Data Security and Privacy for Cloud Storage Using Key Aggregate and Searchable Encryption

Akshatha M
PG Scholar (M.TECH), Dept. of CSE, RRIT, Bangalore-560090, India.

Dhananjaya M K
Assistant Professor, Dept. of CSE, RRIT, Bangalor-560090, India.

Abstract – The competence of encrypting and sharing selected data among different users via public cloud storage may ease security concerns over unintentional data disclosures in the cloud. Designing an encryption scheme depends on the competent administration of encryption keys. The task to design such encryption methods depends on the experienced management of encryption keys. Dissimilar encryption keys should be used for dissimilar documents which are needed to be shared among a group of users. This can be done by distributing a large number of keys effectively. These keys can be used both for encryption and searching. The users who receive these keys have to store it safely. In order to search on the distributed data, keyword trapdoors has to be submitted to the cloud. Having a protected storage and communication on the cloud seems impractical. This problem is made practical in this paper by recommending the perception of searchable cumulative key encryption using the Key Aggregate Searchable encryption (KASE) scheme. The data owner in KASE distributes a single key to a user to share a group of documents. The user submits this key to the cloud along with the trapdoor to extract the documents stored on the cloud. The estimation of performance and security authenticates that the proposed scheme is proficient.

Index Terms – Searchable encryption, data sharing, cloud storage, data privacy.

1. INTRODUCTION

Now-a-days millions of users share data, such as videos, photos and other business purposethrough cloud. Cloud has become a favorable solution for providing on-demand access. The data leaks on the cloud are causing serious obstacles for secure communication.

A common methodology to avoid these leaks on cloud is to use encryption. The owner of the data encrypts the data before uploading, the data can be retrieved by decrypting the data using the key. The challenge here is to search data on the cloud and then retrieve the selected data. The search here is done by providing keywords. This is achieved only when the data owner encrypts the possible keywords. These keywords should be uploaded to the cloud along with the encrypted data. The data matching the keyword will be retrieved when the user performs search on the encrypted data by using corresponding keyword trapdoors.

Here, in this paper we use the searchable cumulative encryption. This method selects a group of files and shares with selected users. These users will search the data based on the keyword. To implement this method the key has to be managed efficiently. There are two major requirements to manage the keys. Firstly, data owner should share a cumulative key instead of large number of keys for sharing any number of files. Secondly, the user should submit only a single trapdoor instead of number of trapdoors to perform search on the shared files based on keywords provided.

2. RELATED WORK

This section reviews different categories of solutions and also explainhow they are related to our work.

2.1 Multiple user Searchable Encryption

The literature of searchable encryption includes SSE scheme and PEKS scheme. In comparison to this, the keyword search in the multi-tenancy model is common. In this case the owner will have to share a document with group of legitimate users, and the user who has the right to access the data has to perform the keyword search on the data that is shared on the cloud by providing a trapdoor.

The main task here is to control which users can access which documents but how to reduce the number of keys and trapdoors that is shared is not considered here.

2.2 Multiple-Key Searchable Encryption

The concept of Multiple-Key Searchable Encryption was first introduced by Popa. In this scheme, the server searches for a trapdoor's keyword in the document which are encrypted with different keywords. But in the cumulative approach the right to search keyword is given to any user. This is done by giving the cumulative key to the user in a group.

The approach of multiple key searchable encryption focuses on the keyword search on a group of data that is shared to a user and even the method to search keyword on a group of documents with a single trapdoor

3. PORPOSED MODELLING

Suggesting the uniquenotion of key aggregate searchable encryption (KASE) and instantiating the notion through actual KASE scheme. Here the data owner is required to issue a single key to other user to whom the large amount data has to be shared, and the user is required to propose a single trapdoor to the cloud in order to search the shared data.

The advantages are:

- Efficient
- Secure

3.1Work Flow

Setup: When a request is submitted by the organization the cloud creates a group ID for the respective organization. It also allocates the manager the admin account. Now the manager will control the system.

Registration: To add a new user, userID, userName. Password and a pair of key is generated. These user information is stored in the database and displayed in a table form. The private key of the user is issued via a secured network.

Login: This system depends on the verification of authenticated users.

Upload:select the document that has to be uploaded. This document is encrypted, keywords are generated and these keywords are encrypted into cipher texts and later uploaded to the cloud. The cloud allocates an id to each document that is uploaded and the path the document is stored is denoted vbyfilePath.

Data distribution: To distribute the selected data share with a user, the data owner generates the aggregate key and the hash key. Later these two keys are aggregated into a single key and this key is sent to the user through a secure network.

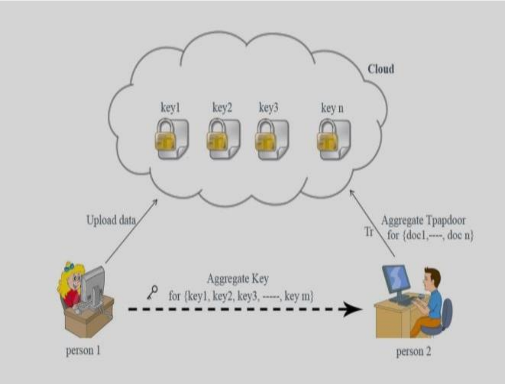

Fig: Distribution of aggregate key.

Keyword Search: The user in order to rec over the encrypted data has to search the document in the cloud by searching the keyword.

Trapdoor: In order to create a trapdoor for the keyword for the data distributed by the data owner the request has to be sent, using which the cloud will run cumulative key search for each trapdoor.

3.2 Design

The design includes seven functions:

- **Setup**: This function is used to initialize the system parameters.
- **Keygen**: This function is used by the data owner to generate the key pair which is cumulative key of master key and hash key.
- **Encrypt:** This function is used by the data owner encrypt the document and generate its keyword cipher texts while uploading the document
- **Extract**: This function is used by the data owner to generate an cumulative key while helps in searching the document.
- **Trapdoor**: this function is used by the user create a trapdoor to search the keyword.

4. CONCLUSION

Considering the practical problem of privacy preserving data distributing system based on public cloud storage requires a data owner to distribute a large number of keys to users. By this the users can access the distributed documents from the cloud. First time the concept of cumulative key and searchable encryption has been proposed. This paper provides a solution to build a data distributing system in the cloud. Here, the owner needs to just share a single key for sharing a large number of documents. The user submits only a single trapdoor to access the distributed documents.

REFERENCES

[1] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance:The Essential of Bread and Butter of Data Forensics in CloudComputing”, Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.

[2] C. Chu, S. Chow, W. Tzeng, et al. “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477

[3] B. Wang, B. Li, and H. Li, “Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud”, Proc. 10th Int’l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012

[4] Y. Hwang, P. Lee. “Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System”, In: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.