International Journal of Advanced Smart Convergence Vol.5 No4 26-31 (2016)
https://doi.org/10.7236/IJASC.2016.5.4.26

IJASC 16-4-5

Key Management Server Design for Providing Cryptographic Service in Cloud Computing Environment (Services in a Cloud Environment)

Ki Hyun Jung[1], Seung Jung Shin[1†]

[1]*Dept. of IT convergence, Hansei University*
jungkh532@gmail.com, †expersin@gmail.com

Abstract

In a cloud computing environment, a cryptographic service allows an information owner to encrypt the information and send it to a cloud server as well as to receive and decode encrypted data from the server which guarantees the confidentiality of shared information. However, if an attacker gains a coded data and has access to an encryption key via cloud server, then the server will be unable to prevent data leaks by a cloud service provider. In this paper, we proposed a key management server which does not allow an attacker to access to a coded key of the owners and prevents data leaks by a cloud service provider. A key management server provides a service where a server receives a coded public key of an information user from an owner and delivers a coded key to a user. Using a key management server proposed in this paper, we validated that the server can secure the confidentiality of an encryption key of data owners and efficiently distribute keys to data users

Key words: *Cloud, Cryptographic service, Access control, Key management, Public key encryption*

1. Introduction

Until now, cloud service providers have served a cryptographic service to safely keep the users' information. Cryptographic service let a user encrypt shared data and send them to a cloud server[1, 2, 3, 4]. A user of cryptographic service generally uses an encryption key when either encoding or decoding data. Therefore, a service provider had to safely distribute encryption keys to the users[5, 6, 7].

To secure the key distribution, a service provider chose an authentication-based encryption system since only certified and trustworthy users should have access to encryption keys. This system only allows those who successfully finish the authentication process to get encryption keys and encode and decode data[8, 9].

However, the Information Security Institute of Johns Hopkins University gave a warning that a cloud service provider could access to an encryption key and decode a coded data with false verification[10]. Even if the authentication-based encryption system is applied, data leaks by a cloud service provider still can happen.

This study suggests an encryption key distribution to users via key management server. A user directly

Manuscript Received: Sep. 25, 2016 / Revised: Oct. 10, 2016 / Accepted: Oct. 25, 2016
Corresponding Author: expersin@gmail.com
Tel: +82-31-450-5274, Fax: +82-31-450-5172
Dept. of IT convergence, Hansei University

registers to a key management server, and the server distributes a registered key to the user.

In order to apply the system referred above, it must maintain the confidentiality of both registered and soon-to-be-distributed encryption keys. In this system, a user first encodes his encryption key into a public key and registers it then he receives and decodes a registered key from a key management server which grants the user an access to an encryption key. Under this circumstance, no data leaks by a cloud service provider will occur since a provider or an attacker cannot access to an encryption key without a personal key.

The paper is organized with five chapters : 1) Introduction, 2)Proposal of a Key Management Server, 3)How to Embody a Key Management Server, 4)Test of a Key Management Server, and 5)Conclusion.

2. Proposal of a Key Management Server

In a cloud computing environment, a key management server authorizes a user to register and distribute an encryption key.

A registration procedure is as follows. First, a user registers a public key to a key management server. The server saves public keys of many users. Second, when the owner chooses a public key of a certain user to grant the authority, the server delivers a selected public key to the owner. Then the owner encodes an encryption key into the user's public key and sends it to the server for the registration.

Next step is a distribution of encryption keys via key management server. A user will need a data ID to request an encryption key. A data ID is a result of the research of coded data in a cloud server and is provided to the user. With this data ID, a user can receive only a necessary encryption key. Following that, a key management server grants a user a key corresponding to a data ID. After all these steps, a user now can decode a granted key into his personal key and use it.

The encryption key registration and distribution procedures are designed to secure the confidentiality of an encryption key through all transmission process between a user and a key management server.

3. How To Embody A Key Management Server

As we previously confirmed, a key management server offers the encryption key registration and distribution services to a user. To enable each function, we need to define the following components.

Key generating component generates an encryption key which a data owner uses to encode data and creates a public key and a personal key in pairs.

Through a key request service, an owner requests a public key from a key management server, or a user requests an encryption key from a key management server.

Key management component helps an owner register an encryption key to a key management server while helping a user either store a personal key in his own database or register a public key to a key management server. With this component, a key management server can bring a registered public key or encryption key, and a user can get a personal key from his database.

Cryptographic service encodes an encryption key into a user's public key for the owner and decodes the encryption key into a personal key for the user.

The encryption key registration and distribution in a key management server can be explained with these components. Figure 1 illustrates the process of encryption key registration and separates the roles of an owner, a user, and a key management server.

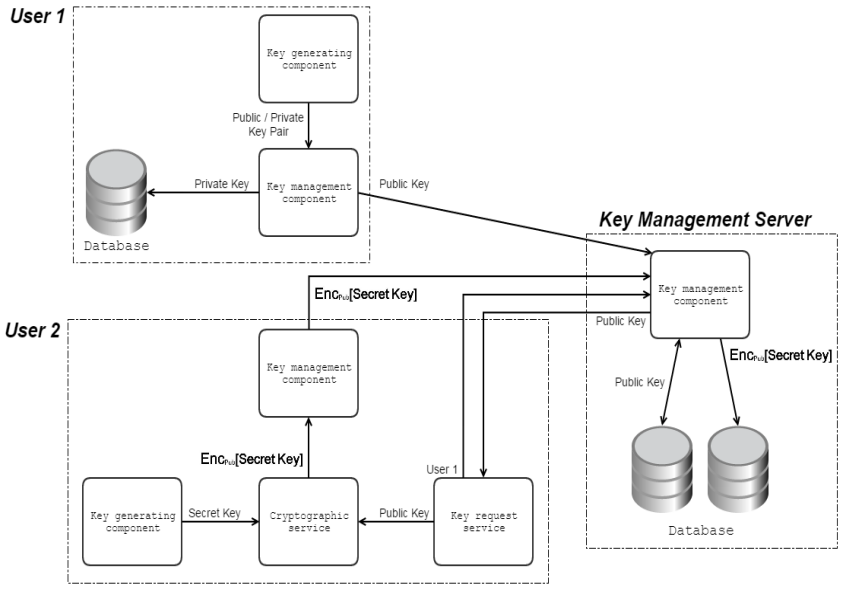

Figure 1. Encryption Key Registration Process in a Key Management Server

During the encryption key registration, a user generates a public key and a personal key in pairs using a key generating component. And a personal key is stored in a user's database, and a public key is sent and registered to a key management server via key management component. In order to encode an encryption key generated by a key generating component, the owner utilizes a key request service to request a user's public key from a key management server. Cryptographic service encodes an encryption key into a user's public key and sends an encryption key coded by a key management component to a key management server for the registration.

Figure 2 represents the process of encryption key distribution and separates the roles of a user and a key management server. During the process, a user requests an encryption key from a key management server with a data ID corresponding to the data coded via key request service. Then a key management server imports an encryption key coded via key management component and sends it to the user. A user takes a personal key using a key management component in order to decode a coded encryption key. Finally, an encryption key is obtained after decoding an encryption key coded via cryptographic service.

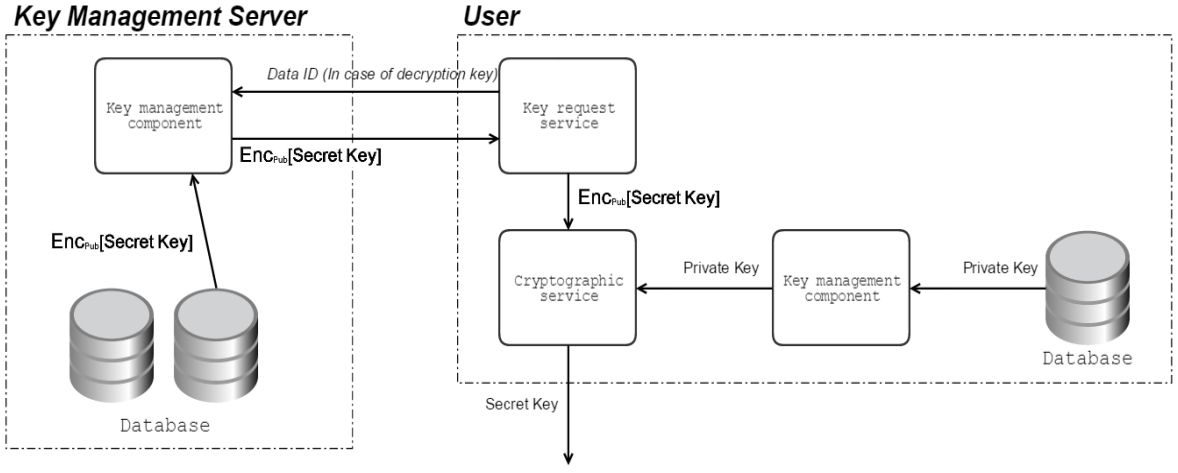

Figure 2. Encryption Key Distribution Process in a Key Management Server

4. Test and Result

In this chapter, we analyzed a case of a user's direct management of an encryption key and a case of an indirect management of an encryption key via key management server and conducted an experiment on the efficiency of key management server.

We assumed that numerous users use a cryptographic service and set the environment using Intel Core i5-3470 CPU, RAM 4GB, and Windows 7 32bit.

First of all, we analyzed the efficiency of key management server as following. A transmitter and a receiver form a security channel for a safe distribution of an encryption key. We calculated the number of security channels regarding the increase in users of a cryptographic service, and the result can be found in Table 1. The number of security channels increased proportionately to the number of users, and the gap between two factors was wider in a case of a user's direct management of an encryption key. This shows that forming a security channel could be a burden for a user's device.

Table 1. Number of Security Channels Regarding the Increase in Users

When a user directly manages an encryption key		*When a user uses a key management server*	
No. of users	No. of security channels	No. of users	No. of security channels
2	1	2	2
3	3	3	3
4	6	4	4
5	10	5	5
6	15	6	6
7	21	7	7
8	28	8	8
9	36	9	9
10	45	10	10

This time we studied if a partial encryption is able to efficiently distribute an encryption key. Partial encryption is a service that allows to use multiple encryption keys for one data. For the experiment, we set a public key cryptosystem in a key management server as RSAES and the length of the key as 2048 bit. With the operation mode CBC, AES was set as a cryptosystem for a user's direct distribution of an encryption key, and the length of the key was set as 128 bit. As referred once, a partial encryption can have multiple encryption keys for one data, so we measured a size of an encryption key distributed regarding the number of encryption keys and checked a network overhead. Table 2 shows a result of the experiment. When transmitting from 1 to 21 128-bit encryption keys, a user directly distributing an encryption key sends a smaller encryption key than a key management server; when transmitting more than 21.75 encryption keys, a key management server sends a smaller encryption key than a user directly distributing a key.

Table 2. Size of Transmission Regarding the Increase in Distributed Encryption Keys

When a user directly manages an encryption key		*When a user uses a key management server*	
No. of encryption keys	Size of transmission(byte)	No. of encryption keys	Size of transmission(byte)
1	16	1	348
2	32	2	350
5	80	5	350
10	160	10	351
15	240	15	352
20	320	20	353
25	400	25	354
30	480	30	353
35	560	35	356
40	640	40	358
45	720	45	360
50	800	50	360
55	880	55	360
60	960	60	362
65	1040	65	359
70	1120	70	360
75	1200	75	362
80	1280	80	364
90	1440	90	365
100	1600	100	368

5. Conclusion

A cloud service provider offered a cryptographic service to keep the confidentiality of the user's data. An encryption key was used in the service, and a provider distributed an encryption key to its users with a cryptography based on the authentication process. However, since an attacker could have access to data with

false verification, we proposed a key management server through the study. A key management server can ensure the confidentiality of a user's encryption key because a user can code an encryption key into a public key and register.

Additionally, a user selects a public key in a key management server to code an encryption key which only gives a user with a certain public key an access to an encryption key and prevents others to do the same. And a key management server is designed for a user to use a data ID provided from a search result in a cloud server and to receive a needed encryption key.

We could see that a key management server creates a security channel on a user's device which enables a key distribution, and especially, a partial encryption allows an efficient distribution of an encryption key.

References

[1] P. Mah, "'Fees? Advanced functions?" A cloud storage selection guide for you", 2016, http://www.itworld.co.kr/t/34/cloud /102173 (Accessed November 25)

[2] S.J. Purewal, "Four types of cloud storage for small and medium enterprises that meets the dropbox's unsatisfactory condition", 2013, http://www.itworld .co.kr/news/83366 (Accessed November 25)

[3] N.S. Jho and D.W. Hong, "Technical Trend of the Searchable Encryption System", Electronics and Telecommunications Trends. Vol. 23, No. 4, 2008

[4] K.M. Kim, K.S. Sohn and S.Y. Nam, "Key Generation and Management Scheme for Partial Encryption Based on Hash Tree Chain", The Korea Society for Simulation. Vol. 25, No. 3, 2016, http://dx.doi.org/10.9709/JKSS.2016.25.3.077

[5] I. Paul, "Privacy tips that Google and Facebook users should be sure to know", 2013, http://www.ciokorea.com/news /18817?page=0,1 (Accessed November 25)

[6] P. Mah, "'Hackers and terrorists target is data' What is corporate defense?", 2013, http://www.ciokorea.com/news /17764?page=0,0 (Accessed November 25)

[7] H. Selden, "Tresorit Encrypted Cloud Storage: What You Need to Know", 2016, http://www.tomsitpro.com/articles /tresorit-review,1-3333.html (Accessed November 25)

[8] S.J. Purewal, "'Specialized in safety' Three kinds of cloud services suitable for the storage of sensitive data", 2014, http:// www.ciokorea.com/news/20189?page=0,1 (Accessed November 25)

[9] P. Mah, "Three misconceptions of the cloud in small enterprises", 2016, http://www.itworld.co.kr /news/97712?page=0,1 (Accessed November 25)

[10] B. Butler, "'Even secure cloud storage is unsafe" ...Johns Hopkins University researcher", 2014, http://www.itworld. co.kr/news/87172 (Accessed November 25)