Research of Key Management Technology on Cloud Storage

http://dx.doi.org/10.3991/ijoe.v9i6.3311

Ningning Song, Zhiwei Wei, Xianwei Xhou and Qian Liu
School of Computer & Communication Engineering,
University of Science & Technology Beijing, Beijing 100083, China

***Abstract*—Since the cloud storage technology has distribution, isolation and sharing characteristics, key management has become more and more difficulty. As a consequence, the research of key management technology has become a hot topic in recent years. In order to solve the untrustworthiness of cloud storage server provider, the complexity, security of key and some other issues under cloud storage environment, this paper proposed a $(n+1, s+1)$ key management technology on the basis of Shamir (n,s) and then this technology was used in cloud storage system. The main idea of the technology is that the whole key spited into n+1 parts and distributed to the different cloud storage service providers and data owner to manage the sub-keys. Through the performance analysis, in this technology, the data owner is the core of the management process. The technology is more secure than the traditional technology and solves the untrustworthiness of cloud storage server provider based on the premise of reducing the burden of data owner.**

***Index Terms*—Cloud storage, Key management, Key escrow, Threshold.**

I. INTRODUCTION

With the rapid development of Internet information, information data net-work has being arises, but how to store the information data has become a topic of increasing concern. In this condition, the modern cloud storage technology [1] has ushered in the good development opportunities, but also huge challenges will be subject to network information security. The rapid development of cloud storage technology, people can basically meet the daily demand for data storage. But when people use data of the storage network, found that the user privacy protection is very important on cloud storage. In recent years, customer privacy breaches have occurred, but also to the user caused huge losses. According to research, data privacy leak is mostly due to loss privacy key, how to ensure the security of key user privacy is an important aspect of the research of cloud storage security.

In key management technology, there are two problems to solve: [1-3] In order to reduce user burden, improve efficiency, we must introduce an automatic key management mechanisms; In order to improve safety, and it should be possible to reduce the system resides key amount

In order to solve these two problems, there are three types of key scenarios: centralized, distributed, hybrid key management scheme. Centralized key management scheme is defined by the key distribution center (KDC) or a group of a hierarchy of nodes responsible for key generation and assigned to the communication parties. Distributed key distribution scheme refers to the various communication network communications side has the same status as key distribution between them depends on negotiation between them, without any restrictions on any other party (step further, you can put the key dispersed distribution center all communication parties, that is, each communication party is also a key distribution center). Hybrid key management scheme mainly mixing the above two programs: the upper (host) using a distributed key distribution scheme, while the lower terminal or communication subnet it belongs to a centralized key distribution scheme.

But the three programs primarily based on symmetric encryption key management scheme to achieve, difficult to adapt and asymmetric key encryption scheme. For the current shortcomings of the key management scheme, the paper describes a distributed key management method, which is mainly the user to effectively break down the key in advance, and then factored different keys entrusted to other fragment unrelated providers, and then design a threshold, when the ISP provides key number is greater than the threshold [4], the data can be decrypted.

II. THE DIVISION OF KEY MANAGEMENT TECHNOLOGY

Threshold key management scheme is based on Shamir key distributed hosting mechanism [5-9], which is mainly the user to effectively break down the key in advance, and then factored different keys entrusted to other fragment unrelated providers, cloud storage ISP technology is isolated from each other, so the keys store to another ISP is safe, so as to achieve the key confidentiality. Finally, it managed to set a threshold, so by different provider key cross-certification to get the correct key.

A. The Definition of Key Division Management Technology

Definition 1: Assume that a full key sK is divided into n parts; each part is a small sub-key, and which are allocated to N different key manager [10]. Therefore, through a collection of some sub keys to deduce the complete key sK principle is:

(1) If the collection is greater than the number of sub-key s, then we can derive the complete key

(2) If the number is less than the collection of sub-key s, then the complete key sK cannot be launched

Then, (n,s) is the Key Division Management Technology s is threshold.

Definition 2: Suppose two sets A and B are independent of each other a key manager (two sets of attributes $A \,\mathrm{I}\, B = \Phi$), A is modulo n, B mold is m, and s is set as the threshold value (s<n), so that the complete key sK is divided into $n+m$ parts, each of which is assigned to the A and B key manager.

(1) If A is greater than or equal to s, the key manager, and then any one of the B can be derived integrity key sK .

(2) There is less than S in the A of key managers, and B which is not in any of a manager can derive the complete key

Then, (n,s) is the Key Division Management Technology, s is threshold. We proposed a $(n+1, s+1)$ key management technology on the basis of Shamir (n,s) .

B. The Implementation of Key Division Management Technology

(1) The design of the basic parameters

Design a matrix M of $n+1 \times n$ is used to represent divided key:

$$M = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \\ a_{11}' & a_{12}' & \dots & a_{1n}' \end{bmatrix} \qquad (1)$$

Each row of the matrix M as a group represented by vectors, $a_1 = (a_{11}, a_{12}, \dots, a_{1n})$ $a_n = (a_{n1}, a_{n2}, \dots, a_{nn})$, $a_n = (a_{n1}, a_{n2}, \dots, a_{nn})$. So M can be simplified to M= $(a_1, a_2, \dots, a_n, a_1')^T$. In this group, each s eigenvectors are linearly independent, but any s +1 vectors are linearly related, M has a rank of s +1.

(2)The key distribution

The matrix M is a vector composed of n +1, then these n +1vectors are assigned to the n provider and User. Assuming matrix M vectors $(a_1'', a_2'', \dots, a_s'',)$ are linearly independent, M of the vectors can be expressed by that $(a_1'', a_2'', \dots, a_s'',)$ linear, so the key matrix can be expressed as

$$M = \begin{bmatrix} a_1 \\ a_2 \\ \dots \\ a_n \\ a_1' \end{bmatrix} = \begin{bmatrix} k_{11}a_1'' + k_{12}a_2'' + \dots + k_{1s}a_s'' \\ k_{21}a_1'' + k_{22}a_2'' + \dots + k_{2s}a_s'' \\ \dots \\ k_{n1}a_1'' + k_{n2}a_2'' + \dots + k_{ns}a_s'' \\ a_1' \end{bmatrix} \qquad (2)$$

Line on M transform can be simplified as, elementary row transformation matrix:

$$E_{i1}E_{i2}\dots E_{is} \begin{bmatrix} k_{11}a_1'' + k_{12}a_2'' + \dots + k_{1s}a_s'' \\ k_{21}a_1'' + k_{22}a_2'' + \dots + k_{2s}a_s'' \\ \dots \\ k_{n1}a_1'' + k_{n2}a_2'' + \dots + k_{ns}a_s'' \\ a_1' \end{bmatrix} \qquad (3)$$

$$= (a_1'', a_2'', \dots, a_s'', a_1', 0, \dots, 0)^T$$

Elementary matrix X is stored by the cloud storage service, used to derive the matrix M, if the s sub-key and user extract from the providers, M can be calculated according to elementary matrix.

(3)Recovery the complete key

Sub-key $a_1'', a_2'', \dots, a_s''$ and user a_1' extract from the providers, according to the nature of M, we can write the matrix for $(a_1'', a_2'', \dots, a_s'', a_1', 0, \dots, 0)^T$.

Remove from the cloud storage server provider elementary matrix, and the inverse matrix $E_{i1}^{-1}E_{i2}^{-1}\dots E_{is}^{-1}$ obtained respectively. Using the following equations：

$$E_{i1}E_{i2}\dots E_{is} \begin{bmatrix} k_{11}a_1'' + k_{12}a_2'' + \dots + k_{1s}a_s'' \\ k_{21}a_1'' + k_{22}a_2'' + \dots + k_{2s}a_s'' \\ \dots \\ k_{n1}a_1'' + k_{n2}a_2'' + \dots + k_{ns}a_s'' \\ a_1' \end{bmatrix} \qquad (4)$$

$$= (a_1'', a_2'', \dots, a_s'', a_1', 0, \dots, 0)^T$$

Elementary transformation to $(a_1'', a_2'', \dots, a_s'', a_1', 0, \dots, 0)^T$:

$$E_{is}^{-1}E_{is-1}^{-1}\dots E_{i1}^{-1} \begin{bmatrix} a_1'' \\ a_2'' \\ \dots \\ a_s'' \\ a_1' \\ 0 \\ \dots \\ 0 \end{bmatrix} = E_{is}^{-1}E_{is-1}^{-1}\dots E_{i1}^{-1}E_{i1}E_{i2}\dots E_{is} \qquad (5)$$

$$\begin{bmatrix} k_{11}a_1'' + k_{12}a_2'' + \dots + k_{1s}a_s'' \\ k_{21}a_1'' + k_{22}a_2'' + \dots + k_{2s}a_s'' \\ \dots \\ k_{n1}a_1'' + k_{n2}a_2'' + \dots + k_{ns}a_s'' \\ a_1' \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ \dots \\ a_n \\ a_1' \end{bmatrix} \qquad (6)$$

III. ANALYSIS AND EVALUATION

A. The Correction of Key Division Management Technology

If you want to encrypt the data, then the user can send a request to the t provider, and then sent to the server out of their sub-key $a_1'', a_2'', \dots, a_s''$, the server joint sub-key, elementary matrix $E_{i1}E_{i2}...E_{is}$ and the inverse matrix $E_{is}^{-1}E_{is-1}^{-1}...E_{i1}^{-1}$ calculation:

$$E_{is}^{-1}E_{is-1}^{-1}...E_{i1}^{-1}\begin{bmatrix} a_1^{''} \\ a_2^{''} \\ ... \\ a_s^{''} \\ a_1^{'} \\ 0 \\ ... \\ 0 \end{bmatrix} = E_{is}^{-1}E_{is-1}^{-1}...E_{i1}^{-1}E_{i1}E_{i2}...E_{is} \tag{7}$$

$$\begin{bmatrix} k_{11}a_1^{''}+k_{12}a_2^{''}+...+k_{1s}a_s^{''} \\ k_{21}a_1^{''}+k_{22}a_2^{''}+...+k_{2s}a_s^{''} \\ ... \\ k_{n1}a_1^{''}+k_{n2}a_2^{''}+...+k_{ns}a_s^{''} \\ a_1^{'} \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ ... \\ a_n \\ a_1^{'} \end{bmatrix} \tag{8}$$

Thus as long as the random s sub-key and the user keys, the full key sK can be deduced.

B. Security of Key Division Management Technology

ISP will devise the key sub-keys into n+1 groups consisting key matrix M= $(a_1, a_2, ..., a_n, a_1^{'})^T$, then are assigned to the n cloud storage service providers and users. Based on the above analysis, the key matrix of rank s +1, where vectors $(a_1^{''}, a_2^{''}, ..., a_s^{''},)$ are linearly independent, so if extracted less than s sub-keys or the lack of data owners sub-key, is based on linear algebra algorithms unable to derive full by linear key, meaning that if less than s sub-keys and key data owners, or the lack of key data owners, then the key cannot be restored. Only greater than or equal to the n-th cloud storage server providers and data owners sub key, then correctly deduced the complete key. Complete key recovery process will be three cases:

(1) Key recovery is less than s a key provider. Suppose there are s-1 provider participate in the key recovery, the key matrix $(a_1^{''}, a_2^{''}, ..., a_{s-1}^{''})$, the data owners sub key $a_1^{'}$ matrix is finally obtained $(a_1^{''}, a_2^{''}, ..., a_{s-1}^{''}, a_1^{'})$,but the key matrix does not exceed s linearly independent, and complete key matrix M has rank s+1, therefore $a_1^{''}, a_2^{''}, ..., a_{s-1}^{''}, a_1^{'}$ cannot be a linear representation of the matrix M, is not able to derive the full key. In summary, if the provider key is less than s, even if there is a sub-key data owner, so it cannot launch a complete key.

(2) Lack of key data owners. Extract from a provider than s sub-keys, but the full key matrix M has rank s+1, therefore cannot be deduced the correct key.

(3) Data owner password greater than or equal s sub-key by cloud storage service provider key. Assuming decryption project has s cloud storage service and data owners sub-key , which together constitute a matrix $(a_1^{''}, a_2^{''}, ..., a_s^{''}, a_1^{'}, 0, ..., 0)^T$, and then the server change with a series of rows can be correctly deduced the complete key, obviously, if cloud storage service providers more than s key can also be deduced correctly complete key.

Thus, the threshold-based management program is a scientific technology.

C. Performance Evaluation

The performance analysis is based on the school cloud storage platform verification, it is mainly from the traditional (n,s) Encryption efficiency and security aspects were analyzed.

Figure 1 with the increase in the number of divided key, the time it takes to performance graph. It can be found that as the number of division increases, the traditional scheme (n,s) and the same programs tend to spend time, which indicates that the segmentation of the program is greater than a certain number of keys on the basis of the traditional partitioning scheme (n,s) and the same performance as the program.

Next, we use traditional hosting ideas (n,s) and this program was the same probability key crack, split scenario assuming full key split into n = 30 copies.

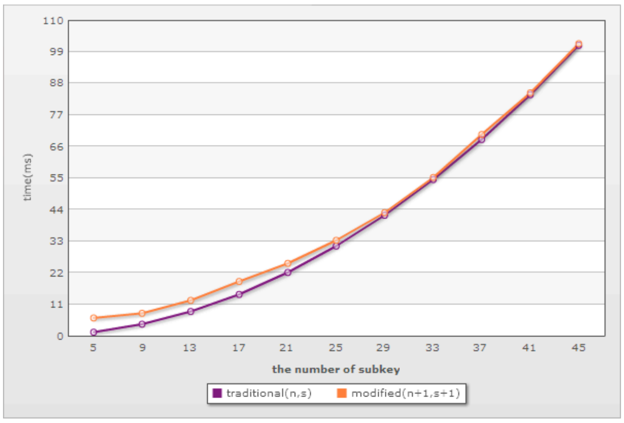

Figure 1. Traditional (n, s), and the new technology comparison

The simulation experiment results are as follows.

(1) When the attacker does not get to the data owner's key, with the increase in the number of the threshold s, the complete recovery success probability key is shown in Figure 2.

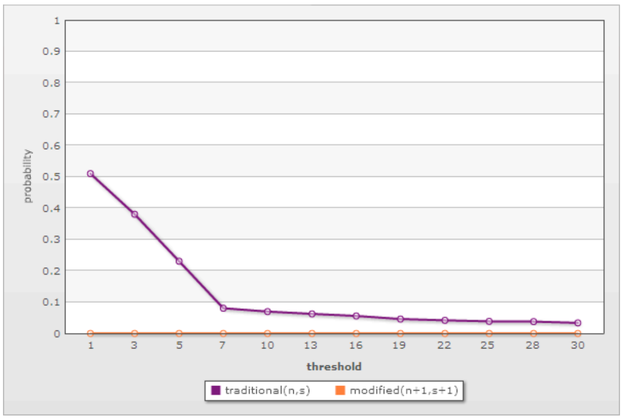

Figure 2. Traditional (n, s) and the new technology (without data owner key) graph comparing crack

From Figure 2, we can see that with the gradual increase in the threshold, the key is to break the traditional (n,s) full probability decreases, but the probability of this scenario to be cracked is 0, which is verified by theoretical analysis above: the program $(n+1,s+1)$, if the owner of the key missing data, then you must not break out the full key under any circumstances.

(2)When the attacker access to the key, with the increase in the number of

The threshold s, the complete key is the probability of successful recovery (Figure 3).

From Figure 2, we can see that, compared with the threshold gradually increased, the two solutions complete key is basically the same as the probability of cracking, and shows that even in the conditions of access to the key, two solutions the same security. Further validation of the program inherits the traditional scheme has the security features

Through this performance analysis, when the number is less than a certain number of split keys, the performance slightly worse with the traditional; But when the number is greater than the number of split keys, the performance is almost identical with the traditional. Meanwhile, the program has strong security, if no sub-key case; regardless of what method the attacker cannot break out of the complete key. Even if the cracks in the access to the data owner sub key case, the program also has the security of a traditional performance.

Thus, we can see that with respect to this program has a strong tradition of safety, because the cloud storage service provider without the user's sub-keys, the key cannot derive the full, so this program effectively solves the cloud storage service providers credible problem. Relative to the complete key, users' only need to save a small a sub-key, so that can be a good drop of data owners manage keys burden.

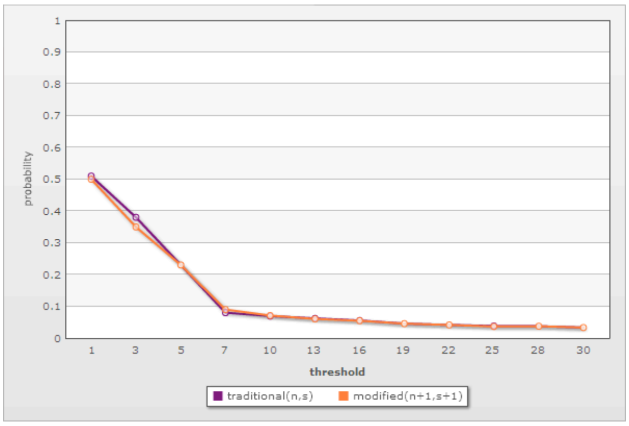

Figure 3. Traditional (n, s) and the new technology (data owner key) graph comparing crack

IV. CONCLUSIONS

Based on the current key management technology research and analysis for key management unilaterally research untrusted cloud storage service provider problem, we propose a key management technology, which is based on Shamir key mechanism based on a distributed hosting threshold Key split on the use of management techniques to achieve. The technique involves key managers to data owners and cloud storage service provider. This greatly reduces the file size of the key data owners, but also a good solution to untrusted cloud storage service provider hidden problems. Because the technology is based on the threshold to restore the original key, even if part of the cloud storage service provider sub key lost key recovery can also be a complete success, thus enhancing the robustness of the key, and their correctness and security both to verify the effectiveness of the technique.

REFERENCES

[1] W. Zeng, Y. Zhao, and W. Song, "Research on cloud storage architecture and key technologies." In *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology,* Culture and Human (pp. 1044-1048). 2009 ACM.

[2] E. Laurent, D. Gligor. "A key-management scheme for distributed sensor networks." *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 41-47.

[3] T. Landstra, M. Zawodniok, and S. Jagannathan, "Energy-efficient hybrid key management protocol for wireless sensor networks." In *Local Computer Networks*, 2007. LCN 2007. 32nd IEEE Conference on (pp. 1009-1016). IEEE.

[4] J. V. Martins, D. Tanré, L. Remer, and Y. Kaufman, "MODIS cloud screening for remote sensing of aerosols over oceans using spatial variability." *Geophysical Research Letters*,2002, 29(12), 8009. http://dx.doi.org/10.1029/2001GL013252

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM*, 1978, *21*(2), 120-126. http://dx.doi.org/10.1145/359340.359342

[6] M. Burmester, Y. Desmedt, "A secure and efficient conference key distribution system." *In Advances in Cryptology—EUROCRYPT'94* (pp. 275-286). Springer Berlin Heidelberg.

[7] M. Naor, A. Shamir, "Visual cryptography." *In Advances in Cryptology—EUROCRYPT'94* (pp.1-12). Springer Berlin Heidelberg.

[8] J. Sherman, W. J. Morrison, "Adjustment of an inverse matrix corresponding to a change in one element of a given matrix." *The Annals of Mathematical Statistics*, 1950,21(1), 124-127. http://dx.doi.org/10.1214/aoms/1177729893

[9] R. N. Calheiros, R. Ranjan, and C. A. De Rose, Cloudsim: "A novel framework for modeling and simulation of cloud computing infrastructures and services." *arXiv preprint arXiv*:0903.2525, 2009.

[10] E. Roe, M. V. Eeten, "Threshold-based resource management: a framework for comprehensive ecosystem management." *Environmental Management*, 2001,27(2), 195-214. http://dx.doi.org/10.1007/s002670010143

AUTHORS

Ningning Song is with University of Science & Technology Beijing, Beijing 100083, China (e-mail: 6221294@163.com).

Zhiwei Wei is with University of Science & Technology Beijing, Beijing 100083, China (e-mail: 5266675@163.com).

Xianwei Zhou is with University of Science & Technology Beijing, Beijing 100083, China (e-mail: 286319203@qq.com).

Qian Liu is with University of Science & Technology Beijing, Beijing 100083, China (e-mail: 1500257378@qq.com).

Submitted 03 October 2013. Published as re-submitted by the authors 05 November 2013.