ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

# KEY AGGREGATE ANONYMS AUTHENTICATION FOR GROUP DATA SHARING VIA CLOUD STORAGE

**Student Name: Amsaleka.D**

**Dept of Computer Science & Engg**

**Mahabarathi Engineering College**

**Chinnasalem 606201.**

**lekha.raj19@gmail.com**

**Guide Name: Dr.V.Ravikumar M.Tech.,Ph.d.,**

**Assistant Professor**

**Dept of Computer Science & Engg**

**Mahabarathi Engineering College**

**Chinnasalem 606201.**

**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 practical problem, which is largely neglected in the literature, by proposing the novel concept of key aggregate searchable encryption 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, data sharing, cloud storage, data privacy.

## I. INTRODUCTION

Cloud storage has emerged as a promising solution for providing ubiquitous, convenient, and on-demand accesses 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 increasingly concerned about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

secrets. To address users concerns over potential data leaks in cloud storage, a common approach is for the data owner to encrypt all the data before uploading them to the cloud, such that later the encrypted data may be retrieved and decrypted by those who have the decryption keys. Such a 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. Christo Ananth et al. [3] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden. 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. In addition, a large number of trapdoors must be generated by users and submitted to the cloud in order to perform a keyword search over many files. The implied need for secure communication, storage, and computational complexity may render such a system inefficient and impractical.

## II. RELATED WORK

Before we introduce our KASE scheme, first reviews several categories of existing solutions and explain their relationships to our work.

### Multi-user Searchable Encryption

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

### Multi-Key Searchable Encryption

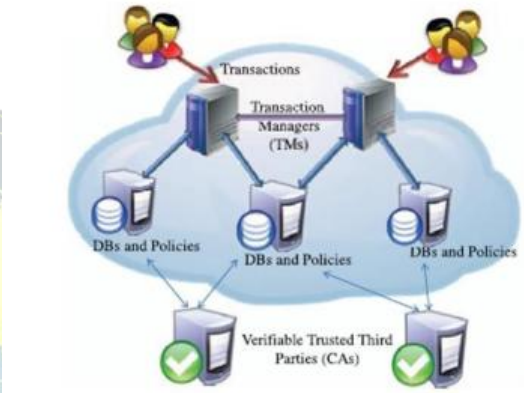
In the case of a. multi- user application, considering that the number of trapdoors is proportional to the number of documents to search over provides to the server a keyword trapdoor under each key with which a matching document might be

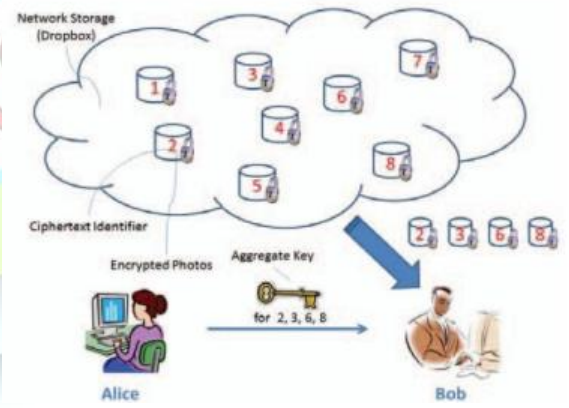
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

encrypted,Pop firstly introduces the concept of multi-key searchable encryption (MKSE) and puts forward the first feasible scheme in 2013. MKSE allows a user to provide a single keyword trapdoor to the server, but still allows the server to search for that trapdoor's keyword in documents encrypted with different keys. This might sound very similar to the goal of KASE, but these are in fact two completely different concepts. The goal of KASE is to delegate the keyword search right to any user by distributing the aggregate key to him/her in a group data sharing system, whereas the goal of MKSE is to ensure the cloud server can perform keyword search with one trapdoor over different documents owing to a user.

## III. PROPOSED SYSTEM

In the novel concept of key-aggregate searchable encryption, and instantiating the concept through a concrete KASE scheme. The proposed KASE 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, while allowing the latter to perform keyword search over the former. To support searchable group data sharing the main requirements for efficient key management are twofold. First, a data owner only needs to distribute a single aggregate key to a user for sharing any number of files. Second, the user only needs to submit a single aggregate trapdoor to the cloud for performing keyword search over any number of shared files. To the best of our knowledge, the KASE scheme proposed in this paper is the first known scheme that can satisfy both requirements. The key-aggregate cryptosystem, which has inspired our work, can satisfy the first requirement but not the second.




## IV. PERFORMANCE EVALUATION

In a practical data sharing system based on cloud storage, the user can retrieve data by any possible device and the mobile devices are widely used now. The performance is highly dependent on the basic cryptographic operations especially in

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

the pairing computation, we study whether the cryptographic operations based on pairing computation can be efficiently executed using both computers and mobile devices.

**Evaluation of KASE Algorithms**

Considering that the algorithms including KASE.Setup , KASE.Adjust and KASE. Test are only run in the cloud server, only the execution times in computer are tested. The execution time of KASE.Setup is linear in the maximum number of documents belonging to one owner, and when the maximum number grows up to 20000, it is reasonable that KASE. Setup algorithm only needs 259 second. The execution time of KASE.Encrypt is linear in the number of keywords, and when the number grows up to 10000, KASE. Encrypt algorithm only needs 206 second in computers, but 10018 second in mobile devices. Therefore, we can draw two conclusions one is that it is not feasible to upload document with lots of keywords using a mobile phone; the other is that the keyword search with pairing computation can be executed quickly in computers now. The execution time of KASE. Extract is linear in the number of shared documents, and when the number grows up to 10000, KASE.Extract algorithm only needs 132 second in computer, but 2430 second in mobile devices. Because the KASE.Extract always runs along with the KASE.Encrypt, it is not suggested to be executed in the mobile devices.

## V. CONCLUSION:

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 multi-owners 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.

## REFERENCE

[1]. 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.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

[2]. R. A. Popa ,N. Zeldovich. "Multi-key searchable encryption" .Cryptology ePrint Archive, Report 2013/508, 2013.

[3]. Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[4]. .F. Chen, J. Li, X.Y. Huang, J.W. Li, Y. Xiang. "Secure Outsourced Attribute-based Signatures",IEEE Trans on Parallel and Distributed Systems DOI.ieeecomputersociety.org/10.1109/TPDS.2013.180, 2013.

[5]. H. Phan, D. Pointcheval, S. F. Shahandashti, et al. "Adaptive CCA broadcast encryption with constant-size secret keys and cipher texts" ,International journal of information security, 12(4):251-265, 2013.