An Efficient Reduction of Encryption Keys for Group Data Sharing via Cloud Storage

ManjulaK.[1],MahalakshmiG.[2],YashaswiniM.S[3]
Department of Information Science, Visveswaraya Technical University, Bangalore-60
manjukarur@gmail.com, mahalakshmi.gk25@gmail.com, yashu.cool968@mail.com

ABSTRACT-The art of selectively sharing encrypted data with different users via public clouds to rage may greatly ease security concerns with unintentional data leaks in the cloud. While sharing any group of selected documents with any group of users demands different encryption keys to be used for different documents.The user receives a large number of keys for both encryption and search. The user should also store the received keys and submit equal number of Keyword Secret door to cloud to perform search over the shared data. Due to the secure communication, complexity and problem, the above approach is impractical. So to address this problem,we propose a novel concept of One Key Search Many(OKSM) and instantiating the concept through a concrete One Key Search Many(OKSM) scheme,in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single Secretdoor to the cloud for querying the shared documents.

IndexTerms-Cloudstorage,Dataprivacy ,Datasharing, Searchable encryption.

I. INTRODUCTION

Nowadays the storage in the cloud has materialized as a capable answer for providing convenient and on-demand access to large amounts of data shared over the Internet. Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better resource utilization.

However, while enjoying the convenience of sharing data via cloud storage, users are also concerned about inadvertent data leaks in the cloud. It is caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets.

To overcome users‘ concerns over potential data leaks in cloud storage, a common approach is for the data owner to encrypt all the data before uploading into the cloud such an cloud storage is often called the cryptographic cloud storage. However, the encryption of data makes it challenging for users to search and then selectively retrieve only the data containing given keywords. A common solution is to employ a searchable encryption (SE) scheme , in which the data owner is required to encrypt potential keywords and upload them to the cloud together with encrypted data, such that, for retrieving data matching a keyword, the user will send the corresponding keyword Secret door to the cloud for performing search over the encrypted data.

Although combining a searchable encryption scheme with cryptographic cloud storage can achieve the basic security requirements of a cloud storage, but not the efficient management of encryption keys. If the need for selectively sharing encrypted data with different users (e.g., sharing a photo with certain friends in a social network application, or sharing a business document with certain colleagues on a cloud drive) usually demands different encryption keys to be used for different files. However, this implies that the number of keys need to be distributed to users, for both to search over the encrypted files and to decrypt the files, will be proportional to the number of such files. Such a large number of keys must not only be distributed to users via secure channels, but also be securely stored and managed by the users in their devices.

Also a large number of secret doors must be generated by users and submitted to the cloud in order to perform a keyword search over many files. The secure communication, Complexity and storage tells that the above system is impractical.

We address this challenge by proposing the novel concept of One Key Search Many (OKSM), and instantiating the concept through a concrete OKSM scheme. The proposed OKSM scheme applies to any cloud storage that supports the searchable group data sharing functionality, which means any user may selectively share a group of selected files with a group of selected users. To support searchable group data sharing the main requirements for efficient key management are twofold.

As shown in the Fig.1,first, a data owner only needs to distribute a single One Key (instead of a group of keys) to a user for sharing any number of files. Second, the user only needs to submit a single secret door (instead of a group of secret doors) to the cloud for performing keyword search over any number of shared files.

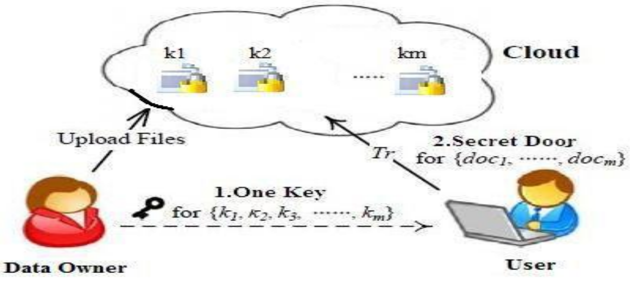
k1
k2
km
Cloud
Upload Files
Tr
2.Secret Door
for $\{doc_1, \cdots\cdots, doc_m\}$
1.One Key
for $\{k_1, k_2, k_3, \cdots\cdots, k_m\}$
Data Owner
User

Fig.1: One Key Search Many

Our main contributions in this paper are as follows:

We first define a general framework of One Key Search Many (OKSM) composed of seven polynomial algorithms for security parameter setup, key generation, encryption, key extraction, secretdoor generation, secretdoor adjustment, and testing. We then describe both functional and security requirements for designing a valid OKSM scheme.

We then instantiate the OKSM framework by designing a concrete OKSM scheme. After providing detailed constructions for the seven algorithms, we analyze the efficiency of the scheme, and establish its security through detailed analysis.

We discuss various practical issues in building an actual group data sharing system based on the proposed OKSM scheme, and evaluate its performance. The evaluation confirms our system can meet the performance requirements of practical applications.

2. RELATED WORK

In Public Encryption With Keyword Search(PEKS) [1], the problem in public cloud system to search for encrypted data through encryption key is examined. Keyword as search query for email gateway is firstly introduced. Then based on the keyword the documents are routed to the gateways.PEKS system implies Identity Based Encryption (IDE) scheme where owner encrypts data such that user having required attributes can only decrypt the shared document. This system considered only single owner and user condition for performing keyword search over multiple shared documents.

In Symmetric Searchable Encryption(SSE)[2] ,one party allows to outsource the storage of its data to another party ,where another party is a server .In SSE there can be no sharing of data between two individuals, hence it is specified for a single user.

In Multi-user Searchable Encryption (MUSE) [3],[4]: It works under multi-tenancy operations where data owner shares documents with group of users and users can receive them by submitting trapdoor for keyword search on shared contents. That means users who have authorization can only retrieve the documents. It advances the single user SSE and PEKS schemes. But access control is not fine grained.

In Attribute Based Encryption(ABE) [5], narrowing the scope of search results to user's decryptable file's group can be done.ABE is of two types Key Policy(KP-ABE) andCipher Policy(CP-ABE) .CP- ABE isused to minimize the information leak and to reduce searching complexity when there are multi-users in cryptographic cloud storage. This system only search for related documents which user can decrypt and so is more efficient. The flexibility of specifying the access rights for individual users in case of user revocation is provided known as fine grained access control.

In Multi-Key Searchable Encryption(MKSE) [6],this system provides flexibility to user for searching over multiple documents which he/she can access say n, with different encryption keys. One search token is provided by user to server instead of n tokens. The user have to provide some public information and token for word to search and the system server then by using this information calculates token for different keys (adjust function) and get all documents with matching word even their encryption keys are different. Only single user and multi-key condition is considered in this system.

In Key Aggregate Encryption (KAE) for Data Sharing [7], the sharing of multiple documents with same user can be done , the data owner needed to distribute equal number of keys to the user. The complexity and security aspects become more subtle and impractical in case of large number of shared documents. In this scheme only single aggregate key to decrypt all documents is provided by owner i.e. compression of secret key. A public-key cryptosystem is introduced which produce constant-size cipher-texts leading to limited secure storage application. The user encrypts data under public key and ciphertext class which is identifier of ciphertext.

3 . IMPLEMENTATION

We first define the OKSM scheme ,which consist of seven algorithm .The algorithms are as follows :

Setup

This algorithm is run by the cloud service provider to set up the scheme. On input of a security parameter and the maximum possible number of documents which belongs to a data owner, it outputs the public system parameter Params.

Keygen

This algorithm is run by the data owner to generate a random key pair (pk,msk).

Encipher

This algorithm is run by the data owner to encrypt the i-th document and generate its keywords' ciphertexts. For each document, this algorithm will create a delta for its searchable encryption key ki. On input of the owner's public key pk and the file index i, this algorithm outputs data ciphertext and keyword ciphertexts Ci.

Onegen

This algorithm is run by the data owner to generate an OneKey ,searchable encryption key for delegating the keyword search right for a certain set of documents to other users. It takes as input the owner's master-secret key msk and set S which contains the indices of documents ,then outputs OneKey.

Secretdoor

This algorithm is run by the user who has the onekey to perform a search. It takes as input the onekey searchable encryption key ok and a keyword w, then outputs only one secretdoor .

Tune

This algorithm is run by cloud server to adjust the combined secretdoor to generate the right secretdoor for each different document. It takes as input the system public parameters params, the set S of documents‘ indices, the index i of target document and the combined secretdoor Sr, then outputs each secretdoor Sri for the i-th target document in S.

Search

This algorithm is run by the cloud server to perform keyword search over an encrypted document. It takes as input the secretdoor and the document index i, then outputs true or false to denote whether the document contains the keyword w.

Designing of OKSM scheme :

For designing of OKSM scheme it should satisfy functional and security requirements , they are as follows:

Functional Requirements

- **Compactness:** The size of the One key has to be independent of the number of files to be shared .
- **Searchability:** This specifies the reduction of encryption has to preserve the keyword search.
- **Delegation :** The goal is to give the keyword search right to the user through One key.

Security Requirements

- **Controlled Searching:** Meaning that the intruder cannot search for an random word without the data owner‘s authorization.

- **Query Privacy:** Meaning that the intruder cannot determine the keyword used in the query because the user hides the actual keyword from the server also.

Evaluation of OKSM scheme

Here ,the various practical issues in building an actual group data sharing system based on the proposed OKSM scheme, and evaluate its performance . Through detailed analysis we achieve the functional and security requirements .

4. RESULTS

Our system is efficient as we can see that ,even when the number of documents increases which are to be shared ,the time cost is linear with the number of documents .It also shows the a single secretdoor will not reduce the efficiency over searching of document. This is showed in Fig.2,

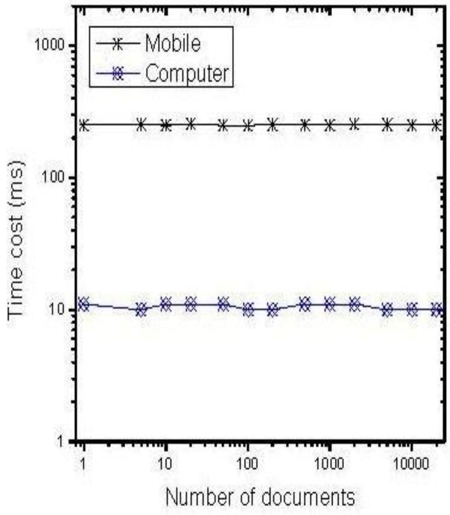

Fig.2: Time cost of secretdoor

5. CONCLUSION

Taking into consideration of the realistic problem of privacy preserving data sharing system based on public cloud storage which is need a data owner to allocate a large number of keys to users to permit them to access the documents, In this proposed concept of One Key Search Many (OKSM) and construct a concrete OKSM scheme. It can provide an efficient solution to building practical data sharing system based on public cloud storage. In a OKSM scheme, the owner needs to distribute a single key to a user when contributing a lot of documents with the user, and the user needs to submit a single secret door when they queries over all documents shared by the same owner.

On the other hand, if a user wants to question over documents shared by multiple owners, that user must produce multiple secret door to the cloud. The future enhancement for this proposed work is to find out how to decrease the number of secret door under multi-owners setting by attaining the security.

REFERENCES

Proceedings Papers:

[1] D. Boneh, C. G, R. Ostrovsky, G. Persiano. ―Public KeyEncryption with Keyword Search‖ eurocrypt 2004, pp.506C522,2004.

[2] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky ―Searchable Symmetric Encryption: improved definitions and efficient constructions‖, In: Proceedings of the 13th ACM conference on Computer

and Communications Security, ACM Press, pp. 79-88, 2006.

[3] Z. Liu, Z. Wang, X. Cheng, C. Jia and Ke Yuan, ―Multi-user Searchable Encryption with Coarsed Grained Access Control in Hybrid Cloud‖, 2013.

[4] W. Li, J. Li, X. F. Chen, et al."Efficient` Keyword Search over Encrypted Data with Fine-Grained Access Control In Hybrid Cloud", In: Network and System Security 2012, LNCS, pp. 490-502, 2012.

[5] F. Zhao, T. Nishide, and K. Sakurai, ―Multi- User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control‖, 2012.

[6] A. Popa and N. Zeldovich, ―Multi-Key Searchable Encryption‖, 2013.

[7] C.Chu,S.Chow,W Tzeng,et al,‖Key Aggregate Cryptosyste for Scalable data Sharing in Cloud Storage‖,IEEE Transaction parallel and distributed system ,2014.