ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(S5), 33–36, March 2015* DOI : 10.17485/ijst/2015/v8iS5/61462

A Study on the use of Secure Data in Cloud Storage for Collaboration

Jae-Young Lee*

Department of Liberal Education, Semyung University, 579 Sinwoul-Dong, Jecheon-City Chungbuk, 390-711, Korea; klitie@semyung.ac.kr

Abstract

Cloud storage for collaboration is a cloud storage that all the users for collaboration share. Integrity and consistency of data stored in cloud storage are more important than in personal storage. In this study, we suggest guaranteeing integrity of data used hash function and digital signature in cloud storage for collaboration, ensuring logical and temporal consistency on shared data by solving the problems occurs when several users access to shared data at the same time.

Keywords: Cloud Computing, Cloud Storage, Collaboration, Consistency, Integrity

1. Introduction

Cloud storage for Collaboration is the way several users share one cloud storage offered by 'Cloud'. It is the best way at these days as distant users or group work has been increased with the proliferation of wireless Internet and mobile devices[1].

Integrity and consistency of data stored in cloud storage are more important than in personal storage as cloud storage for collaboration is the way several users for collaboration access to shared data stored in storage.

In this study, we suggest guaranteeing integrity of data used hash function and digital signature in cloud storage for collaboration, ensuring logical and temporal consistency on shared data by solving the problems occurs when several users access to shared data.

2. Related Study

2.1 Cloud Computing

Cloud Computing is computing offering services by using network and unifying distributed computing resources to virtualization technology. In cloud computing, we call the unified virtual space as 'Cloud', the users connected with network receive service by cloud. The service users borrow resources such as software, storage, server, network and else as needed, and pay the cost that the users use.

Cloud offers three types of virtual services: (1) Software as a Service (SaaS) offering application software that users need, (2) Platform working application, development environment and Platform as a Service (PaaS) offering tools, and (3) No abstracted service offered by PaaS but Infrastructure as a Service (LaaS) offering hardware such as computing ability, storage, database, etc[1–4].

2.2 Cloud Storage

Cloud Storage is one of IaaS offered by cloud and an online-virtual network storage. Cloud storage is the way we save the data in a storage space of 'Cloud', and we can access to the storage with any Web-capable devices in everywhere and it allows us to do diversity works on files by accessing any storage that we need[5,6].

2.3 Hash Function

Hash function is used to compress signature for improving practicality and efficiency of digital signature. Therefore, we must be careful not to hamper the stability of digital signature.

*Author for correspondence

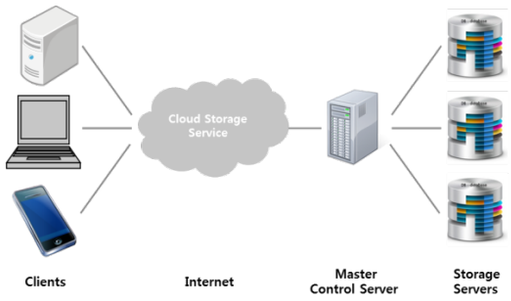

Figure 1. Cloud storage.

Hash function marks H = h(M). M means signature, h means hash function and H is the result of hash function[7].

2.4 Public-key Cryptography

Public-key cryptography is based on mathematical function and is asymmetric cryptographic using two keys connected mathematically.

Public-key cryptography works as follows. All the users who want to participate in public-key cryptography need to make private key and public key related to mathematics. And they keep their private key in secret and open their public key to allow other people to access easily.

Public-key cryptography can keep confidentiality of messages by decrypting encoded public key to the matching private key. And there is no problem with key distribution by using two keys which are private-key and matched public-key. The way encoding private-key is available for digital signature[7].

2.5 Concurrency Control Method

Concurrency control method is a processing technique of simultaneous approach on same data. And it has demanding characteristics of consistency maintenance of shared data and fast reaction time. Concurrency control method is largely divided into pessimistic concurrency control method and optimistic concurrency control method.

Pessimistic concurrency control method called exclusive locking is a method of blocking simultaneous approach on same data at source. The data user prevents simultaneous approach on shared data by blocking the approach of other users who want to use data by running Lock operation. And it also maintains consistency of data by limiting of less than 1 person is approachable to the shared data.

Optimistic concurrency control method always allows access to shared data regardless of access order. However, if there will be data changes from several users at the same time, we need to consider the order of timestamp to maintain consistency of data. We cancel the user's request with late timestamp and make them work again[8,9].

3. Proposed Method

When the users of cloud storage for collaboration want to save their date in storage, form Figure 2 as follows.

In saved data1 of user1 (U_1D_1), $S(H_1)$ is the result of digital signature encoded from H_1(hash result) of M_1 which is same way to save as Figure 3 to private key.

If the user2 wants to read U_1D_1 which is saved by user1, follow as Figure 4: (1) Check first whether other user access to the user1's U_1D_1 or not. (2) If other user is on, wait until the access is finished. (3) If not, block the other users access by running lock operation to the user 1's U_1D_1. (4) When the user2 finishes access to U_1D_1, allow other users access to U_1D_1 by running unlocking operation.

If the user2 can access to user 1's U_1D_1, read as the order of Figure 5: (1) separate $S(H_1)$ from U_1D_1 of the user 1. (2) Find values of H_1 by decrypting $S(H_1)$ to public key of user1. (3) Compare H_1' and H_1 which the user2 finds the values of hash in the user 1's saved message(M_1).

M	S(H)	Creation date	Last change date

M: Message of user, H: h(M_1), S: signature of User

Figure 2. Data of user.

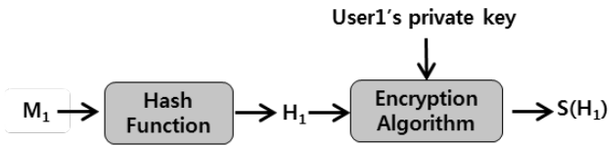

Figure 3. Digital signature value $S(H_1)$.

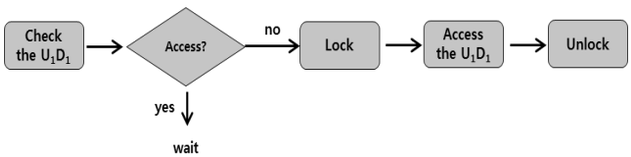

Figure 4. Lock and release.

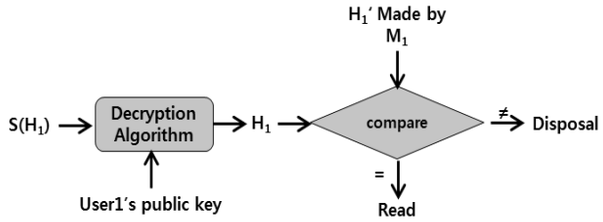

Figure 5. Read the data(user2).

(4) If the compare results are same, use the user1's saved message(M1). If not, abandon it.

If the user 2 want to save the user 1's M_1 after reading: (1) Change the name of M_1 to M_2. (2) Find the value of hash result of $M_2(H_2)$ by using hash function. (3) Make encoded digital signature of user2's private key $[S(H_2)]$ in hash result (H_2). The process is same as Figure 3: (1) Make as Figure 2 by linking M_2, digital signature, the forming date and the change date. (2) Save as U_2D_1 in storage.

When the user1 want to read U_1D_1, do the same way as user 2: (1) Check like Figure 4 whether U_1D_1 is used by other user. (2) If it is not used by other user, read it like Figure 5 after decrypting to public key and comparing the hash results are same.

If the user 1 want to save U_1D_1: (1) Change the name of saving message. (2) Find values of changed data. (3) Do digital signature to the hash result. (4) Attach forming date and change date. (5) Save as U_1D_2.

4. Stability Assessment of Suggesting Way

In the fourth chapter, we evaluate the data stability stored in storage, guaranteeing integrity, logical and temporal consistency in cloud storage for collaboration.

First, if you read the stored data in cloud storage for collaboration, you need to check that there are users who are approaching to the data. After checking, you can use the data only when there are no approaching users. Therefore, concurrency control on data is working, and logical consistency of data is guaranteed. And temporal consistency is also guaranteed by running locking operation and blocking access from other users while the user access to the data and read it.

Second, the data saved in cloud storage for collaboration links saved message, hash result of message, hash encoded electronic signature, message forming data and final change data as one. Therefore, data integrity is guaranteed by using hash result.

Also, Data integrity is guaranteed by another way because the data user can read and use unchanged data as the changed data is saved totally different name.

5. Conclusion

Cloud storage for collaboration is a storage that all the users share public data in storage offered by cloud. We can access to the storage with any Web-capable devices in everywhere and it allows us to do diversity works on files.

Cloud storage for collaboration is a place where several people share. Therefore, it is needed to have specialized security elements unlike normal cloud storage. In this study, we suggest how to use shared data safely by guaranteeing integrity, logical and temporal consistency of saved data.

There are suggesting ways. First, when you read the saved data in storage, check whether there are other users who are approaching to the data. After checking, you can use the data only when there are no approaching users. Therefore, logical consistency of data is guaranteed since there is no problem to change the data result. And temporal consistency is also guaranteed by running locking operation while the user access to the data and read it, and blocking access from other users who probably have different process result.

Table 1. Stability assessment

Classification	Security function	Contents
logical consistency	o	Logical consistency is not changed while the user read data as the other users can not approach to the data at that moment.
temporal consistency	o	When the user read and use the data, the other user can not approach. Therefore, processing result is reflected to the data without any interruption.
Integrity	o	Save data after encoding data hash result to private key and link to data. Save another data when the data is changed after the user approach and read.

Second, the storage users guarantee data integrity by saving not only saved message but also hash result, their electronic signature, data forming date and change data when they save the date in storage.

Third, data integrity is guaranteed by another way because the data user can read and use unchanged data as the changed data is saved totally different name.

We would like to study the possible problems with unlimited waiting when the users approach to the same data at the same time and wait until the other user finish working on that data.

6. References

1. Kim D-H. Design and implementation of authentication system for reinforced security in cloud computing environment. Graduate School of Gachon University; 2013.
2. Park S-N. A study on the security strategy of cloud computing services. Graduate School of Paichai University; 2013.
3. Lim C-S. Design and implementation of a collaborative team-based cloud storage system. Graduate School Soongsil University; 2011.
4. Han J-S. Security threats in the mobile cloud service environment. The Journal of Digital Policy and Management. 2014; 12(5):.
5. Lee H-C, Ware CS. A middleware supporting collaborative workspaces based on cloud storage. Graduate School Ulsan University; 2012 .
6. Armbrust M. Above the cloud: a berkeley view of cloud computing. UC at Berkeley; 2009 Feb.
7. Stallings W. Cryptography and Network Security. Prentice Hall; 2011.
8. Kim C-H. Concurrency control and communication protocol for collaborative virtual environments. Graduate School Korea Advanced Institute of Science and Technology; 1998.
9. Park Y-H, Lee J-H, Kim M-J. Optimistic concurrency control for satisfying temporal consistency in realtime database. Proceeding of KIISE. 2000; 27(2):