Cryptographic Process in Cloud Based System

Kyaw Thu Win
University of Computer Studies, Mandalay, The Republic of the Union of Myanmar
ktwcumdy2009@gmail.com

Abstract

Cloud computing technology becomes most popular in modern technology environment. Users store their data on third-party storage, cloud storage provider. In this case, security concerns arise to protect their stored data. So, secure cloud architecture was proposed and used. In this environment, key manager includes and produces both private and public keys to encrypt and decrypt the user data files. If someone gets the keys in some way from the key manager, the data file can easily be opened and changed. So, I proposed client-side encryption system. This system generates all encryption and decryption keys at the client side. The key owner generates both key pairs instead of generating at key manger location. This system currently uses Rivest-Shamir-Adleman (RSA) public key cryptosystem to generate keys and to perform cryptographic processes.

Keywords*: Cloud security, Encryption, Public key cryptography, RSA*

1. Introduction

Many organizations are increasingly looking toward Cloud Computing as a new revolutionary technology promising to operational and capital costs and, more importantly, let IT departments focus on strategic projects instead of keeping the datacenter running. The main principle is offering computing, storage, and software “as a service” [7]. All user data are stored on remote server refers to as data center. Data center allows the users to run application faster and easier for data management and less maintenance effort. As data owners store their data on external servers, there have been increasing demands and concerns for data confidentiality, authentication and access control [3].

Nevertheless, some security questions arise due to the user data are stored on third party place such as cloud storage provider. In order to protect their data, cryptographic techniques can be used. Secure cloud environment was designed and used in order to have more secured on data. In this environment, key manager, cloud data storage, and users are involved. Currently, key manger stores and produces keys to perform cryptographic process, such as encryption and decryption, on user data.

In public key encryption scheme, the public key is generated by key manager. The user requests the public key pair from key manger. Upon the key, the user performs the encryption process. Finally, the user uploads his/her encrypted data to cloud storage. The decryption key is kept at key manager side. In decryption process, client needs to fetch the decryption key from key manager side and performs decryption on encrypted data file.

In this case, this can be seen it is securely enough. However, if both key manager and storage provider communicate each other in order to decrypt some file not having data owner privilege, the user data can easily be decrypted and used for some purposes. In order to solve this kind of problem, I consider and propose key generation process to be performed at client side. The user or key owner generates both encryption and decryption key at his/her side. In order to store more secure at the key manager side, the decryption key (data key) is also encrypted. The encrypted data key is only stored at the key manager side. So, the key manager doesn't know any information about the encrypted data key. Even though the encrypted data key file is received by intruder, the decryption key can't be easily got. In private and public key pair generation process, the system uses RSA key algorithm. The decryption process on the stored encryption data key is also performed at client side.

The remaining of this paper proceeds as follows. In section 2, describes related works. Section 3 briefly explains the current designing and developing cloud based system and the client side key generation system model and the related theories are mentioned in Section 4. I provide the detailed description of key generation and cryptographic process in Section 5. Section 6 describes advantages of using this system. The current future works are described in Section7. This paper concludes in Section 8.

2. Related Works

Cryptography is playing a major role in data protection in applications running in a network

environment. N. Y. Goshwe [2] proposed a cryptographic approach which is based on RSA public key algorithm. This approach allows a message sender to generate a public key to encrypt the message and the receiver sent a generated private key using a secured database. An incorrect private key will still decrypt the encrypted message but to a form different from the original message.

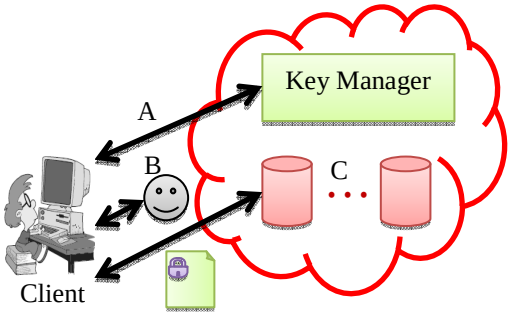
Cryptographic algorithms play a vital role in providing the data security against malicious attacks. RSA algorithm is extensively used in the popular implementations of Public Key cyptosystem. In asymmetric key cryptography, also called Public Key cryptography, two different keys (which form a key pair) are used. Data Cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. A.A. Ayele, et.al [1] implemented an efficient algorithm of RSA algorithm in which two public key are produced and encrypt message using these two keys and sent it separately. This makes the attacker not to get much knowledge about the key and unable to decrypt the message. Their system has high communication overload.

3. System Model

I propose and build cloud based system that can currently apply to university file locker system. In this system, three participants include cloud user, cloud storage provider, and key manager. A cloud user currently is university students or teachers. Users store their university related files in document format, image format on this cloud system. In order to provide access control on the uploaded files, the security and privacy is provided. In order to store securely, the file owner uses the system provided encryption techniques and stores it on the cloud storage provider. In this system, the key generation and encryption is done at the client rather than at key manager.

The proposed system model includes three parts such as key generation, key exchange, and privacy-based file protection. Key generation and encryption is processed at the client side in order to perform cryptographic process on user data file. This paper only mentions this process stage more detail in next section.

Key exchange process will be performed when the cryptographic process has been done. In this process, the data key is exchanged or transferred only between key manger and key owner in order to protect getting from other users such as cloud storage provider or other unauthorized access user(s). The final part of the system is to protect the user files (key and data file) not only the security but also the access privacy. Last two process stages will not mention in this paper. The cloud based university file locker system is shown in Figure 1.



A: Key exchange over protocol
B: Non-stationary key generator
C: Cloud Data Storage (Data Keeper)

Figure 1. University File Locker System

3.1 Key Generation System

This section explains the client side key generation and cryptographic system. In this cloud based system, three entities,

Key Owner. The key owner is one who owns key(s) to be stored at key manger. The key owner generates key pairs to encrypt or decrypt the data file to be stored on the cloud storage.

Key Manager. The key manager is one who stores a lot of keys. The key manager only stores the key not knowing any key nature.

Encryption/Decryption Program. The encryption program generates the private key pair and public key pair and also performs the encryption process at the running side or client side. The decryption program performs the key requesting and decryption process at the client side.

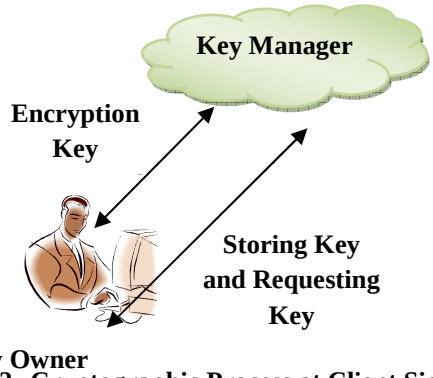


Figure 2. Cryptographic Process at Client Side

Figure 2 shows the proposed key generation program. The key generation scheme works as follows. Whenever the key owner wants to encrypt data file, she must request the encryption program from the key

manager. The key manager sends the encryption program to the requested key owner side. After arriving encryption program and running at the client side, the key owner can generate both private and public key pairs and operates encryption process on her desired file. After generating keys and encryption process on selected data file, the proposed program also generates another key pairs and performs encryption process on data key. The final decryption key is to be used in future process such as decrypting the encrypted data key. The program gives decryption key to the key owner as a file with suitable name and key owner needs to be stored it in his/her own way.

4. Background

Basic cloud consumption: Cloud computing is an information-processing model in which centrally administered computing capabilities are delivered as services, on an as-needed basis, across the network to a variety of user-facing devices [6]. In cloud computing environment, there are three services provided by cloud namely Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS). Nowadays many internet applications such as Google, Facebook, and Twitter move to cloud computing environment. The key finite attributes of cloud are on-demand availability, ease of provisioning, dynamic and virtually infinite scalability. So, user does not need to have any worries about the storage space, needed file system.

Cloud Security: As cloud computing becomes a more important model for enterprise IT, the cloud will necessarily be a more critical part of the overall security infrastructure [9]**.** Since user data are storing at third party places, the user can think that their data is not secure. So, there may need to have security in cloud computing environment. The biggest hurdle to the adoption of cloud storage (and cloud computing in general) is concern over: confidentiality - the cloud storage provider does not learn any information about customer data and integrity - any unauthorized modification of customer data by the cloud storage provider can be detected by the customer of data [4]. So, cryptographic techniques can overcome this security issues. Despite protection of outsourced data by applying cryptographic encryption onto sensitive data with a set of encryption keys, the maintaining and protecting such encryption keys will be another security problem.

In this paper, RSA public key encryption scheme is used in encryption process of user data and key file at the client side.

RSA algorithm: A public-key cryptosystem is a one-way authentication system. If user *A* wishes to send a message *M* to user *B*, he "deciphers" it in his secret deciphering key and sends decrypted message, $D_A(M)$. When user *B* receives it, he can read it, and be assured of its authenticity by "enciphering" it with user *A*'s public enciphering key, E_A [5]. The most successful algorithm that has been proposed for public-key cryptography is Rivest-Shamir-Adleman (RSA) scheme. The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n. A typical size for n is less than 2^{1024}. RSA algorithm works as follows [8]:

1. Generate two large prime numbers, *p* and *q*.
2. Calculate modulus (n) :
$$n = p \times q \quad (1)$$
3. Calculate:
$$\phi(n) = (p-1) \times (q-1) \quad (2)$$
, where □ (n) is Euler totient function.
4. Select *e* such that *e* is relatively prime to □ (*n*).
5. Calculate the decryption exponent d:
$$d \equiv e^{-1} \pmod{\phi(n)} \quad (3)$$
6. The public key pair is (e, n)
7. The private key pair is (d, n)
8. The plain text M can now encrypt using:
$$C \equiv M^e \mod n \quad (4)$$
, where C is cipther text.
9. The decrypt message C using:
$$M \equiv C^d \mod n \quad (5)$$

User K encrypts the message with the public key (e, n) of user T using Equation (4). User T is now the only one who can decrypt this message using his own private key (d, n) and Equation (5).

5. Cryptographic Process

As mentioned in section 3, the proposed key generation and encryption process performs at the client side. In order to do so, the client needs to fetch the encryption program. When the program runs at the client side, the key owner needs to set user name and access password. If valid, she can now create the required encryption and decryption key. If the key owner successfully generates the key pairs, she can now encrypt the data. If all encryption process done, the data key can now be encrypted and sent it to the key manager. The key manager stores the received data key, and generates the key access code to the key owner. The key access code is to be used in decryption process. The storing data key process is done in this case. The more detail of this encryption process will be in section 5.1.

In decryption process, the key owner firstly needs to send the key access code to the key manager. The key manager then checks the key access code is valid. If valid, the key manager retrieves the data key and records the usage information, and then sent the data key to the key owner. If the decryption program successfully receives the data key, the key owner needs

to input the user name and related code, which is generated at the encryption. If the input information is correct, the program decrypts the data key and continuing the data file decryption process. The detail process of decryption is mentioned in section 5.2.

5.1. Encryption

The encryption program works at client side when the client or key owner requests this program form key manager. As shown in Figure 4, the program firstly asks the key owner or user to input the user name and password in order to give legitimate user processes. If the key owner is legitimate user, she can now encrypt the data as she wants as shown in Figure 3. In order to do so, the key owner must select the data file and generate the key pairs (both private key and public key pairs).

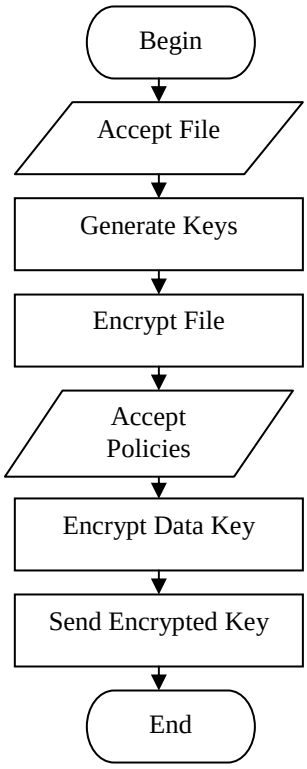


Figure 3. Encrypt Process

Key Owner can now encrypt the selected file. The program will create the encrypted data file. In our proposed system, the key manager only stores the encrypted key files. This means that key manager doesn't know any key to decrypt the file because all keys are generated at the client side. In order to store the data key in more secure, our system also encrypts the key. Figure 5 shows the data encryption process.

Thus, the program will ask the user to fills up any necessary user-defined access policies as shown in Figure 6, if the data file successfully encrypted. These access policies will later be used in accessing the encrypted key file and will send to key manager. The encrypted process of data key is automatically done. The decryption key for data key is given to the user as a file with suitable name in order to use it later. After encrypting the data key, the program will automatically send it to the key manager.

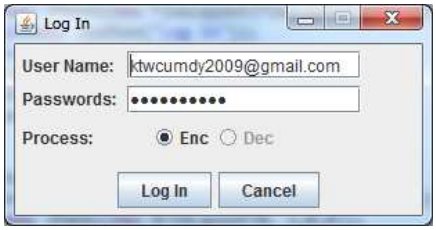


Figure 4. Log In Process

Figure 5. Data Encryption Process

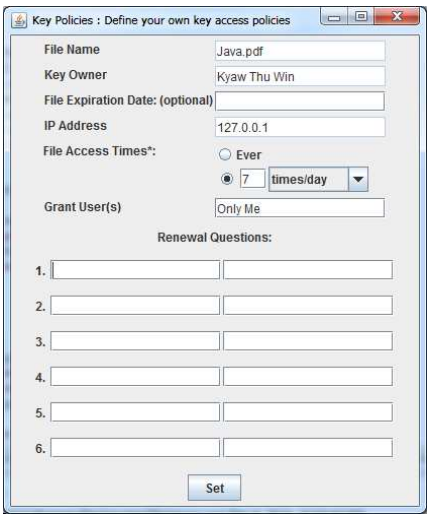


Figure 6. Key Access Policies

In this system, the key manager does not generate any keys. The manager only stores the received key file of key owner. Therefore the key manager stores the received key file in local storage device and records the key file information as shown in Table 1. The "OID" is the owner id of uploaded key file, for instance the keyowner ktwcumdy2009@gmail.com's id is 1, and "KeyID" is the id of current uploaded key file. The "KeyFile" is the current uploaded key file name and the "Keys" indicates the total number of key file which has been uploaded by associated key owner.

Table 1. Key Storage Table

KeyID	OID	KeyFile	Keys
6	1	Java.pdf	5
7	2	OpenStack.pdf	6
8	3	Decrypt.java	2

5.2. Decryption

The decryption program first requests the user to set the file access code and file name as input. The program sends the file access code to the key manager and receives the key file from the key manger if the key manager assumes that the access code is valid for requested key file. Then the program prompts the user to select the related decryption key file in order to decrypt the received key file. Then the program decrypt the received key file using the correct decryption key values. Then the program create key file to decrypt the related data file. User can finally decrypt the data file with the specified key file. The process of decryption program is as shown in Figure 7.

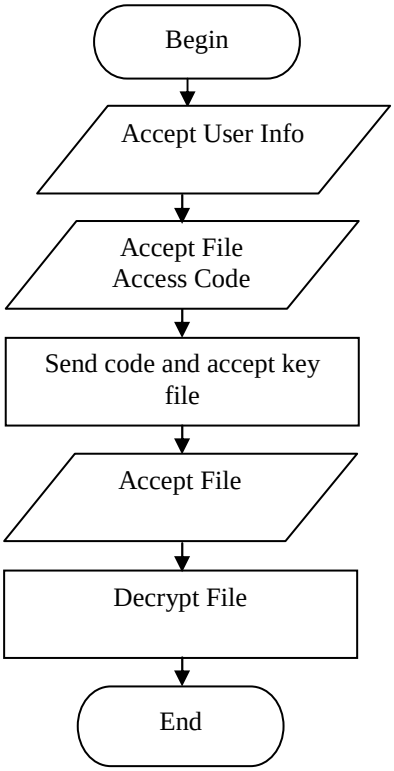


Figure 7. Key File Decryption Process

6. System Advantages

The proposed system uses RSA public key encryption key in cryptographic processes on data file and key file. In the implementation of RSA algorithm, I used Java programming language. In this implementation steps, the class BigInteger is used to hold large prime numbers and keys so that it difficult for hacker to guess or use brute force method to find. The keys are generated at the client side, so the attacker needs to spend much time and more costs in order to learn the encryption key. The attacker may also need to spend double extra time to get the final decryption key for data file because there is two times encryption process, one for data file encryption and another for key file encryption processes.

7. Future Works

The encryption program is normally created the decryption key file and not stored at the key manager so that the user needs to keep the key files with own ways. This can be tackled by using the master key. Nevertheless, if someone gets the master key, all key files can easily get and the data file can easily be encrypted. So, we can future extend this program in order to support the keys owner to be kept the decryption keys in easier ways. This system currently uses RSA public key cryptography in key generation, encryption and decryption processes. This can be future replaced with other newly modern cryptographic approaches.

8. Conclusion

In current cloud security model, keys to encrypt and decrypt files are generated and decryption key are known by key manager and store at the key manager side. In this case, there may have key file access between the cloud storage and key manager. If the cloud storage provider can easily get the key from the key manager, the user data can decrypted and perform some processes on it with no user permission. In order to tackle this problem, this paper has described key generation, encryption and decryption processes at the client side that was implemented. The data key, decryption key of data file, is also encrypted. The key manager only stores the encrypted key file without knowing the decryption key for that file. The key generation and cryptographic process is done by using RSA public-key encryption scheme.

References

[1] A.A. Ayele, and Dr. V. Sreenivasara, "A Modified RSA Encryption Technique Based on Multiple public keys", *International Journal of Innovative Research in Computer and Communication Engineering*, June 2013.

[2] N. R. Goshma, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment", International Journal of Computer Science and Network Security (IJCSNS), July 2013, p.p. 9-13.

[3] S. Jajodia, S. D. C. di Vimercati, S. Foresti, , S. Paraboschi, and P. Samarati, "A Data Outsourcing Architecture Combining Cryptography and Access Control", *Proc. ACM Workshop on Computer Security Architecture (CSAW'07)*, USA, November 2007.

[4] Y. Tang, Patrick P.C. Lee, John C.S. Lui, and R. Perlman, "FADE: Secure Overlay Cloud Storage with File Assured Deletion", *in Proc. SecureComm*, Singapore, September 2010, pp. 1-18.

[5] W. Diffie and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, November 1976, .pp. 644-654.

[6] Brian J.S. Chee and Curtis Franklin, Jr., Cloud *Computing Technologies and Strategies of the*

Ubiquitous Data Center, Taylor and Francis Group, United States of America, 2010.

[7] Buyya, R., J. Broberg, and A. Goscinski, *Cloud computing: Principles and Paradigms*, John Wiley & Sons, Inc, United States of America, 2011.

[8] Stallings W., *Cryptography and Network Security: Principles and Practice*, Prentice Hall, United States of America, 2011.

[9] Tom D., Cryptography, 2000.