Hindawi
Security and Communication Networks
Volume 2023, Article ID 9763947, 1 page
https://doi.org/10.1155/2023/9763947

Retraction

Retracted: Cloud Computing Storage Data Access Control Method Based on Dynamic Re-Encryption

Security and Communication Networks

Received 26 December 2023; Accepted 26 December 2023; Published 29 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] X. Chen, D. Zeng, S. Pang, and F. Jun, "Cloud Computing Storage Data Access Control Method Based on Dynamic Re-Encryption," *Security and Communication Networks*, vol. 2021, Article ID 4953074, 10 pages, 2021.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 4953074, 10 pages
https://doi.org/10.1155/2021/4953074

Research Article

Cloud Computing Storage Data Access Control Method Based on Dynamic Re-Encryption

Xiaodan Chen,[1] Desheng Zeng,[1,2] Shuanglong Pang,[1] and Fu Jun [2]

[1]*School of Information Engineering, Guangdong Innovative Technical College, Dongguan 523960, Guangdong, China*
[2]*School of Artificial Intelligence, The Open University of Guangdong, Guangzhou 510091, Guangdong, China*

Correspondence should be addressed to Fu Jun; jfu@gdrtvu.edu.cn

Received 29 October 2021; Revised 11 November 2021; Accepted 18 November 2021; Published 9 December 2021

Academic Editor: Jian Su

In order to improve data security, ensure user privacy, and solve the problems of low data access control accuracy, long time consumption, and high energy consumption in traditional methods, a cloud computing storage data access control method based on dynamic re-encryption is proposed. The principal component analysis method is used to reduce the dimension of the cloud computing storage data, and the random forest algorithm is further used to classify and process the cloud computing storage data according to the processing results. On the basis of data preprocessing, an access control tree is established to obtain the correlation of data nodes. Finally, the dynamic re-encryption method is used for data security state transformation, and the data access control of cloud computing storage is realized through key generation, encryption, re-encryption key generation, and decryption. The experimental results show that the data access control accuracy of the method in this paper is high, time consumption is small, and energy consumption is small, and it is more suitable for cloud computing systems with huge data and information.

1. Introduction

With the rise and development of cloud computing, Internet of Things, big data, and other new computing technologies, global informatization has caused profound changes in the world, and the national economy, social development, and people's life are unprecedentedly dependent on information technology [1–3]. At the same time, the openness and information sharing of the internet have posed a serious threat to global information security, and information security has become one of the main contents of national security. Access control is an important basis for protecting data confidentiality, integrity, availability, and legitimate use. It is one of the key strategies for network security and resource protection [4–6]. However, with the continuous expansion of the network scale, the number of users and data in the cloud computing environment has increased sharply, and users' demand for data, personal privacy, and permission granularity has been increasing. There is an urgent need to realize fine-grained dynamic authorization for large-scale users; the mode of security requirements has changed from a single user on both sides of the communication to a multiparty communication mode in which at least one party is multiuser, and from "same-domain" communication to "cross-domain" communication, the traditional access control is facing new challenges [7].

In recent years, scholars at home and abroad have carried out extensive research on data access control methods and achieved a large number of research results. Liu et al. [8] proposed a big data access control method based on the blockchain. Firstly, the basic principle of blockchain technology is described, and the attribute-based access control model is formally defined. A big data access control architecture based on blockchain technology is proposed, and its basic framework and access control process are described and analyzed in detail. In order to ensure the operability, reviewability, and verifiability of access control information, the access control strategy and entity attribute information management method based on the blockchain transaction are proposed. The access control method based

on the intelligent contract is adopted to realize user-driven, transparent, dynamic, and automatic access control for big data resources. The validity of this method is verified by simulation, and the research content is summarized and prospected. Wang et al. [9] proposed a Hadoop big data access control model based on data sensitivity. The model uses data content, mode, and data sensitivity to strengthen the access control strategy. In assessing data sensitivity, the user intervention is minimal, and the access control strategy can be adjusted according to the changes in data sensitivity caused by the addition and deletion of datasets. The experimental results show that the model can enhance the access control of nonmultimedia datasets with less overhead and solve the problem of insufficient security of the data access control model. Fu and Zhu [10] put forward the idea of applying blockchain technology to database access control from the blockchain hierarchy, the logic level of access control flow, and the principle of access control implementation. Combined with blockchain technology, the implementation mechanism of database access control based on the blockchain is designed, and on this basis, the performance of the database access control system based on the blockchain is evaluated and provides a complete architecture for the application of blockchain in database access control; access authority and access behavior strengthen authentication and supervision and effectively improve the ability of database access control.

The above several existing data access control methods have basic application requirements, but the traditional methods focus on the deletion of sensitive data and blockchain technology, ignoring the dimensionality reduction of data, and the traditional methods are all single encryption, whose encryption effect is not ideal enough to achieve wide applications, and the application adaptability needs to be further strengthened. In order to optimize the access control precision, time consumption, and energy consumption, this paper proposes a dynamic re-encryption-based access control method for cloud computing storage data.

2. Cloud Computing Storage Data Preprocessing

With the rapid development of cloud computing, software technology and architecture have changed significantly in the cloud environment. Users begin to migrate systems and data to the cloud environment to meet the demand for on-demand access, load balancing, and disaster tolerance. However, the cloud environment also faces attacks such as API, external interfaces, and vulnerabilities, so the problem of data security access and storage in the cloud environment is increasingly serious. Ensuring the security of data stored in the cloud environment is an urgent problem to be solved. The emergence of cloud computing has greatly promoted the development of internet technology in our country. Cloud computing is developed from distributed computing, parallel computing, and grid computing. It is usually a large cluster of servers, including computing servers and storage servers. On the one hand, it solves the contradiction of increasing IT investment and low utilization of IT resources.

More and more systems and data are deployed and stored in the cloud. With the rapid development of cloud computing, the amount of data has reached the level of PB. However, due to the openness of the cloud platform itself, there are serious security risks in the systems and data in the cloud environment, which mainly include the following aspects: first, the system itself is insecure, the use of the system in the cloud environment mainly relies on the external interfaces to provide services, and the system itself does not set the access rights of each external interface so that the data are leaked or destroyed due to human error or hacker attack. Second, network attacks for various purposes: because cloud servers store a large amount of data, cloud servers are increasingly becoming the targets of hackers. Hackers steal information, operate business, and modify data through traditional phishing, fraud software, and other vulnerabilities, thus increasing the attack surface and further launching attacks against other users to steal more data. In order to avoid this kind of risk, this study proposes a new method of cloud computing storage data access.

2.1. Cloud Computing Storage Data Dimensionality Reduction. Before cloud computing storage data access control, related data are generally collected. However, the collected cloud computing storage usually has the characteristics of high dimensionality. In order to improve the efficiency of cloud computing storage data access control, high-dimensional cloud computing is required. Data are stored for dimensionality reduction processing [11, 12]. This article mainly uses the principal component analysis method to reduce the dimensionality of cloud computing storage data. The specific steps are as follows.

First, construct a cloud computing storage data observation matrix G, which is an $n \times m$-type matrix, and its specific expression is

$$G_{n\times m} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ g_{n1} & g_{n2} & \cdots & g_{nm} \end{bmatrix}. \tag{1}$$

Among them, n represents the row rank of the matrix; m represents the column rank of the matrix.

According to the matrix constructed by formula (1), the cloud computing storage data are standardized:

$$\begin{cases} x_u = \alpha \dfrac{t_z}{z} - \dfrac{t_z}{z} u - \left(1 + x^2\right)\omega_x, \\ \\ y_v = \beta \dfrac{t_z}{z} - \dfrac{t_z}{z} v - \left(1 + y^2\right)\omega_y. \end{cases} \tag{2}$$

Among them, x_u and y_v both represent principal component data; α and β both represent principal component contribution rate; t_z represents high-dimensional data characteristics; ω_x and ω_y both represent the attribute category of the data.

Let D_i denote the correlation coefficient matrix between cloud computing storage data samples, and its expression is as follows:

$$D_i = \begin{pmatrix} d_{11}^i & d_{12}^i & \cdots & d_{1n}^i \\ d_{21}^i & d_{22}^i & \cdots & d_{2n}^i \\ \cdots & \cdots & \cdots & \cdots \\ d_{n1}^i & d_{n2}^i & \cdots & d_{nm}^i \end{pmatrix}. \tag{3}$$

Among them, i represents the distance between rows of high-dimensional data. The eigenvector $D_i = (d_{i1}, d_{i2}, ..., d_{iN})$ of matrix D_i can be obtained by the Jacobian method, where N represents the total number of eigenvectors.

In order to simplify the calculation steps, X and Y are used to represent standardized cloud computing storage data; then, the correlation coefficients of the standardized cloud computing storage data are $X(d_i)$ and $Y(d_i)$ [13], which can be calculated by the following formula:

$$\begin{aligned} X(d_i) &= \frac{x_1(d_i) \cdot x_2(d_i)}{\|x_1(d_i)\| \cdot \|x_1(d_i)\|}, \\ Y(d_i) &= \frac{y_1(d_i) \cdot y_2(d_i)}{\|y_1(d_i)\| \cdot \|y_2(d_i)\|}. \end{aligned} \tag{4}$$

Among them, $x_1(d_i)$ and $x_2(d_i)$ both represent the difference feature of the data information volume; $y_1(d_i)$ and $y_2(d_i)$ both represent the correlation feature of the data information volume.

The principal component analysis method [14] is used to obtain H principal components in the cloud computing storage data. The specific principal components can be calculated by the cumulative contribution rate of the data:

$$W_{d_i}(h) = e^{\|X(d_i) - Y(d_i)\|}. \tag{5}$$

Among them, e represents the cumulative contribution rate of the principal components.

The original cloud computing storage data are standardized and input into the principal component expression to obtain the principal component scores of different data. According to the calculation results, the data with high scores can be retained to realize the dimensionality reduction processing of high-dimensional cloud computing storage data [15, 16].

2.2. Cloud Computing Storage Data Classification. According to the dimensionality reduction processing results of cloud computing storage data, they are further refined and classified. The attributes of cloud computing storage have different weights. The attributes of cloud computing storage data are integrated, and the random forest algorithm is used to achieve cloud computing storage data classification, which provides theoretical support for subsequent cloud computing storage data access control research [17–19].

When introducing feature weighting to calculate the information gain of the current attributes of cloud computing storage data, the relevance of this feature to the classification result can be included [20, 21]. The setting of feature weights for each dimension in the system depends on the characteristics of the data stored in cloud computing. Different weights are set for the input data of each dimension so that the dimensionality reduction results of the cloud computing storage data can be effectively integrated into the random forest algorithm. As long as the weight coefficients of each dimension of the data are allocated reasonably, the problem of tilting classification evaluation indicators can be well overcome, and the effect of cloud computing and storage data classification can be improved globally [22–24].

When the random forest algorithm is used to classify and process cloud computing storage data, in the classification training stage, the information gain of cloud computing storage data is described as

$$E_{ij} = P_{\max} \times (1 - g_i). \tag{6}$$

Among them, g_i represents the amount of sampled data; $P_{\max}$ represents the maximum value of the empirical entropy of the training dataset, and its calculation formula is

$$P_{\max} = \frac{\sum_{i=1}^{N} p(u) \times p_i}{(1/n)}. \tag{7}$$

Among them, p_i represents the entropy index; $p(u)$ represents the conditional entropy function of the training data, and its calculation formula is

$$p(u) = \sum_{j=1}^{N} h_j(u) \times \delta_j. \tag{8}$$

Among them, $h_j(u)$ represents the number of data attributes; δ_j represents the training subset.

Substituting the data feature weighting coefficient in formula (8) to improve the information gain index, it can get

$$x\prime = p(u)\left(x_{\max}^t - x_{\min}^t\right) + x_{\text{best}}^t. \tag{9}$$

Among them, $x\prime$ represents the result of the optimal selection of the information gain feature; $x_{\max}^t$ represents the maximum value of the weighting coefficient; $x_{\min}^t$ represents the minimum value of the weighting coefficient; x_{best}^t represents the optimal value of the weighting coefficient. Under normal circumstances, these three parameters are all positive numbers [25]. It can be seen from formula (9) that the larger the value of $p(u)$, the higher the value of $x\prime$. According to the calculation result of $x\prime$, the cloud computing storage data classification can be realized [26–28]. Figure 1 is a flowchart of cloud computing storage data classification.

According to the above steps, different types of cloud computing storage data can be obtained after dimensionality reduction processing, which provides a solid data foundation for subsequent cloud computing storage data access control [29].

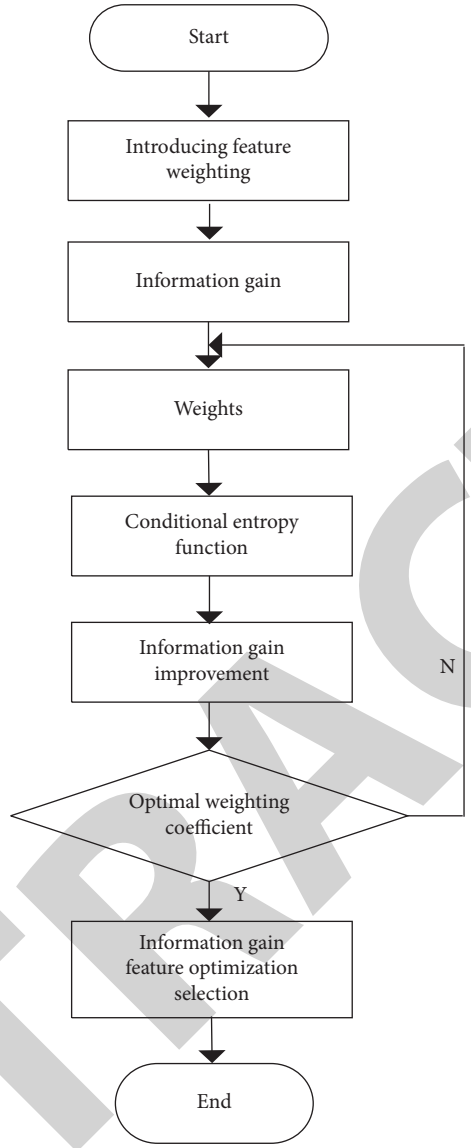

Figure 1: Cloud computing storage data classification flowchart.

3. Cloud Computing Storage Data Access Control Method

Based on the results of cloud computing storage data preprocessing, the data access control method is researched. This paper divides the data access control link into the steps of establishing an access control tree, initialization, key generation, encryption, re-encryption key generation, and decryption. Through multistep encryption and decryption processing, the security of user data is guaranteed, and the user's privacy needs are met. The access control tree is used to obtain the correlation of data nodes and optimize the effect of data access control. In order to improve the efficiency of data access control, I divide the re-encryption key into two parts. One part re-encrypts the original data in cloud computing, and the other part authorizes the decryption of the ciphertext and designs the decryption steps to realize the design of the cloud computing storage data access control method.

3.1. Access Control Tree Construction. In the study of cloud computing storage data access control, first, an access control tree is established to obtain the correlation of data nodes, and the security of data on different nodes is improved [30]. The access control tree is established according to the ciphertext strategy. In the ciphertext strategy, the user's key will be associated with an unlimited number of attributes, which are often represented by strings. When an entity wants to encrypt a plaintext into a ciphertext, first, it needs to define an access structure, which consists of a set of attributes. Decryption can be performed only after the attributes of the key held by the user match the access structure in the ciphertext. The access structure of the ciphertext strategy is a monotonous access tree, which is composed of thresholds and leaves, and the leaf nodes represent attributes [31, 32].

Let tree T represent an access structure, each nonleaf node in the tree represents a threshold, and each threshold

has a threshold. Let N_z be the number of children of node z and K_z be the threshold of node z; then, $0 < K_z < N_z$. When $K_z = 1$, node z is an OR gate. When $K_z = N_z$, node z is an AND gate. Each leaf node z in the tree represents an attribute, and the threshold K_z of the leaf node is always 1.

Suppose the parent node of node z is P_z, and use $\alpha(z)$ to represent the attribute represented by the leaf node when z is a leaf node. Use $\mu(z)$ to represent the number of z's position in the tree. In an access structure, the number of each node z is unique. The visit structure defines the order of all child nodes in tree T and numbers the child nodes.

Let T_σ be an access control tree rooted at σ, which is a subtree of tree T. If a set of attributes ϑ satisfies the access control tree T_σ, then $T_\sigma(\vartheta) = 1$ is defined. When z is not a leaf node, calculate function $T_{z_l}(\vartheta)$ through recursion, where z' is all child nodes of node z, and at least z^2 child nodes return 1 in function $T_{z_l}(\vartheta)$. When z is a leaf node, if and only if $\alpha(z) \in \vartheta$, return 1. If there is a group of attributes ϑ that satisfy the aforementioned conditions, it means that this group of attributes ϑ satisfies the access control tree T_σ. An example diagram of the access control tree is shown in Figure 2.

3.2. Cloud Computing Storage Data Access Control Method Based on Dynamic Re-Encryption. Under the traditional data access control method, once the data are re-encrypted by the ECS, the data owner loses control over the data, the authority of the agent is too large, and the efficiency of data access control is not high due to the large amount of calculation of the encryption key. For this reason, this article divides the re-encryption key into two parts: one part re-encrypts the original data in cloud computing, and the other part is used as an authorization to decrypt the ciphertext. When the sender confirms the recipient's identity, it sends it directly to the recipient. The receiver can obtain the plaintext by using its own private key, re-encrypted ciphertext downloaded from the cloud, and authorization to decrypt the ciphertext.

Specifically, the dynamic re-encryption algorithm is an algorithm that combines the advantages of laziness and complete re-encryption. The main principle of this algorithm is as follows: combined with the coding operation method, in the first step, the cloud computing storage data are divided into M different shared data blocks, and on this basis, they are transmitted to the cloud storage server. The second step is to re-encrypt the data stored in cloud computing. In this process, a data block is randomly determined to replace all re-encrypted data files. See Figure 3 for details. Static data refer to the content in cloud computing storage data that do not need to be re-encrypted. Similarly, dynamic data refer to the content in cloud computing storage data that need to be re-encrypted.

If the access control tree can store data for a long time, the data will be deleted even if the data are transferred to the cloud storage server, and there is also the possibility of data recovery. During the transmission process, as far as the cloud computing storage data are concerned, the security state transition of the data will be described in detail in Figure 4.

According to Figure 4, it can be seen that when data are transmitted to the cloud storage server and valid data cannot be obtained in the process, the locked state is maintained. When the authority is revoked, the user re-encrypts data B_i and, in this way, replaces invalid data L_j. If $i \neq j$ is satisfied, in this case, all valid data can be obtained to form a set $B_{ik} = \{b_{ik1}, b_{ik2}, \ldots, b_{ikN}\}$. However, because cloud computing contains a large number of different types of data, it is inconvenient to reconstruct them. In this case, the security state of cloud computing storage data will become information coding locking. In order to access them safely, it is necessary to further generate a key and realize data security access control through encryption and decryption.

The cloud computing storage data access control method mainly includes five stages: initialization, key generation, encryption, re-encryption key generation, and decryption [33, 34], which will be described in detail below.

If ω_{ik} is a re-encrypted ciphertext, let $\omega_{ik} = [\omega_{ik}(a), \omega_{ik}(b)]$. Decryption is as follows: first, the sender determines the identity of the receiver; if it is illegal, no operation is performed; if it is legal, it sends the authorized decryption ciphertext ψ_k to the receiver, and the receiver combines its own private key, authorized decryption ciphertext ψ_k, and re-encrypted ciphertext ω_{ik} and then obtains the plaintext ξ_{ik}.

As long as receives the ciphertext ω_{ik} and obtains ψ_k, may decrypt the ciphertext and obtains the clear text. Therefore, in the case of multiple receivers, the sender only needs to simply calculate ω_{ik} based on the identity information of different receivers to achieve the purpose of access control without completely recalculating the re-encryption key, which greatly improves efficiency [35, 36]. At the same time, the length of the ciphertext remains basically unchanged as the number of re-encryption increases, saving data storage space.

4. Simulation Experiment

In order to verify the application effectiveness of the proposed method, simulation experiments are designed. The experimental comparison method is the blockchain-based big data access control method proposed in [8] and Hadoop big data access control based on data sensitivity proposed in [9].

4.1. Experimental Environment and Parameter Settings. The simulation platform is MATLAB 2020b. The experimental environment is a CPU server with a frequency of 2.6 GHz, a network framework of TensorFlow 1.8.0, and Python 3.5.2 version for programming. The specific experimental environment parameters are shown in Table 1.

Under the aforementioned experimental environment and parameter settings, the simulation experiment design is carried out. In the experiment, MATLAB software is used to calculate and count the experimental data to ensure the accuracy of the experimental results while keeping other experimental conditions consistent.

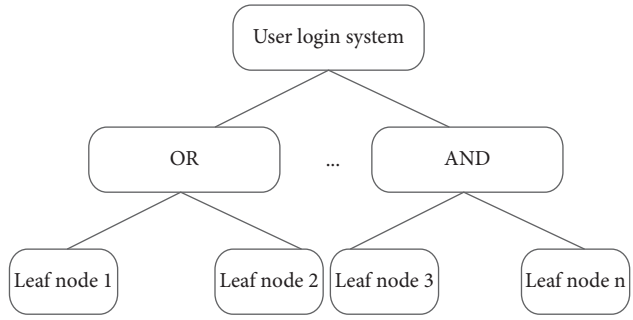

Figure 2: An example diagram of an access control tree.

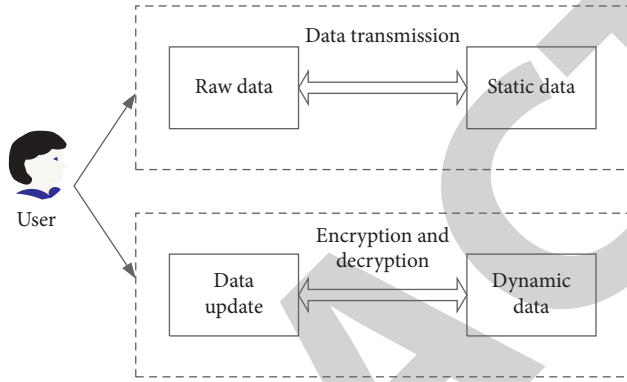

Figure 3: The basic process of dynamic re-encryption.

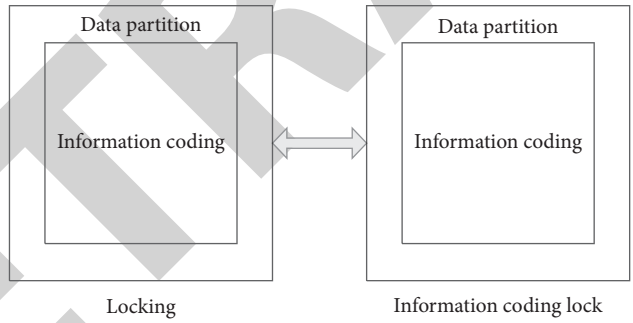

Figure 4: Data security state transition.

4.2. Analysis of Experimental Results

4.2.1. Data Access Control Accuracy. The experiment selects 80 sets of data for testing; the accuracy of three different access control methods is compared. Figure 5 shows the specific comparison results.

It can be seen from Figure 5 that the data access control accuracy of this method is better than that of the two literature methods to varying degrees. In terms of prediction accuracy, the big data access control method based on the blockchain and the Hadoop big data access control model based on data sensitivity have relatively little difference in the accuracy of early access control. However, as the number of iterations continues to increase, the control accuracy gap between the two traditional methods is gradually increasing. However, the control method in this paper has higher control precision, which can effectively improve the information storage capacity of the system, and the control precision is higher than the traditional method. The reason is that the method in this paper first preprocesses the data before performing data access control, which improves the accuracy of access control while ensuring the control efficiency.

4.2.2. Time Consumption. Still, 80 sets of data are selected for testing, and the data access control time consumption of three different methods is compared, respectively. The specific comparison results are shown in Figure 6.

It can be seen from Figure 6 that the time cost of data access control in this method increases slightly with the increase of the number of iterations and basically remains at a level when the number of iterations is 3–5 times. However, the big data access control method based on the blockchain

Table 1: Experimental parameter settings.

Parameter	Default value
Key information length	32 bit
Network bandwidth	10 MB/s
Operating speed	600 MB/s
Encoding speed	MB/s
Memory capacity	4 GB
Byte length	8 bit
Data block size	32 bit
Serial hard disk	1 TB

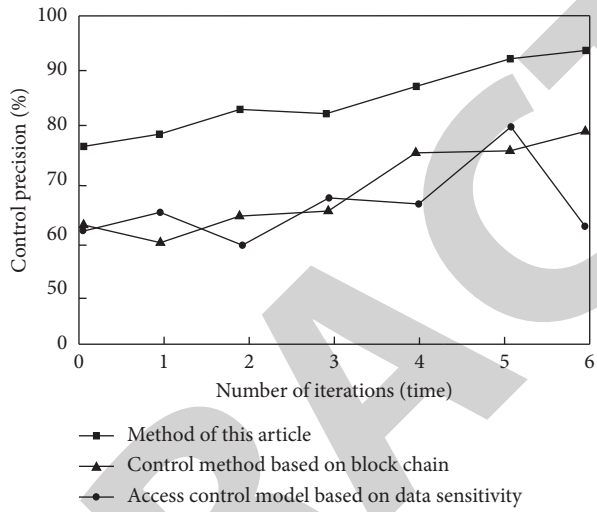

Figure 5: Comparison of data access control accuracy of the three methods.

and the Hadoop big data access control model based on data sensitivity take a long time and fluctuate significantly. Compared with the other two methods, this method has the shortest control time and higher control efficiency.

4.2.3. Comparison of Energy Consumption at Different Stages. The data access control energy consumption of different methods is compared from the user's private key generation phase, data encryption phase, data decryption phase, and revocation phase. The ordinate represents the energy consumption of data access control, and the abscissa represents the number of attributes required for each experiment. The energy consumption comparison results of different methods are shown in Figure 7.

According to the analysis of Figure 7, the data access control energy consumption of the method in this paper is lower than that of the big data access control method based on the blockchain and the Hadoop big data access control model based on data sensitivity in the user private key generation stage, data encryption stage, data decryption stage, and revocation stage. This shows that, in practical applications, this method can greatly reduce the computational burden of users. When revocation occurs, most components of the ciphertext need to be updated. Although the amount of data is very large in the cloud computing environment, the update will not bring great computational overhead, so it will not produce too much energy consumption. The comprehensive analysis of the above experimental results shows that the energy cost of this method in data access control is smaller than that of traditional methods. Therefore, this method is more suitable for the cloud computing system with huge data information.

4.2.4. User Satisfaction. In order to further verify the application effect of this method, 10 testers are selected to evaluate the data access control effect of the three methods, and the evaluation results reflect the control effect. The evaluation results are expressed by specific values. The larger the value, the better the control effect. The specific results are shown in Table 2.

Analyzing the data in Table 2 shows that users are more satisfied with the data access control effect of the method in this paper. It can be seen that the method in this paper has a better control effect, can better meet user needs, and has higher application value in actual scenarios.

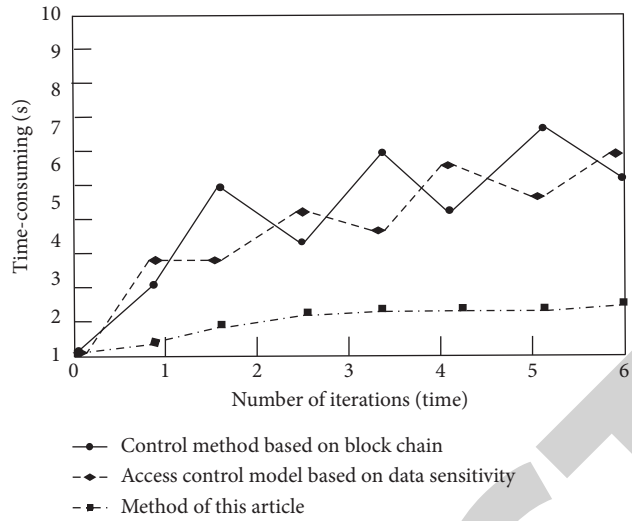

Figure 6: Comparison of time consumption of different methods.

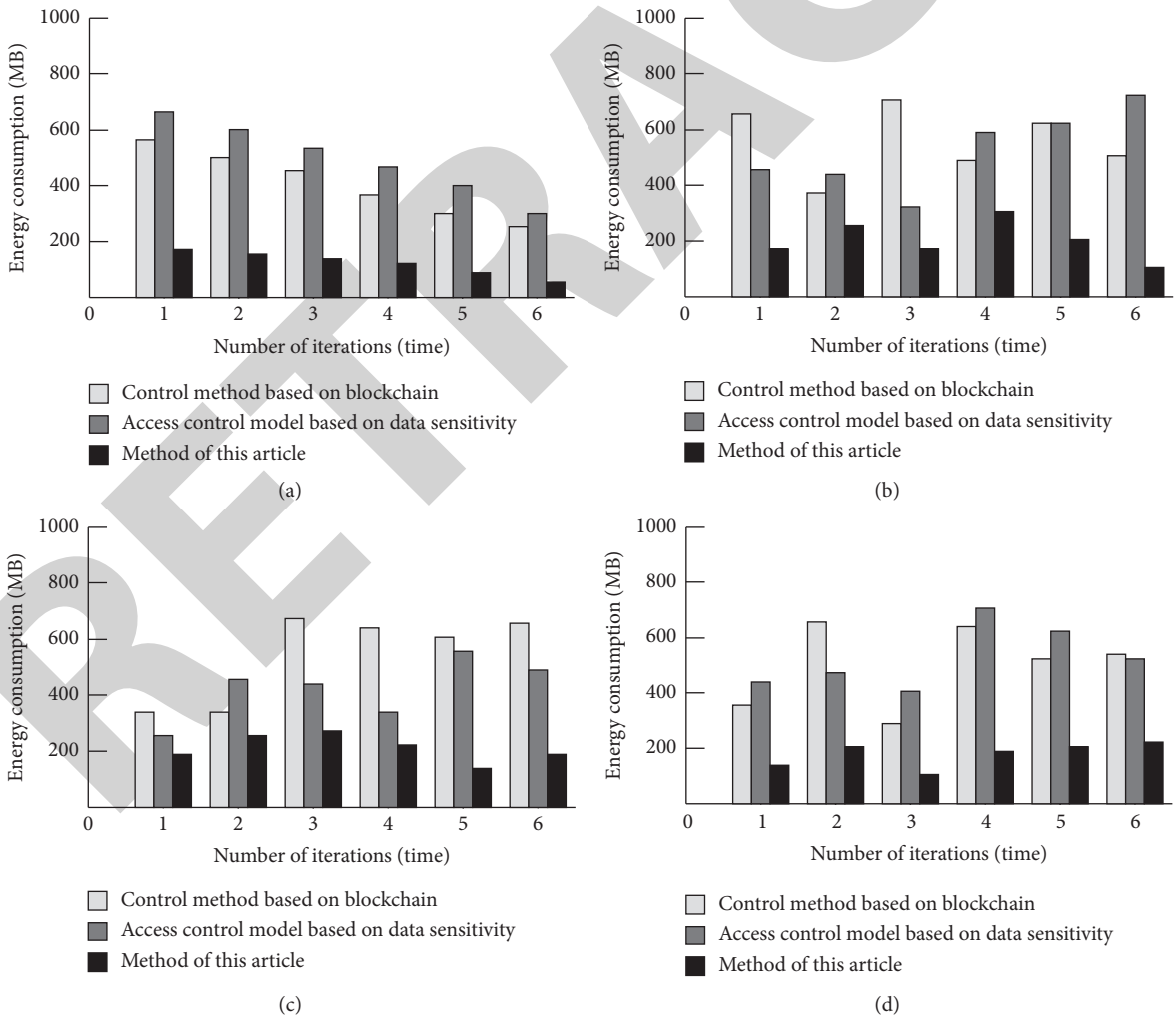

Figure 7: Comparison of energy consumption in different stages. (a) User private key generation stage. (b) Data encryption stage. (c) Data decryption stage. (d) Revocation stage.

Table 2: Comparison results of user satisfaction.

User	Method of this article	Big data access control method based on the blockchain	Hadoop big data access control model based on data sensitivity
1	9.6	7.5	7.4
2	9.5	7.8	7.6
3	9.4	8.0	7.8
4	9.0	8.1	8.0
5	9.9	7.5	7.1
6	8.9	7.1	7.1
7	9.2	7.0	7.0
8	9.3	7.6	6.9
9	9.3	7.2	6.9
10	9.5	7.4	7.6

5. Conclusion

In order to solve the problems of low precision, long time consumption, and high energy consumption of data access control, a data access control method for cloud computing storage based on dynamic re-encryption is proposed.

(1) Firstly, the principal component analysis method is used to refine the system data and obtain data information of different dimensions, so as to reduce the information storage dimension of system cloud computing

(2) Secondly, random forest algorithm is used to classify and process cloud computing storage data

(3) Thirdly, an access control tree is established to obtain the correlation of preprocessing results and data nodes

(4) Finally, the dynamic re-encryption method is used to realize the data access control of cloud computing storage

(5) The experimental results show that this method effectively solves the problems of low precision, long time consumption, and high energy consumption of traditional data access control methods and has higher application value

Data Availability

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding this work.

Acknowledgments

This work was supported by the following: in 2021, Educational Science Planning Project of Guangdong Provincial Department of Education (Special for Higher Education), Research on Studio Manufacturing Talent Cultivation Model of Cloud Computing Technology Application Specialty Based on the Background of Industrial College (Project no. 2021GXJK706), in 2020, the Young Innovative Talents Project of Colleges and Universities in Guangdong Province, Application Research of SDN Architecture in Data Center Network (Project no. 2020KQNCX258), in 2020, Guangdong Provincial Department of Education, Ordinary Colleges and Universities Characteristic Innovation Funding Project, Research on the Application of Container Technology in the Training Room of Information Technology Specialty in Higher Vocational Education (Project no. 2020KTSCX392), and in 2019, the Young Innovative Talents Project of Colleges and Universities in Guangdong Province, Research and Design of Online Cultivation Platform for New-Type Professional Farmers (Project no. 2019GKQNCX016).

References

[1] J. Shi, C. Huang, H. E. Kai, and X. Shen, "ACS-HCA:An access control scheme under hierarchical cryptography architecture," *Chinese Journal of Electronics*, vol. 28, no. 1, pp. 56–65, 2019.

[2] L. Fang, M. Li, L. Zhou, H. Zhang, and C. Ge, "A fine-grained user-divided privacy-preserving access control protocol in smart watch," *Sensors*, vol. 19, no. 9, Article ID 2109, 2019.

[3] R. Xu, C. Yu, E. Blasch, and G. Chen, "Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness," *Optical Engineering*, vol. 58, no. 4, p. 1, 2019.

[4] J. Hao, C. Huang, J. Ni, H. Rong, M. Xian, and X. Shen, "Fine-grained data access control with attribute-hiding policy for cloud-based IoT," *Computer Networks*, vol. 153, no. 22, pp. 1–10, 2019.

[5] H. Gao, Z. Ma, S. Luo, Y. Xu, and Z. Wu, "BSSPD: a blockchain-based security sharing scheme for personal data with fine-grained access control," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6658920, 20 pages, 2021.

[6] X. Hu, R. Jiang, M. Shi, and J. Shang, "A privacy protection model for health care big data based on trust evaluation access control in cloud service environment," *Journal of Intelligent and Fuzzy Systems*, vol. 38, no. 5, pp. 1–12, 2020.

[7] B. Mi, P. Long, Y. Liu, and F. Kuang, "Balancing access control and privacy for data deduplication via functional encryption," *Mathematical Problems in Engineering*, vol. 2020, Article ID 6662662, 11 pages, 2020.

[8] A. D. Liu, X. H. Du, N. Wang, and S. Z. Li, "Blockchain-based access control mechanism for big data," *Journal of Software*, vol. 30, no. 9, p. 19, 2019.

[9] J. Y. Wang, J. Q. Luan, and Y. S. Tan, "Research on big data access control model based on data sensitivity," *Computer Engineering and Applications*, vol. 55, no. 23, pp. 70–77, 2019.

[10] Y. G. Fu and J. M. Zhu, "Design for database access control mechanism based on blockchain," *Journal on Communications*, vol. 397, no. 5, pp. 134–144, 2020.

[11] S. Koziel and A. Pietrenko-Dabrowska, "Low-cost data-driven modelling of microwave components using domain confinement and PCA-based dimensionality reduction," *IET Microwaves, Antennas & Propagation*, vol. 14, no. 13, pp. 1643–1650, 2020.

[12] X. Xu, T. Liang, J. Zhu, D. Zheng, and T. Sun, "Review of classical dimensionality reduction and sample selection methods for large-scale data processing," *Neurocomputing*, vol. 328, no. 7, pp. 5–15, 2019.

[13] Y. Jeong, S. Kim, and C.-Y. Lee, "A restorable autoencoder as a method for dimensionality reduction," *Journal of the Korean Physical Society*, vol. 78, no. 4, pp. 315–327, 2021.

[14] X. Chen, L. Wang, and Z. Huang, "Principal component analysis based dynamic fuzzy neural network for internal corrosion rate prediction of gas pipelines," *Mathematical Problems in Engineering*, vol. 2020, Article ID 3681032, 9 pages, 2020.

[15] L. E. Pirogov and P. M. Zemlyanukha, "Principal component analysis for estimating parameters of the L1287 dense core by fitting model spectral maps into observed ones," *Astronomy Reports*, vol. 65, no. 2, pp. 82–94, 2021.

[16] S. Bhosale, R. Manigiri, R. P. Choudhury, and V. Bhakthavatsalam, "High resolution mass spectrometry and principal component analysis for an exhaustive understanding of acidic species composition in vacuum gas oil samples," *Energy & Fuels*, vol. 34, no. 3, pp. 2800–2806, 2020.

[17] S. Feng, C. Zhao, and P. Fu, "A cluster-based hybrid sampling approach for imbalanced data classification," *Review of Scientific Instruments*, vol. 91, no. 5, Article ID 055101, 2020.

[18] D. Griffiths and J. Boehm, "A review on deep learning techniques for 3D sensed data classification," *Remote Sensing*, vol. 11, no. 12, Article ID 1499, 2019.

[19] X. Zhang, D. Wang, Y. Zhou, H. Chen, F. Cheng, and M. Liu, "Kernel modified optimal margin distribution machine for imbalanced data classification," *Pattern Recognition Letters*, vol. 125, no. 6, pp. 325–332, 2019.

[20] W. He, J. Huang, T. Wang et al., "A high-speed low-cost VLSI system capable of on-chip online learning for dynamic vision sensor data classification," *Sensors*, vol. 20, no. 17, Article ID 4715, 2020.

[21] P. Leszyński, P. Gibas, and P. Sudra, "The problem of mismatch between the CORINE land cover data classification and the development of settlement in Poland," *Remote Sensing*, vol. 12, no. 14, Article ID 2253, 2020.

[22] A. Wang, M. Wang, H. Wu, K. Jiang, and Y. Iwahori, "A novel LiDAR data classification algorithm combined CapsNet with ResNet," *Sensors*, vol. 20, no. 4, Article ID 1151, 2020.

[23] B. Xu, "E-Commerce data classification in the cloud environment based on bayesian algorithm," *Journal of Intelligent and Fuzzy Systems*, vol. 40, no. 7, pp. 1–8, 2020.

[24] F. Bensaid and A. M. Alimi, "Online feature selection system for big data classification based on multi-objective automated negotiation," *Pattern Recognition*, vol. 110, no. 1, Article ID 107629, 2020.

[25] A. Chaudhuri and T. P. Sahu, "A hybrid feature selection method based on Binary Jaya algorithm for micro-array data classification," *Computers & Electrical Engineering*, vol. 90, no. 12, Article ID 106963, 2021.

[26] C. Wang, C. Deng, Z. Yu, D. Hui, X. Gong, and R. Luo, "Adaptive ensemble of classifiers with regularization for imbalanced data classification," *Information Fusion*, vol. 69, no. 3, pp. 81–102, 2021.

[27] X. Gu, P. Angelov, and Z. Zhao, "Self-organizing fuzzy inference ensemble system for big streaming data classification," *Knowledge-Based Systems*, vol. 218, no. 2, Article ID 106870, 2021.

[28] A. Vanarse, J. I. Espinosa-Ramos, A. Osseiran, A. Rassau, and N. Kasabov, "Application of a brain-inspired spiking neural network architecture to odor data classification," *Sensors*, vol. 20, no. 10, Article ID 2756, 2020.

[29] F. Pourpanan, C. P. Lim, X. Wang, C. J. Tan, M. Seera, and Y. Shi, "A hybrid model of fuzzy min-max and brain storm optimization for feature selection and data classification," *Neurocomputing*, vol. 333, no. 14, pp. 440–451, 2019.

[30] S. Kushch, Y. Baryshev, and S. Ranise, "Blockchain tree as solution for distributed storage of personal ID data and document access control," *Sensors*, vol. 20, no. 13, Article ID 3621, 2020.

[31] L. Bai, K. Fan, Y. Bai, X. Cheng, and Y. Yang, "Cross-domain access control based on trusted third-party and attribute mapping center," *Journal of Systems Architecture*, vol. 116, no. 5, Article ID 101957, 2020.

[32] L. Vinothkumar and V. Balaji, "Encryption and decryption technique using matrix theory," *Journal of Computational Mathematics*, vol. 3, no. 2, pp. 1–7, 2019.

[33] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A chaotic-based encryption/decryption framework for secure multimedia communications," *Entropy*, vol. 22, no. 11, Article ID 1253, 2020.

[34] S. S. . Gonge, "Combination of neural network and advanced encryption and decryption technique is used for digital image watermarking," *Journal of Intelligent and Fuzzy Systems*, vol. 38, no. 1, pp. 1–10, 2020.

[35] Z. M. Niu, "High privacy and big data access control based on multidimensional quantitative evaluation," *Computer Simulation*, vol. 37, no. 6, pp. 401–405, 2020.

[36] M. Gafsi, N. Abbassi, M. A. Hajjaji, J. Malek, and A. Mtibaa, "Improved chaos-based cryptosystem for medical image encryption and decryption," *Scientific Programming*, vol. 2020, Article ID 6612390, 22 pages, 2020.