Efficient data security sharing model with integrating of CP-ABE encryption and blockchain

Xixiang Zhang, Zhaoli Chen, Yun Dong*, Xuhua Ai, Zhipeng Meng
Information Center, China Southern Power Grid Guangxi Power Grid Co. Ltd., Nanning, Guangxi, China

ABSTRACT

This paper proposes a novel data security sharing system that integrates attribute-based encryption, keyword fuzzy search, and blockchain technology to address the poor performance and data vulnerability in existing data openness and sharing systems. The proposed system employs the attribute-based encryption algorithm to encrypt data, supplemented by blockchain technology to facilitate system search, thereby establishing the keyword search mechanism and repository for fragile items. The research results demonstrated that the average delay time for data sharing search in the new system ranged from 1.0 to 4.0 seconds, with a reduction of approximately 1100 milliseconds in encryption time compared with other methods. The average initialization time was between 15 and 20 milliseconds. Moreover, at an equivalent transaction volume, the proposed method exhibited a maximum processing time of 11.2 seconds, which was significantly improved by 4.2 seconds compared with other methods. These results underscore the enhanced performance of the proposed method in terms of encryption and keyword search efficiency, indicating its potential to advance data security sharing research and open up a promising path for future investigations.

Keywords: Data sharing, vulnerability, data security, CP-ABE, blockchain

1. INTRODUCTION

In the digital era, the role of data as a core asset has become increasingly prominent, driving progress in a variety of fields ranging from business decisions to scientific research[1]. However, with the surge in data volume, how to achieve efficient sharing and utilization of data while ensuring its security has become a major challenge for the technology and business communities. Secure sharing of data requires not only securing personal privacy and sensitive corporate information but also dealing with a large number of data sets from different data sources to ensure the security and integrity of data during storage and transmission. Attribute-Based Encryption (ABE) is a flexible encryption technique for data whose encryption and decryption processes usually rely on user attributes instead of fixed keys in traditional symmetric or asymmetric encryption[2]. ABE technique is suitable for data sharing environments that require fine-grained access control because it can be based on user attributes dynamically and control access to data dynamically based on user attributes[3]. Generally, ABE can be categorized into two main types, Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE).

In CP-ABE system, the data owner defines an access policy that is embedded in the encrypted ciphertext. Only when the user's attributes satisfy the policy defined in the ciphertext, the user can decrypt the data. With this policy, the data owner can directly control the data access policy, while the user needs to hold a key that matches his/her attributes. Although CP-ABE provides strong security and flexible access control mechanisms, it faces the problem of inefficient keyword searches in practical applications. Especially in the big data environment, users often need to quickly find information matching specific keywords from a large amount of encrypted data[4]. Traditional CP-ABE systems need to encrypt and match every possible keyword, which is extremely inefficient when dealing with large-scale data. Therefore, using an efficient keyword fuzzy search technique enables users to perform efficient searches without knowing the exact keywords. Blockchain, as an innovative distributed ledger technology, provides a new solution for data security through its decentralization, immutability, and transparency. The encrypted and decentralized nature of blockchain makes it ideally suited for processing and storing sensitive data while ensuring security and trustworthiness when data is shared among multiple parties. Another significant advantage of blockchain is that it provides integrity verification and audit trail capabilities for data operations, which is critical for complying with data protection regulations and conducting security audits.

*dong_y.xt@gx.csg.cn

International Conference on Optics, Electronics, and Communication Engineering (OECE 2024), edited by Yang Yue, Proc. of SPIE Vol. 13395, 133954L · © 2024 SPIE · 0277-786X · Published under a Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.3049159

However, despite its significant security advantages, CP-ABE still faces some challenges in practical applications. First, CP-ABE has difficulties in keyword search, and users need to spend a lot of time and computational resources to find specific ciphertexts. Second, the encryption and decryption processes of CP-ABE are less efficient, which limits its application in large-scale data-sharing scenarios. These issues make it complex and difficult to achieve efficient and secure data access in large-scale data-sharing systems. Meng et al.[5] proposed a dual hybrid CP-ABE scheme that does not require a trusted authority (TA) to achieve secure data sharing in order to cope with the burden of the rapid development of IoVs on edge servers and at the same time to make full use of the computational power of idle vehicles. The scheme addresses the limitations of existing schemes, ensures forward security, and reduces storage and communication costs. The results show that the proposed scheme exhibits advantages in both efficiency and cost, providing an efficient and secure data sharing method for Vehicular Opportunity Computing (VOC). In order to overcome the limitations of existing cloud data retrieval schemes in terms of keyword searching and sorting, Yao et al.[6] and Lin et al. [7] proposed a flexible multi-keyword sorting searchable attribute scheme based on a search tree with fuzzy search and AND-OR logic gates. The results show that the scheme not only improves the flexibility and efficiency of search but also enhances privacy protection and realizes semantic search to enhance the user experience. In order to address the problem of malicious users leaking keys or constructing decryption black boxes in cloud storage, Qiao et al. [8] proposed a structural flaw analysis for the tracking algorithms of the existing CP-ABE scheme and reveal its limitations based on unrealistic assumptions. The study proposes the construction of an Alert Decryption Black Box (ADB), and the results show that the ADB is able to differentiate between tracing ciphertexts and normal ciphertexts, thus thwarting the tracing algorithm, and may even be used by malicious users to trap innocent users. Liu et al. [9] proposed a lightweight CP-ABE scheme supporting direct attribute revocation in order to solve the attribute revocation problem of CP-ABE schemes in vehicular ad hoc networks. The scheme simplifies the revocation operation through a proxy mechanism and uses elliptic curve scalar multiplication to reduce the computational overhead. The results show that the overall efficiency of our scheme outperforms existing schemes while ensuring data confidentiality and integrity. In order to improve the Learning by Error (LWE) ciphertext policy attribute-based encryption (CP-ABE) scheme, a new CP-ABE scheme is proposed. In the key generation phase, the model uses a novel lattice two-stage sampling technique by Lai, Liu, and Wang to obtain a CP-ABE scheme with the same security as the original scheme and a shorter ciphertext. The results show that the new scheme provides a new idea for LWE-based CP-ABE design. It can be seen that there have been various researches in CP-ABE security testing that have been analyzed in different ways.

Based on this, the study proposes a new model that incorporates the CP-ABE encryption algorithm and blockchain technology to address the lack of efficiency and poor security performance of data security systems. The new model enhances the ability to search and process data by introducing attribute token data. The new model demonstrates significant performance advantages in data search and encryption by using more efficient search algorithms to improve the overall efficiency of the system. And the model not only ensures data security but also enhances data tracking and auditing capabilities by utilizing the transparency and non-comparability of blockchain, providing a more trustworthy data-sharing environment for data security. The study also innovatively combines the CP-ABE encryption algorithm with blockchain technology, which overcomes the difficulty and inefficiency of keyword search in the traditional CP-ABE system by introducing attribute tokens and efficient search algorithms. The new model not only improves the efficiency of the data-sharing system but also provides stronger security and trust in terms of security and trust, which provides a new direction for future research.

The remainder of this article is organized as follows. We review the related work in Section 2. Section 3 describes the methods proposed in this paper. Section 4 reports the experimental results. Finally, we conclude the paper in Section 5.

2. RELATED WORK

Currently, numerous technologies within data security sharing systems aim to enhance the security of data transmission; however, various challenges persist within research in this domain. For instance, Li et al.[10] introduced a direct adaptive selected ciphertext secure password policy in the standard model to mitigate practical limitations of Attribute-based Encryption and Equality Testing (ABEET) in random Oracle models. The findings indicate that this scheme offers optimizations in computational cost, storage cost, security, ciphertext validity check, and outsourced decryption compared to existing schemes, thereby exhibiting heightened practicality and efficiency. Chen et al.[11] proposed a ciphertext strategy featuring shared decryption functions to address delays in authorized decryption users' access to ciphertext in ABE (Attribute-based Encryption). This scheme enables authorized users to independently recover information, while semi-authorized users can collaboratively obtain access. Experimental results demonstrate the

scheme's notable efficiency in terms of computational and storage costs. Gao et al.[12] introduced a novel blockchain-based trusted secure ciphertext policy and attribute hidden access control scheme to alleviate the high trust establishment costs and single points of failure inherent in CP-ABE. This scheme ensures the privacy of policies and attributes, thus achieving trusted access. Experimental results affirm its superior security and efficiency. Wang et al.[13] proposed a rapid CP-ABE scheme to address computational and storage costs in healthcare networks' mobile terminals, as well as the privacy and security concerns regarding medical data. This scheme alleviates local computational burdens by delegating resource-intensive tasks to semi-trusted third parties while upholding data privacy and security. Experimental outcomes indicate its efficacy in enhancing both network physical security and healthcare data efficiency.

Zhou et al.[14] designed an extended attribute mapping mechanism based on CP-ABE to address data sharing security and policy conflicts in multi-cloud storage systems. Subsequently, they proposed a multi-authorization access control model to meet the requirements of multi-cloud storage access control. The research results indicate that the proposed model outperforms other models in terms of computational time overhead. Horng et al.[15] proposed an identity-based CP-ABE scheme and introduced a revocation mechanism to address the issue of data confidentiality in VANET. This scheme outsourced encryption and decryption operations to cloud computing nodes to reduce the computational burden on onboard units. The experimental results validate the scheme's efficacy in achieving fine-grained access control while protecting user privacy. Zhang et al.[16] proposed a privacy-preserving CP-ABE scheme with an efficient permission verification function to address the privacy protection issues arising from data sharing in cloud computing. This scheme ensures data confidentiality while ensuring that user privacy is not compromised. The research results indicate that this scheme achieves selection security, constant key size, and high computational and communication efficiency under decision n-BDHE problems and decision linearity assumptions. Liu et al.[17] proposed a security-aware information dissemination scheme to address the security and reliability issues of information dissemination within VANET in multi-RSU environments. This scheme used encryption based on ciphertext policy attributes to ensure that only vehicles that meet access control policies can access information. The research results indicate that this scheme achieves fine-grained access control for broadcast information and is efficient in multi-RSU collaborative scenarios.

Nonetheless, there remains a pressing requirement to enhance the efficiency and security of models for data sharing and keyword search. Consequently, this study endeavors to address this imperative by integrating CP-ABE keyword fuzzy search and blockchain technology to build a novel data security sharing system. This initiative aims to mitigate the inefficiencies and security vulnerabilities inherent in traditional methods.

3. DATA SECURITY SHARING WITH CP-ABE KEYWORD FUZZY SEARCH AND BLOCKCHAIN

In this section, the data security sharing model is presented, which integrates CP-ABE keyword fuzzy search and blockchain technology. Initially, a new data security sharing model is established. Subsequently, the model incorporates blockchain technology to improve its effectiveness is enhanced. By integrating these two technologies, a new data-sharing model is developed, which has significant performance improvements in both security and efficiency.

3.1 CP-ABE keyword fuzzy search encryption model

Data sharing refers to providing data to other users or organizations under specific conditions, enabling them to access, utilize, or analyze the data. The shared data can include various types of information, including text, images, audio, and video. Data sharing can help to understand and solve complex problems more comprehensively and accurately. Figure 1 illustrates a traditional data sharing platform. It consists of three major data modules: data users, data platforms, and data owners. Data users primarily utilize data sharing platforms to access and analyze data from various institutions or individuals. The data sharing platform plays a role in sharing, transmitting, and publishing of data. Data owners are the owners of data originating from different entities. Data is published and stored through the data sharing platform. While data utilization can be achieved through data sharing platforms, it also introduces some security concerns associated with data utilization.

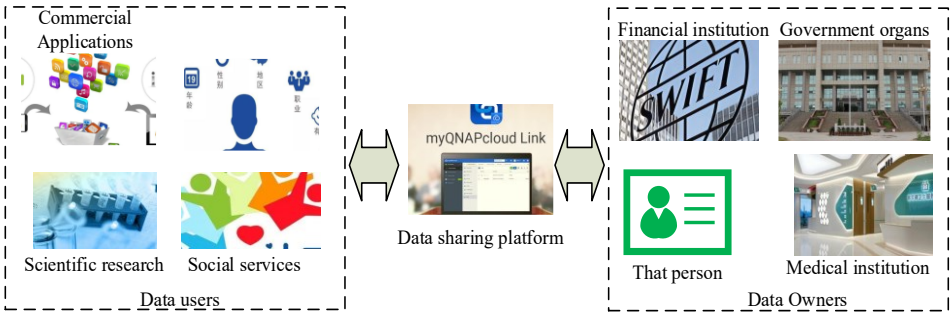

Figure 1. Traditional data sharing platform.

CP-ABE is a pivotal data encryption framework for its native language with enhanced flexibility and scalability. In this strategy, users can represent the execution of attributes and identity key status through a set of encrypted attributes. This enables the strategy to better adapt to dynamic and more complex application scenarios, such as data security sharing[18]. Within the CP-ABE scheme, there are mainly four methods for data encryption and fuzzy search. The system setting algorithm refers to the algorithm that runs the system during system initialization. When the policy parameters are inputted, the algorithm automatically generates public parameters and master keys. The attribute key generation algorithm refers to using the attribute lists of public parameters, master keys, and data as input values, and then reflecting them through the algorithm to form the relative attribute key algorithm. The encryption algorithm refers to executing all data and accessing the message target, then taking public parameters, target messages, and access policies as input values, and outputting access policies and associated ciphertext after processing. The final decryption algorithm mainly runs the data information, and then directly encrypts the ciphertext in the public parameters and target information. If the current attribute list corresponds to the access policy, it directly returns the corresponding plaintext message. The main functional model structure of CP-ABE key under only the encryption strategy is shown in Figure 2.

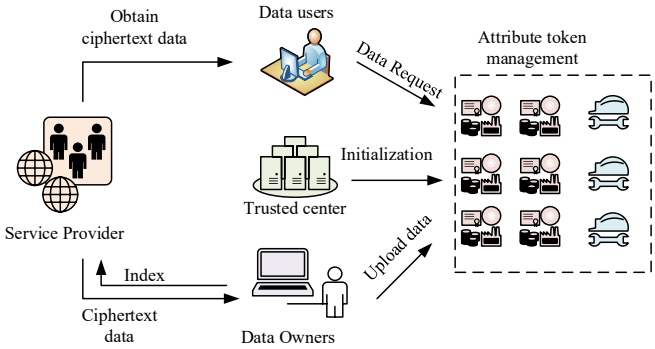

Figure 2. Main function model structure of CP-ABE key.

As depicted in Figure 2, the model structure consists of several components: trusted center, authorization authority, service provider, data holder, data user, and blockchain. The trusted center mainly provides functions such as data information publishing, data user management, and data parameter information initialization. The authorized agency is mainly responsible for the management of the current model and the publication of attribute data. Service providers mainly store current data to reduce server storage pressure. The data holder mainly stores the current data and then uses the CP-ABE algorithm to encrypt the data. Data users mainly transmit the data information obtained by authorized agencies, which gives them the ability to access the data. Finally, blockchain acts as a module that centralizes data, ensuring the authenticity and integrity of current data[19].

The implementation of the system model first requires initializing the system data, running it through a trusted center, and using the received parameters as inputs. Then it is necessary to set the multiplication cycle for operation, as shown in equation (1)[20].

$$e: G * G \to G_r \tag{1}$$

In equation (1), e represents the multiplicative cyclic group of the input, and G represents the corresponding

bidirectional mapping relationship. At this point, the size range of G is defined as [0-1], and then the random numbers a, b are selected. The system initialization data size at this point is shown in equation (2).

$$PK = \{g, e(g,g)^a, g^b\} \tag{2}$$

In equation (2), PK represents the size of the initialized system data, and g represents the generator of G. The size of the master key is g^a. The trusted center will save and upload the obtained initialization data to the blockchain. Secondly, during system operation, it is necessary to register the current identity and attribute information in the trusted center to ensure that registered users can maintain data management permissions. Meanwhile, when generating data information, it is necessary to encrypt the data to obtain new ciphertext information, as shown in equation (3).

$$CT_A = \{C = K_A \bullet e(g,g)^{as}, C = g^s, \forall i \in [1,m], C_i = g^{B\lambda_i} H(p(i))^{-r_i}, D_i = g^{r_i}\} \tag{3}$$

In equation (3), CT_A represents the encrypted ciphertext of the data. A, p both represent the encrypted data. K_A represents the encrypted key. The data owner encrypts and signs the encrypted information, uploads the corresponding hash value, and provides the uploaded data to the service provider. The service provider is responsible for generating a data index for the ciphertext data and transmitting it to the data owner. Finally, it sends the generated raw data to the blockchain section. Data decryption is the process in which users verify the signature of ciphertext data and then calculate the hash value. The trusted center generates the key, as shown in equation (4)[21].

$$SK = \{D = g^a g^{bt}, E = g^t, [D_x = H(x)^t]_{x \in U}\} \tag{4}$$

In equation (4), SK represents the generated key. U represents the user's set of data attributes. E, D represent the user's data encryption process, respectively. It decrypts the attribute key through user shared keys, and then runs the attribute decryption algorithm to obtain a symmetric key. By using symmetric key data to decrypt the original ciphertext, the plaintext data size is obtained. Finally, the decrypted data is obtained.

In terms of computational cost, the complexity of the CP-ABE algorithm is mainly reflected in the consumption of computational resources during encryption and decryption. Assuming that there are n users and m attributes in the system, for each encryption operation, the required computation can be expressed as $O(m*\log(n))$, which is due to the fact that the encryption process of each attribute needs to depend on the combination of user attributes and system parameters. For the decryption operation, the computation amount is mainly determined by matching the user attributes with the access policy embedded in the ciphertext, and its cost calculation process is also $O(m*\log(n))$. In addition, the introduction of blockchain technology increases the computational overhead of the system to a certain extent, mainly in the block generation and verification process. Assuming that the system needs to perform k hash calculations in processing each block, the overall computational cost can be expressed as $O(k*n*\log(n))$. It can be seen that the new system can effectively reduce the computational cost by optimizing the algorithm and system structure while ensuring high efficiency.

In the research proposed method, initial data will not be stored directly on the blockchain, only when the attribute user from the use of attribute data tokens, can get the initial ciphertext from the supplier. At the same time, the authorization authority can directly freeze the abnormal users, which improves the security of data usage. At the same time, the model uses a combination of authorization agencies and multi-block links to isolate the data between different channels, which further ensures that the data channels of the model can be opened only when the data circulation is safe, and the channels in the model can be allowed to circulate the data only if they have carried out the corresponding channel inspection. The security of the model is further guaranteed.

3.2 Improved keyword fuzzy data sharing model assisted by blockchain

To achieve secure search and keyword fuzzy data sharing in data blockchain, it is necessary to encrypt and share keyword fuzzy data with the assistance of blockchain. This study assumes that the current service provider is untrusted, so it is necessary to develop keyword sharing models while ensuring data security. Blockchain technology is a distributed data technology that utilizes cryptographic methods to ensure the security, transparency, and reliability of current data. The traditional blockchain structure model is illustrated in Figure 3.

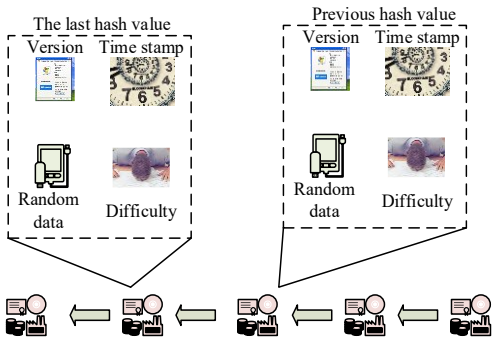

Figure 3. Traditional blockchain structure model.

The blockchain structure comprises several large blocks. The version structure is used to run ciphertext and encryption rules on the specified blockchain. The timestamp structure reflects the timestamp generated by the current blockchain. The difficulty structure of blockchain is usually an area that adjusts the speed of current block generation, ensuring the normal and safe operation of the block. The hash value is a numerical value that facilitates block validation, which can connect the blockchain to ensure its integrity. Since blockchain needs to meet the requirements of both front-end and back-end blockchain modifications when modifying data, it is impossible to modify all data simultaneously. Therefore, adding blockchain can introduce new protection mechanisms to the data security model. Consequently, integrating blockchain and CP-ABE encryption strategies enhances the security of current data, as shown in Figure 4. Figure 4 shows the keyword fuzzy data sharing system after blockchain merging.

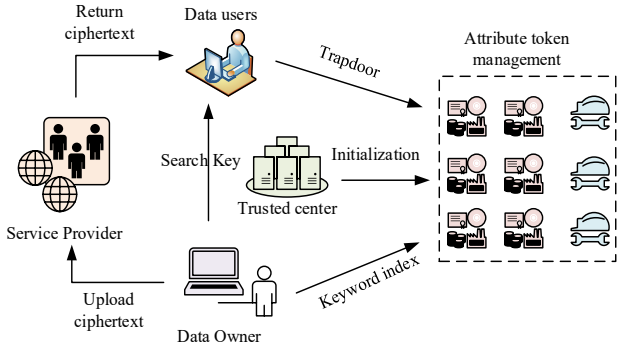

Figure 4. Keyword fuzzy data sharing system after joining blockchain.

As shown in Figure 4, the general modules in the system with blockchain assistance are similar to the CP-ABE keyword system search model. However, the added blockchain module directly returns semi solved ciphertext data to the user through the service provider. Meanwhile, users can obtain key information directly from the data owner and access the owner's data information through blockchain, thus reducing the data transmission process and enhancing overall efficiency and security. Therefore, to query and access any portion of the current key, users must first initialize the data stage, set parameters, and add the information verification stage of ciphertext before guessing the information data. The blockchain is used as a central platform for the model to guarantee the integrity and authenticity of the data. Meanwhile, the searching and pairing of data is carried out through the smart contracts of the blockchain. Since the blockchain is data tamper-proof, the use of the blockchain enables the user application and authorization process to be recorded so that the data can be traced back. And the initial data is not stored directly in the blockchain, but through a new data engine. A new open, secure, and transparent data sample can be built through the blockchain, and the blockchain can more efficiently record data such as user information and application records. For guessing information data, it is necessary to guess the input's requirements, as shown in equation (5)[22].

$$Adv = \left| \Pr\left| b^{'} = b \right| - \frac{1}{2} \right| \tag{5}$$

In equation (5), Adv represents the advantage data obtained from querying ciphertext, and b represents randomly

selecting parameters. $b^{'}$ represents the output value size range between 0 and 1. Pr represents the ciphertext size When the system is running, it is necessary to first initialize the algorithm model for the trusted center. After initializing the attributes, the current legitimate users are identified. The process of assigning data to attribute users is shown in Figure 5.

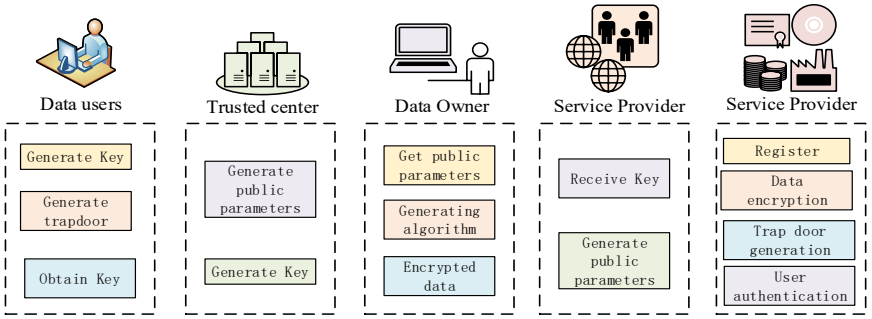

Figure 5. Attribute user allocation data method.

As shown in Figure 5, data users can get data keys by decrypting the data and generating trapdoors to obtain more data keys. The trusted center mainly integrates the generated public parameters into the blockchain. Meanwhile, keys are generated to transmit to the service provider. Blockchain is mainly responsible for user registration, data encryption, trap generation, and user authentication. The owners of the data mainly obtain common parameters to generate search algorithms, build indexes for the data, and encrypt the data. Finally, the service provider receives the uploaded ciphertext and key content. The key generation process in the system requires a trusted center to randomly select data, which satisfies the condition, as shown in equation (6).

$$a = (a_1 + a_2) \bmod q \tag{6}$$

In equation (6), a_1 and a_2 represent randomly selected data, while q represents the user's selection data. At this point, the key size is calculated and inputted into the secure channel, as shown in equation (7)[23].

$$SK_{uid} = g^{a1} \bullet g^{ba} \tag{7}$$

In equation (7), SK_{uid} represents the key size of the user identification flag. Other parameters are consistent with the above. At this point, the trapdoor generation process for keywords requires filling in the current fuzzy search keywords. For example, when the fuzzy keyword for querying and searching is "look", it can be entered into the system by filling in the key and then searching. If "?" is added to the keyword, the resulting keyword is "l? oo? K". Even if the keyword cannot be blurred, the search page can obtain more specific search results. The generation of trapdoors in blockchain is divided into two stages. Firstly, the judgment of attribute data is made. If it is determined as a set of attribute data, region selection is performed. The blockchain attribute data is calculated, as shown in equation (8).

$$T_i = (H(att_i))^{ri} \tag{8}$$

In equation (8), T_i represents the search result, $H(att_i)$ represents the randomly selected attribute data size, and ri represents the shared secret parameter. The obtained node calculation is shown in equation (9).

$$\prod_{i \in I} e(C_i^{'}, g^b, T_i)^{wi} / \prod_{i \in I} e(C_i, T_i^{'})^{wi} = B \tag{9}$$

In equation (9), $C_i^{'}$ represents the search result, g^b represents the reflected data value, and T_i represents the trapdoor size. B represents the set of attribute data obtained. C_i, T represent the parameters that are similar to $C_i^{'}, T_i$, but differ in the results obtained from different attribute data. e represents the natural constant. When the calculated set size matches the set size of the attribute data, the entire key can perform a fuzzy query of keywords through a secure channel. For the security proof of the system, it is necessary to determine the initial parameter size in the bilinear group of the data, as shown in equation (10).

$$\vec{y} = (g, g^{s}, g^{a}, ..., g^{a^{2q}}) \tag{10}$$

Equation (10) represents the given initial parameters. The calculation result obtained through random challenge calculation is shown in equation (11)[24].

$$e(g,g)^{a} = e(g^{a}, g^{aq}) e(g,g)^{a'} \tag{11}$$

In equation (11), q represents the determinant condition. The a in the equation needs to satisfy the condition, as shown in equation (12).

$$a = a' + a^{q+1} \tag{12}$$

In equation (12), the parameters are consistent with the above parameter expressions. The output common parameter values obtained by the challenger are shown in equation (13).

$$PK = \{G, G_T, g, e(g^{a}, g^{aq}) e(g,g)^{a'}, g^{b}, g^{a}, H\} \tag{13}$$

The parameter expression in equation (13) is consistent with the above parameter expression. By setting and calculating common parameters, the security of the current model can be improved.

4. PERFORMANCE RESULTS

The main focus is on analyzing the current keyword fuzzy search and blockchain data security sharing models. Through experimental data simulation testing, this study builds different data security sharing testing and analysis experiments. The feasibility and performance of these methods are elaborated separately to test the effectiveness of using these methods.

4.1 Analysis of feasibility verification results of the experimental method

To verify the feasibility and performance of the current research method, an Intel core CPU is used i7-7700@3.60GHzprocessor, with 8GB RAM. The operating system is Ubuntu 20.04 LTS. Multiple blockchain networks are arranged in the host system, and the performance of the system model is tested by verifying its intelligent search efficiency. The testing tool uses blockchain testing tools for testing and research, and a total of 4 different keywords are tested for verification to obtain the transaction delay situation, as shown in Figure 6.

From Figure 6a, in testing the average delay time of the four keywords, the delay time mostly increased with the increase in the number of transactions, but the overall average delay time remained between 2.0s-5.0s. This indicates that the management of attribute data can achieve a faster response speed when conducting keyword searches. From Figure 6b, the delay time of the data during keyword sharing search was between 1.0s and 4.0s, indicating that the average delay time is shorter and the system response time is faster when sharing data. The average throughput of keyword detection is tested, as shown in Figure 7.

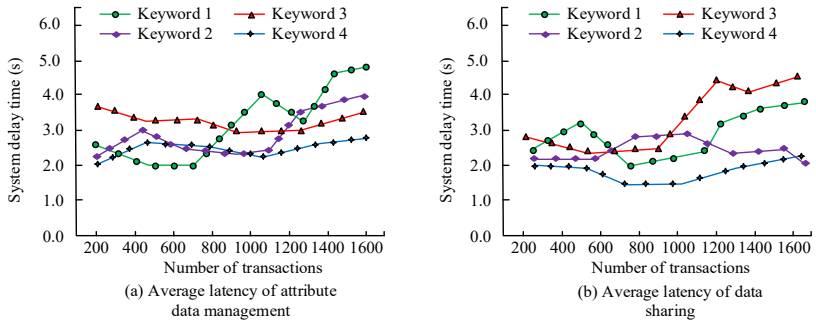

Figure 6. Blockchain transaction latency situation.

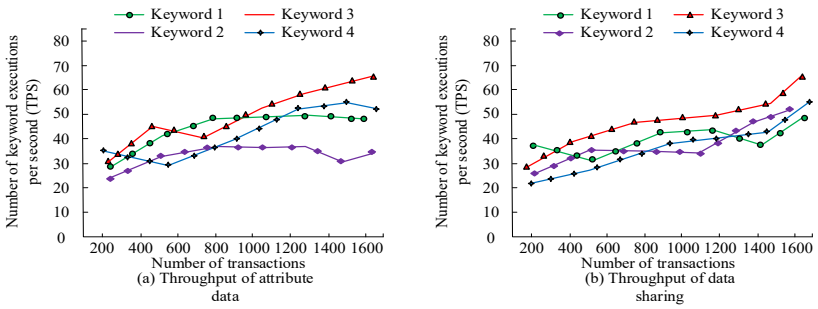

Figure 7. Changes in system test throughput.

From Figures 7a and 7b, the throughput of data sharing and attribute data management increased when the number of transactions in the data ranged from 200 to 800. When the number of transactions exceeded 800, there were fluctuations in data attributes and shared throughput, indicating that the blockchain model constructed in the study is relatively safe and stable. However, due to the randomness and network fluctuations of the algorithm models in the system during the search, there may be some delay and fluctuation in throughput, but it does not have a significant impact on the overall stability of the system.

4.2 Data security performance test results

The research method is compared with current research models. Three blockchain technologies are Blockchain-aided Ranked Multi-keyword Attribute-based Searchable Encryption with Hiding Policy for Smart Health System (BA-RMKABSE), Fast Attribute-based Message Encryption (FAME), and Revocable Data Access Blockchain (RACMA). The obtained results are shown in Figure 8.

From Figure 8a, the encryption time of all four blockchain methods increased with the increase in the number of attributes. The figure showed that the encryption time of the blockchain technology used in the study increased less, with the highest encryption time below 150ms, which was about 1100ms lower than the highest BA-RMKABSE model. This indicates that the technical method used in the study has better encryption and higher system security. Meanwhile, from Figure 8b, the decryption time of the four methods also increased with the increase in the number of attributes. Compared with the four methods used in the study, the decryption time was shorter, and basically stable at around 70-80ms. This indicates that the method used in the study is executed through cloud services, resulting in a shorter time. The time for key generation and data initialization stages is shown in Figure 9.

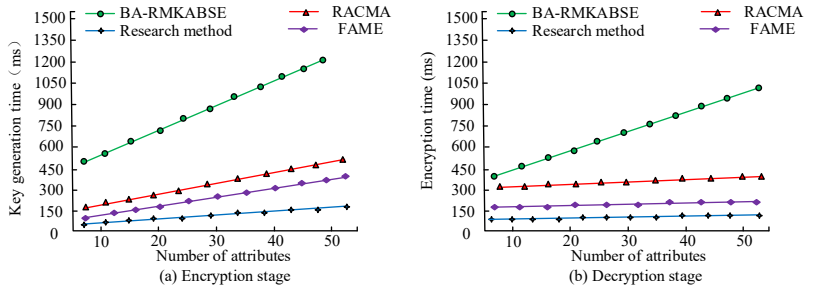

Figure 8. Performance comparison of four blockchain technologies.

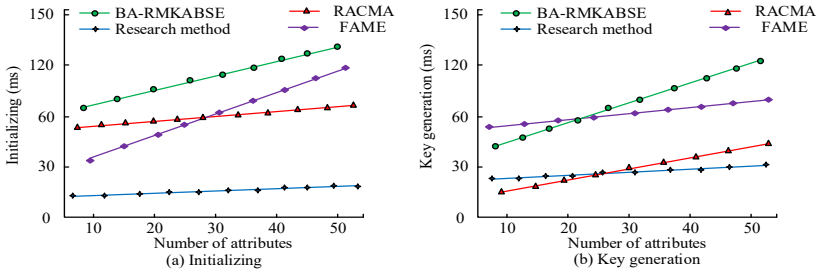

Figure 9. Comparison of four key generation and initialization stages.

From Figure 9a, the initialization time of the research method increased with the increase of the number of attributes in the early stage of the experiment, and the initialization time of the method used in the study was between 15-20ms. The initialization time of other methods is longer. From Figure 9b, the key generation time of the method used in the study was relatively short, but the initial generation time of RACMA was shorter than that of the method used in the study. However, as the number of subsequent attributes increased, the key generation time increased by about 20ms, exceeding that of the method used in the study. This indicates that the method used in this study has a shorter initial time and key generation time compared with other methods. The comparison between the keyword search time and the number of files in the method is shown in Figure 10.

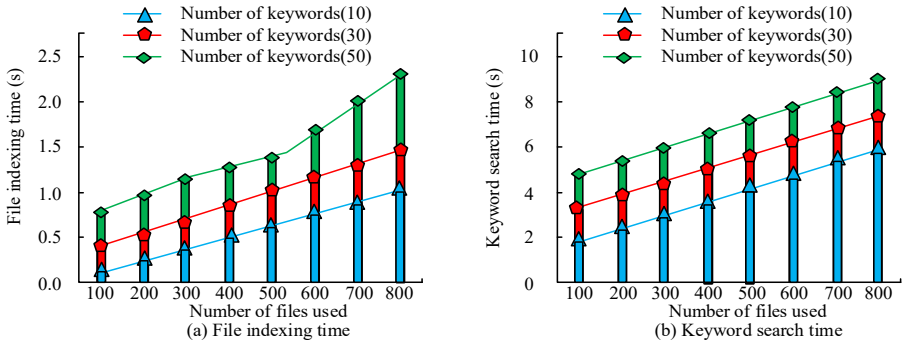

Figure 10. Comparison of search and indexing time for keywords with different numbers of keywords.

From Figure 10a, as the number of keywords increased, the indexing time of the method increased relatively, but its growth program increased proportionally. On average, adding 20 keywords increased the indexing time by 0.32 seconds. From Figure 10b, when the number of keywords increased by 20, the search time of its method increased by 1.4 seconds. This indicates that the number of keywords and the search and indexing time are both showing a proportional increase, and the processing time of the method for keywords is closely related to the number of keywords. The number of keywords for the four methods and the search time for trapdoor generation are compared, the results are shown in Figure 11.

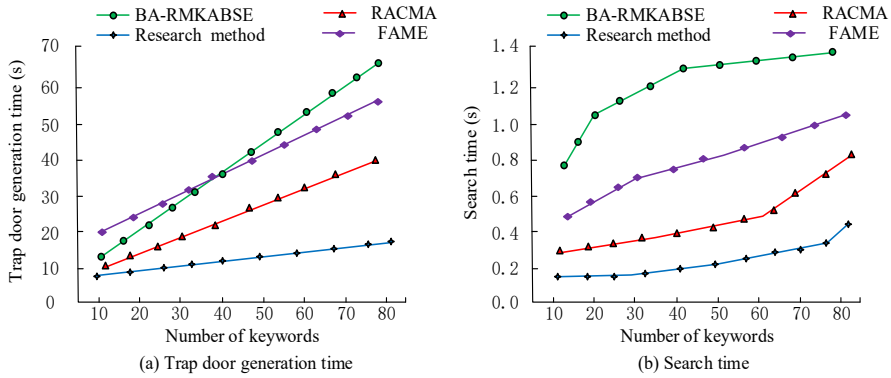

Figure 11. Comparison of search time for trapdoor generation using four methods.

From Figure 11a, the generation time of trapdoors using the research method was shorter, with an average time of about 10 seconds, which was about 30 seconds less than the total time of the BA-RMKABSE model with the highest average time of 40 seconds. This indicates that the generation time of trapdoors using the research method is shorter, and the overall effect of the method is more prominent. From Figure 11b, the average search time of the method used in the study was about 0.3 seconds, which was 0.9 seconds less than the BA-RMKABSE model with the highest average search time of 1.2 seconds. This indicates that the search time effect of the method used in the study is also better than other methods. To test the effectiveness of the four methods after increasing the number of transactions, a comparative analysis is conducted on the four methods. The results are shown in Table 1.

Table 1. Comparison of transaction processing time and throughput of four methods.

Project	Number of transactions	Time (s)	Throughput
Research method	100	3.0	42
	300	6.1	38
	500	11.2	43
BA-RMKABSE	100	5.2	51
	300	7.3	45
	500	13.5	53
FAME	100	6.2	52
	300	8.1	54
	500	15.3	62
RACMA	100	6.8	53
	300	8.6	46
	500	15.4	51

In Table 1, when the number of transactions was the same, the research method had lower time consumption and throughput compared with other methods. When the number of physical objects was 500, the research method took a maximum of 11.2 seconds, which was about 4.2 seconds lower than the highest method, which took 15.4 seconds. The throughput differed from the highest method by about 11 seconds. This indicates that the research method has relatively low time consumption and throughput, and the effectiveness is better.

5. CONCLUSION

This study proposed a data security sharing system based on blockchain technology and the CP-ABE encryption algorithm to address data leakage and failures in current data sharing platforms. The system achieved secure data sharing and keyword fuzzy search. Initially, the study explored the data sharing platform using the CP-ABE encryption algorithm, followed by the integration of blockchain technology to enhance the platform. Subsequently, simulation experiments were conducted to test the performance of the method. Results indicated that the system delay generally increased with the number of transactions, but remained relatively low, ranging from 2.0s to 5.0s. The average latency of data sharing search was reduced by 1.0s to 4.0s. When the number of transactions was between 200 and 800, the throughput of data sharing and attribute data management increased. Although the encryption time increased with the number of attributes, compared with other methods, blockchain encryption time was significantly shortened to 150 milliseconds. The decryption time of the proposed method remained stable between 70ms and 80ms. Although initialization time increased with the number of attributes, it was 15ms to 20ms shorter with the proposed method. Key generation time was relatively short, but the initial generation time of RACMA was shorter. With an increase in subsequent attributes, key generation time exceeded that of the proposed method by approximately 20ms. At 500 transactions, the peak of the proposed method was 11.2 seconds, which was 4.2 seconds higher than other methods. These findings underscore the efficacy of the proposed method in keyword search and data sharing. However, despite notable progress, there are still many challenges that require further research involving extensive and diverse datasets.

ACKNOWLEDGEMENT

This research was supported by the Guangxi Power Grid Technology Project under Grant 046100KK52222001.

REFERENCES

[1] Zheng, W., Chen, B. and He, D., "An adaptive access control scheme based on trust degrees for edge computing," Computer Standards & Interfaces, 82(6), 1-10 (2022).

[2] Tian, H., Li, X., Quan, H. and Chang, C. C., "A lightweight attribute-based access control scheme for intelligent transportation system with full privacy protection," IEEE Sensors Journal, 21(14),15793-15806 (2020).

[3] Zheng, W., Lai, C. F. and Chen, B., "Blockchain-based access control with k k -times tamper resistance in cloud environment," International Journal of Intelligent Systems, 37(10), 7787-7811 (2022).

[4] Rasori, M., Perazzo, P., Dini, G. and Yu, S. "Indirect revocable KP-ABE with revocation undoing resistance," IEEE Transactions on Services Computing, 15(5), 2854-2868 (2021).

[5] Meng, L., Xu, H., Tang, R., Zhou, X. and Han, Z., "Dual hybrid CP-ABE: How to provide forward security without a trusted authority in vehicular opportunistic computing," IEEE Internet of Things Journal, 2(11), 8800-8814 (2023).

[6] Yao, Y., Chen, H., Shen, L., Wang, K. and Wang, Q., "A CP-ABE scheme based on lattice LWE and its security analysis," Applied Sciences, 13(14), 8043-8044 (2023).

[7] Lin, J. K., Lin, W. T. and Wu, J. L., "Flexible and efficient multi-keyword ranked searchable attribute-based encryption schemes," Cryptography, 7(2), 28-29 (2023).

[8] Qiao, H., Ren, J., Wang, Z. and Hu, Y., "Disabling tracing in black-box-traceable CP-ABE system: Alert decryption black box," Symmetry, 16(1), 37-38 (2023).

[9] Liu, Y., Xu, S. and Yue, Z., "A lightweight CP-ABE scheme with direct attribute revocation for vehicular Ad Hoc network," Entropy, 25(7), 979-980 (2023).

[10] Li, C., Shen, Q., Xie, Z., Feng, X. Y. and Fang, Y. J., "Large universe CCA2 CP-ABE with equality and validity test in the standard model," The Computer Journal, 64(4), 509-533 (2020).

[11] Chen, N., Li, J., Zhang, Y. and Guo, Y. Y., "Efficient CP-ABE scheme with shared decryption in cloud storage," IEEE Transactions on Computers, 71(1), 175-184 (2020).

[12] Gao, S., Piao, G., Zhu, J., et al., "TrustAccess: A trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain," IEEE Transactions on Vehicular Technology, 69(6), 5784-5798 (2020).

[13] Wang, S., Wang, H., Li, J. and Wang, H. H., "Junaid Chaudhry. A fast CP-ABE system for cyber-physical security and privacy in mobile healthcare network," IEEE Transactions on Industry Applications, 56(4), 4467-4477 (2020).

[14] Zhou, S., Chen, G., Huang, G., Jin, S. and Ting, K., "Research on multi-authority CP-ABE access control model in multicloud," China Communications, 17(8), 220-233 (2020).

[15] Horng, S. J., Lu, C. C. and Zhou, W., "An identity-based and revocable data-sharing scheme in VANETs," IEEE Transactions on Vehicular Technology, 69(12), 15933-15946 (2020).

[16] Zhang, L., Cui, Y. and Mu, Y., "Improving security and privacy attribute based data sharing in cloud computing," IEEE Systems Journal, 14(1), 387-397 (2020).

[17] Liu, X., Chen, W. and Xia, Y., "Security-aware information dissemination with fine-grained access control in cooperative multi-RSU of VANETs," IEEE Transactions on Intelligent Transportation Systems, 23(3):2170-2179 (2020).

[18] Gupta, I. and Singh, A. K., "SELI: statistical evaluation based leaker identification stochastic scheme for secure data sharing," IET Communications, 14(20), 3607-3618 (2020).

[19] Abidi, M. H., Alkhalefah, H., Umer, U. and Mohammed, M. K., "Blockchain-based secure information sharing for supply chain management: Optimization assisted data sanitization process," International Journal of Intelligent Systems, 36(1), 260-290 (2020).

[20] Yuan, X., Chen, J., Zhang, N. and Fang, X. J., "A federated bidirectional connection broad learning scheme for secure data sharing in internet of vehicles," China Communications, 18(7), 117-133 (2021).

[21] Zhang, Y., Lu, Y., Huang, X. and Maharjan, S., "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," IEEE Transactions on Vehicular Technology, 69(4), 4298-4311 (2020).

[22] Islam, A. and Madria, S. K., "Attribute-based encryption scheme for secure multi-group data sharing in cloud," IEEE Transactions on Services Computing, 15(4), 2158-2172 (2020).

[23] Wang, F., Wang, J. and Shi, S., "Efficient data sharing with privacy preservation over lattices for secure cloud storage," IEEE Systems Journal, 16(2), 2507-2517 (2021).

[24] Hebbi, C. and Mamatha, H., "Comprehensive dataset building and recognition of isolated handwritten Kannada characters using machine learning models," Artificial Intelligence and Applications, 1(3), 179-190 (2023).