Research of Data Security in Cloud Storage

Wenjing Zhang[1,a], Chuanlong Ma[1,b], Weichao Sha[1,c], Qiaoyu Zhou[1,d]

[1]Chongqing Communication Institute, Chongqing, 400035, China

[a]email: 602382254@qq.com, [b]email: 85950300@qq.com, [c]email: 175760261@qq.com, [d]email:23565512@qq.com

Keywords: Cloud Storage; Data Security; Encryption Technology

Abstract. Cloud storage provides a lot of data access service, but may bring serious security problem. In this paper, it discusses cloud storage's demand for data confidentiality, integrity, availability, then puts forward the corresponding solutions. It uses incomplete encryption, users manage the key independently. The cloud storage data is encrypted to ensure the security of data.

Introduction

In the 1990s, parallel computing and network computing technology is developed maturely, and has been successfully applied, cloud computing actually has not far from us [1].Cloud computing has changed the business model, but also changed people's life, work. It really happens in our side. With the gradual development of cloud computing technology, people began to search for a new scheme for mass information-cloud storage. The problem of users most care about is the security of data in cloud storage. It has become the biggest obstacle to the development of cloud storage. In the face of these unsafe factors, we need to improve relevant cloud storage technical means, the user's security awareness, the deployment of cloud service provider's safety equipment and safety measures, and trusted security issues. It ensures the maximum extent safety and availability of cloud storage.

Introduction of the Cloud Storage

The cloud storage is a storage part of cloud computing. It's the storage resource pool which it's virtualization and easy to extend. The emergence of cloud storage means that the storage can be used as a service, through the network to provide to the users. Users can use it to store in several ways, and pay by the way of using time or space.

Compared with the traditional way of data using, the cloud storage access way is more diverse and easy. Any hardware equipment in the cloud storage system is open and transparent for users. Users can use authorized account at any time and everywhere. They can connection with cloud storage through a cable and access data from a cloud storage. Users use the data access service which is provided by entire cloud storage system, not only use a storage device. As shown in Fig.1.

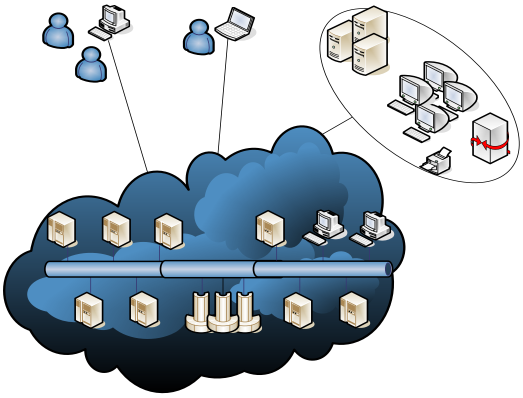


Fig.1. The model of the cloud storage

Security Problem of the Cloud Storage

Cloud security situation

The cloud storage platform solves most of the security issues, but paies less attention on data confidentiality. For example: the Amazon's cloud platform provides a series of powerful cloud services, but the file storage services and database storage service does not provide data encryption; Huawei provides data storage service for the file, and has a strong function of data synchronization and data sharing , but does not support data encryption; HDFS and HBase in Hadoop provide open source cloud storage solutions, but does not support the data encryption. The cloud data which is not encrypted will bring a lot of potential safety problems [2]. Once the cloud storage platform is breached, tens of thousands of users and enterprise data will be leaked, and the interests of the cloud storage service providers and service consumers will suffer a huge loss. So we will improve cloud storage platform in the aspect of data confidentiality, include file encryption, database encryption and key protection three aspects.

Although the cloud storage is the emerging things, we can try to use the traditional features of the C.I.A.(Confidentiality, Integrity, Availability) for the data security in cloud storage.

Cloud storage security technology

(1)File encryption and decryption principle

In the computer file exists in the form of data. Computer files can be considered as the collection of bytes. Encryption transforms the understandable ordered data into disordered incomprehensible data. The file format is damaged, so that it is not available or not readable. The encryption is completed. Encryption improves data security in use, save and transfer. While the decryption can be regarded as the reverse process of encryption, using the same key, through the decryption algorithm, and the file data is restored to its original state which can be understood.

(2)DES algorithm

DES (Data Encryption Standard) is the most typical and the most widely used block cipher Algorithm [3]. The plaintext block length is 64bit as the algorithm input at one end, key's length is 64bit (effective 56bit) as the other end of the input. First, a group of plaintext is disposed by the initial transform (IP), then make the disposed plaintext to the 32 bit left half and right half. After 16 rounds of operations which is related to the key. Finally disposing replacement (IP-1) which is inverted with initial permutation, getting 64bit cipher text output. DES algorithm is converted after 16 rounds of complex transformation. The purpose is to increase its chaos and diffusivity as far as possible, so it can't make translator to get the key from calculating.

(3)AES algorithm

AES (Advanced Encryption Standard) also is known as the Rijndael encryption. Rijndael is safe, effective, high performance and convenient, so it is the AES's best choice. This standard is used to replace the original DES, and it has been used all over the world. AES is an iterative, symmetric key group password. It can use 128, 192 and 256 bit key, and use 128 bit (16 bytes) packet to encrypt and decrypt data. Its operation can easily withstand attack on the time and space.

(4)RSA algorithm

RSA is one of the most influential public key encryption algorithm. It protects against all the passwords attacks as we known, and it has been recommended by ISO for public key data encryption standard. RSA algorithm is a kind of asymmetric cryptographic algorithms. Asymmetric is refers to the algorithm needs a pair of keys, one of them is used to encrypt and the other is used to decrypt.

Analysis of the key issues

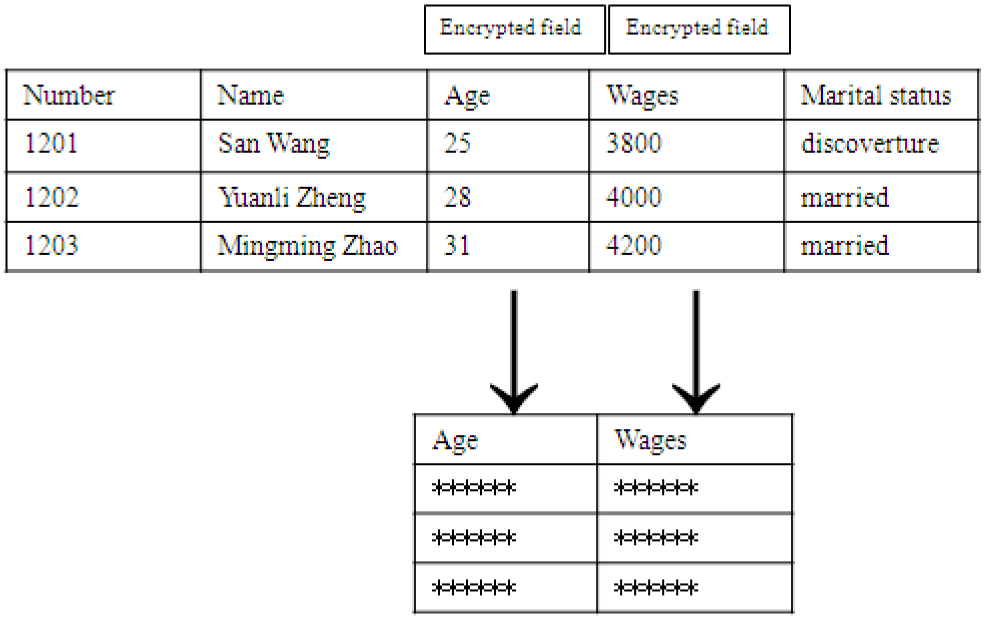
(1) File encryption

To encrypt all file if only consider the confidentiality of the documents, not only waste of computing resources, but also can reduce the performance of the storage service. Not all users' files need to be encrypted. For example, pictures, video, this type of file is public data which is shared with the users, so it is not necessary to encryption. But such as the company's financial statements must be encrypted, to ensure data security [4]. So we can let the user to choose which files need to be encrypted and which does not need to be encrypted, in order to improve the service performance.

Different algorithms for different length of file encryption efficiency is different. If only using an encryption algorithm for different file, so it will reduce the performance of the storage service. We consider a single encryption algorithm for different lengths of file encryption effect is different. It can influence the cloud storage service performance seriously. We consider it from the encryption time consumption and file security, for larger files we use chaotic mapping and DES algorithm to encrypt. This algorithm encrypt large file using short time than other traditional algorithm, and more security. But this algorithm is weak for small files, so we choose safe DES algorithm for small files.

(2) Database encryption

After encrypting database data, some functions of database management system such as indexing, retrieval and so on, will not be able to use directly. We just encrypt sensitive data fields, and retrieval fields who may be used to index is not encrypted, thus we solve the above problems, and cost less time on the encryption. For example: on the payroll, you can encrypt only the "wages" field, but the number of wages, the name which is used to index, retrieve need not encrypt. As shown in Fig.2.



Number	Name	Age	Wages	Marital status
1201	San Wang	25	3800	discoverture
1202	Yuanli Zheng	28	4000	married
1203	Mingming Zhao	31	4200	married

Age	Wages
******	******
******	******
******	******

Fig.2. Database according to the field of encryption schemes

(3) Key protection

If every user only has one key, the key’s oneness can help the attacker to find rules and crack encryption algorithm easily. Each file uses a different key, each field of database also uses different keys, and it will increase the complexity of the secret key, increase the difficulty of the crack.

Most of the data encryption scheme store keys in the form of plaintext after the data is encrypted, so that the attacker is likely to find the key and the decrypt the data. We encrypt the data keys, and keep the encrypted data keys in the cloud storage platform. We encrypt data key using the public key encryption algorithm-RSA [5]. A pair of RSA keys are generated during user registration, and user's public key is kept by the cloud storage platform which is trusted, the key is used to encrypt data. Users’ private key is only the users themselves know. Private key is used to decrypt data. It is provided to cloud storage platform when the data is decrypted. Platform dosen’t keep the users’ private key after data is decrypted. As shown in Fig.3.

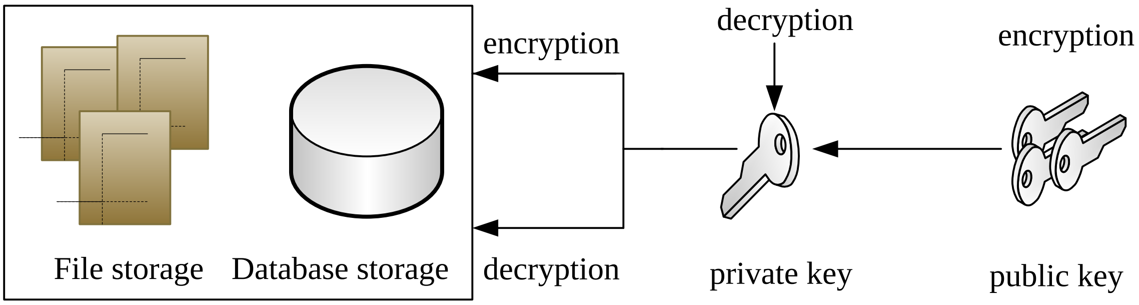


Fig.3. Key diagram

Most of the data encryption scheme store the encrypted data and the key in a module, so that once the attackers break the module, you can get the key and the encrypted data at the same time. It is likely to break the user data. Once the attackers break this module, you can get the key and the encrypted data, it is likely to break the user's data. In order to improve the security of the data, we store all the data keys in a separate module, and user's data completely independent. If the user data's storage module is breached, the attacker can only get some encrypted data. If the key store module is breached, the attackers also don't have access to user data. Both two modules are breached is impossible.

Conclusion

With the expansion of the data storage, the cloud storage technology has been widespread concern and support because its high performance, low cost. This paper combines the knowledge of information security, especially the encryption technology, solves the safety problem of cloud storage, so that users can trust cloud storage service under they distrust of cloud storage service providers. Users can use cloud storage service as very safe and reliable service, and the cloud storage technology get more extensive application. Through the research of cloud storage security, also may can provide cloud storage system's security from the hardware.

References

[1] AtenieseG, BurnsR, CurtmolaR. Provable data possession at untrusted stores[A]. In Proceedings of CCS'07[C], ACM Press, New York, 2007.

[2] Y. Deswarte, J. Quisquater, Remote Integrity Checking [C]. Sixth Working Conference on Integrity and Internal Control in Information Systems. Kluwer Academic Publishers, 2004:1–11.

[3] AtenieseG, DiPietroR, ManciniLV. Scalableand and eficient provable data possession[C]. In Proceedings of SecureComm'08, 2008:16-27.

[4] WangQ, WangC, Li J. Enabling public verifiability and data dynamics for storage security in cloud computing[C]. In Proceedings of ESORICS'09, Saint Malo, France, 2009.

[5] Li D Y, Lin R H. Cloud Computing Technology Development Report[R]. Beijing: Science Press, 2011:84-97.