Hindawi
Scientific Programming
Volume 2023, Article ID 8387441, 11 pages
https://doi.org/10.1155/2023/8387441

Research Article

Data Protection of Accounting Information Based on Big Data and Cloud Computing

Xiaohua Li

Hunan College of Information, Changsha 410200, China

Correspondence should be addressed to Xiaohua Li; lxh202205@163.com

Received 12 June 2022; Revised 26 August 2022; Accepted 6 September 2022; Published 27 April 2023

Academic Editor: Mian Ahmad Jan

Copyright © 2023 Xiaohua Li. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid development of Internet technology, mankind has entered the era of big data. The Internet records all kinds of information, and the amount of information generated in the future is in a state of explosive growth. With the development of enterprises, the data of accounting information have grown, and its security has also been threatened. Once the accounting information is leaked, it will have a great impact on the company. Therefore, it is very necessary to protect accounting information data. This paper aims to study how to protect accounting information data based on big data and cloud computing. Based on this, this paper proposes an attribute-based encryption method based on big data and cloud computing and analyzes the ABE scheme of a single authority and multiple authorities. The multiauthority ABE scheme can effectively solve the problems of low computational efficiency, poor security performance, and high time overhead in the single-authority ABE scheme. The experimental results of this paper show that, under the single-authority ABE scheme in the information data protection of enterprise A, the confidentiality of data is 54% at the highest and 46% at the lowest, which is generally not very high. In the information data protection of the multiauthority ABE scheme in enterprise A, the highest data confidentiality is 86% and the lowest is 79%. The highest is 32% more than the single-authority ABE scheme. The lowest is also 33% more than that. Generally speaking, the confidentiality of its data is very high. In terms of reliability, integrity, and effectiveness, the single-authority ABE scheme is not as good as the multiauthority ABE scheme. It shows that the multiauthority ABE scheme proposed in this paper has a powerful information data security protection function and can be effectively applied to accounting information data protection.

1. Introduction

In this new century, in which the Internet and human culture are highly integrated, the rapid development of the Internet is setting off a new revolution in human beings as a whole. The Internet is infiltrating people's lives at a speed that people can barely perceive. Under the environment of network and e-commerce, the network of accounting information enables the operation of enterprises to transcend the limitations of time and space. In the management mode, it abandons the traditional accounting management mode and realizes business collaboration, remote processing, online management, and other modes. Online office, remote office, and mobile office are supported; in terms of information provision, remote reporting, remote accounting, and online information query are realized. However, due to the openness and sharing of the Internet, there are many unsafe factors in the network itself, which makes the enterprise accounting information in the network face the risk of interception, tampering, and leakage at any time.

Cloud computing is a type of distributed computing, which refers to decomposing huge data computing processing programs into countless small programs through the network "cloud." Due to the economics of cloud computing, more and more individuals and enterprises begin to deliver data storage and platform construction to the cloud, benefiting from the massive storage space and high concurrent computing power of cloud computing. The combination of big data and cloud platforms is becoming more common, which puts forward new security requirements for accounting information data in cloud computing, and the previous access control technology has problems such as

high consumption, low efficiency, and difficult management. Attribute-based encryption technology is an effective method to solve the security problem of cloud storage systems. The innovation of this paper is that it not only proposes an attribute-based encryption scheme based on cloud computing but also proposes a multiauthority ciphertext strategy. The problems of low calculation efficiency and high storage consumption of policy updates are improved, thus ensuring the security of enterprise accounting information data.

2. Related Works

With the in-depth development of the socialist market economy with Chinese characteristics, the security of accounting information and data has attracted more and more attention from the state and society. The rapid development of information technology and its application in accounting practice has endangered the security of accounting data circulating in cyberspace. The purpose of Popivniak's research was to determine how to solve the security problems that arise in accounting information, how to identify cyber threats in the field of accounting information use, and how to identify ways to prevent information theft and damage [1]. Lapitkaia found that, under the conditions of modern economic digitization, traditional accounting needs to make significant changes in the use of new information tools in order to continue to develop healthily. These new information technologies include cloud technology [2]. Pecheniuk confirmed the necessity of forming an effective information security system for enterprises. He emphasized that when designing information policies, companies must organize information security measures to be commensurate with their values, and he identified the main threats to the possible destruction of confidential information [3]. Rasheed and Kouser argued that the legal and governance environment in emerging markets is often weaker, and weak investor execution leads to a poor information environment. A corporate governance mechanism should be established in a timely manner [4]. Xing et al. raised a question whether the quality of accounting information affects capital, which has been a controversial issue. By linking the quality of accounting information with systemic risk, he found that the quality of accounting information is significantly negatively correlated with systemic risk [5]. Scholars agree that only when accounting information is properly protected can an enterprise develop healthily. If the information is leaked, it will not only lead to the loss of the company's economy but also cause the company to be maliciously competed against or even be unable to operate. The viewpoints put forward by scholars are indeed in line with the problems of enterprises in reality, but they only put forward the importance of information security and do not mention how to solve the security problem of information data.

With the rapid development of digitization and Internet technology, the amount of data on the Internet shows a trend of rapid increase. As a result, the Internet's data processing function is relatively insufficient, and many security problems have also appeared. Based on this, scholars have proposed attribute-based encryption algorithms. Francois et al. described a symmetric encryption algorithm based on a bit arrangement. The main advantage of this cryptosystem is that it can securely encrypt bit sequences and ensure the indistinguishability of the cipher. They applied the algorithm to image encryption that treats pure images as binary sequences [6]. Wang et al. proposed a new image encryption algorithm. Using his proposed pixel-swapping model to change the position of the pixels, the effect of scrambled images can be achieved. The simulation results show that the algorithm proposed by him has the characteristics of a large key space, high key sensitivity, and high security [7]. Hsiao proposed a neural network-based secure communication design method in multidelay systems in order to obtain double encryption through elliptic curve cryptography (ECC) synchronization. Its security strength depends on the difficulty of solving the elliptic curve discrete logarithm problem [8]. Luo et al. found that asymmetric, switchable, and reversible encryption is achieved by algorithmic encryption, which occupies an important position in encryption technology [9]. These scholars put forward encryption algorithms for security issues, which are consistent with the attribute-based encryption algorithm proposed in this paper, both to ensure the security of information. These scholars apply encryption algorithms to information encryption in various fields to ensure the security of data, which is worthy of reference in this paper.

3. Protection of Accounting Information by Attribute Encryption Algorithm Based on Cloud Computing

3.1. Network Accounting Information Security Issues

3.1.1. The Hidden Danger of Computer System. Computer hardware and its operating environment are important foundations to ensure the normal operation of network accounting information, and their security directly affects the security of accounting information. The security of the computer operating system is the basis of network information security. All information and security measures depend on the operating system. The vulnerability or improper configuration of the operating system may lead to the collapse of the entire security system. In order to achieve high reliability of application programs and information consistency, confidentiality, availability, and controllability on various operating systems, the system software foundation provided by the operating system must be relied on. But the security of the current operating system is not enough. The unreasonable design of computer operating system, insufficient access control, the existence of super users, and constantly discovered security holes are some of the fatal problems of the operating system.

3.1.2. Network Risks. Information plays an increasingly important role in modern economic life and has become an important means of market competition. Information has become the most important resource of an enterprise.

Whoever possesses more information and has accurate information will have a chance to win. In particular, the commercial secrets about the financial data of the enterprise are directly related to the success or failure of the enterprise.

Under illegal competition with interests and maliciousness, it is not allowed to illegally invade the accounting information systems of enterprises, and criminals who steal corporate secrets often exist. The types of malicious attacks that will appear in the information data are shown in Figure 1.

As shown in Figure 1, the current security situation of accounting information is not optimistic, the number of malicious programs is increasing year by year, and various loophole utilization technologies are constantly emerging, which would cause serious threats to the information security of network accounting. Due to the openness of Internet technology, the development of network accounting is bound to be restricted by the security of accounting information. It can be predicted that threats from all aspects of the network would gradually become the main factor affecting the security of corporate accounting information, and various high-tech network technologies would become the main force to maintain the security of corporate accounting information.

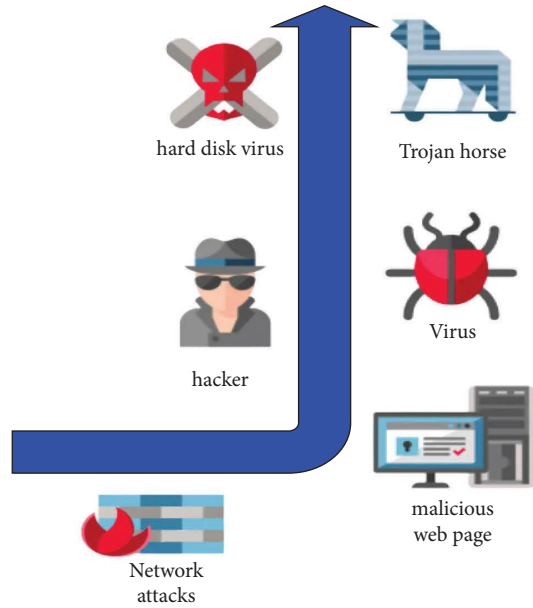

Figure 1: Types of malicious attacks.

3.1.3. Risks Brought by Data Sharing. The data-sharing method can solve the inconvenience caused by traditional accounting work, save the cost of personal and enterprise software and hardware, and promote the centralized management, preservation, and sharing of data. However, in the open cloud environment, there are difficult security issues such as data confidentiality, privacy protection, and access permission control. Data sharing is shown in Figure 2.

As shown in Figure 2, faced with such problems, various technologies emerge in an endless stream, such as the traditional access layer control technology (ACL). The traditional access control technology is mainly completed through network equipment access switches, two-layer semiaccess switches, multilayer switches, and routers. However, there are several major defects in PKI technology. One is that it brings a huge user management burden to the data sender; another is that it causes data redundancy, and the encryption time is proportional to the number of data recipients. It brings about problems such as encryption time and communication consumption. Therefore, traditional encryption and access technologies are not suitable for this new cloud data-sharing model.

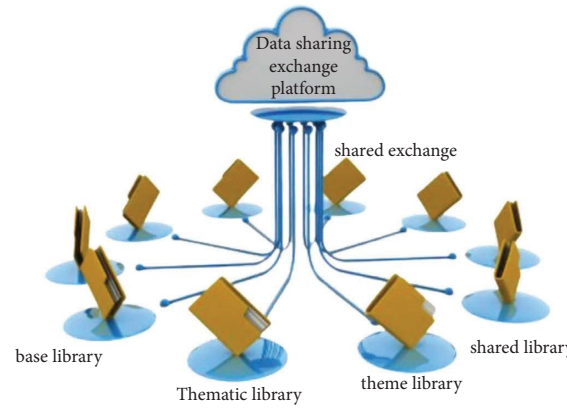

Figure 2: Data sharing.

3.2. Attribute Encryption Algorithm Based on Cloud Computing

3.2.1. The Algorithm Proposed in the Basic Text of Attribute Encryption. In order to solve the shortcomings of traditional KPIs, technology based on attribute-based encryption (ABE) has been proposed and implemented by scholars. The attribute-based encryption technology realizes one-to-many encryption, and the data only need to be encrypted once [10]. Attribute-based encryption encrypts messages according to attributes without paying attention to the identity of the receiver, which ensures the confidentiality of the data. At the same time, the data sender does not need to manage the data user. Therefore, the time and storage overhead brought on by encryption will be reduced, and the privacy of data users will be protected [11]. The attribute encryption algorithm is shown in Figure 3.

As shown in Figure 3, attribute-based encryption technology solves the system bottleneck and data redundancy problems caused by traditional technology. In the attribute encryption mechanism, users and data can be identified by some attribute information. Both the user's decryption key and the encrypted ciphertext are associated with a series of properties. The encryption of attributes reduces the burden of user management of encryption functions and has the characteristics of flexible control, strong security, and protection of user privacy [12]. By associating attribute sets with access resources, data users can access ciphertext information according to their own

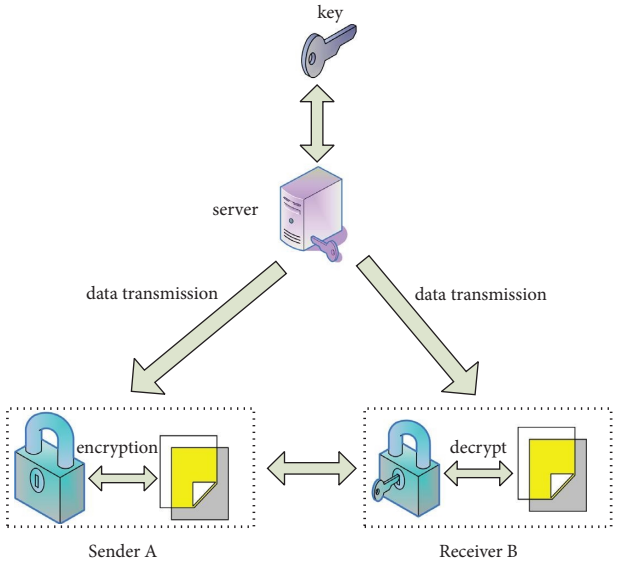

Figure 3: Attribute encryption algorithm.

authorization attributes. This technology is suitable for access applications such as private data sharing.

A finite field is a field containing only a finite number of elements. Compared with the rational number field and the real number field, it has many different properties.

Elliptic curve encryption in cryptography uses elliptic curves over finite fields. An elliptic curve over a finite field means that the curve equation is defined as follows:

$$b^2 = a^3 + ax + y. \tag{1}$$

All coefficients are elements of some finite field E_q (q is a large prime number). The most common of these are

$$E_q(a,b)\colon b^2 = a^3 + ax + y \,(\mathrm{mod}\, q). \tag{2}$$

The attribute-based encryption (ABE) mechanism only supports simple threshold control, and neither the data sender nor the data user can specify flexible access control policies [13]. The logic threshold control strategy is fast, simple, stable, and reliable, with strong practicability, high vehicle control computing efficiency, and less physical memory occupation of the controller. When the number of ciphertext attribute sets intersecting with the user attribute set is not less than the threshold set by the authority, the data user can be decrypted correctly.

The authority initially sets the threshold value d and generates the master key as follows:

$$\mathrm{MSK} = \left(b, \left\{t_i \,\middle|\, t_i \in Z_q\right\} \forall_{i \in A}\right). \tag{3}$$

The authority generates the key of user u and randomly generates a polynomial, and the user key is

$$\mathrm{SK} = \left\{D_i = g^{p(i)}\right\}. \tag{4}$$

The data sender encrypts the message with the ciphertext attribute set, and the ciphertext is as follows:

$$\mathrm{CT} = \left(A_C, E = \cdot B^S, \left\{E_i = T_i^s\right\}_{\forall_i \in A_C}\right). \tag{5}$$

The multiauthority scheme also supports key policies. Each authority generates an access tree for the attribute set and generates key components for each leaf node according to the top-down method. The user's final access policy structure is as follows:

$$T = T_1 \wedge \ldots \wedge T_N. \tag{6}$$

In the encryption algorithm, if the key is modified by an unauthorized illegal user, the encrypted data cannot be restored to the correct original information through the corresponding decryption process. In the decryption process, each T_N value is obtained in a bottom-up manner, and finally the plaintext m can be calculated and the data user can decrypt the ciphertext.

3.2.2. Key Policy Encryption Scheme. In the key-policy scheme, the data user generates an access control policy with his own attribute set, the authority calculates the user key according to the control policy, and the data sender uses the attribute set to encrypt the ciphertext [14]. When the ciphertext attribute set satisfies the access control policy, the user can decrypt it. The control strategy is constructed into a tree structure, as shown in Figure 4.

As shown in Figure 4, the various tree diagrams in the classical data structure have a typical tree structure. A tree can be simply represented as the root, the left subtree, and the right subtree. The left and right subtrees have their own subtrees. The leaf node of the access control tree T is $L(T) = A$, and the ciphertext is related to the attribute set A_{ct}. When A_{ct} satisfies T, the ciphertext can be decrypted. Access control tree: internal nodes represent a threshold; each internal node has a threshold value; and leaf nodes represent attributes [15].

A property set is set; the root node of the access tree T is R; and the access operation of the set to the access tree T node is defined as

$$T_a(A) = \begin{cases} 1, & \mathrm{attr}(a) \in A, \\ 0, & \mathrm{Otherwise}. \end{cases} \tag{7}$$

When $T_a(A) = 1$, the set satisfies the access tree T, otherwise it does not.

The difference between the ciphertext strategy ABE and the basic ABE mechanism lies in the KeyGen and Decrypt steps. KeyGen: a polynomial is randomly generated for each node of T from top to bottom, and

$$P_a(0) = \begin{cases} b, & a = R, \\ p_{\mathrm{parent}(a)}(\mathrm{index}(a)), & \mathrm{othrewise}. \end{cases} \tag{8}$$

Decrypt is a bottom-up recursive process, and when a is a leaf node,

$$F_a = \prod_{z \in s^*} F_Z^{\Delta_{i,s}}. \tag{9}$$

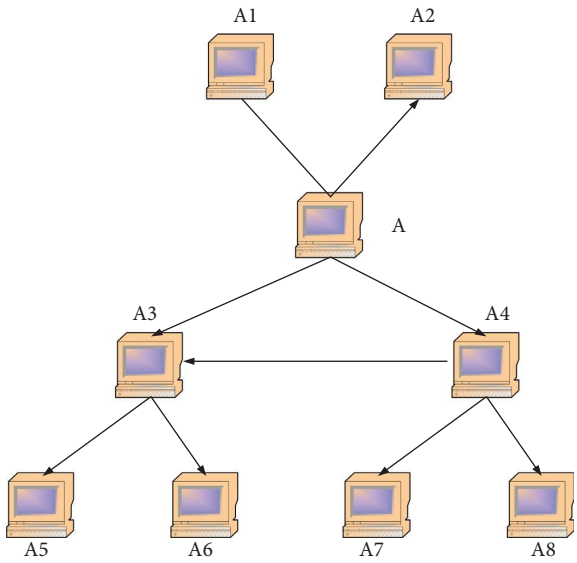

Figure 4: Access control tree.

3.2.3. Ciphertext Strategy Encryption Scheme. The outer and inner layers of a tree structure have similar structures, so this structure can be represented recursively. In the ciphertext strategy scheme, the access control strategy T is specified by the data sender, the control strategy adopts a tree structure similar to the key strategy scheme, and its leaf node is $L(T) = A_{\text{ct}}$; the user key is related to the attribute set. The authorization authority generates user keys according to the attribute set, and the ciphertext policy ABE is different from the above encryption scheme [16].

The authorized agency selects a random number and calculates the master key as

$$\text{MSK} = (g^{\alpha}, \beta). \tag{10}$$

The authority generates the key of user u, selects a random number for each user attribute $i \in A_{ct}$, and calculates the key as

$$\text{SK} = \left(D = g^{(\alpha+r)/\beta}\right). \tag{11}$$

The data sender selects a random number and constructs an access control policy T according to the ciphertext attributes. A polynomial is randomly generated for each node a of T from top to bottom as follows:

$$p_a(0) = \begin{cases} s, & a = R, \\ p_{\text{parent}(a)}(\text{index}(a)), & \text{othrewise}. \end{cases} \tag{12}$$

Decryption is a bottom-up recursive process, as shown below:

$$F_a = \frac{e\left(D_{i,1}, E_{i,1}\right)}{e\left(D_{i,2}, E_{i,2}\right)}. \tag{13}$$

3.3. Attribute Encryption Scheme for Multiple Authorities. The abovementioned ABE models are all single-authorization agencies, and these models have the problem of high management cost of authorization agencies. Some scholars proposed a multiauthority attribute encryption scheme (MA-ABE) [17]. The scheme introduces GID as the user's identification in the system and introduces the central agency to manage all authorized agencies. GID is a general-purpose, adaptable, and user-friendly GUI for geometric simulation, data entry, model transformation, meshing, and visualization of results.

The MA-ABE scheme includes four algorithms: Setup, KeyGen, Encrypt, and Decrypt. Suppose that there are N authorities in the system. Setup means that each authority k chooses $B_k \in Z_q$ as follows:

$$B_k = e(g, g)^{b_k}. \tag{14}$$

Announce B_k to other authorized institutions, negotiate secretly with authorized institution j, randomly select random numbers, and define the pseudorandom function with the authorized institution as

$$\text{PR}F_{k,j}(u) = g^{\left(a_k a_j / \left(s_{k,j}+u\right)\right)}. \tag{15}$$

Each authorized institution k randomly selects $N-1$ random numbers and issues them to user u through an anonymous distribution protocol. The data user u obtains the following key components as follows:

$$D_{k,j} = \begin{cases} g^{R_{k,j}} \cdot \text{PRF}(u), & k > j, \\ \dfrac{g^{R_{k,j}}}{\text{PRF}(u)}, & k < j. \end{cases} \tag{16}$$

The data sender encrypts the plaintext m, selects the ciphertext attribute from each authority k, and calculates the ciphertext as follows:

$$\text{CT} = \left(E_0 = m \cdot B^S, E_1 = g^s\right). \tag{17}$$

MA-ABE ensures the privacy of data by means of public key encryption primitives and realizes one-to-many and fine-grained access control, so it can efficiently and securely share data in cloud environment [18]. Fine-grained is a computer programming term. The fine-grained model, in layman's terms, is to subdivide the objects in the business model to obtain a more scientific and reasonable object model. Intuitively, it is meant to divide many objects, but it has certain shortcomings. Since, in most MA-ABE schemes, the computational overhead of encryption and decryption is linearly related to the number of attributes it contains, users need to deal with a large amount of computational load, which is not good for resource-constrained devices [19]. At the same time, when the user's encrypted data in the cloud need to update the access policy, the traditional methods such as downloading and decrypting and then reencrypting and uploading are unrealistic because this will consume a lot of communication and computing resources, as shown in Figure 5.

As shown in Figure 5, in order to reduce the computational burden of resource-constrained clients and achieve rapid policy update, this paper proposes an outsourced multiauthority ciphertext policy attribute encryption scheme. Most of the existing attribute-based encryption

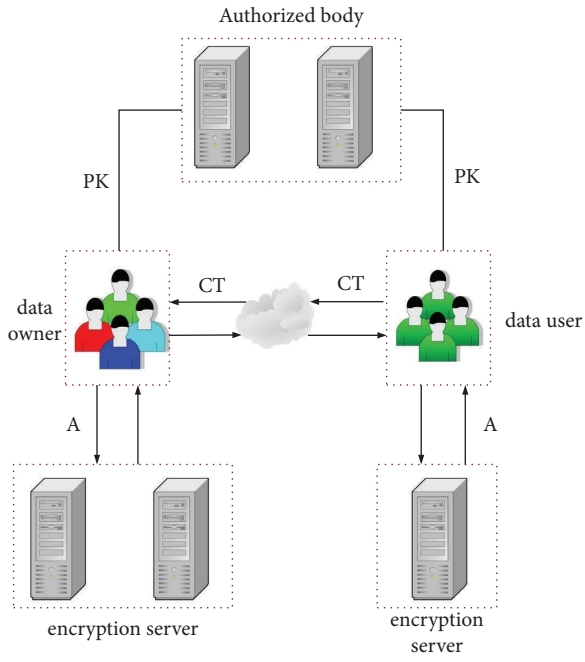

Figure 5: Multiauthority policy update outsourcing model.

schemes are based on a single authority. Once a single authority is attacked, the data security of the entire system cannot be guaranteed. In order to improve the security of the entire system, the multiauthority ciphertext strategy attribute encryption scheme appears. The system supports encryption, decryption, and outsourcing of policy updates on the client side. Under the premise of not revealing data sensitive information, most of the computing work of encryption, decryption, and policy update is outsourced to a third-party service agent, thereby greatly reducing the amount of local work. Therefore, MA-ABE is made suitable for resource-constrained devices [20, 21].

4. Results and Discussion

4.1. Test of Ciphertext Time Overhead. The symmetric elliptic curve of type A is used in the simulation experiment, which is based on a finite field of 512 bits and tested. Mainly, each step (initialization, key generation, encryption, decryption, ciphertext update, and key update) is analyzed and compared theoretically, and simulation data are analyzed and compared.

The experimental environment is built on Cygwin, which simulates a Linux environment under a Windows system. The processor is Pentium CPUG620, and the memory capacity is 4 GB. Their implementation is on a finite field of 512 bits. The experimental code is written based on the cpabe-0.11 library and the kpabe library. For the key-policy attribute encryption algorithm, the time consumption mainly comes from linear calculation. Therefore, for the time consumption of each step, only the calculation results are counted. The performance comparison of the two schemes is shown in Table 1.

Table 1: Performance comparison of the two schemes.

Steps	Single authority ABE (s)	Multiauthority ABE (s)
Initialization	3.8	1.7
Key generation	2.7	1.3
Encryption	3.2	1.0
Decrypt	3.5	1.5
Key update	3.6	0.9
Ciphertext update	4.0	1.1

As shown in Table 1, both single-authority ABE and multiauthority ABE are based on the ABE algorithm. Table 1 shows that, in terms of initialization, key generation, encryption, and decryption time, multi-authority ABEs take significantly less time than single-authority ABEs. This is because the multiauthority ABE has a linear relationship with the number of authorized institutions.

In the simulation experiment, the fixed number of authorized institutions participating is 20, the number of attributes is increased in turn, and all attributes participate in the above six steps, as shown in Figure 6.

As shown in Figure 6, in the encryption and decryption time of ciphertext, there is almost no difference in the time between the two at the beginning. But, as the data increase, multiauthority ABEs begin to outperform single-authority ABEs. This is because the single-authority ABE is linearly related to the number of attributes.

4.2. Test of Key Time Overhead. In order to verify the authenticity of the experiment, the single-authority ABE and the multiauthority ABE are tested in terms of key time overhead, and 5000 pieces of enterprise data are used for experimental analysis, as shown in Tables 2 and 3.

As shown in Tables 2 and 3, in terms of key time overhead, the single-authority ABE scheme takes more time than the multiauthority ABE scheme and its security level is not high. When the amount of data is 1000, the time spent by the single-authority ABE scheme is 5.4 seconds, while the time spent by the multiauthority ABE scheme is 2.1 seconds, which is 3.3 seconds more; when the amount of data is 5000, the single-authority ABE scheme takes 6.2 seconds, while the multiauthority ABE scheme takes 3.2 seconds. Although the time overhead of both schemes increases with the increase of the amount of data, the multiauthority ABE scheme does not change much on the whole.

4.3. Test of Algorithm Efficiency. The above is the analysis of the algorithm overhead, and then this paper analyzes the efficiency of the algorithm. Among them, due to the low efficiency of the attribute encryption algorithm, it was necessary to prove that the key generation time, encryption time, and decryption time of the test scheme in this paper are less in different environments. This article used the multi-authority ABE scheme to encrypt two text files (5 MB and 10 MB). The result is shown in Figure 7.

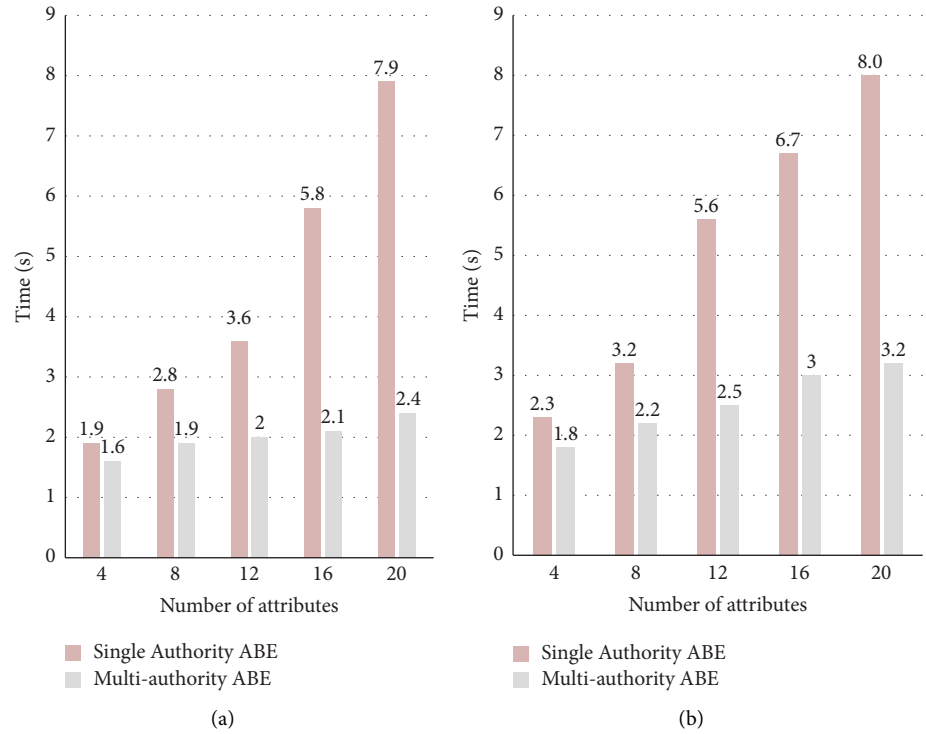

Figure 6: Two algorithms in ciphertext encryption and decryption time. (a) Comparison of ciphertext encryption time. (b) Comparison of ciphertext decryption time.

Table 2: Key time overhead of single-authority ABE scheme.

Test data	Time spent	Efficiency (%)	Degree of protection
1000	5.4	36	Generally
2000	6.8	50	Poor
3000	5.5	48	Generally
4000	5.9	39	Better
5000	6.2	45	Poor

Table 3: Key time overhead of multiauthority ABE scheme.

Test data	Time spent	Efficiency (%)	Degree of protection
1000	2.1	36	Strong
2000	2.5	50	Strong
3000	2.9	48	Generally
4000	3.0	39	Strong
5000	3.2	45	Strong

As is shown in Figure 7, the key generation time and the number of attributes have a linear relationship. With a file size of 5 MB, the multiauthority ABE scheme takes less than 2 seconds. In the case of a file size of 10 MB, although the time spent by the multiauthority ABE scheme has increased, the magnitude of the change is not large. Therefore, it can be seen that the time cost of the multiauthority ABE scheme is more advantageous.

For the encryption algorithm, the running time changes with the change of the leaf nodes in the access structure tree. The encryption efficiency of multiauthority ABE is obviously better than that of single-authority ABE because when single-authority ABE performs one exponentiation operation, single-authority ABE needs to perform two operations, as shown in Figure 8.

As shown in Figure 8, for the decryption algorithm, the efficiency of the modified scheme is higher than the original scheme because, when the multiauthority ABE performs a bilinear mapping once, the single-authority ABE performs a quadratic bilinear mapping. In addition, the sizes of the plaintext file and the ciphertext file are not much different. For simple access structures, the storage overhead can be ignored in this scheme. Through the analysis of the above execution and storage costs, the multiauthority ABE scheme is much more efficient in encryption, decryption, and key generation than the single-authority ABE scheme.

4.4. Testing of Safety Performance. The attribute encryption algorithm is a new type of encryption algorithm. Its biggest advantage is that it can use the user's identity as a key to achieve encryption. There is no longer a need to encrypt data for each decryptor like symmetric encryption, nor are there complex key management systems like public key encryption. In the ABE algorithm, the encryptor does not need to know who the decryptor is, and the decryption rules are contained in the ciphertext. The attribute encryption algorithm is more suitable for application in the cloud computing environment.

At present, user enterprises regard accounting information security as the main problem. Among security issues, users are most concerned about data security, including data confidentiality, reliability, integration, and

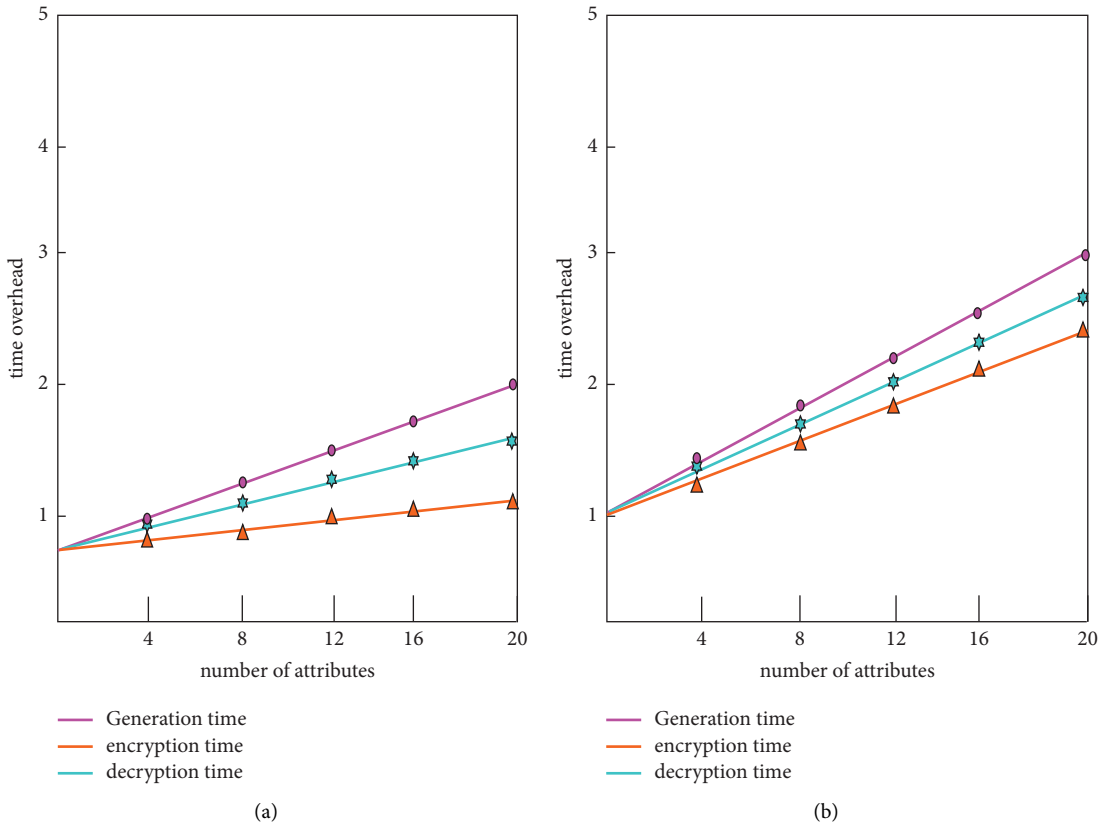

Figure 7: Performance comparison of multiauthority ABE schemes under different files. (a) Performance of multiauthority ABE scheme under 5 MB file. (b) Performance of multiauthority ABE scheme under 10 MB file.

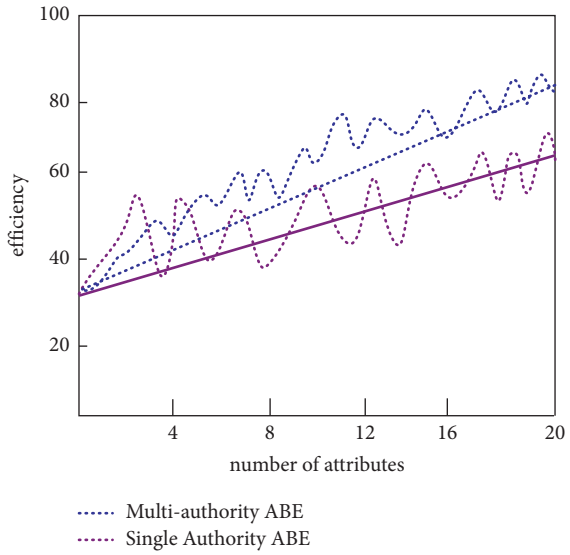

Figure 8: Comparison of decryption efficiency of schemes.

effectiveness. This paper selects 5000 pieces of accounting information data of enterprise A and first compares whether the two algorithms are powerful in accounting information data protection, as shown in Tables 4 and 5.

As shown in Tables 4 and 5, in the information data protection of the single-authority ABE scheme in enterprise A, the confidentiality, reliability, integrity, and validity of the data are the highest at 54%, 55%, 63%, and 58%, respectively.

Table 4: Information and data protection of the single-authority ABE scheme in the enterprise.

Test data	Confidentiality (%)	Reliability (%)	Integrity (%)	Validity (%)
1000	54	55	63	58
2000	53	54	62	55
3000	52	50	60	50
4000	48	46	61	47
5000	46	45	59	46

Table 5: Information and data protection of multiauthority ABE schemes in enterprises.

Test data	Confidentiality (%)	Reliability (%)	Integrity (%)	Validity (%)
1000	79	82	77	75
2000	80	83	79	78
3000	82	85	81	83
4000	84	87	82	85
5000	86	89	85	87

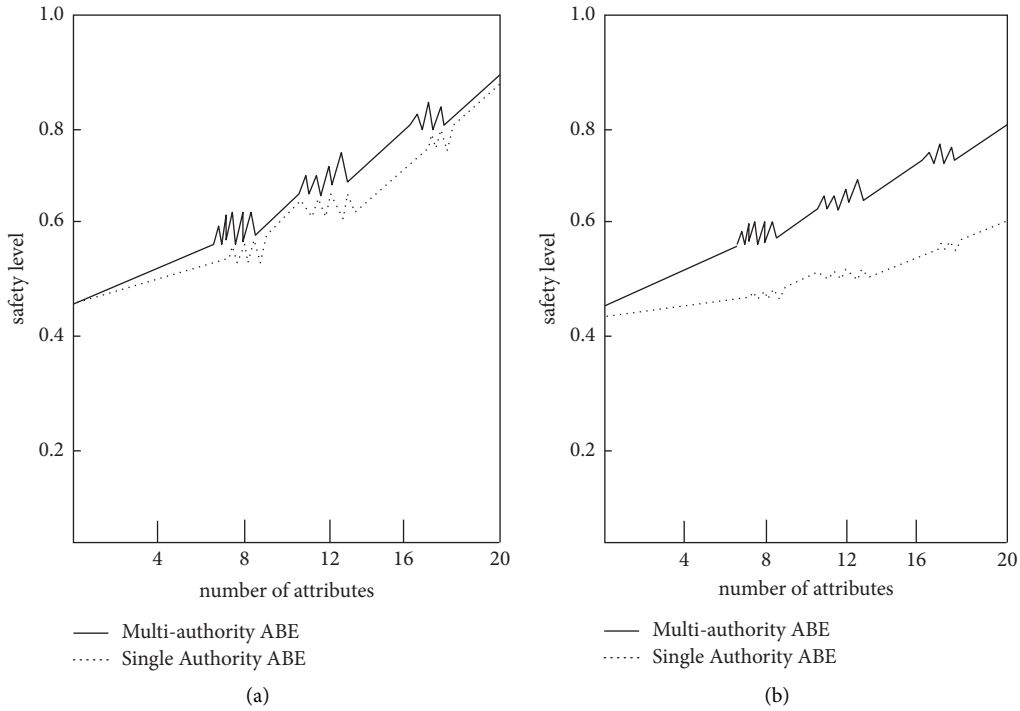

Figure 9: The security index before and after the attack of the two schemes. (a) The security index of the two schemes before the attack. (b) The security index of the two schemes after the attack.

The lowest are 46%, 45%, 59%, and 46%, respectively, and with the increase of information data to be protected, its protection function is getting worse and worse. The confidentiality, reliability, integrity, and effectiveness of the multiauthority ABE scheme in enterprise information data protection are 86%, 89%, 85%, and 87%, respectively. The lowest are 79%, 82%, 77%, and 75%, respectively. With the increase of information data to be protected, its protection function is not only better than that of the single-authority ABE scheme but also the security function is getting stronger.

In order to verify that the security performance of the multiauthority ABE scheme is higher, this paper compares and analyzes the security performance of the single-authority ABE scheme. The two algorithms are encrypted, and then attacked by attack software, and the security index before and after the attack is compared, as shown in Figure 9.

As shown in Figure 9, the security index of the two schemes before the attack is not very different, but after the attack, the security index of the single-authority ABE scheme decreases significantly. However, the security index of the multiauthority ABE scheme has not changed much. It shows that the security index of the multiauthority ABE scheme is more stable. Although the scheme proposed in this paper can improve the efficiency of key generation, encryption, and decryption, the public parameters and master key of the algorithm will increase linearly with the increase of attribute

sets. Therefore, the algorithm proposed in this paper can only be used in the case where the attribute set is small.

5. Conclusions

With the development of network informatization, the problem of accounting information security is becoming more and more serious. Once the accounting information is leaked, it will cause irreversible losses to the enterprise. This paper first analyzed the security problems in the current accounting information and then described the attribute encryption algorithm. Firstly, the algorithm proposed in the basic text of attribute encryption was introduced, and the shortcomings of the single-authority ABE scheme were put forward, thus the multiauthority ABE scheme was described. It was applied to the solution of the accounting information security problem. In order to prove that the proposed scheme was more secure, this paper compared it with the single-authority ABE scheme in various aspects in the experimental part and conducted experiments in terms of time overhead, algorithm efficiency and security performance, respectively. Finally, it is concluded that the proposed scheme has less time overhead, higher algorithm efficiency, and stronger security performance than the single-authority ABE scheme. Therefore, it can be applied to the protection of accounting information data. However, the algorithm proposed in this paper is implemented under the random oracle model, and the scope of application of the algorithm proposed in this paper is very limited, so the data obtained will have certain differences. It will be very meaningful work to construct more attribute encryption schemes with ciphertext strategies in the future.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Hunan Province Vocational Education Teaching Reform Research General Project: Research on Talent Training Evaluation System of Big Data and Accounting Major in Higher Vocational Colleges under the "1+X" Certificate System (project no. Xiangjiaotong (2022) 36, ZJGB2021196).

References

[1] Y. M. Popivniak, "Cybersecurity and protection of accounting data under conditions of modern information technology," *Business Inform*, vol. 8, no. 499, pp. 150–157, 2019.

[2] L. Lapitkaia, "Application of cloud technologies in accounting," *MEST Journal*, vol. 9, no. 1, pp. 90–96, 2021.

[3] A. V. Pecheniuk, "Conceptual principles for ensuring effective protection of information in the context of economic security of the enterprise," *Ekonomika ta upravlinnâ APK*, vol. 1, no. 155, pp. 84–92, 2020.

[4] M. S. Rasheed and S. Kouser, "Corporate governance and stock price informativeness: evidence from an emerging market," *Journal of Accounting and Finance in Emerging Economies*, vol. 6, no. 2, pp. 593–605, 2020.

[5] X. Xing, X. Jia, and M. H. Q. Meng, "Bleeding detection in wireless capsule endoscopy image video using superpixel-color histogram and a subspace KNN classifier," in *Proceedings of the 2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, no. 1, pp. 1–4, Honolulu, HI, USA, July, 2018.

[6] M. Francois, T. Grosges, D. Barchiesi, and R. Erra, "Image encryption algorithm based on a chaotic iterative process," *Applied Mathematics*, vol. 3, no. 12, pp. 1910–1920, 2012.

[7] X. Wang, S. Wang, Y. Zhang, and G. Kang, "A novel image encryption algorithm based on chaotic shuffling method," *Information Security Journal: A Global Perspective*, vol. 26, no. 1-3, pp. 1–10, 2017.

[8] F. H. Hsiao, "Chaotic synchronization cryptosystems combined with RSA encryption algorithm," *Fuzzy Sets and Systems*, vol. 342, no. 1, pp. 109–137, 2018.

[9] T. Luo, T. Zhou, and J. Qu, "Lifetime division multiplexing by multilevel encryption algorithm," *ACS Nano*, vol. 15, no. 4, pp. 6257–6265, 2021.

[10] E. Mendrofa, E. Y. Purba, B. Y. Siahaan, and R. W. Sembiring, "Collaborative encryption algorithm between vigenere cipher, rotation of matrix (ROM), and one time pad (OTP) algoritma," *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, no. 5, pp. 13–21, 2017.

[11] M. Haj and M. Qatawneh, "Parallel hill cipher encryption algorithm," *International Journal of Computers and Applications*, vol. 179, no. 19, pp. 16–24, 2018.

[12] J. Yu, H. F. Kong, and Y. W. Ding, "Privacy protection scheme combining attribute authentication and structure authorization," *Computer Engineering and Design*, vol. 43, no. 6, pp. 1520–1526, 2022.

[13] X. D. Zhang, T. W. Chen, Y. M. Yu, and H. Y. Wang, "Access control scheme based on blockchain and CPABE," *Application Research of Computers*, vol. 39, no. 4, pp. 986–991, 2022.

[14] F. C. Liu, H. T. Hsu, and D. C. Yen, "Technology executives in the changing accounting information environment: impact of IFRS adoption on CIO compensation," *Information & Management*, vol. 55, no. 7, pp. 877–889, 2018.

[15] G. Han, L. Pang, W. Luo, and H. C. Wang, "MSP data access control mechanism based on attribute update," *Journal of Xi'an University of Posts and Telecommunications*, vol. 26, no. 4, pp. 53–59, 2021.

[16] J. T. Dong, P. W. Yan, and R. Z. Du, "Verifiable access control scheme based on unpaired CP-ABE in fog computing," *Journal on Communications*, vol. 42, no. 8, pp. 139–150, 2021.

[17] J. L. Zhang, Y. C. Zhao, B. Chen, F. Hu, and K. Zhu, "Survey on data security and privacy-preserving for the research of edge computing," *Journal on Communications*, vol. 39, no. 3, pp. 1–21, 2018.

[18] Y. H. Zhang, T. Zhu, and D. Zheng, "Multi-keyword fine-grained searchable encryption scheme based on blockchain," *Netinfo Security*, vol. 21, no. 2, pp. 34–44, 2021.

[19] Y. M. Hei, J. W. Liu, H. W. Feng, D. W. Li, Y. Z. Liu, and H. Q. Wu, "Making MA-ABE Fully Accountable: A Blockchain-

Based Approach for Secure Digital Right Management," *Computer Networks*, vol. 191, Article ID 108029, 2021.

[20] T. W. Hazlett, S. Oh, and B. Skorup, "Natural experiments in mobile phone regulation: estimated effects of prohibiting handset bundling in Finland and Belgium," *Journal of Competition Law and Economics*, vol. 14, no. 1, pp. 65–90, 2018.

[21] X. H. Wu, A. X. Zhang, and J. H. Li, "Data outsourcing and sharing scheme based on vector commitment and proxy Re-encryption," *Computer Engineering*, vol. 44, no. 1, pp. 1–5, 2018.