A Design of Privacy Data Encryption and Decryption System for Data Security in Clouds

Cheng Wenjuan[1,a], Tong Bing[2,b], Zhou Miaomiao[3,c]

[1]School of Computer and Information, Hefei University of Technology, Hefei, 230009, China

[2]School of Computer and Information, Hefei University of Technology, Hefei, 230009, China

[3]School of Computer and Information, Hefei University of Technology, Hefei, 230009, China

[a]email:cheng@ah.edu.cn,[b]email:eric_tongbing@163.com,[c]email:miaomiaozhou@mail.hfut.edu.cn

Keywords: Privacy Data; Encryption; Decryption; DES algorithm

Abstract. With the rapid development of the IT technology, users increasingly rely on data. While cloud storage and other online service platform make user's privacy data protection become an important issue. In this paper, we have designed an encryption and decryption system for user's privacy data files, it can be used to encrypt and decrypt the privacy data. The system uses the DES algorithm to provide certain security to the data files, and supports a variety of data types and file types with good operability.

Introduction

Cloud storage is similar to cloud computing. It is derived and extended from the concept of cloud computing. It refers to a system that through cluster application grid technology and distributed file systems and other functions, to make a large variety of different types of storage devices through the application software work synergistically, and provides data storage and business access externally [1] [2]. Cloud storage usually means that source data or backup data will be placed in the storage pool that users can not determine outside, rather than placed in local data center or dedicated remote site.

In fact, when using cloud storage service, internal privacy data in the cloud has a certain risk. Before migrating data to the cloud, whether it is public cloud or private cloud, the fundamental problem must be solved, that is data security issues. Users concern about that once privacy data is uploaded to the cloud, they can not have direct control over the remotely stored data [3].And security of privacy data depends on the service of cloud storage provider, but cloud storage provider can not manage these privacy data in the cloud comprehensively and effectively, and lots of unreliable factors can bring some security management issues [4].Nevertheless, the encryption of privacy data is the basic method to protect data. Before uploading privacy data to the cloud, it has been encrypted in the local, even if attackers stole the encrypted data, they would not know the real content of the data. Therefore, it ensures the security of privacy data in the cloud storage. When users need privacy data, the data can be obtained from the cloud and decrypted in the local as well.

Functional Requirements Analysis

At present, most of cloud platform providers have a series of powerful cloud storage services, For example, Hadoop provides cloud storage solutions, and Amazon cloud platform provides files and data storage service(Simple Storage Service, Amazon S3)etc [5], but they can not provide the data encryption service. Data in cloud is not directly controlled by users. Therefore, the problem of data security is becoming more and more prominent. From the user's point of view, it is necessary to solve the security problem fundamentally before using the cloud storage service. In this paper, we have designed an encryption and decryption system for data security in cloud. Privacy data is encrypted on the local computer before uploading to the cloud, stored in cloud server with encryption form, then obtained from the cloud server, and decrypted in the local. This approach can greatly improve the security of data in cloud.As shown in Figure 1.

© 2015. The authors - Published by Atlantis Press

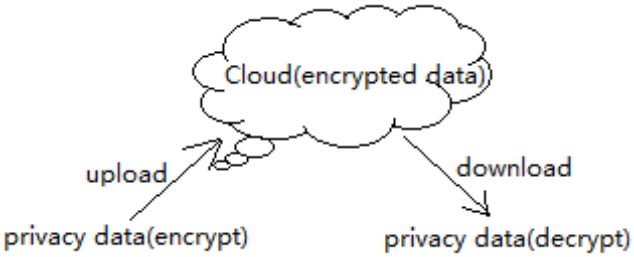

Fig.1. System function diagram

Data Encryption and Decryption Process

According to the requirements, the program flow diagram can be designed. Users first enter a password parameter and keep it. The key is generated from the password parameter. Then users select the data file that need to be encrypted. According to the DES algorithm and the generated key , the system encrypts the data file. When users need the encrypted data, select corresponding ciphertext file and simultaneously enter the reserved password parameter, the system will perform the appropriate decryption operation. As shown in Figure 2.

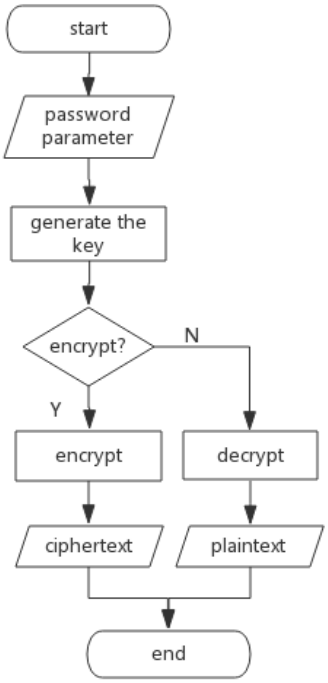

Fig.2. Data encryption and decryption program flow diagram

System Main Function Modules

The system mainly includes three modules: the client module, the key generating module, the encryption/decryption module. As shown in Figure 3.

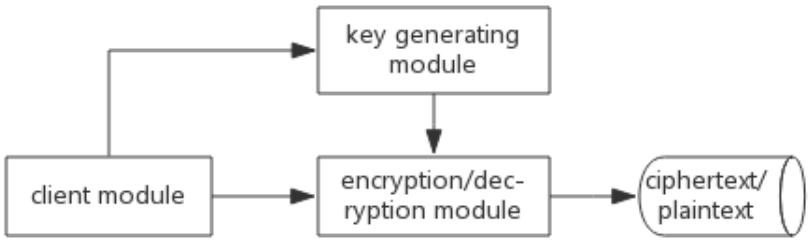

Fig.3. System main function module

The Client Module

The main function of this module is responsible for acquiring file data and storing encrypted/decrypted file data. Through the interface provided by the client, users access the file and read it in the local, then call the system's API to pass the file data to the encryption/decryption module.

Data Encryption/Decryption Module

Data encryption/decryption module is the core module of the system. It mainly encrypts and decrypts the file data passed from the client. Then the processed data are stored in the local. As shown in Figure 4.

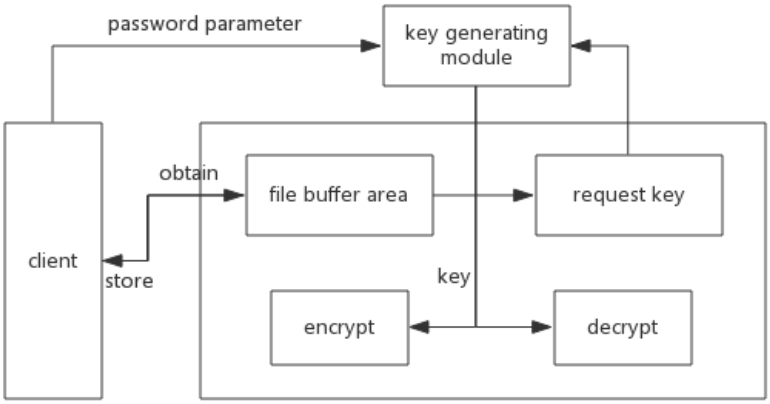

Fig.4. Data encryption/decryption module

Putting the file obtained from the client module into the buffer, and requesting a key to the key generating module. Then the key will be passed to the function of encryption/decryption module to process the file. Finally, the processed file is returned to the client. At the same time, the system provides batch encryption service. Users can pack the file data to the specified folder when they need to encrypt large quantities of data, just get the folder path, all files in the folder will be encrypted immediately, which saves much more time for users.

The Key Generating Module

The encryption key is produced by this module. In order to improve safety, each password has a different key format. To ensure that the key generation is random, the following steps are required:

(1)Get KeyGenerator for encryption algorithm.

(2)Use random source to initialise the KeyGenerator.

(3)Call generateKey method.

As shown in Figure 5. In order to generate a digital sequence at a random point key, users provide a key parameter as a random input source. At the same time, users need to keep the random input source as the password for decryption operation.

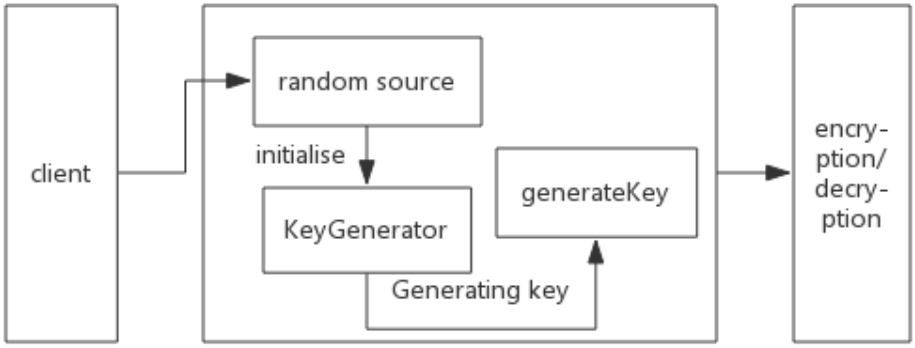

Fig.5. Key generating module

Conclusion

The system uses Java programming language, with good interactivity. The correctness of the algorithm is tested under Windows environment.

When testing, the application is deployed to IBM Bluemix cloud platforms, which is the latest cloud offerings from IBM.When using, users enter a password parameter key and keep it. If processing a single file, through clicking on “Source File/Encrypted File”, users select the location of the file. After determining clicking "encrypt/decrypt to", then select the path of the encrypted/ decrypted file to store. Finally the processes are completed successfully. As shown in Figure 6.

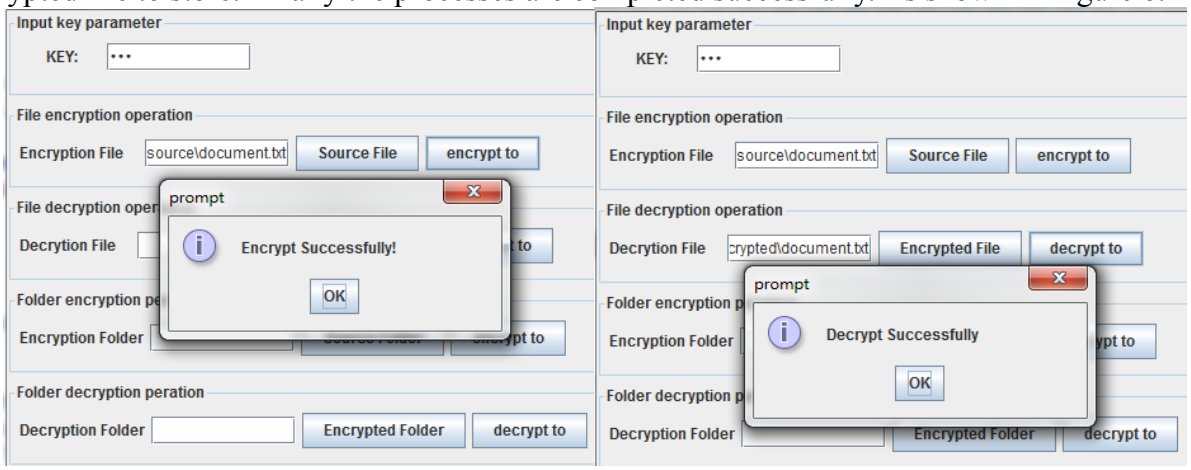

Fig.6. Single file encrypt/decrypt

When users need to handle large quantities of data files, the data files can be placed in a folder to be processed, which can save much more time to complete encryption/decryption simultaneously for all files in the folder.

Summary

Cloud storage and cloud security technology is filled with challenges during the development and breakthrough period, many problems in cloud storage and cloud security required to be solved, such as data encryption, data isolation, access rights, security authentication etc, which are all the core issues that users care about. In this paper, we only studied the encryption/decryption, and many limitations still exist, such as the DES algorithm's key length is too short, which reduces the security of the data, the key can also use encryption algorithm to guarantee data security, and other privacy data encryption and decryption algorithms, which we consider are our future work.

Acknowledgement

In this paper, the research was sponsored by the National Natural Science Foundation of China (Project No. 51274078) and Major Teaching Research Project of Anhui Province (Project No. 2014zdjy015).

References

[1] Hu Jianfeng. Analysis and Design of The Security System of Cloud Security[D], XiaMen University, 2013.

[2] Yang Zhenxian. The Research and Design of Secure Data Storage Based on Cloud Computing [J], Information Security Technology, 2011.

[3] Zhang Fengzhe, Chen Jin, Chen Haibo, Zang Binyu. Lifetime Privacy and Self-Destruction of Data in the Cloud[J], Computer Research and Development, 2011.

[4] Zhao Yinchen, Ma Guohua, Ma Chuanlong, Wang Tingjuan. Research on Secure Data Storage Structure Based on Cloud Computing[J], Computer Knowledge and Technology, 2013.

[5] Fu Yinxu, Luo Shengmei, Shu Jiwu. Survey of Secure Cloud Storage System and Key Technology[J],Development of Computer Research, 2011.

[6] Zhu Zuofu, Fu Chao, Ge Hongmei. Design of DES and RSA-Based Data Encryption Transmission System[J],Communications Technology, 2010.

[7] Wu Hao. Data Encryption Scheme Based on DES Algorithm and RSA Algorithm[J],Journal of Jiaozuo Institute of Technology: Natural Science Edition, 2002.

[8] Feng Guodeng, Zhang Min, Zhang Yan, Xu Zhen. Studying on Cloud Computing Security[J], Journal of Software, 2011.