International Journal of Security and Its Application
Vol.11, No.1 (2017), pp.121-134
http://dx.doi.org/10.14257/ijsia.2017.11.1.11

The Homomorphic Encryption Method for Cloud Computing Storage Security

Jun Wu and Jing Chen

Yiwu Industrial & Commercial College, Yiwu,
322000 Zhejiang province, China
{Jun Wu} 78549608@qq.com

Abstract

Based on the idea of the encryption algorithm, a new method for data storage in cloud computing is designed. First of all, gives the cloud data security framework in 9 steps; secondly, the data encryption and data decryption algorithm is designed by combining the multiplication, addition, update algorithm and the specific operation; thirdly, combining the index and scanning technology and according to the reverse order strategy design a data retrieval algorithm. Experimental results show that the proposed method in data encryption, data decryption, data retrieval and other aspects of the implementation of the efficiency is significantly higher than the BGV algorithm, and more suitable for the safe storage of cloud data.

Keywords*: cloud storage, Homomorphic Encryption, data retrieval, inverted sort*

1. Introduction

Cloud computing provides on-demand services for cloud computing users by using virtualization technology and distributed computing technology to build a huge pool of resources to integrate computing resources in the network idle[1]. Cloud users only need to purchase or lease the computing resources they need without having to care about the sources and management of these resources. It freed from the pressure of the cloud users from infrastructure management and maintenance work, so that users can focus more on their core business [2]. Therefore, more and more enterprises, institutions choose cloud computing services as its information resource management service providers and cloud computing services has become an important business in the field of IT. IBM, Amazon, Google, Microsoft and other companies have also launched their own cloud computing service [3-4].

In order to promote the development of cloud computing faster and better, cloud computing security issues have to be effectively resolved. At present, the research institutions, government organizations and cloud service providers have invested a lot of manpower and material resources to study and solve the security problem of cloud computing [5]. In order to promote the healthy and rapid development of cloud computing and cloud storage services, and to provide safe and effective personal information service for individuals, businesses and society, various research institutions, enterprises have put forward cloud security solutions or suggestions[6].

Kumar proposed a comprehensive cloud computing security framework. The framework includes three parts, cloud security objectives, cloud security services and cloud security evaluation system. Among them, the cloud security service system is the most critical, from three levels of infrastructure services, basic services and application services to ensure the security of cloud computing[7].

Ryoo proposed a secure cloud architecture. The framework uses isolation mechanism, encryption mechanism and VPN channel mechanism to isolate store the data in the cloud ,

ISSN: 1738-9976 IJSIA

and establish a virtual private channel for user communication to ensure the security of data transmission[8].

The cloud security storage model based on encryption storage ensures safe storage of data. However, due to the data is stored in the cloud data center, which set up obstacles for the use of cloud data. In order to facilitate the user to retrieve ciphertext in the cloud, the researchers propose a search encryption mechanism, which supports the data encryption algorithm [9].

The data in the cloud is stored in the encrypted data, and the decryption key is saved by the data of the main users, avoiding the risk of data leakage, but it brings a lot of inconvenience to the cloud. To this end, the researchers proposed the concept of proxy re encryption to solve the problem of sharing[10].

The cloud security data storage scheme based on the encryption mechanism and proxy re encryption scheme can solve the inconvenience caused by the encrypted data storage to a certain extent, but it still can not make the ciphertext is as convenient and efficient as the plain text[11].

The concept of the homomorphic encryption is proposed, which brings the dawn for the convenient use of the ciphertext. Encryption, also known as secret computing, which refers to the implementation of the related operations in the cipher text results, and the same operation of the text message to obtain the results, and after the encrypted encrypted. Therefore, the user can manipulate the cipher text like the plain text[12].

Martini proposed a fully homomorphic encryption algorithm based on the ideal lattice, and the algorithm to regain the new. This fully homomorphic encryption scheme is the first fully homomorphic encryption scheme since the concept has been proposed[13]. This scheme points out the direction for the research of the encryption of the state, and then a lot of the whole encryption schemes are improved and optimized based on the perfect lattice[14-15].

Based on the theory of fault tolerant learning, Chen uses the non - linear technology to construct an all - state encryption scheme which is independent of the ideal lattice.The proposal of this scheme has influenced the development process of the research of homomorphic encryption. In this scheme, the dimension reduction technique is adopted, which can shorten the cipher text and reduce the complexity of decryption[16].

Ruboczki uses asymptotic linear efficiency to establish a FHE, which is the prototype of BGV. Because the program's security parameters of each gate calculation circuit are almost linear, BGV scheme has a very strong practicality[17]. IBM release of the encryption software package, which is based on the BGV program to achieve[18].

Along with the continuous development of the technology of the encryption, The application research of the encryption scheme also has a great breakthrough. Microsoft researchers have developed a system based on the encryption of the system design[19]. After that, the MIT researchers have realized the query computation of the non decryption data, and solved the practical problem of the whole encryption for the first time[20]. After that, Japan's Fujitsu graduate student issued a high speed encryption technology[21].

In this paper, based on the research of the cloud storage security, we use the theory and idea of the encryption to design a new algorithm and model in cloud data encryption and data retrieval.

2. Design of Cloud Data Storage Framework based on the Technology of Encryption

In the cloud data storage model based on the technology of the encryption using the “client encryption-cloud storage mode ". This model avoids the risk of data transmission in the transmission of the plaintext. In the entire cloud computing network, the user's data is in the form of the ciphertext. Its confidentiality has been guaranteed at the initial stage.

In the process of data encryption, a more mature and practical encryption algorithm is adopted.

As shown in Figure 1, this is the cloud data storage framework model based on the technology of encryption.

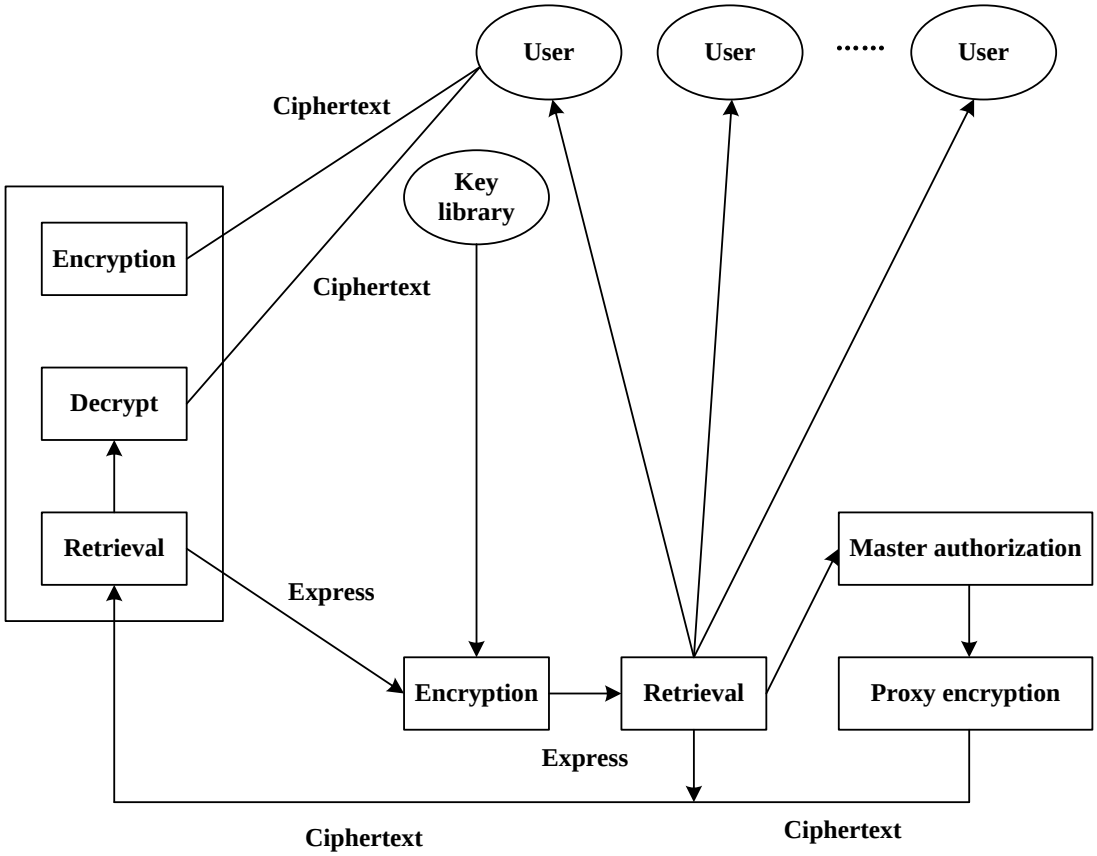

Figure 1. The Homomorphic Encryption Model Cloud Data Storage Framework Proposed in this Paper

In the framework in Figure 1, before users upload the data to the cloud they first encrypt data, and then the data are transmitted to the cloud server in the form of the ciphertext, and according to the user category ,these data are stored to the user's rented storage space. When users need to use the data, then they sent retrieval or updates and other requests to the cloud server .

The specific process of data processing in cloud storage model is as follows:

The first step, cloud authentication center distribute the public encryption key and the the private decryption key to cloud users. When cloud users use cloud storage services, they should first apply to the cloud authentication center for the key. In order to facilitate the processing of cipher later, cloud authentication center for cloud users to distribute the key to the user's encryption key to the cloud server.

Second step, client encryption. Customers according to public key encryption and encryption algorithm to encrypt the data transmitted to the cloud.

Third step, encrypted data transmission. The cloud storage model uses the current public network transmission, no need to build a new transport channel network, and due to the data is in the form of ciphertext, it does not require additional security measures to increase security in the transmission process.

The fourth step, after the data arrived to the cloud, cloud data storage center according to the user's categories to store the data to the user's rented storage space , and the user's public key is stored in the user public key base to prepare the user to retrieve and update the data.

The fifth step, during data retrieval, the user sends the request information to the cloud retrieval server, which is transmitted in plain text mode or transmitted by the cloud storage side encryption public key encryption mode.

The sixth step, the cloud retrieval server encrypt the plaintext. Encrypted separately based on the public key base and the encryption algorithm, then generate the cipher keyword group. Each cipher key corresponds to a user's encrypted database to search separately.

The seventh step, cloud data storage center collect the results of retrieval. If the search results of the information is the ownership of the user, that is, the user has a cipher decryption key, the results can be directly returned to the user application. If the search results are not applied to the user data, the implementation of the eighth step.

The eighth step, data authorization. Because the search results are not owned by the users, and the need to issue an application to the data master to obtain data authorization. If the data master reject the user request, that is, return to the "no relevant information or search results are not readable (not authorized)" and other information. If the data master authorized the user apply , then the implementation of the ninth step.

The ninth step, proxy re encryption. Cloud storage center retrieve the results M1 for proxy re encryption, generating the ciphertext result M2, which is the ciphertext information based on application user encryption public key encryption and then return to the application users.

It can be seen from the above process, data encryption and data retrieval are the most important two steps. Subsequent chapters will detail the two steps of the algorithm design.

2. Design of Data Encryption Algorithm

Based on fully homomorphic encryption and BGV scheme based on LWE, designed to meet the characteristics of fully homomorphic encryption algorithm, the algorithm is divided into five parts: parameter selection, key generation, encryption algorithm, decryption algorithm and cipher algorithm.

The first step, set the parameter selection set, as shown in the formula (1):

$$P(1^{\lambda},1^{L}):P=\{P_1,\cdots,P_j,\cdots,P_L\} \tag{1}$$

Here, P_j is used to represent the parameters of each layer, and can be expressed as follows:

$$P_j=\{r_L,\cdots,r_0,\chi_j,e_j,M\} \tag{2}$$

Here, from r_L to r_0 represent a decreasing mode sequence, χ_j represents the distribution which the ring dimension is e_j , and the calculation of M is $M=\lceil(2n+1)\log r\rceil$.

Second step, generating key $K(P)$ .The key generation algorithm is divided into two parts. First, generate the encryption and decryption key T_j and P_j for each layer. Secondly, combinate the encryption and decryption keys that generated by each layer to generate algorithm encryption and decryption key T_k and P_k .

The encryption and decryption key of each layer generate $T_k\in R_q^2$ and $P_k\in R_q^{N\times 2}$, here the expression of R is as follows:

$$R = \frac{Z[x]}{x^e + 1} \tag{3}$$

Here, e is the power of 2.

Encryption and decryption key generation algorithm is as follows:

$$\begin{cases} T_k = (T_0, \cdots, T_L) \\ P_k = (P_0, \cdots, P_L, \tau(T_1' \to T_0), \cdots, \tau(T_L' \to T_{L-1})) \\ T_j' = T_j \otimes T_j \\ \tau(T_{j+1}' \to T_j) = swithK(T_{j+1}', T_j) \end{cases} \tag{4}$$

The third step, the processing of the encryption algorithm is as follows:

$$\begin{cases} E(P, P_k, n) : d = n + P_L^T \\ n \leftarrow (n, 0) \\ r \leftarrow R_2^N \end{cases} \tag{5}$$

The fourth step, the processing of the decryption algorithm is as follows:

$$E(P, P_k, d) : n^* = ((< d, T_j > \bmod_T) \bmod 2) \tag{6}$$

The fifth step, the design of the computation algorithm of the ciphertext is as follows.

$E(P_k, g, d_1, d_2, \cdots, d_n)$ is used to express the ciphertext, the result D_g obtained from the computation of the ciphertext $d_1, d_2, \cdots, d_n$ in the operation of the function g is equal to the plaintext result N_g generated by the plaintext $n_1, n_2, \cdots, n_n$ in the operation of the function g after decryption. That is :

$$\begin{aligned} D_g &= g_{P_k}(d_1, d_2, \cdots, d_n) \\ &= g(n_1, n_2, \cdots, n_n) \\ &= N_g \end{aligned} \tag{7}$$

Encryption algorithm is the core of the whole fully homomorphic encryption algorithm, so the ciphertext computation algorithm is the most complex. The most complex algorithm in the ciphertext computation algorithm is the operation function $g = \{add, multi, refresh\}$. In the function, add represents the add operation, $multi$ represents the multiply operation, and the $refresh$ represents the update operation.

In the fully homomorphic encryption scheme, both the ciphertext and the key are vectors, the definition of the ciphertext product is a tensor $d_i \otimes d_j$, the corresponding key is $T \otimes T$, so the product will lead to the rapid growth of the ciphertext dimension, $refresh$ is a method of reducing the noise by using the key exchange and the mode switching technology to reduce the dimension of the cipher text to the original dimension.

The ciphertext calculation function g is composed of a series of addition, multiplication and update functions, when the addition or multiplication is performed on the ciphertext d_x and d_y , first determine whether the ciphertext d_x and d_y are at the same level , if they are, it indicated that they have the same key and corresponding to the same key T_j ; if they are not , it indicated that the key are different, and need to do the update

operation to convert the cipher text to the same level. After that, can perform an addition operation or a multiplication operation:

$$\begin{cases} d_S = d_x + d'_y \bmod r_x \\ d_S = d_x \otimes d'_y \bmod r_x \end{cases} \tag{8}$$

At this point, the corresponding key of the ciphertext d_S is T'_j. Finally, the results are updated to reduce the dimension and reduce the noise.

4. Design of Data Retrieval Algorithm

There are three sub algorithms in the data retrieval algorithm: inverted index algorithm, cipher text scan algorithm and search sorting algorithm.

4.1 Inverted Index

Index file is the core technology of full-text retrieval. At present, the most widely used full-text indexing model is inverted index. Inverted index, also call reverse index, is a kind of index structure which is use key words as the index keys and the list access portal, and used to store the mapping of a keyword in a document or a set of documents in a full text search.

The inverted index structure is composed of index files and inverted files, and the index file is made of entries and record data which is consisted of logical record pointer. Logical record pointer point to logical address of the inverted file.The inverted file contains information about the document that contains the corresponding entry, mainly about document address, word frequency and entry position.

Inverted index structure is based on plaintext retrieval, the indexed words are stored in plain text, to facilitate the attacker to analyze the text.

For security reasons, in this paper, we design the inverted index structure of the ciphertext as shown in Figure 2.

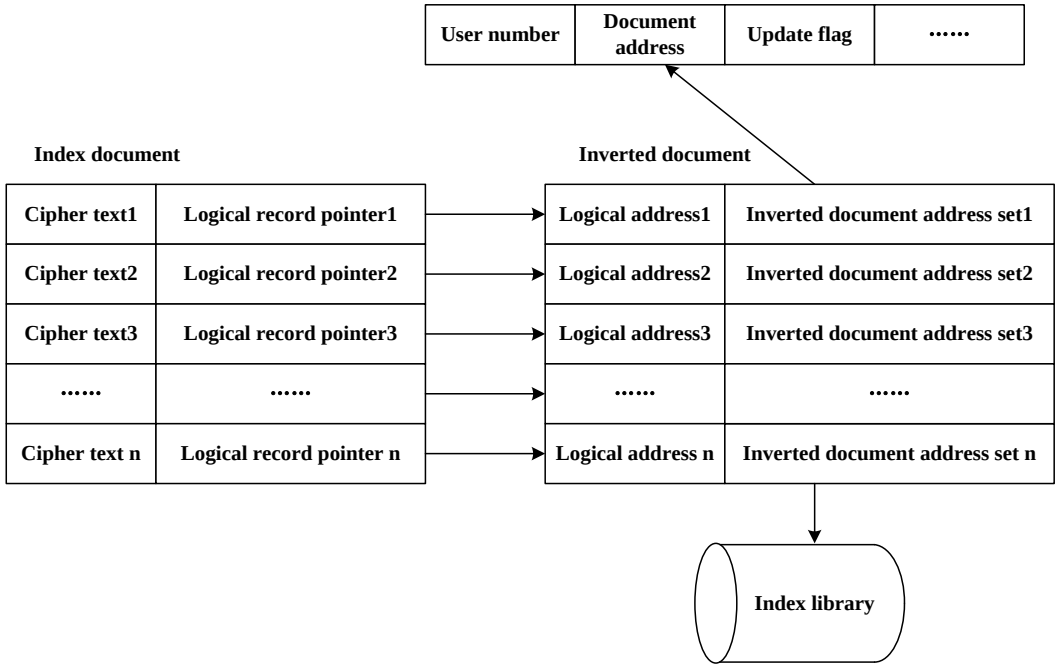

Figure 2. The Inverted Sort Structure

The entries in the index file are stored after encryption to ensure the security of the index entry.The encryption of index entries is done by the cloud server, which can be used by the symmetric encryption mechanism.The cloud index server s responsible for the security of the index library. Because the user data is encrypted with the asymmetric encryption algorithm, the same entry corresponding to the data master of different user data is different, and its ciphertext is also different. Therefore, the incidence relation of the inverted document in the inverted file of the index base is more complex than the traditional inverted file. A inverted document information record should include at least the "user number", "document address" and "update flag" and other information, in the beginning of the search for the text, then according to the document address to retrieve statistical entry information such as word in different documents. The "update flag" is designed based on the operation of the cipher text. Because the data is constantly changing, the inverted file information of the index base should be changed accordingly. When the user data is updated, the update flag is changed (from 0 to 1). This indicates that the corresponding document information has changed, and it needs to be re scanned.

4.2 Ciphertext Scaning

The ciphertext scanning is to query the specified key from the ciphertext set. If the key is in the document, then record the related information of the key words like address, frequency. Ciphertext linear search algorithm is usually used to assume ciphertext scanning , and it can be judged whether the key word is in the query document and the number of times by means of a pair of one to one cipher key word matching.

The linear search algorithm $G_d(T,E)$ of the ciphertext is a linear comparison of the cipher text, to determine whether include the query keywords T. However, the general encryption algorithm does not support linear computation, so we should construct the linear mapping function $U_T = Trap(T,E)$ of the query keywords before the ciphertext retrieval, and then execute linear query.

Encryption algorithm is different, and its key word linear mapping function is also different, so the process of linear retrieval of the text is more complex. The cipher text retrieval process based on the encryption mechanism is more convenient because homomorphic encryption support ciphertext calculation, and plaintext linear search algorithm $G(T,nE)$ can generate the ciphertext linear search algorithm $G_d(T_d,E)$ by the calculation of ciphertext algorithm $Eval()$, so as to complete the calculation of the key words T.

4.3 Search Index

Because cloud computing environment has a huge amount of data resources, users will get a lot of data information when retrieving relevant information, however, many of them are useless or the correlation is not high to users. For this, the cloud storage service providers providing users with the data of the search results also sorting the data by correlation, and return to the users the most needed or higher correlation value of data .

Because of the massive data resources in the cloud computing environment, the user will get a lot of data and information in the retrieval of relevant information, where there is a lot of information to the user is useless or related degree is not high, so the cloud storage service providers in providing search results for user data, but also for sorting data in accordance with the relevant degree of the user, the user needs most related higher values of the data back to the user.

In the calculation of the correlation degree of information retrieval often use the "weight" as an important reference factor of the degree of correlation. Weight is a reference factor that reflects the importance of keywords in a document, and the size of the weight value depends on the frequency of keywords in the document.

The weight formula is $w_{i,j} = g_{i,j}$. $\sum_{i=1}^{t} g_{i,j} = 1$, so $\sum_{i=1}^{t} w_{i,j} = 1$.

Although the frequency reflects the importance of keywords in a certain extent, this frequency and weight dependence between the calculation is not accurate. In the framework of calculating the keyword weight, the frequency and the inverse frequency are the most common, In order to improve the accuracy of the weight calculation, the following methods are used here:

$$w_{i,j} = \begin{cases} (1+\log_2 g_{i,j}) \times \log \dfrac{N}{n_i} & g_{i,j} > 0 \\ 0 & g_{i,j} = 0 \end{cases} \tag{9}$$

The ciphertext document set is $E = \{e_1, e_2, \cdots, e_n\}$, each document is composed of a number of key words, the query key set is $K = \{k_1, k_2, \cdots, k_n\}$, the corresponding weight vector is $w_K = \{w_1, w_2, \cdots, w_n\}$. The similarity formula for calculating the computing document d_j and the query set k_i is as follows:

$$\begin{aligned} sim(e_j, k_i) &= w_{d_j} \times w_K \\ &= \sum_{i=1}^{n} w_{ji}^* \times w_{ni}^* \end{aligned} \tag{10}$$

Therefore, the formula of the similarity between the ciphertext document set E and the query set K is:

$$\begin{aligned} sim(E, K) &= w_E \times w_K \\ &= \begin{bmatrix} w_{11}^* & w_{12}^* & \cdots & w_{1n}^* \\ w_{21}^* & w_{22}^* & \cdots & w_{2n}^* \\ \cdots & \cdots & \cdots & \cdots \\ w_{m1}^* & w_{m2}^* & \cdots & w_{mn}^* \end{bmatrix} (w_1, w_2, \cdots, w_n)^T \\ &= (sim_{e_1}.sim_{e_2}, \cdots, sim_{e_n})^T \end{aligned} \tag{11}$$

5. Experimental Results and Analysis

In order to verify the effectiveness of the cloud storage security method based on the encryption algorithm proposed in this paper, next, expand the experimental study. The computer hardware configuration required for the experiment is: dual core CPU, 3.0GHz single core frequency , 8GB memory, 1T hard disk, the computer software is configured as: Windows 7 operating system, CloudSim simulation environment.

In order to form a contrast with the method of this paper, we choose the most ideal BGV algorithm as the contrast algorithm.

First of all, test the effect of the two algorithms in data encryption.

The encryption key space is gradually increased from 100MB to 700MB according to the step size is the speed of 100M, and the time of data encryption is compared between the two algorithms. The results of the comparison curve are shown in Figure 3.

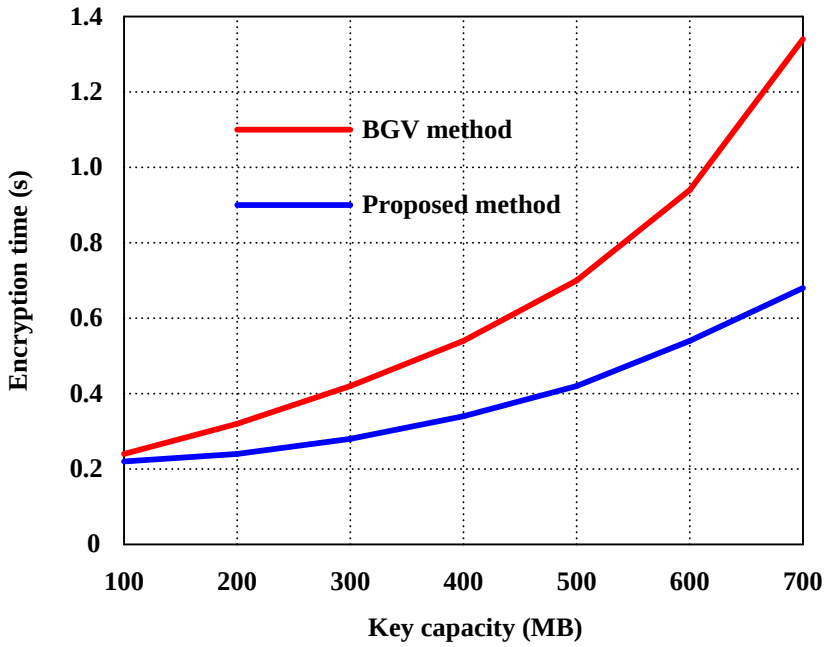

Figure 3. The Comparison Result of Data Encryption Time between the Two Kinds of Results

From the results in Figure 3, we can see that with the gradual increase of the key space, the encryption time of the BGV algorithm increases gradually from 0.2 seconds, and the encryption time increases rapidly. When the key space is increased to 700MB, the encryption time has reached 1.38 seconds.

For the cloud storage data based on homomorphic encryption algorithm encryption method, with the increasing of the key space, its encryption time is also increased, but the increase amplitude was significantly less than the BGV algorithm. When the key space is increased to 700MB, the encryption time is also less than 0.7 seconds.

Next, to test the effect of the two algorithms on data decryption.

The encryption key space is gradually increased from 100MB to 700MB according to the step size is also the speed of 100M, comparison of the two algorithms in the implementation of data decryption time, the results of the comparison curve are shown in Figure 4.

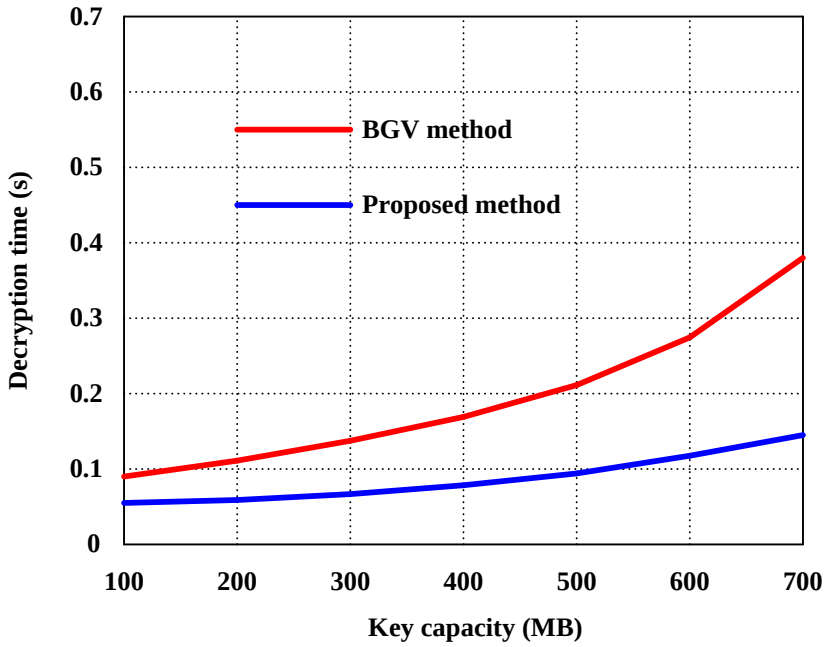

Figure 4. Comparison Results of Data Decryption Time of the Two Algorithms

From the results in Figure 4, we can see that with the gradual increase of the key space, the decryption time of BGV algorithm increases from 0.1 seconds, and the encryption time increases rapidly. When the key space is increased to 700MB, the decryption time has reached 0.38 seconds.

For the cloud storage data decryption method based on homomorphic encryption algorithm, with the increasing of the key space, the decryption time is also increased, but the increase was significantly less than the BGV algorithm. When the key space is increased to 700MB, the decryption time is also less than 0.15 seconds.

Finally, compare the performance of the two algorithms in data retrieval.

Data retrieval times from the 200 times start gradually increased to 600 times at the speed of 100 times. Compared to the data retrieval time in the two algorithms, the results of the comparison curve are shown in Figure 5.

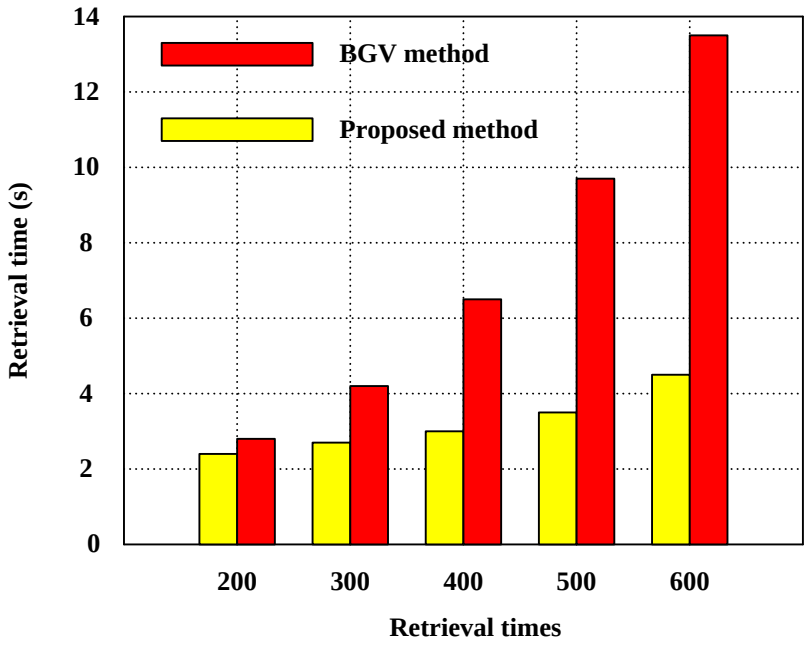

Figure 5. Data RetrievalTime Comparison Results of Two Algorithms

From the results of Figure 5, we can see that, with the increase of the retrieval times, the retrieval time of BGV algorithm is gradually increased from 2.8 seconds, and the increase amplitude is rapidly expanding. When the number of searches is increased to 600 times, the retrieval time has reached 13.5 seconds.

For the cloud storage data retrieval method based on the encryption algorithm proposed in this paper, because of the design of the three step method, especially the inverted sort method, the increase of retrieval time is far less than the BGV algorithm. When the retrieval times is increased to 600, the retrieval time is still only 4.4 seconds.

Based on the above three sets of experiments, we can prove that the cloud storage data retrieval method based on the encryption algorithm in this paper has better performance in data encryption, data decryption and data retrieval, for the safe storage of cloud data has a stronger applicability.

6. Conclusion

Aiming at the security problem of cloud computing data storage, this research work is carried out, and a new storage framework based on the idea of the encryption algorithm is designed. The two most critical content in the framework of as the focus of research, respectively, set the data encryption and data decryption algorithm design and the design of the data retrieval algorithm. In the design of data encryption and data decryption algorithm, the strategy of combining the operation of multiplication, addition and update algorithm is adopted. In the design of data retrieval algorithm, adopt the method of index, scan and sorting. A comparison experiment with BGV algorithm is performed, experimental results show that the proposed method for cloud storage data retrieval based on homomorphic encryption algorithm in data encryption, data decryption, data retrieval has a better performance.

Appendix

This paper is a revised and expanded version of a paper entitled [Research on the Method of Cloud Computing Storage Security based on the Homomorphic Encryption

Method] presented at The 5th International Conference on Cloud-Computing and Super-Computing (SecTech 2016), 24-26 November 2016，Jeju Island, Korea.

References

[1] B Duncan, M Whittington. Reflecting on Whether Checklists Can Tick the Box for Cloud Security[C]. IEEE International Conference on Cloudcom, 805-810. (2014)
[2] J Singh, T Pasquier, J Bacon, H Ko, D Eyers. 20 Cloud Security Considerations for Supporting the Internet of Things[J].Internet of Things Journal of IEEE Transaction, 28: 1-16. (2015)
[3] Bo Xu, Zhiping Peng, Fangxiong Xiao, Antonio Marcel Gates, Jian-Ping Yu. Dynamic deployment of virtual machines in cloud computing using multi-objective optimization [J]. Soft Computing, 2015, 19(8): 2265-2273
[4] A Sari. A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications[J]. Journal of Information Security, 6(2): 142-154. (2015)
[5] GJW Kathrine, AO Joseph, R Vijayan. Cloud Security Mechanisms for Data Protection: A Survey[J]. International Journal of Multimedia & Ubiquito, 9(9):81-90. (2014)
[6] Bo Xu, Zhiping Peng, Fangxiong Xiao, etc. Dynamic deployment of virtual machines in cloud computing using multi-objective optimization [J]. Soft Computing, 2015, 19(8): 2265-2273
[7] SN Kumar. A Survey on Secure Cloud: Security and Privacy in Cloud Computing[J]. American Journal of Systems and Software, 4(1): 14-26. (2016)
[8] J Ryoo，S Rizvi，W Aiken，J Kissell. Cloud Security Auditing: Challenges and Emerging Approaches[J]. IEEE Security & Privacy Magazine, 12(6): 68-74. (2014)
[9] S Sharma, G Gupta, PR Laxmi. A Survey on Cloud Security Issues and Techniques[J]. Computer Science, 4(1): 111-118. (2014)
[10] B Martini, Q Do, KKR Choo. Conceptual evidence collection and analysis methodology for Android devices Cloud Security Ecosystem[J]. Cloud Security Ecosystem, 285-307. (2016)
[11] L Khansa，CW Zobel. Assessing innovations in cloud security[J]. Journal of Computer Information Systems, 54(3): 45-56. (2014)
[12] A Taha, R Trapero, J Luna, N Suri. AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security[C]. IEEE International Conference on Trust, 284-291. (2014)
[13] B Martini, Q Do, KKR Choo. Mobile cloud forensics: An analysis of seven popular Android apps Cloud Security Ecosystem[J]. Cloud Security Ecosystem, 309-345. (2015)
[14] B.T.; RESENDE, B.D. A System for Social Network Analysis[C]. In: The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), London, UK, 126-131. (2013).
[15] B Duncan，M Whittington. The Importance of Proper Measurement for a Cloud Security Assurance Model[C]. IEEE International Conference on Cloud Computing, 517-522. (2015)
[16] X Chen, C Chen, Y Tao, J Hu. A Cloud Security Assessment System Based on Classifying and Grading[J]. IEEE Cloud Computing, 2(2):58-67. (2015)
[17] ES Ruboczki, Z Rajnai. Moving towards Cloud Security[J]. Interdisciplinary Description of Complex System, 13(1): 9-14. (2015)
[18] A Hendre，KP Joshi. A Semantic Approach to Cloud Security and Compliance[C]. IEEE International Conference on Cloud Computing, 1081-1084. (2015)
[19] N Gajra，SS Khan，P Rane. Private cloud security: Secured user authentication by using enhanced hybrid algorithm[C]. International Conference on Advances in Community, 788-793. (2014)
[20] D Petcu. A Taxonomy for SLA-Based Monitoring of Cloud Security[J]. IEEE Computer Software & Applications Conference, 640-641. (2014)
[21] Muthu Ramachandran，V Chang. Cloud Security proposed and demonstrated by Cloud Computing Adoption Framework[J]. Workshop on Emerging Software, 62-70. (2014)

Authors

Jun Wu (1979-), Associate Professor，Master, mainly engaged in internet safety and cloud computing.

Jing Chen (1980-), Associate Professor, Master, mainly engaged in computer application research.