Cloud Data Life Cycle Security Issues and Research of Encryption Technology

Nengneng Li[1,2], Yongsheng Zhang[1,2,*] , Yueqin Fan[1,2] and Liang Chang[1,2]
[1]School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China
[2]Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan, 250014, China
*Corresponding author

***Abstract*—With the further development of the cloud computing, the security of the cloud computing is becoming increasingly prominent. Based on analyzing the development status of cloud computing, this article will focus on studying the security of cloud computing in data, and discuss the data security problems in the process of data life cycle in cloud environment. Then the paper will put forward the corresponding measures and data encryption technology, in order to protect the data security of cloud computing.**

Keywords-cloud computing; cloud security; data security; encryption; erase technology

I. Introduction

Cloud computing as a new mode of operation or a new concept of information services, its development has gradually become mature. But anyway, many companies still hold a wait-and-see attitude to the commercial application of this model. The main reason is that the cloud computing has low security. Cloud computing user diversity, structural complexity and the dynamics of the data are likely to make the data in the cloud environment be extremely uncertain, and even cause huge losses [1]. This paper will analyze some problems about the data security of data life cycle in cloud environment, and give the corresponding solutions.

II. Development Status of Cloud Computing

A. Cloud Computing Concept

Cloud computing is a model that is paid according to the usage. This model can provide a convenient and available, on-demand network access and enter configurable computing resources shared pool (including network source, server resources, storage resources, software resources and service resources etc.). These resources can be quickly provided and only need to put a few management work, or rarely interact with service providers.

B. Research Status at Home and Abroad

Cloud computing as a new concept is put forward in August 9, 2006 SES San Jose 2006 by Google CEO Eric Schmidti for the first time. It gradually develop such a mature level according successively experienced a power plant model, utility computing, network computing and cloud computing four stages. At present, more and more organizations and structures including the International Telecommunication Union[2], cloud security alliance[3] and structured information standards of[4] have been joined in the rank of research and development of cloud computing standards[5]. And Amazon, IBM, Sales, force, Microsoft and Google IT giant enterprises invested a lot of manpower and material resources and financial resources to the research of cloud computing, and have launched their own cloud computing platform[6].

III. Data Life Cycle

In cloud computing, data has experienced six processes from generation to destroy, being referred to as the life cycle of cloud data which includes six stages: data creation, data storage, data transmission, data using, data archiving and data destruction. The specific process is as follows Figure I shows:

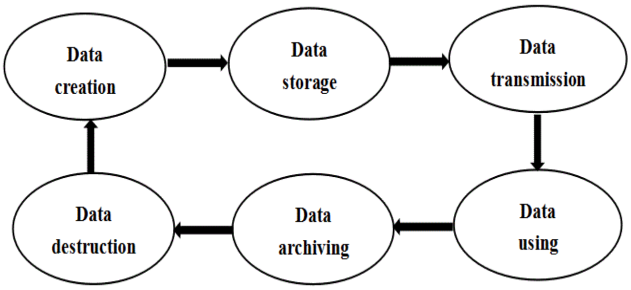

FIGURE I.DATA LIFE CYCLE

In the various stages of the data life cycle of cloud computing, there are security issues. In order to reduce the security risks of cloud data, we must do a good job in safety treatment in the various stages of data development.

A. Data Creation

The process of creating data is done by individuals. Individuals or enterprises create their required data according data collection, input, query, processing etc. on their own equipment. The safety problems including data leakage and external personnel access in this process may appear. To ensure the safety and reliability of data in the whole process, we need to carry through access control, encryption and security and other aspects of the data control.

B. Data Storage

The data after producing is stored in the storage space, such as memory, hard disk. But the storage space must be in geographical location allowed in the contract, service level agreements and regulations. All stored data must be guaranteed including copies and backups to prevent causing loss by data loss. For example, the use of electronic health records managed by the European Union's regulations to comply with storage regulations may provide a challenge for the owner of the data and the cloud services provider [7]. The data should be considered the reliability, confidentiality, integrity, and whether the security permissions management of suppliers is perfect, whether the stored data is managed safely, whether data storage format is reasonable after it is stored in the cloud [8]. So, in order to ensure the safety of data in this process, we need to take measures including data integrity, data encryption and data isolation and etc. to data.

C. Data Transmission

The biggest feature of the data is its sharing. Data provides data for other customers through the transmission to achieve the sharing of data. Cloud data is transferred to other customers and virtual services to use through the network, the process of communication and other ways. Due to the openness of the network, the data can not be carried out in the situation of without security control. The data creator needs to consider whether to set administrative permission to data. So in order to guarantee the security of data transmission, we need to use data encryption technology while maintaining confidentiality in the process of data transmission and integrity after data transmission.

D. Data Using

Data using is the ultimate purpose of data that is created in the life cycle. The user should check the source of the data before using the data. Then we conduct data decryption after determining its security. And we can to conduct data operation. Before using the data we must make a backup of it, not casually assume that the cloud environment data has backup and can be recovered. In order to prevent the loss of data in the process of using, we must have an effective backup of the data and make an effective recovery plan for the data.

E. Data Archiving

Data archiving is to save the old data that has been used according to certain rules. These old data are very important data and has a certain reference value in the back of the process. Data archive has index and search function, so that the data can be easily found in the future. But these data require high security and access control. In the absence of a careful examination of the third party services, the compliance data is stored in the cloud archive that may bring risks in the cloud environment. Therefore, in the process of data archiving, we must keep the data secret, such as disk backup and other long-term storage media.

F. Data Destruction

After cloud data is saved in the external storage space, if the data has been used up, it must be cleared so that storing other services data is more convenient. More important thing is to ensure the safety of the data. In the original destruction of the work, the most commonly used method is to delete. But this method of knowledge destroyed the file pointer and did not completely destroy the document. For the core documents and confidential data of enterprise users, it is necessary for cloud service system to set up an erase, or to provide a more direct method to remove the medium corresponding to protect sensitive data.

IV. DATA SECURITY TECHNOLOGY

In cloud computing, data security issues run through the use of the entire cloud terminal. The place where data flows need to establish a security mechanism. In the process of data life cycle, data encryption, data backup, data isolation and data erase are essential to ensure the confidentiality and integrity of data.

A. Data Encryption Technology

Data encryption is the core content of ensuring data safety in the life cycle process. Cloud computing service providers and businesses need to use data encryption technology to ensure the security and integrity of data transmission in process of data creation, storage, transmission, use and archiving. Now, cloud computing service providers improve and promote the data encryption environment. But users still need to encrypt own data by himself and can also encrypt the data in the service process by using third party technology [9,10].

Encryption technology consists of two parts, the algorithm and the key. The algorithm refers to the process of how to combine the data with the key to output cipher text and decipher the original data into the original data. The key is the data encryption and decryption algorithm. Password mechanism can be divided into symmetric encryption and asymmetric encryption technology. The classic symmetric encryption technology is DES algorithm and the classic asymmetric encryption technology is the RAS algorithm.

1) Symmetric encryption technique DES: Symmetric encryption technology refers to use the same encryption keys and decryption keys in the process of data encryption and data decryption to ensure the safety of data. The symmetric technology has the advantage of simple and easy to use, and can meet the basic requirements of data encryption. Symmetric encryption technology is the most common use of data encryption technology. Figure II is the flow chart of the symmetric encryption algorithm.

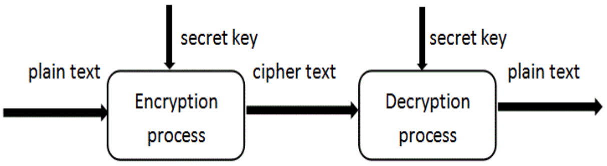

FIGURE II.FLOE CHART OF ENCRYPTION ALGORITHM

Symmetric encryption algorithm includes two types: block cipher and stream cipher. Block cipher algorithm is to deal with the plain text based on the data block as a unit. It will enter the plain text as a whole and output a length of the cipher text group. In most cases, the block cipher adopts Feistel structure, and improve the security of encryption algorithm through the same operation. In each round, it only substitute half of the packet. After the exchange, it substitute the other half in the next round. Each round operational use keys are different. Stream cipher algorithm known as the sequence cipher algorithm, is a continuous processing of the plain text and usually the bits or bytes are used as the object of operation. The typical structure of stream cipher includes a pseudo-random number generator. When the key is not known it can produce a predictable pseudo random flow. The input plain text conducts XOR with the pseudo-random stream successively to encrypt data. The typical symmetric encryption technology DES is introduced in the following.

The DES[11] design of the core idea of is to make all of the secret key in it. Prior to encryption, DES is divided into 64 bits as a packet unit, and the whole text is divided into groups. Then each packet is encrypted to generate a set of cipher text. Each cipher text message still is 64 bits. Finally connecting each group cipher text obtains encrypted information. Figure III is the schematic diagram of DES encryption.

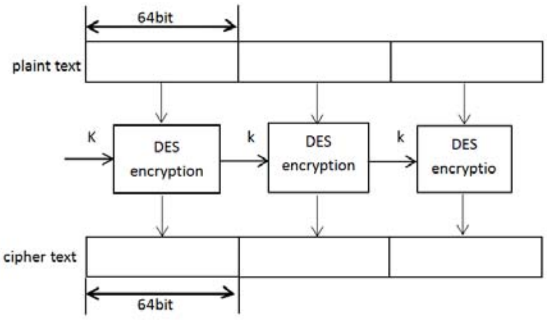

FIGURE III.DES ENCRYPYION SCHEMATIC

DES algorithm is mainly divided into three stages to deal with the text.

Phase 1: Replacement IP. In the process, each 64bit packet is reorganized in accordance with the bit and does not need to use the key. The initial replacement is simply shift operation. The 0 and 1bit series in plain 64bit are arrayed according 8 * 8 matrix and are numbered. Then disrupt according to rule that the original packet fifty-eighth plain text and fiftieth positions substitute to first and second place and rearrange.

Phase 2: Replacement and replacement. It conducts 16 times cycle encryption algorithm related to the cipher text. The 64bit that has been performed initial replacement will conduct 16 times cycle encryption algorithm related to the cipher text.

Phase 3: IP^{-1}. It is the inverse of the initial replacement. This process is the inverse operation of the replacement process, so it will not use the key.

In the process, the function of initial displacement is to recombine 64bit data blocks that have already input and respectively output L1 and R1 two parts. Each part has 32 bits length. The replacement rule is to change the input fifty-eighth to the first, the fiftieth to the second......and so on. The last one is the original seventh. R1 and L1 is the two part of the output after conversion. L1 is 32 in the left and R1 is 32 in the right.

For example, the input value before the replacement is N1N2N3...... N64, then the output value after the initial replacement is: L1=N58N50...... R1=N57N49; N8...... N7. Replacement rule can be listed as follows.

58, 50, 42, 34, 26, 18, 10, 2, 60, 52, 44, 36, 28, 20, 12, 4,

62, 54, 46, 38, 30, 22, 14, 6, 64, 56, 48, 40, 32, 24, 16, 8,

57, 49, 41, 33, 25, 17, 9, 1, 59, 51, 43, 35, 27, 19, 11, 3,

61, 53, 45, 37, 29, 21, 13, 5, 63, 55, 47, 39, 31, 23, 15, 7.

2) Asymmetric encryption technology RAS: Asymmetric encryption algorithm can also be called public key encryption algorithm. Asymmetric encryption algorithm mainly includes six key elements: encryption algorithm, decryption algorithm, plain text, cipher text, public key and private key. The public key and private key are two components of the key. The public key is registered in a trusted public database, which is open and accessible to all people. The private key is kept by the user himself, which is private and not open to the public. The data sender uses the public key to encrypt the plain text according to the encryption algorithm, then sends the cipher text to the data receiver. The receiver decrypts the cipher text using his own private keys and reads the data. Asymmetric encryption algorithm process is shown in figure 4.

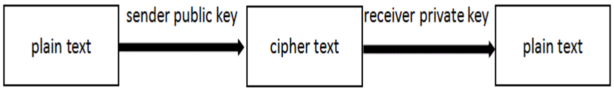

FIGURE IV.NON SYMMETRIC ENCRYPTION ALGORITHM

RAS public key cryptography algorithm is a typical representative of the asymmetric cryptography algorithm, which is divided into two parts: the key generation method and the encryption (decryption) algorithm. RSA algorithm involves three parameters: n, e1, e2. Among them, “n” is the product of two large prime numbers P, Q. “n” binary represent the occupied bits, and is called a key length. e1 and “e2” are a pair of related values. “e1” can be any number, but e1 and (p-1) * (Q-1) must be coprime. Then to choose e2, it requires to meet the formula that is (e2*e1) mod ((p-1) * (Q-1) * ()) =1. (n, e1) and (n, e2) is the key pair. Among them, (n, e1) is the public key and (n, e2) is the private key.

RSA encryption algorithm and decryption algorithm is exactly the same, Let A as plain text and B as the cipher text. Then: A=B^e2 mod n; B=A^e1 mod n.(In the system of public key encryption, the public key is used to encrypt, and the private key is used to decrypt.) “e1” and “e2” can be exchanged to use, which is A=B^e1 mod n; B=A^e2 mod n.

RSA public key and private key are generally constructed by two decimal prime numbers that are greater than 100. So it is difficult to crack them and it has high security. But the disadvantage is that it has a very large amount of computation, resulting in slow computing speed. Compared to DES, it is nearly 100 times slower. Because of the speed limit, RSA is generally used for some encryption that has a small amount of data[12,13].

B. *Data Erase Technique*

After the data is used, there will be a lot of data manipulation traces in the system. These records include a lot of personal privacy information, it is extremely easy to pose a threat to personal information security. A great majority of users will delete the data after using them, or clear the use records. But a lot of data recovery software can recover the information. So, after the data is used, we should erase data and destroy the use record.

In cloud computing, data erasure technique positions to these data and eliminates them in an irreversible way mainly based on the user's need of information elimination. The main purpose of data wiping technology is to resist the data recovery technology, and achieve data elimination authentically. At present, the mainstream information technology is to cover meaningful data storage area with meaningless data, to achieve the purpose that data can not be recovered by repeatedly writing.

V. Conclusions

This paper gives a brief description of the life cycle of cloud computing data. It introduces the security problems that we encounter in the process of generation, transmission, sharing and use of data, and gives the related solutions. This paper expounds two kinds of technology to ensure data security, data encryption and data erasing technology. But the use of this data security technology is confined to the enterprises and users that have a higher security conscious. It is not popular in the general users. Ordinary users are lack of safety awareness to cloud computing data, and not to realize the importance of using the data security technology. Therefore, it become extremely important to closely interrelate cloud computing data security with people's daily life.

Acknowledgments

This research was supported by the Postgraduate Education Innovation Projects of Shandong Province of China under Grant No.SDYC15042. In addition, the authors would like to thank the reviewers for their valuable comments and suggestions.

References

[1] Cheng Fenggang, “Data security risk and prevention strategy based on Cloud Computing,” J. Library Science Research, 2014, 02:15-17.

[2] International Telecommunications Union [DB/OL]. http://www.itu.int/en/pages/default.asp

[3] Cloud Security Alliance [DB/OL]. http://www.cloudsecurityalliance.org/

[4] Organization for the Advancement of Structured Information Standards [DB/OL]. http://www.oasia-open.org/

[5] Han Shuai, Research on Key Technologies of data security based on Cloud Computing [D].University of Electronic Science and technology, 2012.

[6] Duan Chunyue, Research on security of cloud computing and data security transmission [D].Chengdu University of Technology, 2012.

[7] Wang Xinlei, Research on data security technology of cloud computing[D].Henan University of Technology, 2012.

[8] Liu Shaoxing, Research on Key Technologies of data security in cloud computing [D].Qingdao Science & Technology University, 2014.

[9] Wang Qingbo, He Le,Zhao Yang etc, The technology and practice of cloud computing. [M].Beijing Electronic Industry Publishing House, 2012:3-110.

[10] Chen Junjian. Research on the security technology of object oriented storage system [D].Huazhong University of Science and Technology, 2011.

[11] W Stallings writing, Meng Qingshu etc. translating, Cryptography and network security: Principles and practices (Fourth Edition)（M）. Electronic Engineering Publishing House, 2006.11.

[12] Su Hongyi, Research on the method of data privacy protection in cloud computing [D].Nanjing University of Posts and Telecommunications, 2012.

[13] (American) John W. Rittinghouse, James F. Ransome. Tian Siyuan, Zhao Xuefeng translating. Implementation, management and security of cloud computing .Beijing: Mechanical Industry Press, 2010.