File Encryption Transmission Method Based on Cloud Computing

XiangYi Hu [12, a], LiPing Du [12, b] , GuanNing Xu[12, c]

[1] Beijing Municipal Institute of Science & Technology Information, Beijing, 100044, China

Beijing Key Laboratory of Network Cryptography Authentication, Beijing, 100044, China

[a]email: huxy368@sohu.com, [b]email: duliping_419@163.com, [c]email: xuguanning@263.net

Keywords: Cloud Computing; Big Data; Mass Use; Lightweight Cryptography; Combined Key

Abstract. This paper proposed a security single key management technology to solve the problem of symmetric key rapid exchange for lightweight cryptography in the cloud computing environment. The fast, secure and integrity verification file transmission protocol between cloud users is built both in the smart chip of client end for cloud user and encryption card in the authentication center for cloud computing platform. Thus, a cloud computing based information security system is established.

Introduction

With the development of cloud computing application, the security problem for cloud computing is very urgent, especially the information security for network application service industry which has mass users. The safety requirements of this cloud computing is mainly to increase the speed of key exchange and data integrity verification for mass uses. The current technology cannot meet security requirements of processing large data, and only through increasing the hardware equipment to the authentication centre cannot solve the security problem utterly. At present, the users with the social security card and transportation card have reached hundreds of millions of people, a very large user amount, which already belongs to the context of large data processing. It is feasible theoretically but can not be achieved in fact to use dual-key cryptography such as RSA or ECC algorithm to build all the security protocol. In order to improve the speed of key exchange, data encryption and integrity verification, the social security card and transportation card use the lightweight cryptography based authentication, data encryption and integrity verification protocol which is against the existing law about information security regulations and standards, and the user's key is not changed. However, the lightweight cryptography based security protocol must ensure the symmetric key is changed each time which is a common sense. The fixed symmetric key leaves the significant hidden danger to key management and secure protocol.

To solve the mass users' information security in cloud computing environment, this paper proposes a lightweight cryptography algorithm and a secure single-key management to build the file encryption and data integrity verification protocol to ensure the key is changed every time and not used repeatedly. And the social security card, transportation card and other with mass users' market needs are met. Thus a cloud computing based large data file encryption transmission system is established.

The Information Security Architecture of Cloud Computing

The Information Security Architecture for Cloud User Client. In cloud client side, the USB interface based smart card is used as the encryption hardware device for cloud user. In the smart chip, the encryption system for cloud user is built, and the lightweight cryptography algorithm, hash algorithm, single key combined algorithm, and the security protocols including encryption/decryption and signature/verification protocol for cloud user side are all written into the smart card chip. Also the data including the identifier of smart card chip and a set of key seeds table Ci: C1,C2,……,Cn, i=1~n, n is for the sum of all the cloud user.

The smart card chip for every cloud user's client end has the unique identity number. Each cloud

user has the only one smart card chip with the USB interface.

The Information Security Architecture for Authentication Center of Cloud Computing. The authentication centre is built in the cloud computing platform, and it is composed of the authentication server and encryption card hardware. The encryption card which deployed in the PCI interface of the authentication server is the hardware device for encryption system of authentication centre of cloud computing platform. The encryption system of authentication centre is established in the encryption card chip. And the encryption chip also includes the lightweight cryptography algorithm, hash algorithm, single key combined algorithm, a set of key seeds table D, the encryption and data signature protocol of key seeds table C and the key exchange protocol between the cloud users. All cloud users' key seeds table Ci which is stored in each user's smart card chip are also store in the hard disk storage area of authentication centre server for cloud computing platform, that is, the user key database. Each record of the user key database includes the following fields: ①the identify number of smart card chip for cloud user's client; ② the cipher of key seeds table element Ci' ; ③ the digital signature of Ci element of key seeds table, that is, the cipher of the digest information Gi for key seeds table element Ci; ④a group of timestamp Hi and random number Ji. The time stamp and random number are as the parameter of the single key combined algorithm. This algorithm choose the elements from the table D as a group of storage key Ki, and the storage Ki is used to encrypt the Ci element of key seeds table, then sign the key seeds table element Ci, i=1~n. Hi is namely H1,H2,……,Hn. Ji is namely J1, J2, ……Jn. Ci is namely C1, C2,……,Cn, Ci' is namely C1', C2',……, Cn'. Gi is namely G1, G2, ……,Gn, and n is the number of sum of all the cloud users.

Key Management of Lightweight Cryptography

A security single key management technology is used to manage the lightweight cryptography key and to establish the file encryption transmission and key secure exchange system for big data in cloud computing environment. The big data refers to the file num is very large or the file length is very long.

The Process Key. The process key CK is a group of 128-bit random number generated by the random generator in the smart card chip of the cloud user client. CK, as the process key for cloud user, is used to encrypt and sign the file of cloud user. Another user key SK, is used to encrypt the process key CK, and generate the cipher of process key CK, that is CK'. CK' will be decrypted by the authentication centre and encrypted again by the authentication centre and transferred to other cloud user. The plain text of CK is not out of the smart card or encryption card chip. So the process key CK is securely exchanged between the two cloud user through the authentication centre.

The User Key. The user key, namely SK, is real-time generated by the single key combined algorithm in the smart card chip of cloud user. The user key SK is used to encrypt the process key CK. In the initial phrase of key, the random generator of encrypt card in the authentication centre generates a group of F1 bytes random number. F1 is composed of 1424 bytes or 1680 bytes random number, and can be expressed as a set of W×Y key seeds table C:

$$C = \begin{bmatrix} C_{0,0}, C_{0,1}, ..., C_{0,y-1} \\ C_{1,0}, C_{1,1}, ...C_{1,y-1} \\ ..... \\ C_{w-1,0}, C_{w-1,1}, ...C_{w-1,y-1} \end{bmatrix}_{w \times y} \quad (1)$$

In the above table, Cu, v is the element of table C, u=0~w-1, v=0~y-1.The element Cu, v is 0.5 byte or 1 byte. The value of W is 89 or 105 and the value of y is 16 or 32.

The identifier Ti of smart card chip of cloud user client is corresponding to the key seeds table Ci. The elements of key seeds table Ci are stored in the smart card chip of cloud user client. When the file encryption and signature protocol for cloud user client is running, the single key combined

algorithm which is composed of a group of time stamp and random number is used to select the elements from the key seeds table Ci. The selected Y elements are combined to a group of user key SK. Y=16 or 32. Every set of key seeds table Ci is corresponding to a smart card. The key seeds in the smart card chip for all cloud user client is C1, C2, … , Cn, n is the number of sum of the whole cloud users. And the elements for Cd, Ce(（1≤d 或 e≤n，d≠e）are different from each other.

The single key combined algorithm and key seeds table Ci are both stored in the smart card chip of cloud user client, and the user key message are generated inside the smart card chip. The storage security and process security of user key are ensured in the cloud user side.

In the encryption card chip of authentication centre, the elements of key seeds table Ci is encrypted to cipher by storage key Ki. The cipher elements of key seeds table Ci, with each cloud user's smart chip identifier and the choice parameters including timestamp and random number, are all stored in the user key database of the authentication centre.

When the cipher of key seeds table Ci in the authentication centre is called, it will be decrypted to plaintext at first in the encryption card of the authentication centre. The plaintext of all the key seeds table Ci are not out of the encryption card chip, so the storage security and running security of all key seeds table Ci are ensured in the authentication centre. Among these, i=1~n, n is the number of sum of all cloud users.

Storage Key. Storage key, namely K is generated by the single key combined algorithms in the encryption card chip of authentication centre. The storage key K is used to encrypt all the elements of key seeds table C. In the initial phrase of key, the random number generator of encryption card chip of authentication centre produces a group of F2 bytes random number, while F2 = 1424 or F2 = 1680 bytes. The F2 bytes random number forms the following W×Y key seeds table D:

$$D=\begin{bmatrix} D_{0,0}, D_{0,1}, ..., D_{0,y-1} \\ D_{1,0}, D_{1,1}, ...D_{1,y-1} \\ ..... \\ D_{w-1,0}, D_{w-1,1}, ...D_{w-1,y-1} \end{bmatrix}_{w\times y} \tag{2}$$

In the above table, the elements of table D is Du, v, u=0～w-1， v=0～y-1. Du, v occupies 0.5 bytes of 1 byte space. W=89 or 105, Y=16 or 32.

The elements of table D are stored in the encryption card chip of authentication centre. A single key combined algorithm which is composed of a group of time stamp and random number is used to choose Y elements from key seeds table D and combined a group storage key K.

The storage key Ki which used to encrypt the elements of key seeds table Ci has the total number of n, that is, K1, K2,……,Kn. The storage key Ki is used to encrypt the corresponding key seeds table Ci to generate cipher of key seeds table Ci, namely C1',C2',……Cn'. The Ci' is stored in the user key database of authentication centre, i=1~n, and n is the total number of all cloud users.

Single Key Combined Algorithm. The single key combined algorithm selects the elements from the key seeds table according to a group of time stamp and random number. The timestamp is used to choose the "line" elements from the key seeds table and form the Y lines and Y columns the sub table of key seeds table. The random number is used to choose the "column" elements from the sub key seeds table which is Y lines and Y columns and got the Y elements. The Y elements are combined a group of key, the value of Y is 1 or 32. The storage key K and user key SK both are generated by the single key combined algorithms in time.

The time stamp is composed of 10 digital numbers. That is, the "year" is composed of 4 digital numbers: xxx0 year~ xxx9 year, the "month" consists of 2 digital numbers which is from January to December. The "day" is also composed of 2 digital numbers which are from 1 to 31. The "hour" is composed of 2 digital numbers which are from 0 hour to 23 hours. For example, the time 2013122819 means that the December 28, 19, 2013.

The random number is composed of Y bits binary number. While Y is 16 bits binary, each random

number is 4 bits binary number, and each binary number value for the random number is from 0 to 15. For example, 0011, 1010, 0000,…., 1111m, 0110, the corresponding decimal number is 3, 10, 0, …., 15, 6. While Y is 32 bits binary number, each binary number value of the random number is from 0 to 31. For example, for example the binary data 00110, 10100, 00000, ..., 11111, 01100, the corresponding decimal value is 6, 20,0,…….,31,12.

The Key is One-Time-One-Variant. The process key CK, user key SK and storage key K are all 128 bytes long. The reputation rate of CK is 1/2128, and the one time one key is almost realized.

The user key SK and storage key K both are Y elements selected and combined from the key seeds table D or B according to a group of time stamp and random number. If the random number is 16 bits long, the elements of key seeds table D or B is 8 bits long and the time stamp is expressed as "year/month/day/hour", the reputation rate for user key SK and storage key K is 1/264. If the parameter random number is 32 bits long, the elements of key seeds table D or C is 4 bits long and the time stamp is expressed as "year/month/day/hours", the reputation rate of user key SK and storage key K is 1/2160 in one hour. So the user key SK and storage key K are almost one time one variant.

The Security Protocol for Cloud Computing

The File Encryption/Data Signature Protocol for Cloud User. The encryption system of cloud user client A calls the digest algorithm in the smart chip to get the "digest" information L1 through computing the hash value of file of cloud user client A. Then a group of random number which generated by the generator is as the process key CK of cloud user client A. The process key CK is used to encrypt the file of cloud user client A and the file cipher is computed for the cloud user client A. CK is also used to encrypt the "digest" information L1 and get the cipher of L1, that is the file signature of cloud user client A. In the smart chip, a group of time stamp 1 and random number 1 is generated, and they are used as the parameter of single key combined algorithms to select the elements of key seeds table CA. The Y elements selected is combined to a user key SKA for cloud user client A. SKA is used to encrypt the process key CK to cipher CK'. The identifier of smart card chip of cloud user client A, the file cipher, the digital signature of file, the cipher of process key CK, the random number 1and the time stamp 1, totally six group of data, are sent to the authentication centre of cloud computing platform. Among these, CA=C1～Cn， i=1～n，Y=16 or 32.

The Encryption/Digital Signature Protocol for Elements of Key Seeds Table C. In the encryption system of authentication centre of cloud computing platform, a group of time stamp Hi and random number Ji is generated in the encryption card. The time stamp Hi and random number Ji are used to select the elements from key seeds table D according to the single key combined algorithm. The Y elements selected are then combined to a set of storage key Ki, and the Ki is used to encrypt the elements of key seeds table Ci to get the cipher Ci'. Also the storage key Ki is used to sign the elements of key seeds table Ci, that is, encrypt the digest information Gi of key seeds table Ci to get the cipher of Gi, namely the digital signature. Finally the identifier of smart card chip of cloud user client, Ci' which is cipher of key seeds table elements Ci, the digital signature of key seeds table Ci, and the time stamp Hi and random number Ji which is used to generate the storage key Ki, are all stored in the user's key database of authentication centre. Among this, Hi=H1~Hn，Ji=J1~Jn， Ci=C1~Cn，Ci'＝C1'~Cn'，Gi=G1~Gn，Ki=K1~Kn，i=1~n ， Y=16 or 32.

The Key Exchange Between the Cloud Users. When the authentication centre receives the 6 group of data from the cloud user client A, the encryption system of authentication centre will first locate the record which corresponding to the identifier of smart card chip of cloud user client in the user key database. The cipher of key seeds table CA, which is CA' in this record, a group of time stamp HA and random number JA which is used to generate the storage key KA are all imported into the encryption card chip of authentication centre. In the encryption card, a group of time stamp HA and random number JA which is used to generate the storage key KA are used to select Y elements from table D according to the single key combined algorithm. These Y elements are

combined to the storage key KA. KA is used to decrypt the CA' (the cipher of CA elements) to get the plaintext of key seeds table. KA is also used to decrypt the signature of key seeds table CA elements to get GA which is the digest information of key seeds table CA. Then the digest algorithm is called to compute the digest value of CA elements and get the digest information GA1. Comparing the digest information GA and GA1 can determine whether the key seeds table CA is tampered and whether the elements of table CA is integrity and credible. Then the time stamp 1 and random number 1 which is used to generate SKA for cloud user client are used to select plaintext elements of the key seeds table CA to get the Y elements which can combined to the user key SKA1 according to the single key algorithm. If the elements of CA has passed the completeness, SKA=SKA1. SKA1 is used to decrypt the CK' (the cipher of process key CK for cloud user client) to get the plaintext of CK. Next, according to the identifier of cloud user B's smart card, the corresponding key seeds table CB's cipher for user B, the digital signature of key seeds table CB, the time stamp HB and random number JB which are parameters used to generate the storage key KB are got out from the user key database. In the encrypt card, The parameter time stamp HB and random number JB which are used to generate the storage key KB are used again to select Y elements from key seeds table D. And the Y elements are combined to a group of storage key KB. The cipher of key seeds table CB for cloud user client B are decrypted to plaintext by KB. KB is also used to decrypt the digital signature key seeds table CB to get the plaintext of digest information GB for key seeds table CB. Then hash algorithm is called again to compute the digest for elements of CB and get the digest information GB1. Through comparing the GB and GB1, the completeness and credibility of key seeds table CB can be determined. Then a group of time stamp 2 and random number 2 is generated and used to select the elements from the key seeds table CB for cloud user B according to the single key combined algorithm. The Y elements selected are combined to a group of user key SKB for cloud user B. SKB is used to encrypt the process key CK of cloud user A. The identifier for cloud user B smart card, file cipher of cloud user client A, signature for cloud user A's file, cipher of process key CK and the time stamp 2 and random number 2, totally 6 group of data, are all sent to the cloud user B' client end.

In the exchange key protocol between the cloud users, the decryption and verification protocol for key seeds table CA, CB are also included. Among this: CA=C1~Cn, CB=C1~Cn, CA≠ CB, HA=H1~Hn, HB=H1~Hn, HA≠ HB, JA=J1~Jn, JB=J1~Jn, JA≠ JB, KA=K1~Kn, KB=K1~Kn, KA≠ KB, GA=G1~Gn, GA＝GA1 or GA≠ GA1, GB=G1~Gn, GB＝GB1 or GB≠ GB1, GA ≠ GB, i=1~n.

The Decryption/Verification Protocol for Cloud User's Cipher File. When the cloud user end receives the 6 groups of data from the authentication centre, the encryption system for cloud user B will call the single key combined algorithm to select elements from the key seeds table in smart card through the time stamp 2 and random number 2 for cloud user B which are used to generate the user key SKB. The Y elements selected are combined to a group of user key SKB1 for cloud user client B. if the element of table CB is complete, SKB is equal to SKB1. SKB1 is used to decrypt cipher of process key CK to the plaintext CK. The process key CK is used to decrypt the file cipher and get the file plaintext for cloud user end. The CK is used to decrypt the digital signature for cloud user to get the digest information L1 of file for cloud user client A. The digest algorithms in the smart card chip is called to compute the digest value for cloud user A's file and get the digest information L2 for cloud user A's file. Through comparing the L1 and L2, the credibility and completeness for signature file from cloud user A can be determined. Among above, CB=C1~Cn, i=1~n.

The Advantage of Key Management and Security Protocol for Cloud Computing Encryption System

Generation and Storage of Keys are all Secure. The process key, user key and storage key are all generated in the smart card chip or encrypt card. The plain texts are not out of chip. The key seeds which are used to generate the user key are stored out of chip as cipher.

1) Process Key: The process key is generated in the smart card chip. It is transported as cipher between two cloud users through the authentication centre, and the process key's exchange is secure.

2) User Key: The user key SK is generated in the smart card chip of cloud user client. The single key combined algorithm and a set of key seeds table Ci which are both used to generate the user key SK, are stored in the smart card chip. In the authentication centre, the single key algorithm used to generate the user key SK is stored in the encryption card. The key seeds table Ci is stored in the user key database as cipher in the authentication centre. The storage, exchange and process of user key SK are ensured both in cloud user client and authentication centre. Among these, i=1~n.

3) Storage Key: The storage key K is generated in the encryption card chip. The single key combined algorithm and a group of key seeds table D are also stored in the encryption card chip to ensure the storage and running security for storage key K.

Key's Dynamic Characteristics. The user key is one time one variant, and the process key is also one time one variant. So the process key cipher which use user key to encrypt process key, is also has randomness, and is one time one variant. The cipher of process key is a group of garbled, no regularity. The decipher cannot get the large number of cipher for process key in public, which is as the decipher conditions, namely repeat message which use the same single key to encrypt multiple message to cipher to decrypt process key or user key or the elements of key seed table which is used to generate user key.

The storage key Ki which changed each time is used to encrypt the key seeds table Ci which has the characteristic of randomness to cipher Ci'. The Ci' is also randomized and garbled. Deciphers cannot make the Ci' as the decryption condition, namely repeat message to decrypt the table Ci or to decrypt the storage key Ki. I=1~n, and n is the summary number of all the cloud users.

Save the Storage Space. The number of cloud user is very large, and the data stored in the authentication centre is also large. Every key seeds table Ci which corresponding to each cloud user end and is used to generate the user key SK occupy 1424 bytes or 1680 byte storage space. When the number of cloud user reaches to 5~6 hundred million, the corresponding amount of cloud user data belongs to mass data range. Using the single key combined algorithm to generate one time one variant storage key Ki, and to encrypt the key seeds table Ci which used to generate user key SK , can ensure the storage security of key seeds table Ci in authentication centre which corresponding to all cloud user. The large number of encryption card hardware devices does not need to purchase to store the mass data of key seeds table Ci, which can greatly save the construction cost of authentication centre. The single authentication centre can manage the mass data such as 5~6 hundred million, i=1~n.

Chip Based Security. A secure single key management technology is used to build various security protocols. Based on the credibility of smart card and encryption chip, the encryption/digital signature protocol for file of cloud user, the decryption/verification protocol for cipher file of cloud user are computed completely in the smart card chip. The encryption/digital signature protocol for key seeds table Ci and the key exchange protocol between cloud users are finished in the encryption card. All protocols are based on the chip level and the security level is high.

Ensure the Key Seeds Security in Authentication Center. In the protocol of key exchange between cloud users, the encryption system of authentication centre for cloud user platform, not only to verify the completeness of the key seeds table Ci corresponding to the file sender, but also verify the Ci completeness for file receiver. So the elements of key seeds table Ci in the authentication centre can be protected to not be tampered with or be cloned. i= 1~n.

Conclusion

This paper proposed to use the lightweight cryptography technology to build the file encryption transmission protocol both in the smart card of cloud user client and encryption card chip of authentication centre. And secure single key management technology is used to solve the problem of key update for lightweight cryptography. The cloud users exchange the key and transport the file cipher through the authentication centre of cloud computing platform to protect the security,

credibility and completeness of file transmission. Especially to ensure the mass users' file encryption transmission and escort for the application and development of cloud computing in China.

Acknowledgement

This work was financially supported by Program of Large-scale Network Authentication Center affiliated to Beijing Municipal Institute of Science & Technology Information (No. PXM2012_178214_000005).

References

[1] X.Y. Hu, File encryption method for large data based on cloud computing; China, 20130101882.6.

[2] C.Y. Shen, Cloud Computing Security and Level Protection,China information security, 2012,(1).

[3] D.G. Feng, Open Cloud Computing Security Ear, Netinfo security, 2011,(3).

[4] W.K. Zhang, G.F. Liu, Data security and privacy protection of cloud computing, China information security, 2012,(11)

[5] Y.Y. Zhang, Chen Qing-jin, Pan Song-bai, Wei Jin-wu, Key Security Technologies on Cloud computing, Telecomunications science, 2010,26(9)

[6] Z.G. Feng,C. Ma, The Cloud Computing Security, Technology wind, 2010,(4)

[7] J.C. Tian, Cloud Computing and Cryptography, China information security, 2012,(11)

[8] X.D. Wu, Research of Cloud Computing Data Secure, Netinfo security, 2011,(9)