ISSN 2186-5647

2-88

The Design of An Intelligent Router to Solve Security Problem in Cloud Computing

China University of Technology ○Chen-Yuan CHANG
China University of Technology Juhui HU

1. Introduction

In the foreseeable future, cloud computing will be the core technology in the information industry, and then the thin client will become main stream. However, the maintenance engineers in the cloud computing center have administrative privilege, they can easily leak customer's information without authorization. Security breach of this nature has caused a series of disputes; it is the main reason the public cloud is still not a preferred infrastructure, and cannot have the customer's trust. Although one of the popular solutions is to set up a strict discipline to control permission of maintenance engineers in the cloud computing center, however, this cannot still be able to prevent all the drawbacks mentioned.

2. Related Work

The telecommunications services have become complements for transportation, books for printed matter, and culture for recreation services, and then it has substituted for culture and recreation durable goods. Consequently, the increase in the expenditure on telecommunications is the migration of many services from offline to online by means of telecommunications [1].

However, the fact is that 62 percent of respondents had been notified that their confidential data was lost or breached, and that 84 percent of these consumers expressed increased concern or anxiety due to the data loss [2]. Therefore, this study is to explore how to protect information security issue of cloud computing from two ways of preventing data from stealing and missing.

According to our research, there are three aspects to solve data stolen and loss problems. The first is to control access permissions of users in the cloud computer center. The second is to encrypt the important information to prevent theft. The third is to use a backup server to prevent data loss due to server miss-management.

As for data encryption technology, there are two types of cryptographic systems: symmetric cryptographic system and asymmetric cryptographic system. The most widely use of symmetric cryptographic system is Data Encryption Standard (DES) encryption algorithm [6]. The most well known in asymmetric cryptographic system is RSA encryption algorithm proposed by the MIT scholars Ron Rivest, Adi Shamir, and Leonard Adleman.

Symmetric Key Cryptosystem is the most widely used as an encryption and decryption mechanism. When the cipher text is sent to the recipient, senders and recipients must use the same key to restore data. DES (Data Encryption Standard) is the most widely used, and officially adopted by the U.S. National Bureau of Standards in 1976. Instead of DES, Advanced Encryption Standard (AES) can do a faster encryption and decryption regardless of the hardware and the software. It is easy to implement, and it requires less memory. Since 2002, AES has been used and sustained promotion in practical application.

Asymmetric Key Cryptosystem is also known as Public Key Encryption. The most difference from the symmetric cryptosystem is encryption and decryption keys. The user must first generate a pair of keys; one for encryption and the other for decryption. One can be open to others, known as the Public Key, and the other, called the Private Key is not open to the public. In 1977, Ron Rivest, Ali Shamir, and Len Adelman [7] developed one of the first public-key encryption systems and published in 1978. This public key encryption has been the most popular method. RSA encryption algorithm is a special asymmetric cryptography. There are two keys called the public key and private key (or secret key).The key length is about 40 to 1024 bits. Public key is for encryption and the private key is for decryption, As long as descriptors do not give away private key to others, even if others have the public key, it is very difficult to deduct and calculate the private key. It is not a simple matter to decrypt by using reverse engineering. In other words, RSA is a very safe encryption and decryption algorithm.

In order to prevent software system from attack, which causes system crash and data leakage, and to reduce system recovery time, France proposed a framework of software distributed storage and deducted a mathematical model of queuing theory in the most cost-effective method [8][9][10]. This software dispersed storage method can effectively avoid invasion and attack, and also improve the efficiency of the firewall. Of course, it will increase the compatibility of the software and the maintenance costs. The longer web site uses, the higher survival rate is [11].

While these methods can effectively solve the security problem, they were only proposed solutions before cloud computing became popular. Therefore, there are some difficulties in using these methods directly. Dong-Joo Lee thought that the protection was related to the size of the system scale either in symmetry or in asymmetry [10]. In other words, the investment cost of the above methods is considerable for large-scale cloud computing.

IBM scholar Craig Gentry first proposed homomorphic encryption theory in 2009. Both encryption can be effective for information retrieval and query processing [12]. Any cloud computing service providers are completely inaccessible to the raw data, and the results only can be accessible by the user's local key after completing the operation. This fully ensures that the information does not leak. However, basic addition or multiplication will take up to hundreds even thousands of times higher than that on raw data. U.S. Department of Defense research institutions invested more than $ 20 million in 2011 to accelerate the research project. In August 2011, though Microsoft might implement the prototype, there were no commercial products of Fully Homomorphic Encryption available. Industrial Technology Research Institute of Taiwan (ITRI) also proposed a Partial Homomorphic Encryption [13] which does not support any combination of computing, but only Partial Homomorphic Encryption. The algorithm is designed to limited applications. However, it has not issued any commercial product.

Therefore, this paper proposed a management strategy of data encryption, partition and storage based on Chinese Tic-Tac-Toe game. The strategy does provide not only high efficiency of the implementation but also solves the problem of the information security in cloud computing, even cloud computing service providers can access split raw data, the data cannot be recovered.

3. The Proposed Strategy Based on Tic-Tac-Toe game

Based on Tic-Tac-Toe game, the purpose of this paper is to propose a management strategy of data encryption, partition and storage applied to cloud computing [14]. According to the private key, the client data is first encrypted and then these encrypted data are broken up into several modules. Finally, each module in a certain order is stored in different cloud servers, such as Figure 1.

Based on Tic-Tac-Toe game, the purpose of this paper is to propose a management strategy of data encryption, partition and storage applied to cloud computing [14]. According to the private key, the client data is first encrypted and then these encrypted data are broken up into several modules. Finally, each module in a certain order is stored in different cloud servers, such as Figure 1.

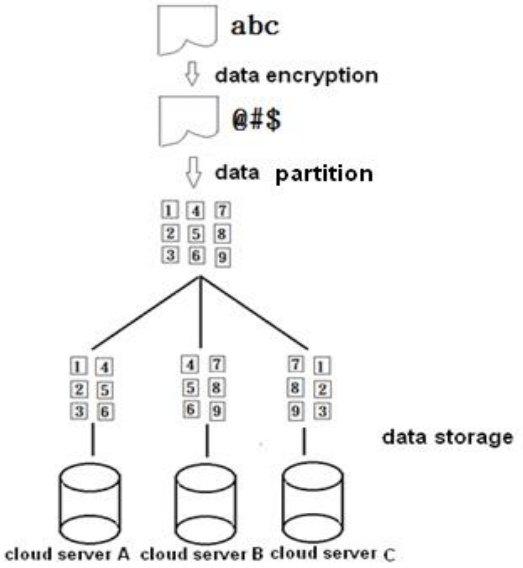

Figure 1. Data management strategy in public cloud computing

From Figure 1. maintenance staff of public cloud services can only access parts of information, but they cannot recover the original file by the brute force method. However, a proper access to the information stored separately on these two existing cloud servers, these two sets of data with some relationship can be recovered to the original file. The related information is also

likely to be intercepted and cracked if it is monitored in a long term.

Since the raw data should be divided into at least nine modules and then divided into three sets to store, the latter should be mutually related and easily combined to recover the original data. If one of the servers crashes, data stored in the other two servers can be recovered easily. This method not only provides data confidential benefit, but also reaches data security, the dual effects. How to randomly distribute these nine modules in three or more servers without being easily found by the cloud administrator? This is the focus of the proposed strategy in this paper.

Three sets of data among those servers must have some relation to each other. For example as Figure 1, 1-2-3-4-5-6 six data modules are stored in server A, 4-5-6-7-8-9 in server B and 1-2-3 and 7-8-9 in server C. When server B is old and damaged, nine data modules (1-2-3-4-5-6-7-8-9) are easily recovered from the other two sets of six modules stored in the server A (1-2-3-4-5-6) and the server C (4-5-6-7-8-9).

These three sets of data stored in the servers should have some connection, so that original nine modules can be restored from the other two sets of six. According to our findings, Tic-Tac-Toe game just can be applied. As long as one of these three sets can fall on a straight line of three-point relation in Tic-Tac-Toe game, it is consistent with this association. Therefore, this study refers Tic-Tac-Toe game directly. The client will select some cloud servers randomly and automatically distributed data to store in these servers. It can achieve both data security and data confidentiality. For illustrating these principles, in particular, an example is given as follows:

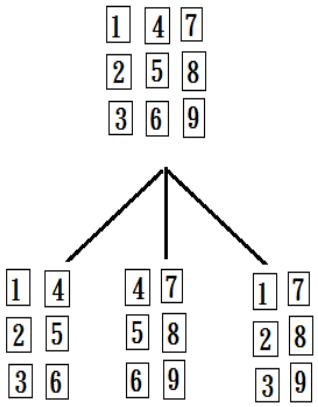

Figure 2. Relationships of 1-4-7 in 3X3 game

4.The Design of an Intelligent Router

With the previous discussions about the security problem in cloud computing, we proposed an intelligent router for each cloud user. In this router architecture, each user have split their data into several data bunks, then pass their data through different routing path to different cloud center immediately, however, this data path and row data can be encrypted and storied in local File Description Database (FDD). User do not need to keep in mind the details. This intelligent router will do all for you, the architecture is shown as in Figure **3**.

5.Conclusions

It is obvious that data are easily being uploaded at least more than three cloud servers in a cloud environment as the number of servers is increasing. In case of one server failure, the distributed stored data modules can be recovered to the original file. Due to parallel upload and download in the network, the number of the servers is increased, the faster the data access speed is. With the increase of the quantity of data, new data may be placed on the new cloud server. According to the management strategy of data encryption, partition and storage based on cloud computing, we can achieve the best overall performance of the data access speed due to the parallel in internet. In addition, based on the relationship of data encryption and distributed storage, the combinations of data storage identification just become as 2^2, 2^3… 2^n pattern when we increase the number of the servers. As long as the data storage identification is recorded, the original file can be easily recovered. However, the exponential increase makes network hackers hardly guess the combination of storage identification of each file in the servers. Although homomorphic encryption methods can solve information security issues of cloud computing [13], unfortunately data processing speed is too slow, and data parallel upload and download are not emphasized.

The cloud management strategy, proposed in this paper, will not only solve the most important problem of the information security issues in public cloud today, but also speed up data access in the network. In case of data corruption, furthermore, data modules in the other servers can be recovered as soon as possible. The related studies in this area should be more investigated in the future.

References

[1]. Dong Hee Lee, & Duke Hee Lee, Increase in Telecommunications Expenditure and the Migration of Consumption Online: The Case of South Korea, *The Information Society 28*, (2012) 61-82.

[2]. H. Jeff Smith, Information Privacy Research: An Interdisciplinary Review, *MIS Quarterly Vol. 35 No.4.4*, (2011) 989-1015.

[3]. David Ferraiolo & Richard Kuhn, Role-Based Access Control, *The 15th National Computer Security Conference*, (1992) 554-563.

[4]. Ravi Sandhu, Edward J. Coyne, Hal L, Feinstein & Charles E. Youman, Role-Based Access Control Models, *IEEE Computer Security, Vol.29, Issue 2*, (1996) 34-47.

[5]. Ravi Sandlhu, David Ferraiolo, & Richard Kuhn, The NIST Model for Role-Based Access Control, *The 5th ACM workshop* , (2000) 47-63.

[6]. Stallings William, Network Security Essentials: Prentice Hall, (2007)

[7]. Ron Rivest, Ali Shamir, & Len Adelman, A Method for Obtaining Digital Signature and Public Key Cryptosystems, *Communications of the ACM*, (1978) 6-8

[8]. France Belanger & Robert E. Crossler, Privacy in the Digital Age: a Review of Information Privacy Research in Information Systems, *MIS Quarterly Vol. 35 No4. 4*, (2011) 1017-1041.

[9]. Pei-yu Chen, Gaurav Kataria, & Ramayya Krishnan, Correlated Failures, Diversification, and Information Security Risk Management, *MIS Quarterly Vol. 35 No4. 4*, (2011) 397-422.

[10]. Dong-Joo Lee, Jae_Hyeon Ahn, & Youngsok Bang, Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection, *MIS Quarterly Vol. 35 No2*, (2011) 423-444.

[11]. Kihoon Kim & Edison Tse, Dynamic Competition Strategy for Online Knowledge-Sharing Platforms, *International Journal of Electronic Commerce, Vol. 16, No1*, (2011) 41-76.

[12]. Craig Gentry, Fully Homomorphic Encryption Using Ideal Lattices, *the 41st ACM Symposium on Theory of Computing (STOC)*, (2009)

[13]. Zhuan-Yu Zhuo, Trends of Cloud Computing Privacy Protection Technology, *NCP Newsletter No.39 , National Council*, (2012) 10-13.

[14]. Kurose and Ross, Computer Networking A Top-Down Approach, pp. 320-331

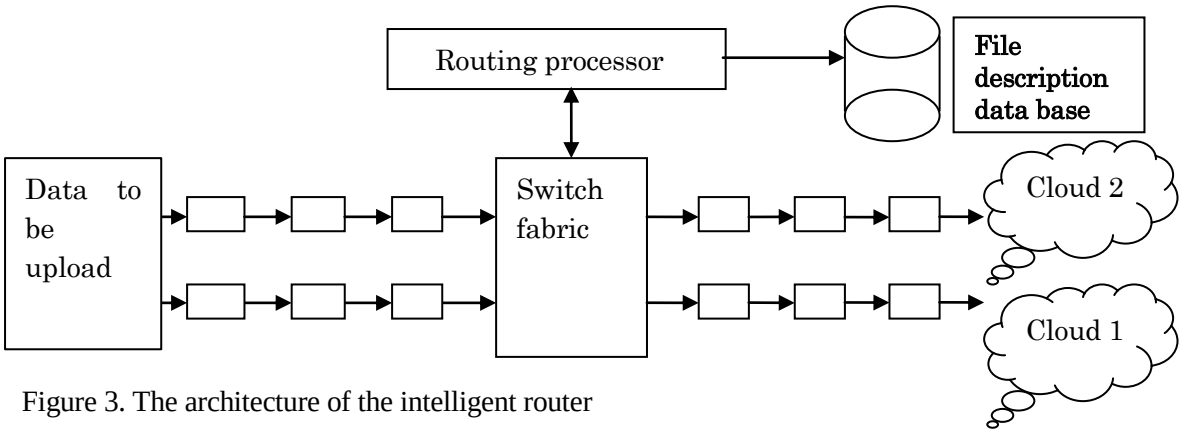

Figure 3. The architecture of the intelligent router