering, single points of failure, and hacking [25]. Therefore, the system proposed in this study builds a decentralized data storage and management module by introducing blockchain technology to ensure data security, transparency,, and

non-tampering. The data storage security assessment formula is shown in (3).

$$DSI = \frac{1}{P_a + P_s + P_h} \tag{3}$$

Among them, ***DSI*** represents the data security index, P_a represents the probability of unauthorized access to data, P_s represents the probability of a single point of failure, and P_h represents the probability of being hacked. The tamper resistance coefficient formula is shown in (4).

$$TRC = \frac{B_c \cdot H_r}{I + A_r} \tag{4}$$

Among them, ***TRC*** represents the tampering resistance coefficient, B_c represents the number of confirmed blocks, H_r represents the total hash rate of the network, and A_t represents the attacker's computing power ratio. As a distributed ledger technology, the core characteristics of blockchain are decentralization, transparency, and non-tampering. In this module, every social assistance data generated by the Internet of Things will be encrypted and written to the blockchain. Each "block" in the blockchain contains a certain amount of social assistance data. When a block reaches a certain size, it will be linked with the previous block through encryption to form a chain structure. This process ensures that the data cannot be tampered with in the blockchain. Once the data is written to the blockchain, no one can modify or delete the data, which provides a strong guarantee for the authenticity and integrity of the data [26]. The encryption write delay formula is shown in (5).

$$EWL = \frac{S_d}{R_e} \tag{5}$$

Among them, ***EWL*** represents data encryption write delay, S_d represents data volume, and R_e represents encryption speed. The formula of data integrity guarantee rate is shown in (6).

$$DLAR = \frac{N_\nu}{N_t} \tag{6}$$

Among them, ***DIAR*** represents the integrity guarantee rate, N_v represents the number of data verified by hash, and N_t represents the total number of written data. In this module, the blockchain network is jointly maintained by multiple nodes, and each node has a complete copy of the ledger, which ensures the consistency and security of blockchain data through a consensus mechanism [27]. Different from the traditional centralized data storage

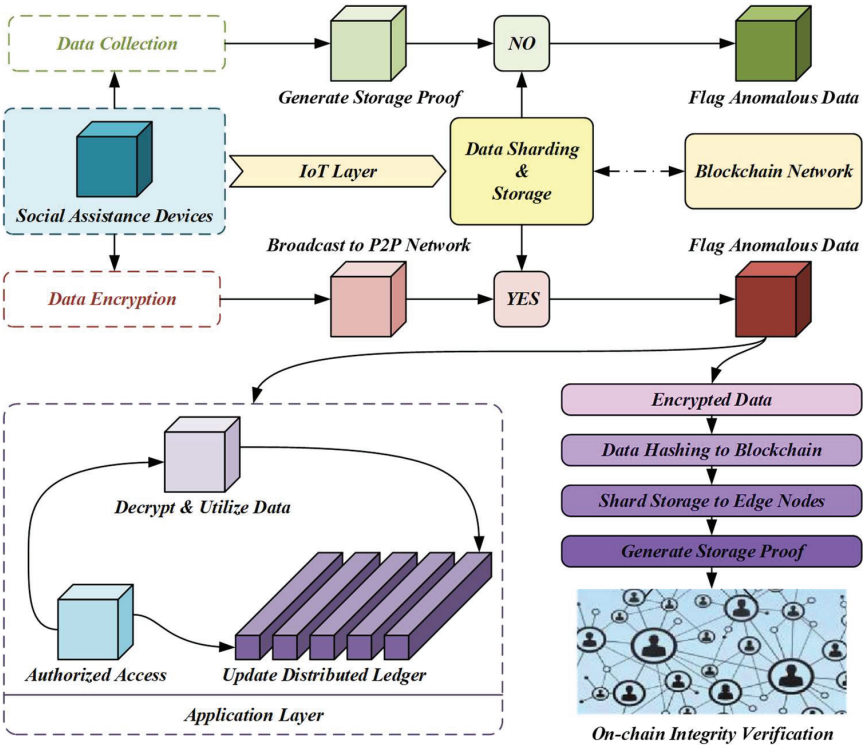

Figure 2 Decentralized data storage and consensus mechanism in blockchain network.

model, the decentralized nature of blockchain eliminates the risk of single point of failure and improves the stability and reliability of the system. At the same time, all data writing operations will be verified by nodes in the network to ensure that only legitimate data can enter the blockchain, thus avoiding tampering and forgery of illegal data. The decentralized data storage and consensus mechanism in the blockchain network is shown in Figure 2.

This process shows the complete data collection path, encryption, shared storage, and consensus verification in the IoT social assistance system. First, the social assistance equipment collects raw data and generates storage credentials after processing by the IoT layer. It is marked as abnormal data if it cannot be verified, and the process is aborted. The data will be encrypted and broadcast to the P2P network if the verification is passed. Then, the system hashes the encrypted data on the chain, fragments it, stores it in edge nodes, and generates storage credentials again to support on-chain integrity verification. Authorized users can decrypt data and perform business layer

operations on this basis. At the same time, the distributed ledger is updated synchronously to ensure the data utilization process is open and trustworthy. The entire mechanism realizes efficient sharing and secure storage of social assistance data in a decentralized environment through multi-layer security control and on-chain verification.

The blockchain network adopts a distributed storage method to solve the huge data storage problem in the Internet of Things. Each node only stores part of the data while maintaining the encryption and privacy of the data. In this way, the storage cost can be effectively reduced while ensuring that the data privacy of each node is not compromised [28]. The encrypted data storage also makes it impossible for attackers to obtain the specific data content stored in the blockchain even if certain nodes are attacked, thus effectively preventing data leakage and tampering. The average node storage cost formula is shown in (7).

$$ANSC = \frac{D_t \cdot C_s}{N_n} \tag{7}$$

Among them, *ANSC* represents the average storage cost of a single node, D_t represents the total data volume, C_s represents the storage cost per unit of data, and N_n represents the total number of nodes. The privacy guarantee coefficient formula is shown in (8).

$$PPC = \frac{1}{V_d \cdot A_c} \tag{8}$$

Among them, *PPC* represents the privacy guarantee coefficient, V_d represents the data visibility, and A_c represents the node access control level.

In addition, the transparency of blockchain allows all social assistance data to be reviewed by anyone, ensuring the openness, fairness and transparency of data sharing. In this mode, all data access and modification operations will leave unalterable records on the blockchain, thus providing strong support for data traceability and auditing.

3.3 Data Access Control and Sharing Module of Smart Contract

As an automated protocol execution mechanism, smart contracts are widely used in blockchain to achieve data access control and sharing. Traditional data-sharing mechanisms usually rely on centralized rights management systems, and there are security risks such as rights abuse and data leakage [29]. The access control and sharing mechanism based on smart contracts can

realize the automation, transparency, and decentralization of data sharing while ensuring data security. The core goal of this module is to achieve fine-grained permission control over social assistance data through smart contracts, ensuring that data can only be shared if authorized.

In this module, smart contracts manage data access rights and automate the authorization, approval, and sharing processes. The access rights of each social assistance data will be defined in the smart contract, and the rights will be divided according to different roles and needs [30]. Only certified social assistance agencies or related personnel can access specific sensitive data, while ordinary users or the public can only access publicly available data. By automating the enforcement of these access control rules, smart contracts eliminate the need for human intervention and intermediaries, improving the efficiency and transparency of data sharing. The access control strength index formula is shown in (9).

$$f'(x) = f(x) + Lap\left(\frac{\Delta f}{\epsilon}\right) \tag{9}$$

Where $f(x)$ represents the true query value, ε represents the privacy budget, Δ_f represents the sensitivity, and *Lap* represents the Laplacian noise. The edge node block synchronization algorithm is shown in (10).

$$B_{i+1} = Pull(B_i, \delta) \tag{10}$$

Where B_i represents the current block state, δ represents the synchronization delay, and B_{i+1} represents the edge node. The execution of smart contracts is completely decentralized, and all operations are performed on the blockchain without relying on any third-party authority. This reduces the intermediary cost in data transmission and improves the system's security. Whenever a data-sharing request occurs, the smart contract will automatically determine whether to allow access according to preset conditions and perform data-sharing operations if the conditions are met. If a request does not comply with access rules, the smart contract rejects the request. It records the reason for the rejection on the blockchain to ensure transparency and traceability of the access control process. The intermediary cost-saving index formula is shown in (11).

$$ICSR = \frac{C_t - C_s}{C_t} \tag{11}$$

Among them, *ICSR* represents the intermediary cost saving rate, C_t represents the data sharing cost of traditional manual or centralized methods,

and C_s represents the data sharing cost after using smart contracts. To further improve the system's security, smart contracts can combine multiple encryption technologies to encrypt and protect data. During the data-sharing process, the data can be stored in encrypted form in the blockchain, and only authorized users with the corresponding keys can decrypt the data. In this way, even if the key of a node is leaked, the attacker cannot obtain the plaintext content of the data, thus avoiding the risk of data leakage.

Another important role of smart contracts is to ensure the automation of the data-sharing process. Traditional data-sharing models typically require human intervention and approval, while smart contracts automate data-sharing operations through pre-written rules. This automated feature improves efficiency and reduces human error or corrupt practices, ensuring fairness and transparency in the social assistance data-sharing process. With a clearer understanding of the current state of IoT-based social assistance and the role of blockchain, we now turn our attention to the proposed algorithm model. This model integrates blockchain with smart contracts to address privacy protection, integrity, and data sharing security in real-time social assistance applications.

4 Experimental Results and Analysis

This experiment simulates the social assistance scenario of the Internet of Things. It uses sensitive data, including personal identity, assistance needs, and material distribution, to explore how to achieve efficient data sharing while ensuring data security. The experiment uses a high-performance computing platform and distributed storage system, combined with network security technologies such as blockchain technology, encryption algorithm, digital signature, and identity authentication, to ensure that data is not tampered with or leaked during transmission, storage, and sharing. At the same time, through wireless sensor nodes, data transmission gateways, and cloud computing platforms, the real-time data acquisition and processing in the Internet of Things environment are simulated, which provides technical support for the research on the safe sharing of social assistance data in the Internet of Things. The blockchain data transmission efficiency evaluation is shown in Table 1.

In the table, this paper evaluates the transmission efficiency of four blockchains. The private chain has the fastest data transfer time and the highest processing power, indicating that it stands out in low latency and high throughput. Although the cost of private chains is relatively low, their

Table 1 Evaluation of blockchain data transmission efficiency

Blockchain Type	Data Transfer Time (s)	Processing Power (TPS)	Cost (Yuan/GB)	Safety Score
Public chain	2.5	500	0.5	80
Private chain	1.8	1000	0.2	85
Alliance Chain	2.2	800	0.4	90
Mixed chain	1.9	900	0.3	88

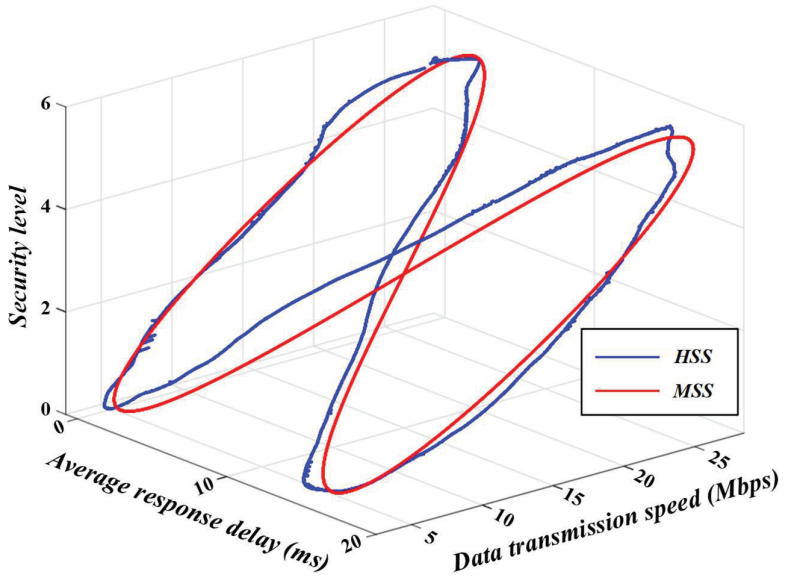

Figure 3 Relationship between security score and data transmission speed of IoT devices.

security scores are slightly inferior to those of consortium chains. The hybrid chain strikes a good balance of cost and security, and data transmission time and processing power are maintained at a high level. The public chain's low processing power and security scores indicate that it is suitable for scenarios with low-security requirements and allowing large transmission latency.

This paper analyzes the relationship between the security score of IoT devices and the data transmission speed to explore this relationship, and the results are shown in Figure 3.

As can be seen from the chart, HSS is distributed in areas with higher security levels as a whole, and at the same time, it still maintains a low response delay when the transmission rate exceeds 20 Mbps, indicating that it still has good security capabilities under high-performance transmission.

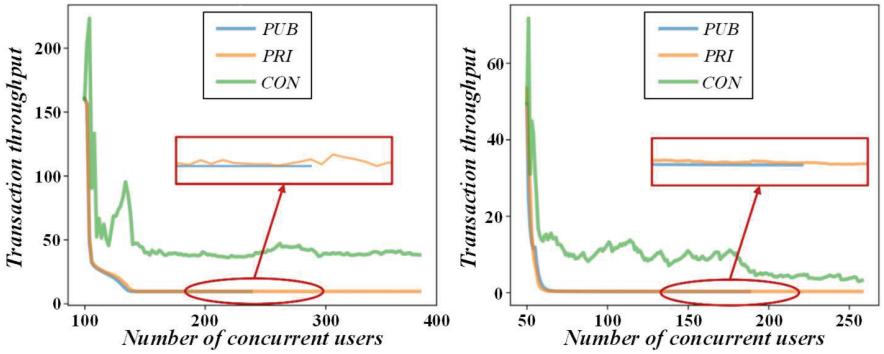

Figure 4 Comparison of transaction throughput of different blockchain types.

However, MSS is mainly concentrated in security levels 2–4. Although it can achieve transmission speeds similar to HSS in some sections, its average response delay is generally higher than 10 ms, and its performance fluctuations are more obvious. The overall trend shows that HSS devices strike a better balance between data transmission efficiency and security and are suitable for deployment in social assistance systems in highly security-sensitive scenarios. In contrast, MSS devices are more suitable for secondary or secondary node roles.

This paper compares the transaction throughput of different blockchain types to evaluate their application effect in Internet of Things social assistance data sharing. The results are shown in Figure 4.

According to the data in the figure, when the number of concurrent users increases from 100 to 400, the CON has the highest throughput in the initial stage, exceeding 200 TPS, but rapidly decreases and tends to stabilize at about 30 TPS after 150; PRI performance is the most stable, and the overall performance is maintained at around 90 TPS; PUB starts at only about 50 TPS, decreases slightly with concurrency growth and then stabilizes. The graph on the right further refines the trend of 50 to 250 concurrent users, where PRI always maintains the smoothest processing power, stabilizing at about 40 TPS in the 150-250 user range; PUB is slightly below PRI at around 30 TPS, while CON drops quickly from its initial high of 60 TPS and fluctuates around 20 TPS.

This paper analyzes the relationship between the sharing amount and access frequency of different types of social assistance data to study the differences in these, optimize data-sharing strategies, and improve the real-time performance of data. The results are shown in Figure 5.

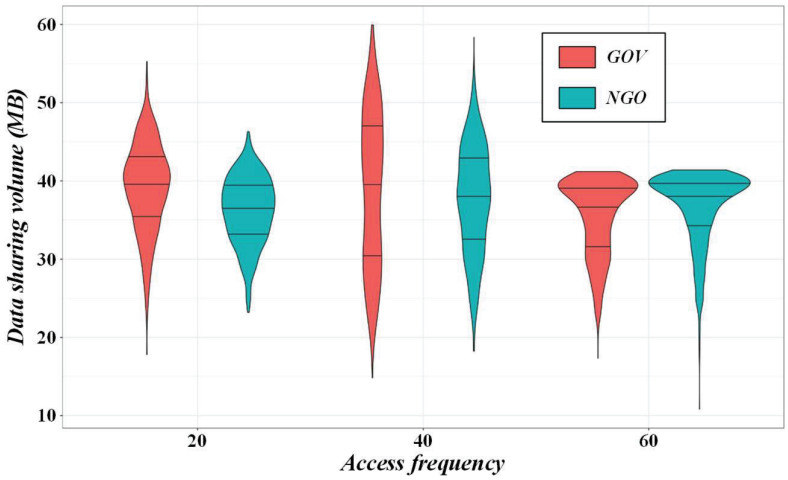

Figure 5 Relationship between the amount of social assistance data shared and the frequency of visits.

It can be seen from the figure that the amount of data sharing between government departments (GOV) and non-governmental organizations (NGOs) under different access frequencies shows obvious distribution differences. At a frequency of 20 visits, the amount of data sharing for GOV is concentrated between 35–45 MB, with a narrow distribution, while for NGO is between 30–42 MB, with a slightly higher concentration. When the frequency is 40, the data volume of GOV fluctuates, with a distribution span of 20–60 MB, indicating that the government sharing behavior is unstable at this frequency. NGOs are concentrated at 30–50 MB and are more dense. When the access frequency is increased to 60, the data shared between GOV and NGO tends to be concentrated around 40 MB, and the fluctuation range is significantly reduced. Government nodes have uneven sharing in the intermediate frequency access stage. In contrast, non-governmental organizations have more stable sharing in the high-frequency access stage (60 times), indicating that the data transmission efficiency of NGOs in high concurrency sharing is more consistent, and the blockchain social assistance system has strong load control capabilities.

The amount of social assistance data sharing is shown in Table 2. The table reflects the sharing of different social assistance data types. As the main data type, rescue information has the largest monthly sharing and the highest frequency of access. This shows that real-time updating and sharing of rescue information is very important for users. In contrast, device data is at

Table 2 Sharing amount of social assistance data

Data Type	Monthly Share Volume (GB)	Data Sources	Frequency of Visits (Times/Month)	Average Response Time (s)
Rescue information	500	5	100	3.2
Allocation of funds	300	3	80	4.5
User Feedback	200	6	120	2.9
Device Data	150	4	60	5.1

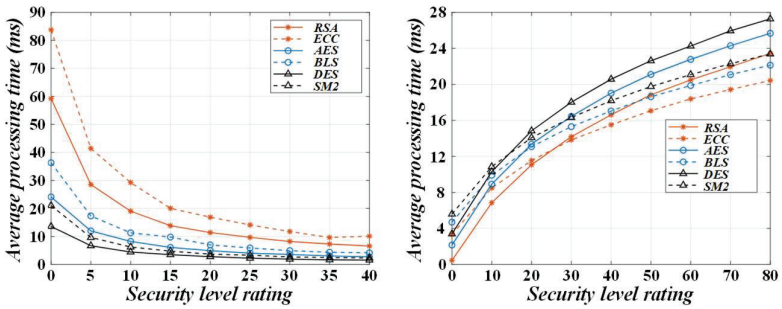

Figure 6 Comparison of security and processing time of different blockchain encryption algorithms.

least shared and accessed less frequently. Although the device data sharing is small, its average response time is the slowest of the four types of data, which may be related to its data processing complexity. Overall, the efficiency and response time of data sharing directly impact the user experience and need to be further optimized.

Compare the performance of data processing time of blockchain encryption algorithms while ensuring data security. This paper compares the security and processing time of different blockchain encryption algorithms, and the results are shown in Figure 6.

As can be seen from the figure, as the security level in the left figure increases from 5 to 40, the processing time of all algorithms drops rapidly. The initial processing delay of RSA is as high as about 85 ms, ECC is about 60 ms, and AES and DES are about 30 ms and 25 ms, respectively. In comparison, SM2 and BLS have the lowest processing time and are always controlled within 20 ms, reflecting their computing efficiency advantages in low-security scenarios. The picture on the right shows that during the safety level lifting from 0 to 80, the overall processing time shows an upward trend: SM2 processing time is about 27 ms, DES is 26 ms, and AES is about

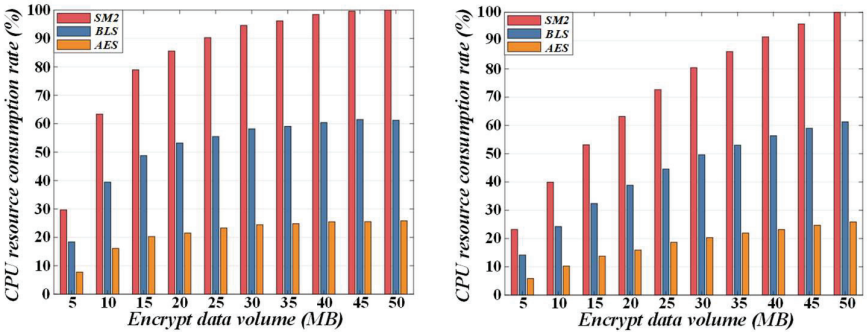

Figure 7 Comparison of encryption costs of blockchain algorithms in social assistance data sharing.

24 ms. At the same time, RSA and ECC are relatively better, stable at around 21 ms and 19 ms respectively. Taken together, RSA and ECC have both security and performance stability at high-security levels. In contrast, SM2 has the fastest processing speed at low-security requirements and is suitable for resource-constrained IoT scenarios.

The encryption cost generated by different blockchain encryption algorithms in data sharing, especially in the practical application of social assistance data sharing in the Internet of Things, is an important factor affecting system deployment and maintenance. This paper compares the encryption cost of blockchain algorithms in social assistance data sharing, and the results are shown in Figure 7.

It can be observed in the figure that the CPU resource consumption rate of the SM2 algorithm is close to 100%, BLS is about 60%, and AES is only about 30%, showing a significant advantage of AES in computing resource consumption. With the data volume increase, the CPU consumption rate of SM2 and BLS shows an obvious upward trend, while the growth of AES is slow. This shows that if efficient resource utilization is pursued in the social assistance data-sharing scenario, AES has more practical application value. Although SM2 has high security, its high encryption cost may limit its promotion in large-scale data processing.

This paper analyzes the correlation between the security score of IoT devices and the security score of blockchain to understand whether the two have some internal relationship and whether they are secure. The results are shown in Figure 8.

According to the data in the figure, as the number of connected devices increases to about 200, the average security score of the system generally rises

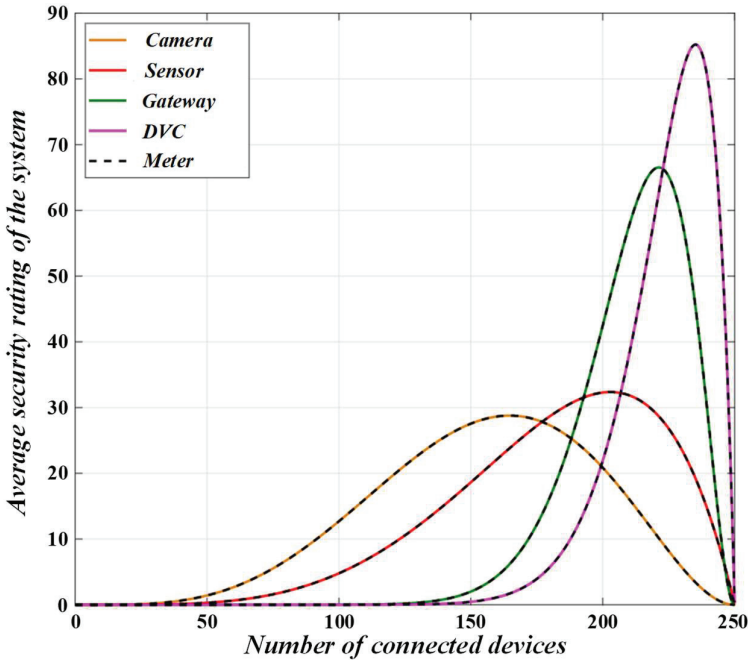

Figure 8 Correlation analysis diagram between IoT devices and blockchain security scores.

and peaks under different device types. DVC and Meter reached the highest point of safety score at 230 units, about 88 points, and performed the best; Gateway's peak score reached about 70 points at about 210 units; Sensor and Camera reached the maximum score at around 200 and 180 units respectively, only around 40 and 30 points. All device types followed a downward trend in scores. Overall, DVC and Meter are more conducive to the enhancement of system blockchain security. At the same time, Camera and Sensor have a relatively low contribution to security after the number of accesses increases, suggesting that the system needs to consider the impact of device types on blockchain security in its node deployment strategy. Differentiated impact on chain security performance.

The security performance comparison of blockchain algorithms in data sharing is shown in Table 3. This table shows the security performance of different blockchain algorithms in data sharing. SHA-256 algorithm has the best performance in data security score and anomaly detection rate, which shows that it has high reliability in ensuring data security. However, the encryption cost of RSA and ECDSA algorithms is high, which may trigger

Table 3 Comparison of security performance of blockchain algorithm in data sharing

Algorithm Type	Data Safety Score	Data Processing Time(s)	Encryption Cost (Yuan/MB)	Anomaly Detection Rate (%)
SHA-256	92	1.5	0.8	95
RSA	88	2.0	1.2	90
ECDSA	90	1.8	1.0	92
AES	85	1.2	0.6	85

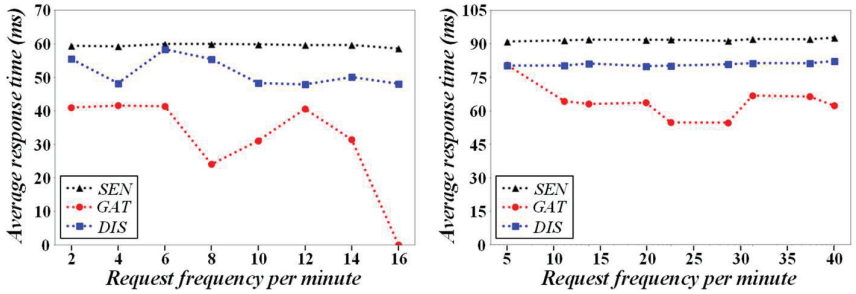

Figure 9 Relationship between response time and equipment type of social assistance data sharing.

cost pressure when data is shared on a large scale. The AES algorithm has a low security score, but its data processing time and encryption cost are the lowest, making it suitable for use in scenarios with high-speed requirements. According to these data, choosing the appropriate algorithm must be comprehensively considered according to requirements such as application security, processing speed, and cost.

To explore the response time difference of different types of IoT devices in social assistance data sharing, this paper analyzes the relationship between the response time of social assistance data sharing and device types. The specific results are shown in Figure 9.

It can be seen from the figure that when the request frequency rises from 2 times/min to 16 times/min, the response time of the sensor (SEN) is stable at 58–62 ms, showing the characteristics of high response delay but small fluctuation; The overall display terminal (DIS) is maintained at 45–55 ms; The gateway device (GAT) has the best response, rapidly dropping to below 30 ms after the frequency rises to 8 times/minute, and reaches as low as 5 ms at 16 times/minute, showing strong concurrent processing capabilities. In the figure on the right, at higher request frequencies, SEN is still maintained at about 95 ms, and GAT is maintained at about 85 ms. Although DIS

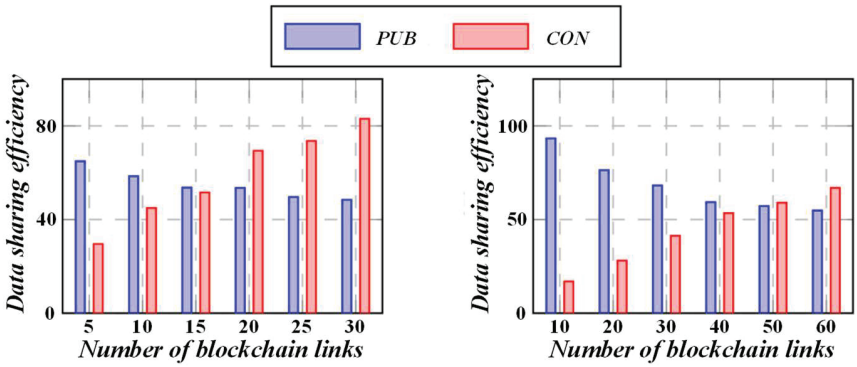

Figure 10 The relationship between the number of blockchain nodes and data sharing efficiency.

fluctuates between 75–80 ms, the response time increases significantly when the frequency reaches 35 times/min to about 85 ms then drops slightly. A Gateway device (GAT) responds most quickly to high-frequency requests and is suitable as the controller node of data sharing; SEN and DIS need to optimize the response mechanism to improve processing efficiency in complex scenarios.

This paper analyzes the relationship between the number of nodes and data sharing efficiency in blockchain to study and explore how to balance the number of nodes and data processing efficiency. The results are shown in Figure 10.

The data in the figure on the left shows that when the number of nodes increases from 5 to 30, the sharing efficiency of PUB decreases from about 70 to 45. In contrast, CON steadily increases from about 30 to 82, showing that the scalability of the alliance chain is stronger at medium and high node scales. In the figure on the right, when the number of nodes is 10, the PUB efficiency is as high as about 95, while the CON is only 20. But as the number of nodes rises to 60, PUB drops to about 60, and CON rises to more than 70. PUB is more efficient in small-scale networks, but its efficiency decreases significantly with the increase of nodes. In contrast, CON has better horizontal scalability and stability and is more suitable for blockchain application environments for large-scale social assistance data sharing.

In this paper, the "complex network environment" refers to scenarios that involve high concurrency, low bandwidth, and the presence of malicious attacks, all of which are common in IoT-based social assistance systems. Specifically, high concurrency scenarios arise when a large number of IoT

devices attempt to access or share data simultaneously, leading to potential network congestion and delays. Low bandwidth conditions can exacerbate these issues, causing data transmission inefficiencies and slow response times. Furthermore, malicious attacks, such as man-in-the-middle or denial-of-service attacks, pose serious risks to data security and integrity. The proposed blockchain-based security sharing algorithm addresses these challenges by leveraging its decentralized structure and smart contracts. The algorithm ensures that even under high traffic, it can maintain efficient data processing by utilizing blockchain's scalability features, while smart contracts automate data access control to reduce vulnerabilities to attacks. This adaptability makes the algorithm particularly suitable for securing data in complex, real-time, and high-security-demand scenarios in IoT-based social assistance systems.

Future research will delve into low-power optimization, with a focus on algorithm structure optimization, hardware selection, energy efficiency data transmission, and energy harvesting technology. In terms of algorithm structure optimization, research will focus on optimizing consensus mechanisms and reducing block generation frequency to reduce computational complexity and power consumption. In terms of hardware selection, future work will explore low-power sensors and processors, combined with dedicated hardware such as FPGA or ASIC, to improve the energy efficiency of IoT devices. In terms of energy-efficient data transmission, optimizing communication protocols and reducing transmission overhead will be key, with the aim of achieving efficient data transmission compatible with blockchain. In terms of energy harvesting technology, research will focus on integrating solar or vibration energy harvesting technology to enable IoT devices to operate autonomously for longer periods of time, reduce dependence on external power sources, and enhance the sustainability of blockchain systems. These strategies will make blockchain based IoT social assistance systems more efficient and adaptable to power constraints in large-scale deployments.

5 Conclusion

Aiming at the problem of insufficient data security and sharing efficiency in traditional social assistance systems, this study proposes an IoT data security sharing model that integrates blockchain and smart contract technology. Through theoretical design and simulation experiment verification, the model shows significant advantages in improving data security, sharing efficiency, and system stability.

(1) In terms of data security, the system designed in this study uses high-strength encryption algorithms such as SHA-256, and its data security score reaches 92 points, and the anomaly detection rate is as high as 95%. Compared with algorithms such as RSA and AES, SHA-256 is more suitable for scenarios with high-security requirements. The system also introduces a multi-level encryption mechanism and blockchain log audit function in its structure, which effectively guarantees the integrity and privacy of data in collection, transmission, and storage. It avoids data tampering and leakage risks common in traditional centralized structures.
(2) Regarding sharing performance, the measured data of four blockchain architectures show that the private chain performs best in data transmission time (1.8 seconds), with a processing capacity of 1000 TPS and the lowest cost. The safety score of the alliance chain reaches 90 points, balancing efficiency and safety. The hybrid chain balances security score and processing power well and is suitable for high-load multi-node environments. In addition, the introduction of smart contracts has improved the contract execution efficiency to more than 20 times/per second, and the intermediary cost-saving rate has exceeded 50%, greatly enhancing the automation and controllability of data access.
(3) From the perspective of IoT devices, there is a significant difference between response time and device type. The gateway device has the lowest response time under 16 frequency visits/minute, while the sensor device maintains about 95 ms; The display terminal is about 80 ms, and the performance stability is medium. Regarding data-sharing responsiveness, gateway devices show strong concurrent processing advantages and are suitable for deployment as controller nodes. The type of devices and the number of accesses also impact system security. Among them, the security scores of DVC and Meter devices peak when 230 units are connected, while the scores of Sensor and Camera devices decrease after more than 200 units are connected.

This study has made significant contributions to the intelligent and trustworthy construction of future social assistance systems. By integrating blockchain and IoT technologies, the proposed algorithm ensures secure, transparent, and efficient data sharing, which is crucial for the scalability and reliability of social assistance systems. Specifically, the research findings support the development of an automated and tamper proof data management system that directly meets the growing demand for real-time and reliable data

in social assistance. In addition, the adoption of smart contracts enhances data access control, reduces reliance on intermediaries, and lowers operational costs. These improvements are directly consistent with the digitalization and decentralization trend of public sector management, in which efficiency, security, and transparency are crucial. In the future, the proposed model can further adapt to intelligent decision-making processes, improve resource allocation, and achieve cross departmental data collaboration, which will be the key to building a more efficient and trustworthy social assistance framework.

Despite the significant advantages of the proposed model, some limitations exist. First, the scalability of blockchain remains a challenge, particularly when dealing with large amounts of data generated by numerous IoT devices. The system's performance may degrade under high data volumes, necessitating further optimization of the blockchain's storage and processing capabilities. Second, while the proposed model reduces reliance on intermediaries through the use of smart contracts, it still requires substantial computational resources, especially for encryption and consensus mechanisms, which could increase operational costs. Finally, the interoperability between different IoT devices and blockchain platforms remains a key challenge. In future research, addressing these limitations by exploring more efficient consensus algorithms, enhancing blockchain scalability, and improving energy efficiency will be critical to the broader adoption of blockchain-based solutions in social assistance systems.

Future research can further explore the following directions: 1. Algorithm low-power optimization, targeting the energy efficiency issues of IoT devices, optimizing algorithms to reduce energy consumption while ensuring data security and sharing efficiency; 2. Multi chain collaboration mechanism, studying the interaction and interoperability between different blockchains to enhance the flexibility and scalability of data sharing; 3. Cross departmental data collaboration, exploring the integration of data from multiple government and private sectors, adopting a decentralized model to ensure secure sharing, and promoting collaborative solutions to social needs; 4. The combination of blockchain and AI, studying the synergistic effect of AI and blockchain, improving the accuracy and efficiency of data sharing, such as anomaly detection and predictive analysis of resource allocation.

The security sharing algorithm proposed in this paper effectively improves the security and availability of IoT social assistance data in complex network environments. It provides strategic references for blockchain architectures and device deployments through data-driven methods. Future

research can further focus on the low-power optimization of algorithms, the integration of multi-chain collaboration mechanisms, and cross-departmental data collaboration models to realize the deep evolution of social assistance systems in the direction of intelligence and credibility.

References

[1] Alkhudhayr, H. "Internet of things based parking slot detection and occupancy classification for smart city traffic management," Engineering Applications of Artificial Intelligence, vol. 152, pp. 110802, 2025.

[2] Dhanasekar, S. "A comprehensive review on current issues and advancements of Internet of Things in precision agriculture," Computer Science Review, vol. 55, pp. 100694, 2025.

[3] Geng, C., Zhang, Y., Xu, X., Yao, Y., Lu, C., and Zhi, Z. "Blockchain-based identity authentication and data interaction scheme for Industrial Internet of Things," Computers and Electrical Engineering, vol. 123, pp. 110143, 2025.

[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, no. 3, pp. 777–792, 2024.

[8] Chen, X., Cao, F., Wang, Q., Ye, Z., Chen, X., Ye, Z., Cao, F., Chen, W., Cui, W., Feng, D., Ji, G., Lin, Z., Meng, Q., Luo, M., Luo, Y., Lv, W., Qin, Y., Qin, X., Si, X., ... Xie, Y. "2024 Chinese guideline on the construction and application of medical blockchain#," Intelligent Medicine, vol. 5, no. 1, pp. 73–83, 2025.

[9] Li, T., Han, D., Li, J., and Li, K.-C. "Asynchronous Tiered Federated Learning Storage Scheme Based on Blockchain and IPFS," Computers, Materials and Continua, vol. 83, no. 3, pp. 4117–4140, 2025.

[10] Zhao, F., Yang, B., Su, Z., Li, C., and Ding, Y. "A blockchain-enabled privacy-preserving and incentive mechanism-driven federated learning scheme for IoV," Computer Networks, vol. 264, pp. 111262, 2025.

[11] 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.

[12] Jasrotia, S. S., Rai, S. S., Rai, S., and Giri, S. "Stage-wise green supply chain management and environmental performance: Impact of blockchain technology," International Journal of Information Management Data Insights, vol. 4, no. 2, pp. 100241, 2024.

[13] Jia, X., Xu, J., Han, M., Zhang, Q., Zhang, L., and Chen, X. "International Standardization of Blockchain and Distributed Ledger Technology: Overlaps, Gaps and Challenges," CMES - Computer Modeling in Engineering and Sciences, vol. 137, no. 2, pp. 1491–1523, 2023.

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

[15] 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.

[16] 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, no. 2, pp. 100188, 2024.

[17] Kumar, N., Kumar, K., Aeron, A., and Verre, F. "Blockchain technology in supply chain management: Innovations, applications, and challenges," Telematics and Informatics Reports, vol. 18, pp. 100204, 2025.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] Nabli, A., Mokrini, A. E., and Aouam, T. "Enhancing Healthcare Supply Chains In Developing Countries: The Role Of Blockchain Technology," Procedia Computer Science, vol. 253, pp. 2327–2336, 2025.

[23] Nasser, A., Ouzayd, F., and Ech-cheikh, H. "Blockchain technology in maritime single window and port community systems: A bibliometric analysis and systematic literature review," Telematics and Informatics Reports, vol. 18, pp. 100206, 2025.

[24] Palagan, C. A., Joe, S. S. A., Mary, S. J. J., and Jijo, E. E. "Predictive analysis-based sustainable waste management in smart cities using IoT edge computing and blockchain technology," Computers in Industry, vol. 166, pp. 104234, 2025.

[25] Pathak, R., Soni, B., Muppalaneni, N. B., and Deveci, M. "Interval-valued q-rung orthopair fuzzy complex proportional assessment-based approach and its application for evaluating the factors of blockchain technology in various domains," Journal of Industrial Information Integration, vol. 42, pp. 100718, 2024.

[26] Pathak, R., Soni, B., Muppalaneni, N. B., and Deveci, M. "Assessing the factors of blockchain technology-enabled hospitals using an integrated interval-valued q-rung orthopair fuzzy decision-making model," Engineering Applications of Artificial Intelligence, vol. 139, pp. 109641, 2025.

[27] Payandeh, R., Delbari, A., Fardad, F., Helmzadeh, J., Shafiee, S., and Ghatari, A. R. "Unraveling the potential of blockchain technology in enhancing supply chain traceability: A systematic literature review and modeling with ISM," Blockchain: Research and Applications, vol. 6, no. 1, pp. 100240, 2025.

[28] 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.

[29] Rani, P., Mishra, A. R., Alshamrani, A. M., Alrasheedi, A. F., and Tirkolaee, E. B. "Picture fuzzy compromise ranking of alternatives using distance-to-ideal-solution approach for selecting blockchain technology platforms in logistics firms," Engineering Applications of Artificial Intelligence, vol. 142, pp. 109896, 2025.

[30] 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.

Biographies

Xiuli Yang, Ph.D. in Management, Associate Professor, Master's Supervisor. Science and Technology Commissioner of Heilongjiang Province; Civil Service Interview Examiner of Heilongjiang Province; Peer Reviewer for Journal of Wuhan University (Philosophy & Social Science Edition); Member of the Chinese Social Security Association; Member of Heilongjiang Management Association. Main research fields: Poverty Governance, Social Security Theory and Practice, Rural Development Studies.

Xinyuan Wang, Master's candidate in Administration at Northeast Agricultural University; Member of Heilongjiang Provincial Science and Technology Commissioner Program Team. Main research fields: Social Assistance, Social Governance, Poverty Governance.