Impact Factor: 4.14 (Calculated by SJIF-2015)

e- ISSN: 2348-4470
p- ISSN: 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 4, April -2016

Key-Aggregate Searchable Encryption for Group Data Sharing via Cloud Storage

Kelji Divyashree[1], Waghmode Manisha[2], Kharat Pallavi[3], Mane Rani[4] ,Sinkar Y. D.[5]

[1-4]Student,[5]Asst. Professor, Department of computer Engg, SVPM's COE,Malegaon (Bk), Baramati, Pune

Abstract *— The capability of selectively sharing encrypted data with different users via public cloud storage may greatly ease security concerns over inadvertent data leaks in the cloud. A key challenge to designing such encryption schemes lies in the efficient management of encryption keys. The desired flexibility of sharing any group of selected documents with any group of users demands different encryption keys to be used for different documents. However, this also implies the necessity of securely distributing to users a large number of keys for both encryption and search, and those users will have to securely store the received keys, and submit an equally large number of keyword trapdoors to the cloud in order to perform search over the shared data. The implied need for secure communication, storage, and complexity clearly renders the approach impractical. In this paper, we address this practical problem, which is largely neglected in the literature, by proposing the novel concept of keyaggregate searchable encryption (KASE) and instantiating the concept through a concrete KASE 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 trapdoor to the cloud for querying the shared documents. The security analysis and performance evaluation both confirm that our proposed schemes are provably secure and practically efficient.*

Keywords- *Searchable encryption, Broadcast encryption, data sharing, cloud storage, data privacy*

I. INTRODUCTION

Over the Internet for providing convenient, ubiquitous and for large amounts of shared data's on-demand accesses, there has emerged as a promising solution by cloud storage. Today, based on cloud storage through social network applications, personal data such as photos and videos are shared by millions of users with their friends on a daily basis. Due to its numerous lower cost, better resource utilization and greater agility, by cloud storage the business users are also being attracted . However, concerned of users about inadvertent data leaks in the cloud also increasingly via cloud storage while enjoying the convenience of sharing data. There can usually lead to serious breaches of personal privacy or business secrets due to such data leaks. Over potential data leaks in cloud storage to address users' concerns, all the data encrypted before uploading them to the cloud is the common approach for the data owner, such that later by those who have the decryption keys, the encrypted data may be retrieved and decrypted which is called the cryptographic cloud storage. However, for users to search and then selectively retrieve only the data containing given keywords, the encryption of data makes it challenging. To employ a searchable encryption (SE) scheme, a common solution is in which potential keywords are encrypt by data owner and together with encrypted data upload them to the cloud, such that, for performing search over the encrypted data, the user will send the corresponding keyword trapdoor to the cloud for retrieving data matching a keyword. The basic security requirements of a cloud storage can achieve by the cloud storage although combining a searchable encryption scheme with cryptographic, for large scale applications, implementing such a system involving millions of users and by practical issues involving billions of files may still be hindered the efficient management of encryption keys, which, are largely ignored in the literature to the best of our knowledge. First of all, for different files which the need for selectively sharing encrypted data with different users, there usually demands different encryption keys to be used. Such a large number of keys must be securely stored and managed as well as distributed to users via secure channels, by the users in their devices. In addition, by the users there must be generated a large number of trapdoors and in order to perform a keyword search over many files submitted to the cloud. Such a system inefficient and impractical the implied need for secure computational complexity, communication and storage may render.

In this paper by proposing the novel concept of KASE, we address this challenge and through a concrete KASE scheme instantiating the concept. To any cloud storage there applies the proposed KASE scheme which supports the functionality of searchable group data sharing, which means that, any user may selectively share the group of selected files with a selected users group, to perform keyword search over the former while allowing the latter. For efficient key management the main requirements are twofold for supporting searchable group data sharing. First,for sharing any number of files, a data owner only needs to distribute a single aggregate key to a user. Second, over any number of shared files for performing keyword search, there only needs to submit the user to the cloud a single aggregate trapdoor.

To the best of our knowledge, in this paper the KASE scheme proposed can satisfy both requirements. Our main three contributions are as follows.

1) The first contributions the KASE System composed different seven polynomial algorithms such as setup, key generation , encryption , key extraction , trapdoor generation , trapdoor adjustment , trapdoor testing. Then we define functional and security requirement of KASE system.

2) After designing scheme of a concrete KASE, we then instantiate the KASE framework. For the seven algorithms after providing detailed constructions, we establish its security through detailed analysis and analyze the efficiency of the scheme.

3) Based on the proposed KASE scheme, in building an actual group data sharing system we discuss various practical issues and evaluate its performance.

II. MOTIVATION OF THE PROJECT

- The motivation of this document is to define the requirements of credit card fraud detection.
- This document will provide a general description of our project, including user requirements, product perspective.
- It will provide the specific requirements and the functionality need in the project such as interface, functional requirements and performance requirements.

III. EXISTING SYSTEM

3. 1 Multi-user Searchable Encryption : Including PEKS as well as SSE schemes, on searchable encryption there is a rich literature. The keyword search under the multi-tenancy setting is a more common scenario in the context of cloud storage in contrast to those existing work. In such a scenario, to share a document with a group of authorized users the data owner would like, and over the “mult i-user searchable encryption” (MUSE) scenario, each user can provide a trapdoor who has the access right to perform the keyword search. To such a MUSE scenario some recent work focus, although to achieve the goal with access control they all adopt single-key combined. With all users by sharing the document’s searchable encryption key who can access it, MUSE schemes are constructed, and to achieve coarse-grained access control broadcast encryption is used. To achieve fine-grained access control aware keyword search attribute based encryption (ABE) is applied. As a result, in MUSE, how to control which users can access which documents is main problem, whereas There is not considered how to reduce trapdoors and shared the number of keys. The solution for the latter can provide by key aggregate searchable encryption, and it can be make more practical and efficient for MUSE.

3 .2 Multi-Key Searchable Encryption : In the case of application which has a multi-user, to search over considering that there is proportional the number of trapdoors to the number of documents, The concept of multi-key searchable encryption (MKSE) was introduced by Popa.

IV. PROPOSED SYSTEM

From both the encryption of multi-key searchable scheme as well as the key-aggregate data sharing scheme, there draws its insights the design of our KASE scheme. Specifically, instead of many independent keys, in order for creating an aggregate searchable encryption key, we adapt the idea presented in. With a particular index of document each searchable encryption key is associated, and into the product of public keys embedding the owner’s master-secret key which is associated with the documents, the aggregate key is created. Over different documents, in order to implement keyword search using the aggregate trapdoor. To produce an adjusted trapdoor, the cloud server can use this process for every document.

4 . 1 The KASE Framework : There composed of seven algorithms by The KASE framewors. Specifically, to set up the scheme, the public parameters of the system would generate by the cloud server through the Setup algorithm, and by different data owners these public parameters can be reused to share their files. A public/master-secret key pair should produce by him/her for each data owner, through the Keygen algorithm. With the unique searchable encryption key, via the Encrypt algorithm the keywords of each document can be encrypted. Then, to generate an aggregate searchable encryption key, via the Extract algorithm the master-secret key can be used by data owner for a group of selected documents. To authorized users who need to access those documents the aggregate key can be distributed securely. After that, as shown in Fig.2, via the Trapdoor algorithm a keyword trapdoor can produce using this aggregate key by an authorized user, and for the cloud there submit the trapdoor. The cloud server will run after receiving the trapdoor over the specified set of documents for performing the keyword search**.**

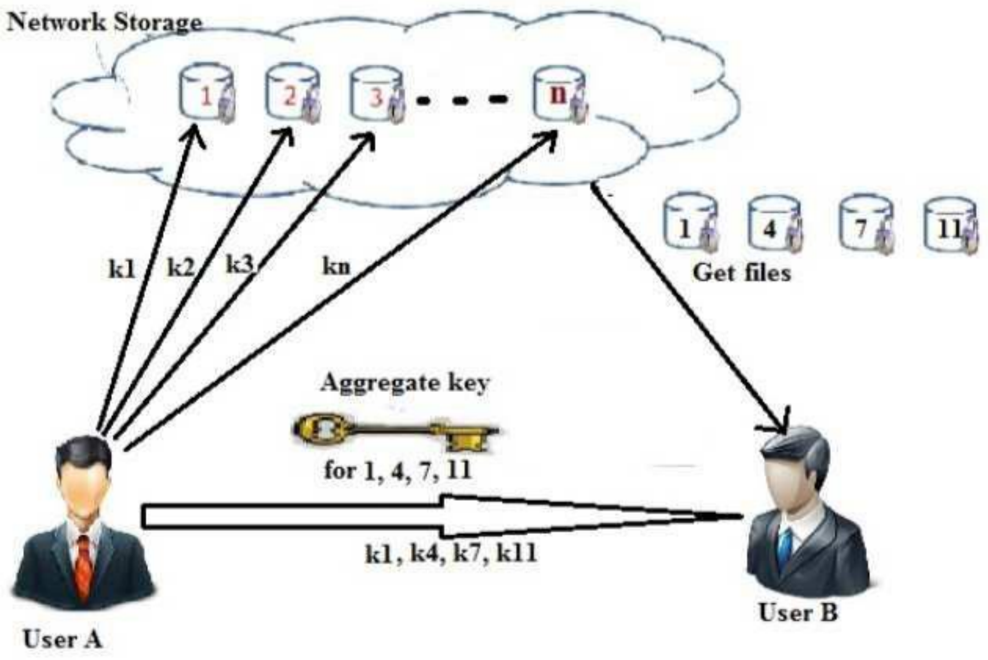

Fig. 2. Framework of key-aggregate searchable encryption.

For each document the right trapdoor generate by the Adjust algorithm, and then for testing whether the document contains the keyword, run the Test algorithm

4 .2 Description of the Scheme:

The proposed KASE system described working as follows:

1 . Setup : This algorithm is work in cloud server sides to set up the system .In this generate public parameter for every n no. of document which is belongs to the data owner.

2. Keygen : This algorithm is work in data owner sides to generate a random key pair such as key pair is public key and master key for every data owner.

3. Encrypt : This algorithm also work in data owner side. In this data owner encrypt all data files before uploading cloud server using AES encryption algorithm.

4.Extract : This algorithm also run in data owner sides to generate an aggregate searchable encryption key using input as it’s own master key and user provided file index. Also data owner extract related keyword for search these file in cloud.

5.Trapdoor : This algorithm work in user sides to generate a single aggregate trapdoor using input is aggregate key and keyword which send by data owner.

6. Adjust : This algorithm run in cloud server to adjust the aggregate trapdoor to generate the right trapdoor for each different document.

7.Test : This algorithm work in cloud server sides to perform keyword search over an encrypted document. The searched document downloaded in user sides.

V. ALGORITHM

AES Algorithm

Step 1: Key Expansions

For each round AES needs a different 128-bit block of round key also one more.

Step 2: Initial Round

AddRoundKeywith a block of the round key, each byte of the state is combined using
bitwise xor.

Step 3: Rounds

- Sub Bytesin this step each byte is replaced with another byte.
- Shift Rows for a certain number of steps, the states last three rows are moved cyclically.
- Mix Columns on the columns of the state a mixing operation operates, in each column combining the four bytes.

Step 4: AddRoundKey

Stpe 5: Final Round (no Mix Columns)

- Sub Bytes
- Shift Rows
- AddRoundKey.

VI. GOALS

1. Securely distributing to users a large number of keys for both encryption and search.
2. Those users will have to securely store the received keys.
3. The user submit an equally large number of keyword trapdoors to the cloud in order to perform search over the shared data.

VII. APPLICATIONS

1. It can be very useful for sending data over insecure network.
2. Private and Hybrid cloud computing.
3. Privacy preservation in Defence Application.
4. On-line Transaction security.

VIII . RESULT ANALYSIS

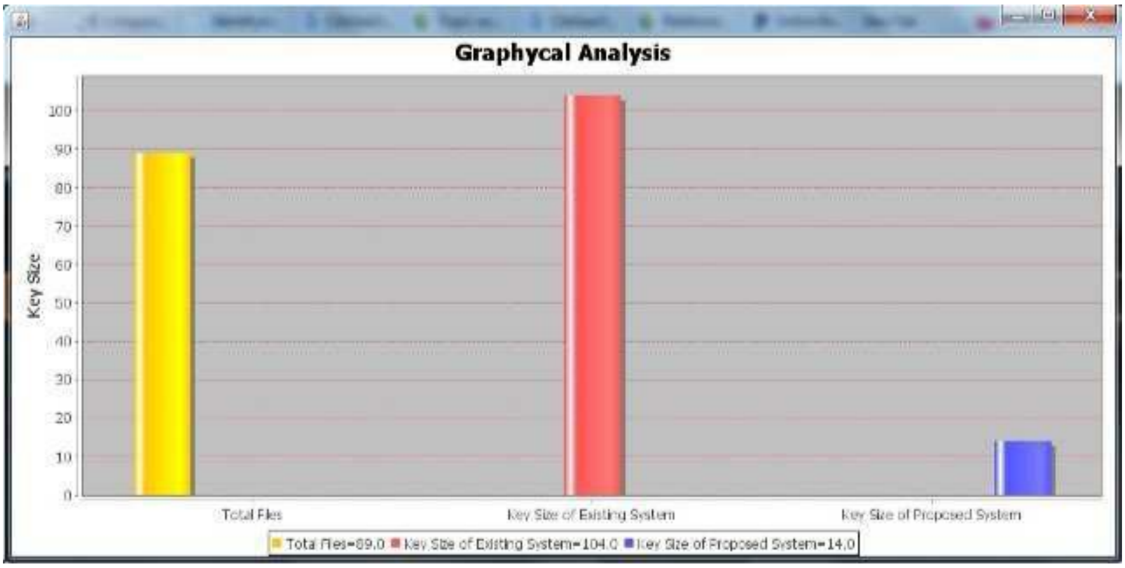

Fig. Result Analysis Graph

This analysis graph show s that key size of exiting system is so large and in proposed system maintenance key size easy. we can see that the number of keys of a member is linear in the number of users who share documents with anther user. Compared to traditional data sharing solutions ,this system has better efficiency.

IX. CONCLUSION AND FUTURE SCOPE

Considering the practical problem of privacy preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users to enable them to access his/her documents, we for the first time propose the concept of key-aggregate searchable encryption (KASE) and construct a concrete KASE scheme. Both analysis and evaluation results confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage.

In a KASE scheme, the owner only needs to distribute a single key to a user when sharing lots of documents with the user, and the user only needs to submit a single trapdoor when he queries over all documents shared by the same owner. However, if a user wants to query over documents shared by multiple owners, he must generate multiple trapdoors to the cloud. How to reduce the number of trapdoors under multiowners setting is a future work. Moreover, federated clouds have attracted a lot of attention nowadays, but our KASE cannot be applied in this case directly. It is also a future work to provide the solution for KASE in the case of federated clouds.

REFERENCES

[1]. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing”, Proc. IEEE INFOCOM, pp. 534-542, 2010.
[2]. R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing”, Proc. ACM Symp. Information, Comp uter and Comm. Security, pp. 282-292, 2010.
[3]. X. Liu, Y. Zhang, B. Wang, and J. Yan. “Mona: secure multiowner data sharing for dynamic groups in the cloud”, IEEE Transactions on Parallel and Distributed Systems , 2013, 24(6): 1182- 1191.
[4]. C. Chu, S. Chow, W. Tzeng, et al. “Key-Aggrega te Cryptosystem for Scalable Data Sharing in Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.
[5]. X. Song, D. Wagner, A. Perrig. “Practical tech niques for searches on encrypted data”, IEEE Sympos ium on Security and Privacy, IEEE Press, pp. 44C55, 2000.
[6]. R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. “Searchable symmetric encryption: improved defini tions and efficient constructions”, In: Proceedings of the 13 th ACM conference on Computer and Communications Security , ACM Press, pp. 79-88, 2006.
[7]. P. Van,S. Sedghi, JM. Doumen. “Computationally efficient searchable symmetric encryption”, Secure Data Management, pp.87-100, 2010.
[8]. S. Kamara, C. Papamanthou, T. Roeder. “Dynamic searchable symmetric encryption”, Proceedings of t he 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965-976, 2012.
[9]. D. Boneh, C. G, R. Ostrovsky, G. Persiano. “Pu blic Key Encryption with Keyword Search”, EUROCRYPT 2004, pp. 506C522, 2004.
[10]. 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 2 007, LNCS, pp. 2-22, 2007.
[11]. J. Li, Q. Wang, C. Wang. “Fuzzy keyword searc h over encrypted data in cloud computing”, Proc. IE EE INFOCOM, pp. 1-5, 2010.
[12]. C. Bosch, R. Brinkma, P. Hartel. “Conjunctive wildcard search over encrypted data”, Secure Data Management. LNCS, pp. 114-127, 2011.
[13]. C. Dong, G. Russello, N. Dulay. “Shared and s earchable encrypted data for untrusted servers”, Jo urnal of Computer Security, pp. 367-397, 2011.
[14]. F. Zhao, T. Nishide, K. Sakurai. Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control. Information Security and Cryptology, LNCS, pp. 406-418, 2012.
[15]. J. W. Li, J. Li, X. F. Chen, et al. “Efficien t Keyword Search over Encrypted Data with Fine-Grained Access Control in Hybrid Cloud”, In: Network and System Se curity 2012 , LNCS, pp. 490-502, 2012.