A Study of Secure and Efficient Data Sharing Scheme for Cloud Storage Architecture

Sun-Ho Lee¹, Jeong-Bae Lee² and Im-Yeong Lee¹,*

¹ Department of Computer Software Engineering, Soonchunhyang University, Asan, Chungnam, Korea
² Department of Computer Engineering, Sunmoon University, Asan, Chungnam, Korea

sunho431@sch.ac.kr, jblee@sunmoon.ac.kr, imylee@sch.ac.kr
*Corresponding Author

Abstract. Keeping pace with the increase of digital information in use, Cloud storage is in service, which can store one’s data from distance through network and various devices and easy to access. Unlike the existing removable storage necessary in order to carry data, it is used many users because it has no limit of memory capacity and no need to carry storage medium. As many users save a great volume of data in Cloud storage, its reliability has become a focus of issue. To protect it from unethical managers and attackers, researches are being conducted on application of a variety of cryptography systems such as searchable encryption and proxy re-encryption to Cloud storage system. However, existing searchable encryption technology is inconvenient in the cloud storage environment in which the user uploads data in person, and those data are shared with others, whenever it is necessary to do, and those with whom data are shared change frequently. In this paper, we propose a searchable re-encryption scheme by which user can share data with others safely by generating searchable encryption index, and re-encrypting it.

Keywords: Searchable encryption, Proxy re-encryption, Cloud computing, Storage.

1 Introduction

As the volume of digital information has rapidly expanded, storage medium has also developed rapidly to store data. Particularly for mobile storage that can enable us to carry data, tape drivers appeared first in 1951. Since then it has developed to floppy disks, optical media, and flash memory cars and now to USB flash drivers. Because such mobile storage media are easy to carry, it has high risk of loss or theft, which may lead to the discloser of personal information saved in the media. However, those media, because of portability, are also in danger of being stolen and lost, causing data in them to be leaked outside. As the development of network makes it possible for data communication to speed up, cloud computing service made its appearance that can store own data in distant storage and retrieve them to one’s own device to have access to them. Recently many companies are providing free storage service of high
capacity competitively. Accordingly, more and more people are currently using Cloud storage service to save their data in it. Like this, storing many users’ data in the system increases the possibility of ‘big brother problem’ and risk of disclosure by data attackers and unethical managers.

Data encryption may be one of the measures to tackle such problems, but it has its own hassle of making access to data hard. Therefore, searchable encryption system appeared that can encrypt the indexes of data and allow searching of the indexes without having data information be exposed to attackers and unethical managers [1-11]. However, this method is not applicable to Cloud environment where data sharing is frequent among users because of encrypted indexes. Subsequently, searchable re-encryption system entered that re-encrypt encrypted indexes to allow users to search data to be shared without decoding process for safe data sharing in Cloud storage [12]. However the existing systems do not place in consideration the case where those who share data share them with other users and the storage structure of Cloud, so that they handle indexes and data encryption in a single process. Actually Cloud storage system has separate server systems: master server that stores indexes and data information and a server to store data. Therefore, searchable re-encryption system is difficult to be applied to Cloud. Accordingly this study tries to propose a technical measure to allow safe sharing of Cloud users’ data, considering Cloud storage structure.

2 The preliminaries

2.1 Requirements

The following requirements should be met for safe search and sharing to be secured under Cloud storage environment.

Confidentiality: Data transmitted between remote data server and client terminal should be identifiable only by proper persons.

Search speed: The client who has limited system resources should be able to quickly search documents including word files from documents stored in cloud storage systems.

Traffic efficiency: Communication volume should be small for the energy efficiency between client and server, and efficiency of network resources.

Calculation efficiency: Calculation efficiency should be provided for index generation and execution of search, and for sharing data with other users safely.

Sharing efficiency among users: it must make encrypted data saved in distant data be protected and shared to those users who share them safely and efficiently from an unreliable server.

2.2 Bilinear pairing

The bilinear map was originally suggested as a tool to attack elliptical curve encryption, by reducing the problem of discrete algebra on elliptical curve into the problem of discrete algebra on finite field, and thus reducing the difficulty of it. However, it began to be used recently not as an attacking tool, but as an encryption
tool for information protection. Bilinear pairing is equivalent to a bilinear map. The following terms are used, as stated in this paragraph, and this theory is defined below.

**Definition 1** Characteristics that satisfy an admissible bilinear map are as follows;

Bilinear: Define a map \( e = G_1 \times G_1 \rightarrow G_2 \) as bilinear if \( e(aP, bP) = e(P,Q)^{ab} \) where all \( P, Q \in G_1 \), and all \( a, b \in \mathbb{Z} \).

Non-degenerate: The map does not relate all pairs in \( G_1 \times G_1 \) to the identity in \( G_2 \). Observe that since \( G_1 \) and \( G_2 \) are groups of prime order, this implies that if \( P \) is a generator of \( G_1 \), then \( e(P,P) \) is a generator of \( G_2 \).

Computable: There is an efficient algorithm to compute \( e(P,Q) \) for any \( P, Q \in G_1 \). The following definition was constructed based on the bilinear map \( e(aP, bQ) = e(aP,Q)^b = e(P,Q)^{ab} = e(abP,Q) = e(P, abQ) \). From this map, for ellipses, the D-H decision problem can be easily solved using the following equation. \( e(aP, bQ) = e(cP,P) \Rightarrow ab = c \). Therefore, the following is the basis for resolving the difficulties of the bilinear map used as an encryption tool by many encryption protocols.

**Definition 2** When elements \( G_1, P, aP,bP, cP \) (BDHP, Bilinear Diffie–Hellman Problem) are given, this refers to \( e(P,P)^{abc} \) calculation problem. In this research, the admissible bilinear map was used as the basis of the secret numbers production in the key construction process between heterogeneous devices. This problem can be solved, if the ellipse curve discrete mathematics problem can be solved. For example, \( a \) can be calculated from \( aP \), then \( e(P,P)^{abc} \) can be calculated through \( e(bP, cP)^a \).

### 3 Proposed Scheme

The proposed scheme defined above satisfies requirements by performing detailed calculation as follows.

#### 3.1 System parameters

- **p**: prime number
- **G**: Cyclic additive group of order \( p \)
- **\( G_T \)**: Cyclic multiplicative group of order \( p \)
- **g**: generator of \( G \)
- **e**: bilinear map, \( G \times G \rightarrow G_T \)
- **sk\_**: \( * \)'s secret key
- **pk\_**: \( * \)'s public key
- **w\_**: \( * \)_th keyword of data
- **H\_1()**: hash function, \( \{0,1\}^* \rightarrow G \)
- **H\_2()**: hash function, \( G_T \rightarrow \{0,1\}^* \)
- **T\_**: trapdoor searching keyword
- **rk\_a\_t\_**: re-encryption key changing \( A \)'s crypt to \( B \)'s crypt
3.2 KeyGen

TA generates a pair of keys and sends them safely to cloud storage user.

\[ x \in Z_q \text{ selection} \]
\[ \text{sk} = x \text{ setting up} \]
\[ \text{pk} = g^x \text{ setting up} \]

3.3 Enc(\(sk_a, pk_a, w\))

Data owner A generates the cipher-text which can be used for secure search

\[ A = pk_a^r \quad (r \in Z_p) \]
\[ B = e(g, g)^{sk_a r} \]
\[ C_i = H_2(e(g, H_1(w_i))^r) \]
\[ E_a = (A, B, C) \text{ output as encrypted index} \]

3.4 ReKeyGen(\(sk_a, pk_b\))

When the data owner wants to share his data with other users, he generates keys for re-encryption. When user A wants to share his data with user B, A generates re-encryption key using A’s secret key and B’s public key as follows.

\[ rk_{a\rightarrow b} = pk_b^{sk_a} \mod p \]

3.5 ReEnc(\(rk_{a\rightarrow b}, E_a\))\(\rightarrow E_b\)

The cloud storage service server, with re-encryption key inputted by the user, the target crypt intended to be re-encrypted, and public key, performs re-encryption as follows.

\[ A' = A^{sk_b/\text{sk}_a} \]
\[ B' = e(A, rk_{a\rightarrow b}) \]
\[ E_b = (A', B', C) \]

3.6 TrapdoorGen(\(sk_b, w\))

The user wanting to search the data generates trapdoor with keywords and his secret key.

\[ Tw = H_1(w)^{sk_b} \]
To confirm whether the data contain the keywords he intends to find, the user performs the following tests, by his public key, trapdoor, and crypt inputted from the server.

\[ C = H_4(e(A,T_w)) \]

4 Analysis

The proposed method satisfies the following requirements.

**Confidentiality:** By using pairing, the proposed method makes it difficult for a vicious third party to decode communication contents even if he bugs communication between client and server.

**Search speed:** By doing single pairing calculation and hash calculation, user can check whether the document contains keywords. The method provides quick search speed.

**Traffic efficiency:** Since keyword search and re-encryption need only one round of communication process, the method provides efficiency in communication volume.

**Calculation efficiency:** Based on lighter pairing calculation, the method allows user to generate index, search documents, and do re-encryption, providing calculation efficiency

**Sharing efficiency among users:** By re-decoding them, it must make encrypted and saved in unreliable distant data server be shared safely and efficiently regardless of time of use.

5 Conclusion

With the advent of cloud storage service, many users can store and get access to data by using it. To secure the security of data stored in such a storage place, researches designed to apply searchable encryption technology to cloud storage have begun recently. However, most of existing researches have problems in the sense that, since they are based on e-mail environment, and, thus decide objects with which data can be shared, they become inefficient in adding more objects to share data. In Cloud storage environment, users upload data to use by themselves. And they share them in a safe manner that they want. Therefore, data information like indexes and data are separated, so that the existing methods are hard to be compatible with Cloud storage system. Therefore, considering such requirements in the cloud storage environment, we set up security requirements, and proposed a method of providing the two functions simultaneously – Proxy Re-encryption function and searchable encryption function. This method provides efficiency in terms of calculation volume.

To make it flexible and easy to search data in cloud storage, it seems that the search method using multiple keywords will become an important issue. Therefore, it will be necessary to do research in the future on a re-encryption system where the
index composed of multiple keywords with variable length can be encrypted, and can
be searched flexibly.

Acknowledgments. This research was supported by Basic Science Research Program
through the National Research Foundation of Korea(NRF) funded by the Ministry of
Education, Science and Technology(2010-0022607)

References

3. Curtmola, R., Garay, J., Kamara, S. and Ostrovsly, R., Searchable Symmetric Encryption:
4. Boneh, D., Crescenzo, G., Ostrovsly, R. and Persiano, G., Public Key Encryption with
6. Hwang, Y. H. and Lee, P. J., Public key encryption with conjunctive keyword search and its
7. Bao, F., Deng, H. Robert., Ding, D. and Yang, Y., Private Query on Encrypted Data in
   Multi-User Settings, international conference on Information security practice and
8. Kamara, S. and Lauter. K., Cryptographic Cloud Storage. Financial Cryptography and Data
   Security, 6054 (2010), 136-149.
   Cloud Databases. International Symposium on Policies for Distributed Systems and
10. Zhang, B. and Zhang, F., An efficient public key encryption with conjunctive-subset