Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5994628, 11 pages
https://doi.org/10.1155/2022/5994628

Research Article

Enterprise Financial Data Sharing Based on Information Fusion Cloud Computing Environment

Yanqing Chen

College of Accounting, Zhanjiang Science and Technology College, Zhanjiang, 524000 Guangdong, China

Correspondence should be addressed to Yanqing Chen; 20162103779@mails.imnu.edu.cn

Received 22 November 2021; Revised 15 December 2021; Accepted 22 December 2021; Published 13 January 2022

Academic Editor: Deepak Kumar Jain

Copyright © 2022 Yanqing Chen. 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.

At present, many companies have many problems such as high financial costs, low financial management capabilities, and redundant frameworks; at the same time, the SASAC requires that the enterprise's financial strategy transfer from "profit-driven" to "value-driven", finance separate from accounting to improve the operational efficiency of the company. Under this background, more and more enterprise respond to the call of the SASAC; in order to achieve the goals of corporate financial cost savings and financial management efficiency improved, we began to provide services through financial sharing. The research of information fusion theory involves many basic theories, which can be roughly divided into two large categories from the algorithmic point of view: probabilistic statistical method and artificial intelligence method. The main task of artificial intelligence is to realize the computer for some learning, thinking process, and wisdom formation of simulation, and an important goal of information integration is the human brain comprehensive processing ability simulation, so artificial intelligence method will have broad application prospects in the field of information fusion; the common methods have D-S evidence reasoning, fuzzy theory, neural network, genetic algorithm, rough set, and other information fusion methods. The purpose of this paper is to proceed from the internal financial situation of the enterprise, analyze data security issues in the operation of financial shared services, and find a breakthrough in solving problems. But, with constantly expanding of enterprise group financial sharing service scale, the urgent problem to be solved is how to ensure the financial sharing services provided by enterprises in the cloud computing environment. This paper combines financial sharing service theory and information security theory and provides reference for building financial sharing information security for similar enterprises. For some enterprise that have not established a financial shared service center yet, they can learn from the establishment of the financial sharing information security system in this paper and provide a reference for enterprise to avoid the same types of risks and problems. For enterprise that has established and has begun to practice a financial shared information security system, appropriate risk aversion measures combined with actual situation of the enterprise with four dimensions related to information security system optimization was formulated and described in this paper. In summary, in the background of cloud computing, financial sharing services have highly simplified operational applications, and data storage capabilities and computational analysis capabilities have been improved greatly. Not only can it improve the quality of accounting information but also provide technical support for the financial sharing service center of the enterprise group, perform financial functions better, and enhance decision support and strategic driving force, with dual practical significance and theoretical significance.

1. Introduction

Information in the physical world often comes from a wide number of all kinds of perceptual equipment, and a variety of forms, information capacity, information relationship is complex; the human brain information comprehensive processing ability is far from meet the needs of timely and accurate processing of the information, so there was a need to use machine comprehensive processing analysis, so also produced the information fusion technology. At the beginning, information fusion mainly targets multisensor data, so also known as multisensor data fusion four or data fusion. In the 1980s, due to the urgent military and civilian requirements, the concept of "data integration" quickly became one of the hot issues of the world, and further research was quickly carried out quickly. Multisensor data fusion technology has now been combined with a variety of cutting-edge technologies such as expert systems, fuzzy mathematics, and wavelets and has attracted a lot of attention in China and abroad. The financial sharing in the era of cloud computing is based on modern information technology and the business processes of financial business personnel through different enterprises and different locations. It effectively organizes and shares, separates complex and trivial financial services, and establishes standardized financial business management methods [1]. Financial data is the most important and largest data information in enterprise management. As the scale of the enterprise grows, the financial activities of the enterprise become more and more complex, and the level of financial data management is also higher [2]. Improving the level of financial data processing, improving financial management efficiency, and strengthening financial security management are important guarantees for the healthy and effective development of enterprises. Facing the cloud-based big data era sharing model, it can help companies accurately manage financial processes and improve the efficiency of financial processing.

The advantage of AI-based information fusion methods is that such methods have strong learning ability and adaptive ability to realize the fusion process of information not affected by the supervisor; the disadvantage is relatively large operation volume, difficult rule establishment or long learning time, difficult to meet the timeliness and space-time sensitivity to information integration, real-time control for timely decision making, and not easy to achieve. Cloud computing observation of the same thing object may be multiangle and layered, through different attributes, so the type of sensing device may be different, and the same type of sensing device may realize the perception, but the corresponding data types are different and oneself. The data corresponding to these properties used to characterize things may be regular data of a character or numerical type, or time type data, location information, etc. Therefore, it is necessary to study a set of methods that can solve the collaboration and fusion of multi-source heterogeneous data information in the cloud computing. The financial sharing model under the background of the big data era can improve the scale efficiency of enterprises and bring the knowledge concentration effect, the influence of enterprise expansion, the goal of integrating knowledge resources within the enterprise, and the ability to expand the financial management of enterprises. It can be seen that financial sharing in the context of the era of big data has certain significance for the survival and development of enterprises [3]. It can not only improve the economic benefits of enterprises but also enhance the social benefits of enterprises, thereby promoting the sustainable development of enterprises. Drawing on existing accounting cooperation models, such as the accounting cooperation mechanism of China, Japan, and South Korea, accelerate the establishment of the “Belt and Road” accounting cooperation mechanism. China should play a leading role and concentrate accounting scholars and experts from the “Belt and Road” countries to seriously analyze and study the accounting convergence of the “Belt and Road.” Through the establishment of the “Belt and Road,” accounting cooperation mechanism, the coordination between the accounting standard-setting and supervisory bodies of each country should be strengthened to enhance the accuracy, reliability, and comparability of accounting information, which is conducive to the protection of investors and the promotion of regional economic development [4].

Ali et al. proposed the secure data sharing (SeDaSC) method in the cloud, which provides (1) data confidentiality and integrity; (2) access control; (3) data sharing (forwarding), without computationally intensive reencryption; (4) internal threat security; and (5) forward and backward access control. The SeDaSC method encrypts files using a single encryption key. Two different key shares for each user were generated, and the user gets only one share. Having a part of a key allows the SeDaSC method to combat internal threats. Another key share is stored by a trusted third party, which is called an encryption server. The SeDaSC method is suitable for both traditional and mobile cloud computing environments [5, 6]. By using key agreement and group signature, Jian and other scholars proposed a new traceable group data sharing scheme to support anonymous multiple users in the public cloud. On the one hand, group members can communicate anonymously with group signatures and can track the true identity of members as necessary. On the other hand, public conference keys are derived based on a key agreement to enable group members to securely share and store their data [7]. In practical applications, we must solve more challenging problems, such as attribute revocation and data search. How do data users search the vast amounts of data they need? When users leave the system, they will lose the right to decrypt shared data [8]. In this case, how do we ensure that the revoked user cannot decrypt the shared data? In this paper, Axin and other scholars successfully solve these problems by proposing a hidden data sharing scheme based on policy attributes and direct undo and keyword search. In the proposed solution, the direct revocation of an attribute does not require updating the private key of the user who has not been revoked during revocation. In addition, keyword search is implemented in our scheme, and the search time is constant as the attribute increases [9]. Nada et al. investigated the problem of estimating wheelchair position with noise measurements in an indoor environment. The data from the sensors are combined and used as input to the unscented Kalman filter (UKF). Two data fusion architectures are proposed: measurement fusion (MF) and state vector fusion (SVF) to merge the available measurement data. A comparative study of these two architectures shows that the MF architecture provides relatively less uncertainty in the state estimates compared to SVF. However, the uncertainty in the position determined by the odometer measurements is relatively high, followed by the accelerometer measurements. Therefore, fusion in the navigation system is needed. The simulation results obtained show the effectiveness of the proposed architecture [10].

Throughout the literature at home and abroad, there have been many research results in cloud computing, financial sharing, and information security. Domestic and foreign scholars mainly analyze the concept, feasibility, and advantages of cloud computing. The core concept of cloud computing is its virtualized resource pool and pay-as-you-go model. Cloud computing can bring low-cost and wide-access advantages to enterprises. Moreover, the emergence of cloud computing has transformed corporate financial management into financial sharing. Foreign studies have been earlier, but Chinese scholars have proposed to localize financial sharing services, pointing out that the advantages of financial sharing services provide a good foundation for the development of management accounting and promote the improvement of corporate performance. Emphasis is placed on the direction of financial sharing and the refactoring of financial processes. Most of the literature is based on the evaluation of information security. The method of empirical research is generally the design evaluation index of the information system. Information security risks mainly occur during the storage, transmission, and use of accounting information. Finally, how to conduct information security assessment under the new technology environment is a major challenge facing the current financial sharing information security issue. Establishing a set of financial sharing information security assessment system in cloud computing environment has certain practical significance for China's financial sharing information security management.

In this paper, by analyzing the privacy protection issues in industry financial data sharing, static data blocks can be traditionally encrypted using the RSA algorithm and dynamic data blocks are encrypted using CP-ABE algorithm, carrying out the basic theories and key technologies related to cloud computing information fusion, constructing a set of information security evaluation system for financial sharing, and realizing enterprise financial based on information fusion cloud computing environment data sharing based on the information fusion cloud computing environment.

2. Proposed Method

2.1. Cloud Computing Security. Security is an important factor affecting the promotion of cloud computing and the core of ensuring special financial sharing issues. This topic describes privacy protection issues in enterprise financial data sharing, including data sharing and research. At present, the data storage scheme in cloud computing can solve the problem of trust concentration to a certain extent, but the data partitioning mode and computational overhead are flawed. In the process of data sharing, there is an urgent need to propose an effective encryption scheme to ensure the confidentiality of shared data and the ability to resist collusion attacks. When the user completes the sharing of the attribute revocation, it is necessary to continue to optimize the immediacy and efficiency of the user attribute revocation. In response to the above problems, this article trusts the decentralized storage strategy from the following points. First, the uploaded data is divided into dynamic data and static data by using a fixed value extraction method, wherein the dynamic data is a data portion that is encrypted only when the encryption algorithm is canceled. The ciphertext is often dynamically changing; static data is part of the data that is not reencrypted each time it is revoked, so part of the data changes less frequently in the cloud. Then, the two pieces of data are, respectively, encrypted, the static data is encrypted by the RSA algorithm, and the dynamic data is encrypted by the CP-ABE (ciphertext-policy attribute-based encryption) algorithm. Finally, the encrypted two data is stored on two different cloud servers. Decentralized storage and encryption processing not only increases the security of shared data but also reduces computational overhead during encryption and decryption, while taking into account security and applications. The technical roadmap for the study is shown in Figure 1 below.

2.2. Data Trust Decentralized Storage Policy CP-ABE Algorithm Encrypts Dynamic Data. Trusted storage policies include data segmentation, data encryption, and data decryption. The fixed data extraction method is used to divide the raw data into dynamic data and static data and then store the static data and the dynamic data in different clouds. The enterprise financial data sharing encryption part needs to ensure the security and efficiency of data sharing in the process through variable encryption. Encrypt dynamic data using the CP-ABE algorithm. In the case of multiple sensors periodically acquiring multiple encrypted measurements, the process of obtaining each target trajectory by analysis. The data sharing decryption module is mainly used to verify data integrity and manage data decryption and authorization work and then obtain decryption authority to successfully obtain enterprise financial data sharing data. If the data sharing verification cannot be completed, the user cannot obtain the shared resource.

Encryption is performed on the divided data blocks, and a flexible encryption strategy is adopted according to the characteristics of the data blocks. Static data blocks can traditionally be encrypted using the RSA algorithm, and the dynamic data blocks are encrypted using the CP-ABE algorithm. The advantage of the RSA algorithm is that the encryption overhead is low, and the disadvantage is that the flexibility and confidentiality are not high; the advantages of the CP-ABE algorithm are flexibility, privacy, and dynamics. Dynamic data blocks have higher privacy requirements and smaller data blocks, so they are encrypted using the CP-ABE algorithm. Static data blocks have lower confidentiality requirements and larger data blocks than dynamic data blocks. If the two types of data blocks use a consistent encryption strategy, the dynamic data requirements for security and static data cannot be met. For example, if static data blocks are also encrypted by the CP-ABE algorithm, there are a large number of bilinear operations in the data encryption and decryption process. For more and more mobile devices, there is an additional burden on data sharing.

A trusted third-party TTP performs CP-ABE encryption on dynamic data. The specific process is as follows:

(1) Setup: the algorithm sets TTP to generate parameter 0 as the input of the Setup algorithm, Let $u = \{1, 2, \cdots, n\}$ be the system attribute set space, optionally two p-order cyclic groups G, G_T, bilinear map to $e : G_1 \times G_2 \longrightarrow G_T$, and select the anticollision hash function $H : G \longrightarrow Z_p^*$, optionally $\alpha \in Z_p^*$, $\beta \in Z_p^*$, input parameters $Y = e(g, g)^\alpha$ and generate random

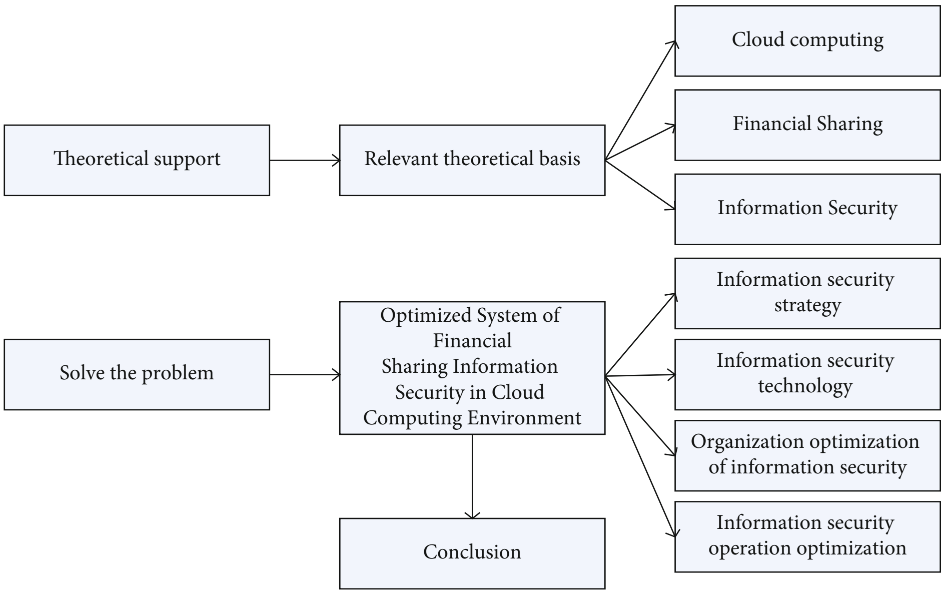
Theoretical support
Relevant theoretical basis
Cloud computing
Financial Sharing
Information Security
Solve the problem
Optimized System of Financial Sharing Information Security in Cloud Computing Environment
Information security strategy
Information security technology
Organization optimization of information security
Information security operation optimization
Conclusion

Figure 1: Technical road map.

values g^{β} is assigned to each attribute, where $\mathrm{t}_{i,j} \in Z_p^*$ $(1 \le i \le n, 1 \le j \le n_i)$, the output master key $T_{i,j} = g^{t_i, j}$, and the public key $PK = (G, g, g^{\beta}, H, Y)$, and the cloud storage system generates the attribute set $\Omega = \{\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_n,\}$

(2) The KeyGen algorithm cloud storage system generates unique identification information g^{u_i} and attribute set $A = \{\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_j,\}$ for each registered user in the group. The user sends the corresponding parameter g^{u_i} and sends $A = \{\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_j,\}$ as an input to the KeyGen algorithm to the trusted third party TTP

$$\mathrm{SK} = \left(D = g^{u_i e/\beta} g^{\alpha/\beta}; \forall \lambda_{\mathrm{j}} \in A : D_k = g^{eu_i} H(\lambda_j)^{rj}, D_k' = g^{rj}\right), \quad (1)$$

$$\mathrm{SK}_k' = \left(D = g^{\alpha + u_i e/\beta}; \forall \lambda_{\mathrm{j}} \in A : D_k = g^{eu_i} H(\lambda_j)^{rj}, D_k' = g^{rj}\right). \quad (2)$$

The trusted third party TTP calculates the private key SK with the global identification information for the user, and the calculation formula of the user private key SK is Equation (3). The GSK is obtained as the group private key $u_0 \in Z_p^*$ and sent to the user in the group synchronously. The group public key is as shown in Equation (4):

$$\mathrm{SK}_{u^i} = \left(D = g^{\alpha + u_i e/\beta}; \forall \lambda_{\mathrm{j}} \in A : D_k' = g^{eu_i} H(\lambda_j)^{rj}\right), \quad (3)$$

$$\mathrm{GSK} = g^{u_0}, v_n = 0 \quad (4)$$

(3) The Encrypt algorithm data belongs to the master DO. The attribute access structure is $W = [W_1, W_2, \cdots, W_n]$. The dynamic data is selected as the plain text data to be encrypted, that is, $m \in G_T$ is the input of the Encrypt algorithm. The C_0 and C_0, C_1, C_2 formulas are calculated and output as follows:

$$C_0 = mY^s e(g, g)^{us} = me(g, g)^{\alpha s + us}, \quad (5)$$

$$C_1 = g^{\beta \cdot s}, \quad (6)$$

$$C_2 = g^{\delta \cdot s}. \quad (7)$$

Extract $s \in Z_p^*$ arbitrarily. Set the root part node of the dynamic data block access structure to s. If the root part node s is the acquisition identifier and the child node is not acquiring the identification status, the part that is not the identifier that is not the leaf can be calculated by budget. Select any $s \in Z_p^* (1 \le s_i \le p - 1)$ and give the tail node a value of s_j and calculate s_j as shown in the formula to set the status of this node as identified.

$$s_j = s - \sum_{i=1}^{j-1} s_i \bmod p. \quad (8)$$

When it is an "OR" gate, it changes any node value under the node and changes the state of the node to recognized. For leaf node s, the cipher text is calculated by the following formula:

$$\begin{cases} C_{i,j,1} = g^{s_i}, \\ C_{i,j,2} = T_{i,j}^{s_i}. \end{cases} \quad (9)$$

Then, the ciphertext CT can be calculated and output by the formula (10), wherein i and j have a value range of $1 \le i \le n, 1 \le j \le n$:

$$CT = C_0, C_1, C_2, \left\{C_{i,j,1}, C_{i,j,2}\right\}. \tag{10}$$

2.3. Risks of Enterprise Financial Sharing in the Age of Cloud Computing

(1) System's own risk: due to the high investment cost of financial shared service center construction, the financial risk of enterprises engaged in financial sharing construction in the era of big data is high. When the financial shared service center is in the early stage of construction, more human investment, capital investment, and equipment investment are needed. At the same time, it is necessary to provide financial support for personnel travel expenses, engineering construction costs, and personnel equipment transfer costs, resulting in relatively high investment in the financial center construction. After the enterprise financial sharing in the era of big data enters the postconstruction, it needs to provide corresponding financial support for equipment maintenance, information system update, and technical personnel management. And under the high capital input cost, financial sharing does not necessarily bring about the expected target benefits, and it is also likely to cause the debt crisis of the enterprise group. In addition, after implementing a centralized management approach to financial sharing, financial personnel changed from a business front end to a back end. Under the influence of such business sensitivity and subjectivity, it is inevitable that business data is incomplete, information data is inaccurate, and false information is generated. There are too many management loopholes in the financial sharing management center

(2) Personnel management risk: in the era of big data, the enterprise financial sharing service center adopts a centralized financial management method. Will not continue to work in the front-end of the line, and the specific business with the various departments of the enterprise is gradually decreasing, so that the financial management personnel can not grasp the specific business data, can only rely on the relevant data for analysis and integration, and thus the staff. The first-line business capability has gradually declined. Compared with the financial management work of the front-end frontline, the standardized management mode of the financial sharing center makes the financial sharing workflow very strict and boring. Under the long-term work of high-complexity financial data, documents, and reports, the financial staff will inevitably lose patience and enthusiasm for work. There is a situation in which the work attitude is not serious and the job is changed. The phenomenon of high turnover ratio of financial personnel makes it difficult for enterprises to reselect new employees for management, because of the unskillful business of new employees, and the integration of financial data of enterprises is wrong

(3) Information security risk: under the mode of centralized management of financial business, the information transmission and processing traffic of enterprises will increase correspondingly. As the amount of information rapidly expands, it will inevitably lead to congestion of enterprise information channels, leading to corporate finance. Information processing efficiency is affected. Since the processing capacity of the enterprise financial shared service center is generally 100,000 TB, the efficiency of the data filtering, screening, and analysis functions of the financial shared service center becomes more and more important. At present, enterprises are in a semi-intelligent state in the filtering, analysis, and screening of information data, failing to achieve fully intelligent management, making it difficult to effectively handle complex information and exchange requirements. In order to facilitate financial sharing management, some enterprises have developed and shared the financial sharing network, which makes the enterprise financial network vulnerable to information leakage and virus intrusion, resulting in system flaws and data theft

2.4. Construction of Information Security Evaluation System for Financial Sharing. When evaluating financial shared information security systems, the following principles should be followed when designing assessment indicators. The design of the indicators should be carried out on the premise of scientific basis. It must have a theoretical basis as a support. According to the specific situation of information security of the financial sharing center, the selection of indicators should be representative. If the scientific principles are not followed, the evaluation results of the selected indicators will mislead the actual situation. There are many indicators that can evaluate the financial security center information security system. If too many indicators are selected, the economic benefits are not high, and we cannot evaluate all aspects of the information security system. Therefore, it is necessary to select representative indicators that reflect the operation and internal laws of the financial shared information security system based on the importance of importance. When design indicators evaluate the system, if the selected indicators only value the results, the actual selection of the data is not good, and the choice of indicators is not reasonable. Therefore, when you design indicators, you need to refine each of them in terms of development quality, development capability, and suitability. In these aspects, an information security assessment indicator system for financial sharing is proposed.

Financial sharing mainly relies on the advantages of information technology and data technology and interactively sharing data to implement financial sharing reform within the enterprise through the implementation of the new management model concept. When financial sharing is implemented in the era of big data, it is basically to integrate different enterprises or different accounting units, so that decentralized financial work can be integrated and integrated and then the centralized financial analysis, analysis,

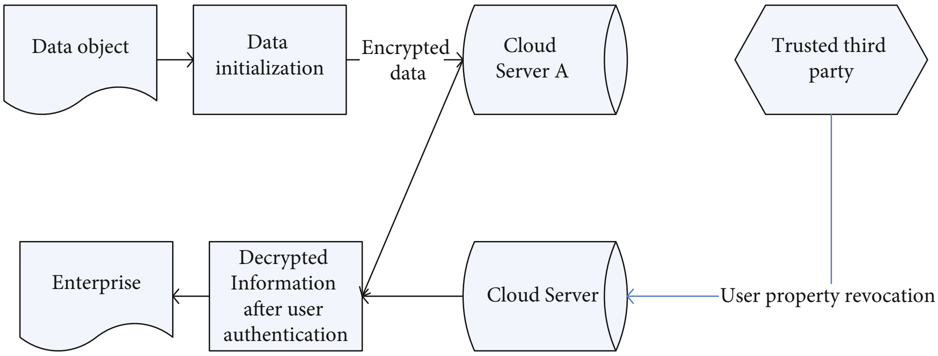

Figure 2: Experimental steps.

and utilization of complex financial data. The earliest enterprises in China that began to use the concept of financial sharing to carry out internal financial management reforms were Haier Group and China Telecom. And with the in-depth development of the concept of financial sharing, the financial sharing level of Haier Group and China Telecom has been continuously improved. Affected by the trend of large-scale enterprises using financial sharing to carry out financial reforms, small- and medium-sized enterprises have also begun the construction and reform of financial sharing. Compared with other financial management methods, financial sharing can effectively integrate and analyze different types of accounting work data of the enterprise. This enables companies to form a correct understanding of accounting data and propose a rationalized corporate development strategy.

3. Experiments

3.1. Experimental Data Set. The data comes from the common word database of Sogou input users and used to simulate and upload corporate financial data and stored data. The data is mainly in text form. The common word file for each user is small, but the number of files is large due to the large user base. In an actual cloud computing environment, not only large files are stored but also a large number of small files are stored. The DBMS divides the data into n shares, each stored in a different service provider (DAS). The data here is the value of the attribute that the user wants to hide on an untrusted server, and the DBMS is responsible for generating a random polynomial function of the same degree for each valuable attribute value. This polynomial is not stored in the data source but is generated by the DBMS when the user's query is accepted.

3.2. Experimental Environment and Conditions. The hardware configuration uses the CPU as the Intel Core i5-7120M 2.50 GHz, the memory is 16.00 GB, and the operating system is a Win7-64 bit computer for the analog data sharing process. In the simulation experiment, Cloud Server1 is used as a cloud server, and Enterpise is used as a client on a computer at one end. The data sharing process was simulated by performing information exchange between the cloud server and the client user. The simulation platform is NetBeans8.0 platform, JDK1.6, and the simulation is implemented by Java programming. The encryption algorithms used are based on the open source code base JDBC2.0.0 (Java pairing-based cryptography library), which is used to implement repetitive linear matching and functions such as the CP-ABE algorithm and PRE encryption and decryption algorithm in cryptography. On the software NetBeans 8.0 platform, the data segmentation part is simulated using the commonly used Java object-oriented programming language. The same method is used for the data encryption part and the data decryption part.

3.3. Experimental Procedure. In the cloud computing, the security of enterprise financial data security storage requires not only users with only permission to access shared data but also for cloud servers and users without permissions. The solution uses ciphertext for cloud storage, which makes it difficult for an attacker to obtain complete shared data and ensures that illegal visitors cannot obtain shared resources. Not only that, if there is a data leak on the cloud server that uses the PRE secondary proxy reencryption technology to change or update the active data for a trusted third-party TTP when a key leak is discovered or the administrator user does not exist to request the user to be revoked, users who revoke after undoing cannot continue to share data. Even if a revoked user throws access to and can view the decrypted Jintai data, due to the lack of a dynamic data file, the integrity of the file cannot be verified and all file information cannot be viewed. The revoked user cannot continue to access the shared data to ensure the confidentiality of the shared data, and the experimental steps are shown in Figure 2.

The plaintext attack game was selected to set the game character, cloud server Cs was defined as challenger s in the system, and user A was defined as the opponent User access system. The security of a trusted storage strategy was demonstrated. ① Start phase Start. Challenger s selects parameter η of the secure partition file and a sufficiently large CP-ABE algorithm parameter λ to encrypt the dynamic data plain text m and hand the dynamic public key and static key to the opponent A. ② Query phase Step1. The attacker A submits the challenge plain text W_0 and W_1, and the access tree w and asks the challenger s about the user dynamic attribute private key SK corresponding to the

Table 1: Accurate query time comparison chart.

Contrast algorithm	20.50	20.00	19.20	18.00	21.00
The algorithm in this paper	16.84	15.34	14.10	13.98	15.10

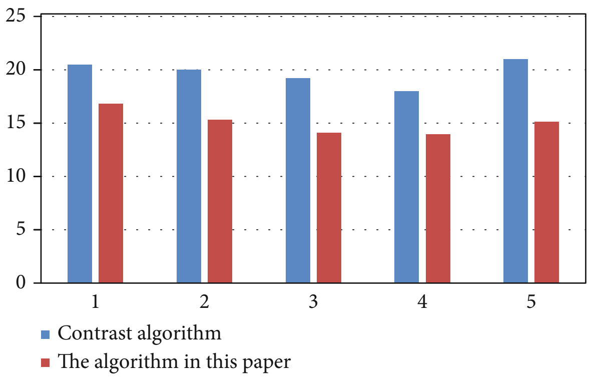

Figure 3: Algorithm comparison chart.

Table 2: The main financial index of the company.

Contrast algorithm	Total number of listed companies	Disclosure of the number of XBRL companies	Percentage
Shanghai stock exchange	963	919	95.43%
Shanghai stock exchange A	909	909	98%
Shanghai stock exchange B	1339	10	18.52%
Shenzhen City A	1009	1325	98.95%

dynamic data attribute set. If the queried dynamic data attribute set does not satisfy the requirements of the dynamic data access tree, attacker A sends the plain text W_0 and W_1 and access tree w to challenger s. Challenger s performs a coin flip experiment to randomly generate parameter $\beta \subset \{0, 1\}$ and segmentation parameter $\beta \subset \{0, 1\}$, encrypt plain text M_β, and send dynamic cipher text c to opponent A. ③ Query phase Step2. Attacker A continues to query the challenger's dynamic data attribute set. ④ Guess stage Guess. The challenger s guesses the dynamic data cipher text c, and the response result is only two $\beta' = 0$ or $\beta' = 1$ equal. At that time, $\beta' = \beta$ determines that the enemy A wins, and at this time, the probability of winning the enemy A is defined as the winning probability $\mathrm{Adv}(A) = |\Pr [\beta' = \beta] - 1/2|$. Under normal circumstances, the probability of an enemy successfully decrypting the game is about zero, which is negligible, indicating that the proposed trusted distributed storage strategy can guarantee the security of shared data.

Table 3: The staffing requirements of project implementation.

Post	Role	Require	Staffing needs
Project management and business analysis	Project manager	Advanced	1
	Demand management	Advanced	1
	System engineer	Advanced	2
Software framework design, market software integration, performance optimization	Configuration engineer	Intermediate	1
	Software engineer	Advanced	1
	Software engineer	Intermediate	2

Table 4: The cost of the cloud computing model is analyzed with 3 years as a construction cycle and the analysis.

Cloud computing mode			Traditional mode		
The first year	The ensuing year	The third year	The first year	The ensuing year	The third year
988	988	988	33800	0	0
0	0	0	60000	0	0
0	0	0	2400	2400	2400
0	0	0	6000	6000	6000
0	0	0	5000	0	0

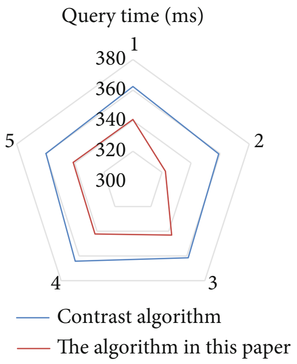

Figure 4: Range query time comparison chart.

4. Discussion

4.1. Experimental Results and Comparison. The experiment uses the JAVA language to simulate data retrieval and data encryption and decryption processes. A comparable assessment was made between shared NetDB2 using the company's private sharing algorithm and NetDB2 using the Blowfish encryption algorithm. This comparison shows a comparison between three types of queries, namely, exact queries and aggregated queries.

Table 5: Range query time comparison table.

Contrast algorithm	362.36	359.00	361.41	364.22	359.83
The algorithm in this paper	340.801	322.32	343.10	342.23	341.12

4.1.1. Accurate Inquiry. The experiment compares the data retrieval time cost of the shared NetDB2 model established by the secret sharing algorithm and the NetDB2 model established by the blowfish algorithm in the process of exact matching algorithm. Table 1 and Figure 3 show that the algorithm consumes more time than the private sharing algorithm because of the time loss of the blowfish algorithm during decryption.

The results of the data retrieval in the case of different copies of the secret sharing algorithm in the shared NetDB2 were also evaluated. As the number of copies of data increases, the time for data retrieval is also increasing. On the other hand, as the number of copies of data increases, the security level of the data increases, because DAS needs to obtain more values to see the data hidden on the DAS. The main financial index of the company is shown in Table 2.

The staffing requirements of project implementation are shown in Table 3.

The cost of the cloud computing model is analyzed with 3 years as a construction cycle, and the analysis results are shown in Table 4.

4.1.2. Scope Query. Set the two algorithms to search within the same data range (1000~9000). Figure 4 shows that the decoding operation in NetDB2 and the process of retrieving different values from the data source take longer than retrieving the same value from different shares in shared NetDB2. From the experimental results in Table 5, the shared NetDB2 model has higher retrieval efficiency than the NetDB2 model for different data retrieval methods, but the shared NetDB2 model also has certain drawbacks, that is, the retrieval time will follow the number of copies in the secret sharing algorithm. Increases and increases, but as mentioned earlier, the increase in the number of copies also increases the security of the system to a certain extent, which allows the attacker to obtain more copies to obtain data.

4.2. Experimental Conclusions. From the above chart, financial security is very important to the enterprise. According to the trust allocation policy, the solution does not trust any cloud servers and opens and stores encrypted data, which solves the problem of trust concentration during data storage. By using the data segmentation method, the original data is divided into dynamic data and static data according to certain rules and are stored in different cloud servers. For dynamic data, the CP-ABE encryption method can make the access structure of the entire sharing process more flexible and meet the "one-to-many" requirements of data sharing in the cloud environment. The static data uses the traditional RSA encryption method, so that the calculation of encryption and decryption is lower than the complete CP-ABE encryption and decryption as shown in Figure 5. Data is divided into dynamic data and static data, which are encrypted using attribute-based encryption and symmetric encryption, respectively, and stored in different cloud environments. It not only reduces the risk of cloud servers leaking shared data but also reduces the amount of computing and decryption of the system as shown in Figure 6.

But, we still have to establish a risk assessment system. In order to ensure risk reduction and avoid financial sharing systems, companies should establish a corresponding evaluation system to make full use of the data information on the platform. A comprehensive assessment of the risks that the company can generate, enabling the company to develop

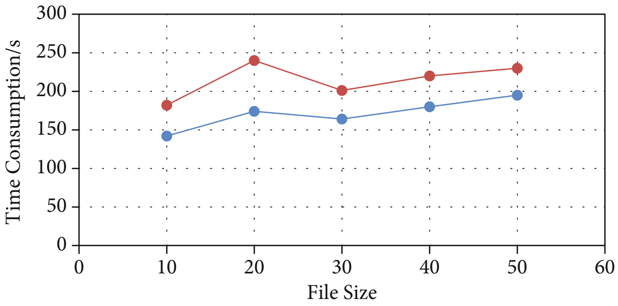

Figure 5: Different file size encryption time consumptions.

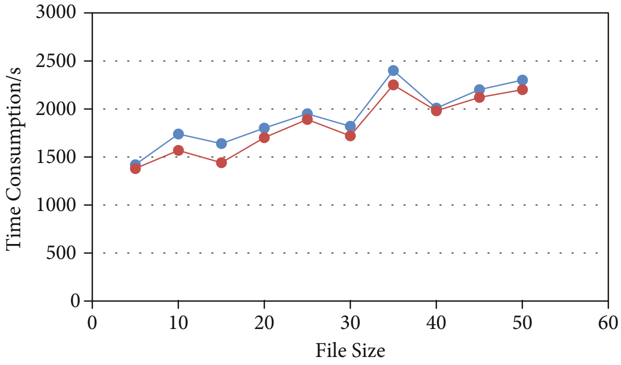

Figure 6: Data segmentation and computational cost change diagram.

Table 6: The evaluation results.

Secondary	One-level	Section
Like	Two stage	(4,5]
It's better	Three-level	(3,4]
Beyond compare	Level four	(2,3]
Appraise	Pyatyi	(1,2]

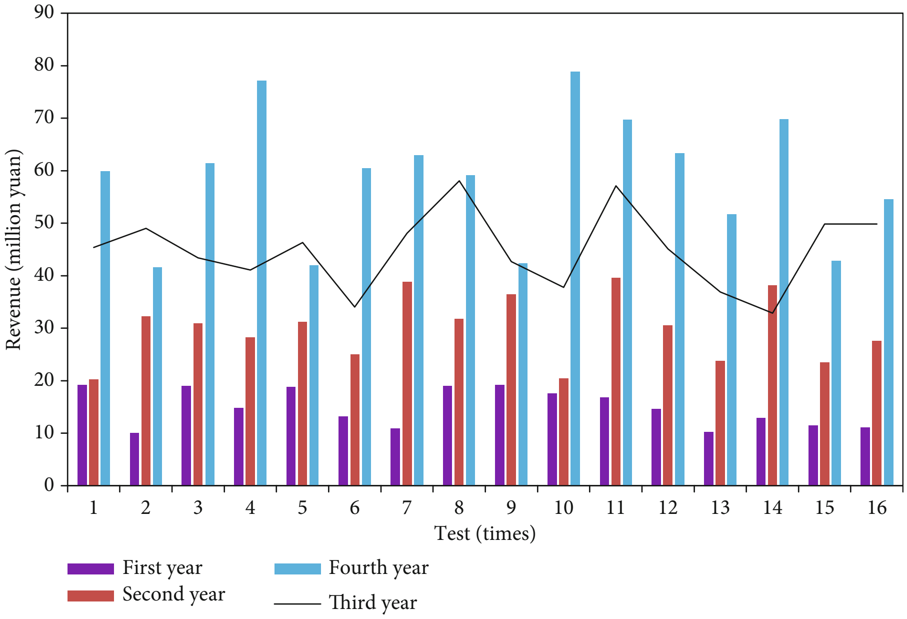

FIGURE 7: The company income after the implementation of this study scheme.

effective measures to avoid losses caused by risk issues. After the completion of the construction of the financial sharing center, the enterprise shall conduct corresponding performance evaluation, evaluate the investment efficiency of the enterprise and improve the operational efficiency of the enterprise. When using the system, senior leaders should establish a management system and interpret their processing procedures. We coordinate the relationship between employees in each link, reduce the risk of using the system, and strengthen the management of financial personnel. When the company expands, the financial staff should also keep up with the development trend and improve the professional level. Finance personnel must delve into the knowledge of the sharing center and become familiar with other knowledge related to the center to ensure that the financial sharing center can proceed smoothly. The financial position of an enterprise is the assets and equity of the enterprise at a certain time and is an expression of the movement of funds at a relatively static state. We grasp the financial status of the company's subsidiaries, pay attention to its changes, respond in a timely manner, and promote the smooth operation of the financial sharing center. Relevant staff members should also communicate with the local tax authorities in a timely and effective manner to ensure that the company scientifically handles tax-related issues, thereby avoiding losses caused by legal problems. Cloud service QoS evaluation metrics such as "Service Credit" indicators generally indicate a comprehensive service request evaluation of a service provider after the end of the service transaction. This section divides the evaluation level into five levels: "very good," "better," "general," "medium," and "relatively poor." The evaluation results are shown in Table 6.

The company income after the implementation of this study scheme is shown in Figure 7.

5. Conclusions

The purpose of financial sharing information security evaluation is to improve the information security in the process of financial sharing of enterprise groups and improve the level of financial sharing information security management. Therefore, we must pay attention to the use of financial sharing information security evaluation results. For the difference between the result and the target, it is necessary to carefully analyze the cause of the difference and the reason for the low level of information security and provide reference for the next year's financial shared information security management. The financial sharing information security evaluation reflects the real implementation of the financial sharing information system security, and based on the principle of information security, reasonably evaluates the information security situation of the financial sharing center, and judges whether the financial sharing information security optimization has achieved the expected effect. Whether the resources used to optimize the information security system are valid. The investigation is divided into two aspects. On the one hand, whether the configuration of the information security protection system of the financial sharing center meets the actual needs of financial sharing information security; on the other hand, whether the efficiency of resource utilization is maximized. By constructing a financial shared information security evaluation index system, comprehensively evaluate the specific situation of the information security system of the financial sharing center in the cloud computing environment and the impact on the long-term development of financial sharing. The evaluation results of the financial shared information security system can not only serve as an assessment basis for the implementation but also provide suggestions for the optimization of the information security protection system in the future, thus improving the information security protection system of the financial sharing center.

This paper to build thorough information perception, comprehensive intelligent service cloud computing system as the goal, to cloud computing information multisource heterogeneous, noncertainty, massive features as the starting point, analyzed the new problems facing intelligent information processing in cloud computing environment, new needs, combined with the current development of sensor network, and carry out the cloud computing information fusion-related basic theory and key technology. This paper focuses on the thorough analysis of the nature of cloud computing from the perspective of data information, and with the information resource development chain "a information data a knowledge a wisdom" high-level data information evolution mechanism discusses the information complete state evolution of cloud computing and its law, its goal is to achieve a complete effective intelligent information processing system in the cloud computing environment. The structure will play a reference and guiding role in the future development of cloud computing information integration. This paper combines the theory of financial shared services and information security theory to provide a reference for the construction of financial sharing information security for the same type of enterprises. For some enterprises that have not yet established a financial sharing service center, we can learn from the establishment of the financial sharing information security system in this paper and provide reference for enterprises to avoid the same types of risks and problems, for the financial sharing information that has been established and has begun to be implemented. For the enterprises of the system, the four dimensions related to the optimization of the information security system described in this paper can be combined with the actual situation of the enterprise to formulate corresponding risk aversion measures. In summary, this paper is devoted to the analysis of the security problems existing in the operation of financial shared services from the actual financial situation of the enterprise and finds a breakthrough point to solve the problem, which has dual practical significance and theoretical significance.

The problem of information fusion in the cloud computing environment is a basic scientific problem in the intelligent information processing of cloud computing. Its basic task is to synthesize the information flow of a large variety of perceptual devices to form an intelligent model with higher characteristics of monitoring and control environment. Its research level directly determines the ability of cloud computing intelligent services. Among them, the key lies in the architecture and algorithm of information integration. Under the cloud computing environment, it should realize the effective integration of the information collected in the physical world and the information world, provide better decision-making, achieve the purpose of comprehensive intelligent services, and meet its spatial and temporal sensitivity and timeliness. In the past, the research on financial sharing of enterprise groups was mainly based on the financial process reengineering and the construction of financial sharing centers. There were few researches on how to implement financial sharing, and the security of financial shared information resources has become a part that cannot be underestimated. This paper proposes information security protection under the new situation of financial sharing, which has certain practical significance. The financial sharing information security assessment system is results-oriented and strengthens the information security construction of enterprise groups. We create a safe and secure environment for financial sharing of corporate groups. Although there are a large number of enterprises that have begun to practice financial sharing services in China, financial sharing is still a new type of industry. In order to study the development of financial sharing in depth, it is not enough to have management and finance. It also needs the support of many disciplines, especially information technology. The financial shared information security system constructed in this paper needs to be further strengthened through practice. The research in this paper may not be comprehensive enough and needs further in-depth refinement.

Data Availability

This article does not cover data research. No data were used to support this study.

Conflicts of Interest

The author declares that he has no conflicts of interest.

Acknowledgments

This work was supported by the Quality Edition Promotion Project of Zhanjiang Science and Technology College: Data Intellectualized Finance Teaching team (project no.: PPJH202107JXTD).

References

[1] L. Chunlin, T. Jianhang, and L. Youlong, "Hybrid cloud adaptive scheduling strategy for heterogeneous workloads," *Journal of Grid Computing*, vol. 17, no. 3, pp. 419–446, 2019.

[2] M. Montagnuolo, P. Platter, A. Bosca, N. Bidotti, and A. Messina, "Realtime semantic enrichment of video streams in the age of big data," *SMPTE Motion Imaging Journal*, vol. 128, no. 1, pp. 1–8, 2019.

[3] J. Zhuang and C. Xu, "Profit-sharing and financial performance in the Chinese state enterprises: evidence from panel data," *Economics of Planning*, vol. 29, no. 3, pp. 205–222, 2018.

[4] Q. Yao, H. Ao, T. Huang, and H. Jie, *The research of implementing enterprise financial shared service center information system*, Nrnaonal Onfrn on Omng Marmn, 2018.

[5] M. Ali, R. Dhamotharan, E. Khan et al., "SeDaSC: secure data sharing in clouds," *IEEE Systems Journal*, vol. 11, no. 2, pp. 395–404, 2017.

[6] K. J. Dibete, O. C. Potokri, and B. Roberts, "Policy compliance of SGB members on their financial management roles in selected no-fee schools in Limpopo Province of South Africa,"

International Journal of Educational Management, vol. 32, no. 5, pp. 799–812, 2018.

[7] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," *IEEE Transactions on Information Forensics & Security*, vol. 13, no. 4, pp. 912–925, 2018.

[8] M. Jin, Y. Wang, and Y. Zeng, "Application of data mining technology in financial risk analysis," *Wireless Personal Communications*, vol. 102, no. 4, pp. 3699–3713, 2018.

[9] A. Wu, D. Zheng, Y. Zhang, and M. Yang, "Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing," *Sensors*, vol. 18, no. 7, p. 2158, 2018.

[10] D. Nada, M. Bousbia-Salah, and M. Bettayeb, "Multi-sensor data fusion for wheelchair position estimation with unscented Kalman filter," *International Journal of Automation and Computing*, vol. 15, no. 2, pp. 207–217, 2018.