Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 15, no. 3, March 2019, pp. 1023-1032
DOI: 10.23940/ijpe.19.03.p32.10231032

Security Storage of Sensitive Information in Cloud Computing Data Center

Zhong Li[a] and Jia Wang[b,*]

[a]*Changzhou Liu Guo-jun Branch, Jiangsu Union Technical Institute, Changzhou, 213000, China*
[b]*Experimental Instrument Center, Dalian Polytechnic University, Dalian, 116034, China*

Abstract

In order to increase the security of sensitive information, we need to research the security storage of sensitive information in CCDC (Cloud Computing Data Center). The traditional algorithm cannot guarantee the security of sensitive information when the hacker attacks the data center. Therefore, this paper proposes the three-dimensional CCDC sensitive information security storage algorithm. This algorithm uses the feature combination to filter the sensitive information and uses the sensitive information phase extraction technology to encrypt the sensitive information that was screened. This algorithm also uses three dimensional storage principle for the security storage of sensitive information. Experimental results show that this algorithm can effectively enhance the security of the sensitive information of CCDC.

Keywords: cloud computing; data center; sensitive information; information security storage

(Submitted on November 10, 2018; Revised on December 12, 2018; Accepted on January 8, 2019)

1. Introduction

In recent years, CCDC is demanding higher and higher, which promotes the development of it. The energy consumption of CCDC is larger. The flexible service and extendibility features of cloud computing make CCDC rapidly expanding. The original disperse energy consumption problem evolves into the centralized energy consumption problem [1]. Undeniably, the application area of CCDC becomes more broad. In everyday lives, we often use CCDC, such as at work, shopping, chatting with social software, and product development. We can see that CCDC is widely a part of people's lives [2]. The problem about the security storage of sensitive information of data center cloud computing has always been around us, and the situation where sensitive information is stolen is repeatedly arising. So, CCDC security sensitive information storage problems become the main problem of current research [3]. The current CCDC cannot resist hacker attacks [4]. In this case, three dimensional CCDC sensitive information security storage is an effective method to solve the above problems [5]. This algorithm uses the feature combination of sensitive information to extract CCDC information and uses the sensitive information phase extraction technology for the encryption and decryption of sensitive information. Besides, this algorithm also hides the sensitive information according to the attribute of sensitive information and carries out safe savings of sensitive information for it according to the storage theory of three-dimensional algorithm. Because CCDC sensitive information security storage is related to cloud computing user's benefits and social stability, research on the security storage of sensitive information stored in CCDC has important significance. The three-dimensional CCDC sensitive information security storage method is an effective way to solve the above problems, which has become a hot topic of research in the industry. At the same time, we have achieved some research results [6-8].

The existing sensitive information security storage algorithms were as follows. Yang et al. proposed CCDC sensitive information security storage algorithm based on cluster control [9]. This algorithm can resist the system failure of CCDC. The cluster control algorithm had sensitive information security storage personalized encryption library. We used the addressing algorithm to encrypt sensitive information in CCDC. Robustness of sensitive information was good after encryption. The sensitive information security storage personalized encryption library has the ability of regular updates and

* Corresponding author.
E-mail address: wangjia@dlpu.edu.cn

file regeneration. This replaced the sensitive information files at the end of the life cycle of records, in order to ensure the continuity of CCDC sensitive information security storage. However, the algorithm had poor defensive. Ren et al. proposed CCDC sensitive information security storage algorithm based on virtualization [10]. The algorithm is based on the secret sharing algorithm and uses the SMS verification technology of CCDC, the KEY sensitive information security verification technology and the security mechanism of CCDC service providers to integrate the sensitive information of the CCDC, forming CCDC sensitive information security storage algorithm. This algorithm effectively ensures the completeness of sensitive information and improves the defensiveness of CCDC, but the algorithm takes too long to encrypt the sensitive information. Celdrán et al. proposed the distributed CCDC sensitive information security storage algorithm [11-12]. This algorithm is based on the encryption of sensitive information file and cache switching sensitive information, and designed a sensitive information gap to coordinate CCDC in order to read the contradiction between sensitive information and sensitive information security storage. This algorithm can avoid the current sensitive information security hidden danger but faces the security hidden danger in virtual management [13-17].

Therefore, this paper proposes the three-dimensional CCDC sensitive information security storage algorithm. Simulation results show that the proposed algorithm can effectively enhance the security of sensitive information in CCDC.

2. Significance and Target of CCDC Sensitive Information Security Storage

The secure storage of CCDC sensitive information is closely related to the interests of cloud computing users and social stability. CCDC providers need to conduct in-depth research in this regard. The sound computing data center sensitive information security technology can effectively guarantee the information security storage of computing data center, and increases the degree of security of data center. With the development of modernization, the amount of information of CCDC also increases. The information also becomes more complex and diversified. The time of network attack increases with network technology used by the current network hacker. Hiding the security of CCDC sensitive information is to protect the security of user personal information. The level of each system of CCDC has security hidden danger. These security issues have been thoroughly studied in the field of information security and have the comparatively mature sensitive information security storage technology. The security storage system of CCDC mainly analyzes the service computing mode of CCDC, the dynamic virtualization management mode of CCDC and the CCDC multi-tenancy sharing operation mode. Three modes bring security hidden danger for CCDC sensitive information.

(1) Security risks caused by the service computing mode of CCDC. When CCDC user entrusts the sensitive information to CCDC or entrusts to the related application of cloud data center, CCDC has priority rights to access the sensitive information. However, in actual operation, the negligence of internal staff, attack of network hackers or CCDC system failure causes the loss of sensitive information. At this point, CCDC does not allow users to safely entrust the sensitive information to CCDC.

(2) Security risks caused by the dynamic virtualization management mode of CCDC. In the CCDC service system, we provide resources for users with virtual mode and rental mode. CCDC is the multi user shared resource, which often has the situation that multi information is bound on the same physical information resources at the same time, and CCDC virtualization technology is not perfect. Many hackers use the loophole of virtualization technology to attack; thus, users' information of the CCDC is accessed by all users.

(3) Security risks caused by CCDC multi-tenancy sharing operation mode. CCDC develops to the professional service orientation. So, CCDC not only provides the service for users in the data center, but also needs to buy services from related service providers. The service that users in CCDC enjoy is related to the service involved multiple service providers, which further increases the security risks of CCDC.

The above content is the problem that CCDC needs to challenge. This is also the problem to be solved by the proposed algorithm in this paper, in order to provide a secure CCDC for the vast number of users in CCDC.

3. Encryption Algorithm of CCDC Sensitive Information

3.1. Design of CCDC Sensitive Information Security Storage System

The design of the CCDC sensitive information security storage system based on 3D algorithm is mainly divided into four modules known as the sensitive information filtering, the sensitive information encryption, the sensitive information hiding and the sensitive information security storage. The sensitive information filtering is synchronized when the user fills in the information. The selected sensitive information is transferred to CCDC for the encryption. We use the optical modulator to

translate the complex amplitude of three-dimensional information into the complex amplitude of two-dimensional information in the encryption process while using the spatial modulator to encrypt the sensitive information. Then, the attribute matrix of sensitive information hides and saves it. It is shown in Figure 1.

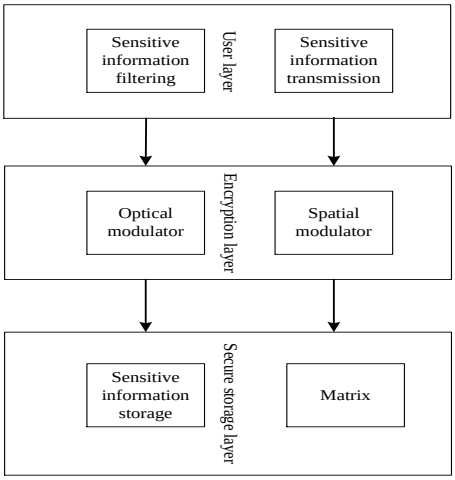

Figure 1. CCDC sensitive information security storage system

3.2. Filtering of CCDC Sensitive Information

There is a great variety of CCDC information. We focused on the security storage of sensitive information. We filter the information in CCDC, screen out the sensitive information, and judge the sensibility of data center information for sifting. Some sensibility of information is independent presentation, and some sensibility of information presents by the specific combinations of multiple information. This case is also very important. The original feature of information can be combined in CCDC, and the feature combination can be modelled. The process of modelling can be defined by Equation (1), where I represent the power of CCDC information feature combination with certain constraints. The combination of information characteristics in CCDC constitutes the monomial expression based on the product of the feature term of the original information. All sensitive feature combination satisfies the constraint conditions of $I \in CondSet$, forming the sensitive information feature set. $CondSet$ represents the set formed by different constraint conditions in CCDCs. So, we use $CondSet$ as constraints, which can form different sensitive information feature space in CCDC. When the original feature x_i of any of sensitive information in any features combination $\Phi_I(x)$ of CCDC is equal to 0, the feature combination of sensitive information of CCDC will not exist. In this case, we cannot perform arithmetic on them. If the original sensitive information feature x_i of CCDC is not zero, we can use the product to represent the strength of sensitive information feature combination.

$$\Phi(x) = \left\{ \Phi_1(x) = x_1^{i_1}, x_2^{i_2}, \cdots, x_n^{i_n} \,\middle|\, I(i_1, i_2, \cdots, i_n) \in CondSet \right\} \tag{1}$$

The three dimensional function polynomial sensitive information features sets of CCDC sensitive information features is composed of all sensitive information feature three-dimensional function monomial expressions in $1 \sim d$ order. The three-dimensional polynomial has some disadvantages when describing the computing data center sensitive information feature combination because there is the unbalanced sensitive information feature term in feature combination of sensitive information. For example, a 4-order polynomial sensitive information mapping $K_{M(3)}(x, z)$ in a data center has two kinds of sensitive information feature terms $x_1^2 x_2$ and x_1^3. In the feature term of sensitive information, the components x_1, x_2 of the combination features are not balanced, causing increases in the amount of calculation of CCDC sensitive information feature three dimensional function polynomial as well as increases in calculation error. This phenomenon increases with the increase of the order of the polynomial of the three-dimensional function because the three-dimensional function polynomial cannot be calculated according to the characteristics of the CCDC sensitive information. We generally use three-dimensional polynomial function in the lower order. There is a problem in that sensitive information features three-dimensional polynomial is not suitable for the low order of sensitive information feature combination. Thus, we propose to use the subsets combined with the monomial expressions of high order polynomial to filter the low order of sensitive information feature combination. The low order three-dimensional function definition of CCDC sensitive information

feature combination and the mapping of sensitive information feature are defined as Equation (2).

$$K_{\subseteq}(x,z)=\prod_{i=1}^{n}(1+x_i z_i)\Phi_{\subseteq}(x)=\left\{\Phi_I(x)=x_1^{i_1},x_2^{i_2},\cdots,x_n^{i_n}\,\middle|\,I(i_1,i_2,\cdots,i_n)\in\{0,1\}^n\right\} \tag{2}$$

In CCDC, we use variance analysis to overcome the problem of the three dimensional function polynomial algorithm of CCDC. The definition is shown in Equation (3).

$$K_{CA(d)}(x,z)=\lambda Trans\left(\prod_{k=1}^{d}x_{j_k}z_{j_k}\right)+(1-\lambda)K_1^n(x,z) \tag{3}$$

In Equation (3), $K_s^n(x,z)$ represents that containing in CCDC original sensitive information includes n d^{th} order standard deviations of sensitive information characteristics. $K_1^n(x,z)$ represents first order standard variance in the data center three dimensional function variance analysis; the variance is belong to (x,z) in theory. The composite variance algorithm is very suitable for filtering CCDC sensitive information. The composite variance algorithm is combined and weighted by two parts of sensitive information feature. In the first part, $Trans\left(\sum_{s=2}^{e}K_s^n(x,z)\right)$ represents a sensitive information feature combination of each order in CCDC. The first part is the basis of the data center sensitive information feature combination modelling. In the second part, $K_1^n(x,z)$ represents the single sensitive information features in the CCDC. The second part is the basis of the data center highly sensitive information modelling. Thus, we can integrate the sensitive information that independently presents the sensitivity with the sensitive information features combination through the variance analysis algorithm. It uses the information provided by the sensitive information feature set to improve the effectiveness of CCDC sensitive information filtering.

Using the order controlling parameter d of variance analysis can prevent unstable feature terms in CCDC three-dimensional function polynomial, but can control the monomial expression which is lower than d order 1 power. No sensitive information feature combination of data center will be excluded. Some sensitive information in the cloud data center, which can be directly determined as the CCDC sensitive information, does not need the feature combination.

3.3. Encryption and Decryption Algorithm of CCDC Sensitive Information

The three dimensional algorithm is the effective algorithm proposed by CCDC sensitive information security storage at present. Before the sensitive information security storage, we encrypt the sensitive information and ensure the security of information. The information phase extraction algorithm is the most important step in three dimensional information encoding. We build the three-dimensional information in CCDC and store the sensitive information in the three-dimensional information module in order to get the complex amplitude distribution diagram of three vertical and horizontal line. We can use three-dimensional function to represent the three-dimensional information, and can use a two-dimensional function set to represent the three dimensional information.

The main purpose of CCDC sensitive information phase extraction is to transform the three dimensional information into two-dimensional complex amplitude information, and express the corresponding quadratic function of sensitive information phase. The specific process is as follows. Simulate that three dimensional information plane wave pierces vertically into CCDC, receives diffraction wavelength from three dimensional sensitive information complex amplitude to the plane wave of the output data center, and extracts the phase part of three dimensional sensitive information. Suppose that the wavelength of plane wave is λ. The plane wave diffraction distance is z. The plane wave diffraction is used $FrT_{A\cdot z}\{\cdot\}$ to express. The extracted phase function of three-dimensional sensitive information is used $Q(x_i,y_i)$ to express. The process that three-dimensional sensitive information complex amplitude is transformed into the two-dimensional information complex amplitude can be expressed as Equations (4) and (5).

$$SLM(x_i,y_i)=FrT_{A\cdot z_3}\left\{FrT_{A\cdot z_2}\left\{FrT_{A\cdot z_1}\left\{C(x_1,y_1)\right\}\times A(x_2,y_2)\right\}\cdot S(x_3,y_3)\right\} \tag{4}$$

$$Q(x_i,y_i)=SLM(x_i,y_i)/\left|SLM(x_i,y_i)\right| \tag{5}$$

$SLM(x_i, y_i)$ represents the process of converting the complex amplitude of the three dimensional information into the complex amplitude of two dimensional information on the optical modulator of CCDC.

The three-dimensional random phase encryption is carried out in the plane wave diffraction region, which is realized in the cloud data center optical modulator. The extracted three-dimensional sensitive information phase $Q(x_i, y_i)$ will be loaded into CCDC special modulator, and the sensitive information is encrypted with the three-dimensional random phase encryption system. The first sensitive information phase of cloud computing data is RPM_1. This phase plate of the sensitive information clings to the three-dimensional sensitive information to be encrypted. Because of the use of special modulator, we can superpose the random phase of the first sensitive information phase plate and three-dimensional phase sensitive information. After superposing second sensitive information phase plate, we can achieve the purpose of encryption of sensitive information. Assume the corresponding function of the first sensitive information phase plate and the second sensitive information phase plate are $R_1(x_1, y_1)$ and $R_2(x_2, y_2)$. The three-dimensional sensitive information complex amplitude distribution is $R_0(x_0, y_0)$. Observe and record the three-dimensional sensitive information complex amplitude distribution. A bunch of referenced plane wave can be introduced. The interference of referenced plane wave can be ignored, and the distance from CCDC special modulator to second sensitive information in the plane wave diffraction region is z_1, and the plane wave diffraction distance of the output CCDC is z_2. The three-dimensional sensitive information complex amplitude distribution can be expressed as Equation (6).

$$R_0(x_0, y_0) = FrT_{A \cdot z_2}\left\{FrT_{A \cdot z_1}\left\{\exp\left[jQ(x_i, y_i)\right] \times \exp\left[jR_1(x_i, y_i)\right]\right\} \times \exp\left[jQ(x_i, y_i)\right]\right\} \tag{6}$$

The process of decryption of sensitive information in CCDC is the reverse process of encryption of three-dimensional sensitive information. Suppose that $IFrT_{\lambda \cdot z}\{\cdot\}$ represents the transformation of plane wave diffraction region, the computational formula of CCDC space modulator reverse operation is defines as Equation (7).

$$DeSLM(x_i, y_i) = FrT_{\lambda \cdot z_1}\left\{FrT_{\lambda \cdot z_1} \times \left\{\exp\left[jR_0(x_0, y_0)\right] \times \exp\left[jR_2(x_2, y_2)\right]\right\} \exp\left[jR_1(x_1, y_1)\right]\right\} \tag{7}$$

The secret keys of three-dimensional CCDC are the phase-key and additional key. The phase-key is the information phase distribution function of random phase plate RPM_1 and RPM_2 of sensitive information phase. The additional key is the wavelength of plane wave λ. The distance from CCDC spatial modulator to second sensitive information is z_1, and the distance to the plane wave diffraction of output CCDC is z_2. The phase-key and additional key guarantee security of CCDC sensitive information together.

3.4. CCDC Sensitive Information Hiding

In order to ensure that the encrypted sensitive information is more secure, we need to improve the secret degree of sensitive information. We use the clustering process to hide CCDC sensitive information. According to the attribute of sensitive information, the matrix is composed. The matrix can show the influence and influence level of sensitive information on the CCDC sensitive information hiding. Suppose that the influence of e^{th} sensitive information attribute on l^{th} sensitive information can be expressed as U_{el}. F_l represents the influence level of sensitive information attribute son l^{th} sensitive information. F_{el} represents the difference of the influence level of the e^{th} sensitive information attribution the l^{th} sensitive information. CCDC sensitive information influential factor matrix is a $q \times p$ matrix. q is used to represent the number of sensitive information data; p is used to represent the number of sensitive information attribute. The expression is as follows in Equation (8).

$$N = (U_{el})q \times p = \begin{bmatrix} r_1, r_2, r_3, \cdots, r_p \\ 0, 4, 7, \cdots, 3 \\ 4, 3, 6, \cdots, 7 \\ \vdots \ \vdots \ \vdots \quad \vdots \\ 2, 1, 4, \cdots, 7 \end{bmatrix} \tag{8}$$

$F_g = \sum_{l=1}^{l} U_{gl}$ is used to calculate the influence of sensitive information attributes on the attribute of the g^{th} CCDC sensitive information attribute, $x_{lg} = U_{gl} / F_g$ calculates the influence of the l^{th} sensitive information attribute on the g^{th} CCDC sensitive information. The distance between two sensitive information can be expressed as $E_{mg} = \sum_{k=1}^{P} \left| u_{mk} - u_{gk} \right|$.

CCDC sensitive information attribute classification can be expressed as Equation (9).

$$Q(u) = \sum_{k=1}^{n} x_{lk} \cdot \frac{size(u)}{\left| B_l \right|} \tag{9}$$

By combining the numeric sensitive information attributes with the classified sensitive information attributes, we get the penalty factor of the CCDC sensitive information, which can be expressed by Equation (10).

$$Q_j(u) = Q_p(u) + Q(u) \tag{10}$$

According to the above formula, we can get the penalty factor of CCDC losing and compensate it, which implements the hiding of CCDC sensitive information.

3.5. CCDC Sensitive Information Security Storage Mechanism

The three-dimensional storage is to divide stored the sensitive information into k sensitive information fragmentation with the same size, and then to encode k sensitive information fragmentation through the three-dimensional storage algorithm. The sensitive information fragmentation after encoding uses n to express. The sensitive information fragmentation after encoding is the same as the original sensitive information fragmentation, but there is no correlation between them. We select r sensitive information fragmentation in the sensitive information fragmentation after encoding, which is restored as much as possible to the original sensitive data. $n \geq r \geq k > 1$. The sensitive information after the mathematical three-dimensional storage encoding can be expressed as Equations (11)-(13). Y represents the sensitive information fragmentation after the encoding in CCDC, F represents the original sensitive information in CCDC and G is the matrix of $n \times k$, which is also called CCDC three-dimensional storage matrix

$$Y = F \cdot G \tag{11}$$

$$F = (F_1, F_2, \cdots, F_n) \tag{12}$$

$$Y = (Y_1, Y_2, \cdots, Y_k, Y_{k+1}, \cdots, Y_n) \tag{13}$$

In G, we arbitrarily select k columns that are combined to form the sub-matrix. Suppose that the sub-matrices are all reversible matrices. We can use any k sensitive information fragmentation received by the CCDC to restore the original sensitive information. Y' is the vector combined by any k fragmentations of the sensitive information fragmentation of CCDC after encoding. G' is the submatrix formed by that CCDC three-dimensional storage matrix randomly selects k column, which is obtained according to Equations (14)-(15). The submatrix G' is the invertible matrix.

$$Y' = F \cdot G' \tag{14}$$

$$F = Y' \cdot (G')^{-1} \tag{15}$$

According to Equation (15), the original sensitive information F can be restored. In the above formula, n and k can be dynamically set according to the actual application. In any event, when sensitive information fragments are less than k, the original sensitive information of CCDC cannot be restored. When restoring the original sensitive information, the k columns in invertible matrix must be consistent with the original order of sensitive information fragments after encoding.

Otherwise, the CCDC original sensitive information will not be restored.

The original sensitive information in CCDC is segmented according to the user requirements, which is divided into k sensitive information fragments. Then, these sensitive information fragments are encoded and encrypted, forming n hidden sensitive information files. The files are sent to n different three-dimensional storage nodes. When restoring the sensitive information, the system needs to select k sensitive information from n hidden files, and decrypt the CCDC sensitive information. fin Equation (15) can restore the original sensitive information.

4. Simulation Results and Analysis

According to the security risks of the CCDC security sensitive information storage in the second part, we carry out the experiment. The experimental platform uses Microsoft Windows XP operating system. The hardware environment of this system is PC frequency1GHz, AMD Athlon TM II X255 processor and 2GB memory. The experimental data are taken from the cloud center of Intel. The experimental results are predicted by the proposed method. We observe the security and defensiveness of CCDC. Firstly, for the security risks caused by CCDC service computing mode, we carry out the experiment, verifying whether the proposed method solves the hidden trouble, which allows users safely to entrust the sensitive information to the CCDC.

Three modules in the second part propose the security hidden danger. The main hidden danger is that hackers attack. In order to provide a secure platform for CCDC users, this experiment will be based on the completeness and safety degree of CCDC. The proposed algorithm adds CCDC security metrics algorithm on the current algorithm, and controls the credibility of the sensitive information in the data center. Because CCDC is measured in real time, it can provide a complete secure CCDC for the majority of users. The current algorithm is used to read CCDC sensitive information. The probability of disclosure of sensitive information is greater. When there is malicious information in stored sensitive information, the completeness of CCDC will be destroyed. In this paper, the three-dimensional algorithm is used to optimize the current algorithm, and the reliability of CCDC is divided into different levels to control the completeness and availability of the CCDC. Figure 2 shows that reading and writing range of CCDC of the proposed algorithm is higher than the current algorithm.

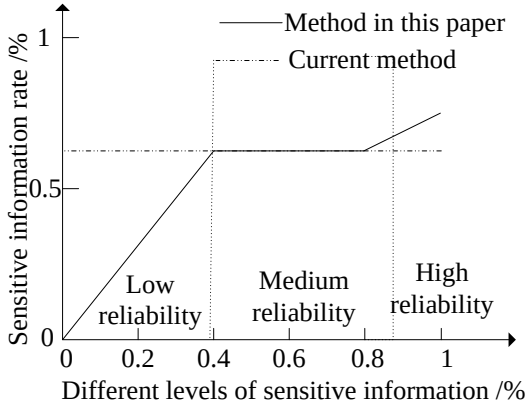

Figure 2. Reading and writing rate of different levels of reliability sensitive information in CCDC

For users of the CCDC with lower credibility, the reading and writing of sensitive information will be limited. Its range is limited to the minimum, which is more secure relative to the current algorithm. Table 1 shows that the proposed method forbids the writing of sensitive information user containing malice, ensuring the completeness of CCDC sensitive information.

Table 1. Security rules of multilevel credible topics

Current algorithms	General safety conditions	Attributes of sensitive information
Low confidence level data center [0, 0.4)	√	×
Medium confidence level data center [0.4, 0.8)	√	√
High confidence level data center [0.8, 1)	×	×

When verifying the effectiveness of CCDC sensitive information security storage, we take the sensitive information

storage time as the standard for measuring the effectiveness of sensitive information storage security. Compared with the current algorithm, the experiment uses the same size of CCDC for the sensitive information storage experiment. The experimental results are shown in Table 2.

Table 2. Comparison of CCDC sensitive information storage time

Order number	Sensitive information file size/MB	Proposed algorithm		Current algorithm	
		Direct storage time/ms	Security storage time/ms	Direct storage time/ms	Security storage time/ms
1	4	235	298	256	69
2	8	302	352	352	198
3	12	352	420	402	268
4	16	420	862	480	756
5	20	698	1025	759	803
6	24	856	1503	905	1056
7	28	1052	1720	1235	1252
8	32	1086	2015	1526	1532

The analysis of Table 2 shows that when the proposed algorithm stores the sensitive information, the security storage time increases with the increase of the sensitive information file. However, compared with the current algorithm, the time of three-dimensional algorithm proposed in this paper is relatively short, which improves the efficiency of cloud computing data counter security sensitive information storage.

We take the safety of the sensitive information security storage as the standard for measuring the proposed algorithm. Table 3 shows when the security storage in the proposed algorithm and the current algorithm are in the same level, how long the encryption keys need and safety of each line is the same. From the table, the key size of the current algorithm with the same degree of safety is 1456 b , and the key size of the proposed algorithm is 235 b . It shows that the degree of safety of the proposed algorithm is much higher than the degree of safety of the current algorithm. With the increase of the key size, the difference between the proposed algorithm and the current algorithm also increases, which shows that that the degree of safety of the proposed algorithm is much higher than the degree of safety of the current algorithm.

Table 3. Comparison result of key size of two algorithms

Key size of proposed algorithm/ b	Key size of current algorithm/ b
235	1456
254	1865
286	2014
305	2324
362	2541

In order to intuitively reflect the impact of the current algorithm and the proposed algorithm on the security of CCDC, this paper compares and analyses the security of the proposed algorithm and the current algorithm, as shown in Figure 3.

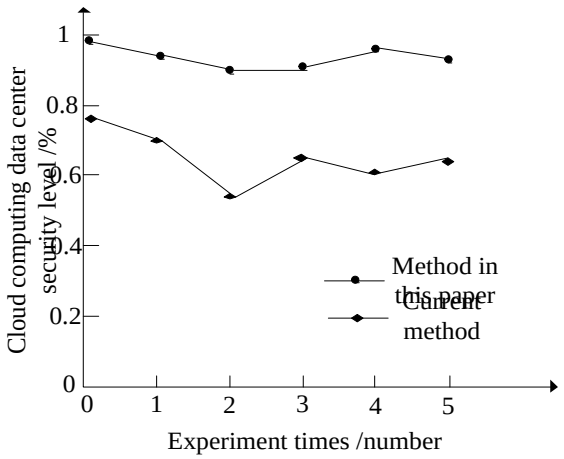

Figure3. Comparison result of safety of two methods

Under the same conditions, the degree of security of CCDC is about 95% using the proposed algorithm, and the degree of security of CCDC is about 61% using the current algorithm, which effectively improves the degree of security of CCDC

sensitive information security storage. In this paper, the algorithm improves the degree of security of CCDC. This experiment will verify the using effect of the proposed algorithm and the current algorithm for CCDC. Experimental results are shown in Table 4.

Table 4. Performance data of CCDC under two algorithms

order number	Proposed algorithm		Current algorithm	
	Occupancy rate of server CUP/%	Sensitive information storage speed/ (Mb/s)	Occupancy rate of server CUP/%	Sensitive information storage speed/ (Mb/s)
1	2.96	13.4	19.2	4.23
2	3.05	12.5	15.23	5.62
3	2.87	13.85	14.15	10.25
4	3.56	11.86	11.26	4.96
5	3.42	14.25	10.08	5.76
6	4.02	15.63	12.35	8.24
7	3.51	13.52	9.25	6.32
8	3.26	14.25	10.52	7.52

From the analysis of Table 4, the average value of CUP occupancy rate of CCDC using the proposed algorithm is 3.33%. The average value of sensitive information storage speed is 12.75 Mb/s . Using the current algorithm, the average value of CUP occupancy rate of CCDC is 13.66%. The average value of sensitive information storage speed is 6.61 Mb/s . In this paper, the CUP occupancy rate of CCDC is reduced by 10.33%, and the storage speed of sensitive information is increased by 6.14 Mb/s . After using the three-dimensional algorithm, the performance of CCDC improved significantly. This shows the algorithm itself has little effect on CCDC, which further verifies the effectiveness of the three-dimensional algorithm. Simulation results show that this algorithm can effectively enhance the degree of safety of CCDC sensitive information.

5. Conclusions

Using the current algorithm, CCDC had poor defence when attacked by hackers. Therefore, this paper proposes the sensitive information secure storage algorithm of CCDC based on 3D. Simulation results show that the proposed algorithm can effectively enhance the security of sensitive information of CCDC.

Acknowledgements

This research is supported by Jiangsu Province Education Science “13th Five-Year” (project supported by the key program number: B-a/2016/03/06).

References

1. Y. Yu, M. H. Au, Y. Mu, S. Tang, J. Ren, W. Susilo, et al., “Enhanced Privacy of a Remote Data Integrity-Checking Protocol for Secure Cloud Storage,” *International Journal of Information Security*, Vol. 14, pp. 307-318, 2015
2. R. Jin, H. -J. Cho, and T.-s. Chung, “An Encryption Approach to Secure Modification and Deletion for Flash-based Storage,” *IEEE Transactions on Consumer Electronics*, Vol. 60, pp. 662-667, 2014
3. J. Kaczmarek and M. R. Wrobel, “Operating System Security by Integrity Checking and Recovery using Write-Protected Storage,” *IET Information Security*, Vol. 8, pp. 122-131, 2014
4. A. S. Rawat, O. O. Koyluoglu, N. Silberstein, and S. Vishwanath, “Optimal Locally Repairable and Secure Codes for Distributed Storage Systems,” *IEEE Transactions on Information Theory*, Vol. 60, pp. 212-236, 2014
5. S. Distefano and A. Puliafito, “Information Dependability in Distributed Systems: The Dependable Distributed Storage System,” *Integrated Computer-Aided Engineering*, Vol. 21, pp. 3-18, 2014
6. M. Liu, S. Liu, W. Fu, and J. Zhou, “Distributional Escape Time Algorithm based on Generalized Fractal Sets in Cloud Environment,” *Chinese Journal of Electronics*, Vol. 24, pp. 124-127, 2015
7. A. N. Singh, “Information Security Management Maturity: a Study of Select Organizations,” 2014
8. W. Au and B. White, “Integrating Information Technology in a Discovery Achool-A Case Study,” in *Proceedings of International Conference on Computers in Education*, pp. 701-702, 2002
9. B. Yang, X. Tang, and J. Li, “A Systematic Piggybacking Design for Minimum Storage Regenerating Codes,” *IEEE Transactions on Information Theory*, Vol. 61, pp. 5779-5786, 2015
10. Y. Ren, J. Shen, Y. Zheng, J. Wang, and H.-C. Chao, “Efficient Data Integrity Auditing for Storage Security in Mobile Health Cloud,” *Peer-to-Peer Networking and Applications*, Vol. 9, pp. 854-863, 2016
11. A. H. Celdrán, G. D. Tormo, F. G. Mármol, M. G. Pérez, and G. M. Pérez, “Resolving Privacy-Preserving Relationships over Outsourced Encrypted Data Storages,” *International Journal of Information Security*, Vol. 15, pp. 195-209, 2016
12. B. Jia, S. Liu, and Y. Yang, “Fractal Cross-Layer Service with Integration and Interaction in Internet of Things,” *International Journal of Distributed Sensor Networks*, Vol. 10, pp. 760248, 2014

13. S.-W. Park, J. Kim, and D. G. Lee, "SecureDom: Secure Mobile-Sensitive Information Protection with Domain Separation," *The Journal of Supercomputing*, Vol. 72, pp. 2682-2702, 2016
14. H. Wu, X. Dang, L. Wang, and L. He, "Information Fusion-based Method for Distributed Domain Name System Cache Poisoning Attack Detection and Identification," *IET Information Security*, Vol. 10, pp. 37-44, 2016
15. G. Yang and S. Liu, "Distributed Cooperative Algorithm for k-M Set with Negative Integer k by Fractal Symmetrical Property," *International Journal of Distributed Sensor Networks*, Vol. 10, pp. 398583, 2014
16. H. Jiang, F. Shen, S. Chen, K. -C. Li, and Y. -S. Jeong, "A Secure and Scalable Storage System for Aggregate Data in IoT," *Future Generation Computer Systems*, Vol. 49, pp. 133-141, 2015
17. Y. Djemaiel and N. Boudriga, "Modeling and Assessing the Impact of Security Attacks on Enterprise Information Systems," in *Proceedings of International Conference on Business Information Systems*, pp. 281-292, 2014