INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

Key – Aggregate Searchable Encryption

Kiran Kawale
kiran.kawale2@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Ankita Angre
ankitaangre74@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Pranita Shinde
pranita4101996@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Sumit Sakpal
sumitsakpal1012@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

Prof. Kishor Sakure
kishore.sakure@gmail.com
Terna Engineering College, Navi Mumbai, Maharashtra

ABSTRACT

The capability of sharing encrypted data with unlike users via public cloud storage may greatly ease security concerns over accidental data leaks in the cloud. Hence there is a need for efficient management of encryption keys. In this group of selected documents need to be shared with any group of different user's desire by right different encryption keys to be used for different documents. However need of producing a complex number of keys for both processes i.e. encryption and search, and distributed to different users and those users will have to safely store the keys and put forward complex number of keywords trapdoors to the clouds in order to search for data. However, because of large complexity, this way is unmanageable and almost practically not possible. In this paper, we are proposing the concept of Key- aggregate searchable encryption in which data owner needs to make distribution a single key to a user for having the same complex number of documents, and user needs to put forward a single trapdoor to the cloud for the query the Shared Documents. However, the complexity is reduced in relation to looking for of Documents in a separate part of the cloud.

Keywords: *Searchable Encryption, Data Sharing, Aggregate Key, Data Owner, Trapdoor.*

1. LITERATURE SURVEY

[1]BAOJIANG CUI,ZHELI LIU,LINGYU WANG paper is based on various existing systems that is, Multi-user Searchable encryption(MUSE), Multi-Key Searchable Encryption(MKSE), Key-aggregate Searchable Encryption(KAE) and various other parameters like efficiency, performance evaluation and security analysis of KASE Scheme.[2]K.SWETHA,LALBAHADUR KETHAVATH paper is based on KASE construction(Framework) and various algorithms and evaluation of various algorithms for KASE scheme.[3] R.RAKESH,ANOOP.S paper is based on a comparison of the various method used for KASE scheme and future work of KASE.[4]NIKESH PANSARE,SATYAM SHRESTHA paper is based on various methodologies used for KASE SCHEME.

2. INTRODUCTION

Cloud storage has come out of as a hoping answer for providing ubiquitous, right way to access large amounts of data shared over the web. Because of social networking applications, millions of users are sharing data such as photos and videos with their friend which is based on cloud storage. Because of, in relation to its great number of benefits like a lower price, better resource utilization, quick- moving business users are likely to be get attracted the most. However, while getting the pleasure of sharing data via cloud storage users are also troubled by accidental data leaks in the cloud. To address users concerns over data leaks in cloud storage we use cryptographic cloud in which data owner has to encrypt all the data before uploading them to the cloud, so that later the encrypted data may be retrieved and decrypted with the decryption keys to only those who have that keys. However looking for data and getting back only the data having in it given keywords in such large cloud are key challenges to the user. To over-come this, searchable encryption (SE) has been used in which data owner has to encrypt possible unused quality keyword and upload them to cloud together with encrypted data such that for getting back data, the user will send the corresponding keyword which is known as trapdoor to the cloud for performing a search over the cloud. Although basic security requirements can be achieved while combining searchable encryption scheme with cryptographic cloud storage. Implementing this system on a greatly sized scale where the application involves millions of users and billions of files may still be hampered by some practical issues. Suggested need of secure communication, a place for storage and computational complexity may give such system inefficient and impractical to use in real-time applications.

3. EXISTING SYSTEM

3.1 Multi-user Searchable Encryption

In common event-ready space, keyword search is done under multi-tenancy system. . In this system, a group of documents is being shared by data owner with a group of authorized users, and each user who has the privilege rights can put forth trapdoor to cloud in order to perform a keyword search over shared documents which is known as Multi-user Searchable encryption(MUSE) scenario.

3.2 Multi-Key Searchable Encryption

It lets the user 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 is like KASE but the point or amount of difference is that the purpose of KASE is to depute the keyword search right to any user by making distribution of the aggregate key to user in group data sharing search with one trapdoor over system, whereas the purpose of MKSE is to make certain that the cloud server can perform keyword different documents owing to a user. The approach of MKSE is to give all attention to the problems of keyword search over a group of shared documents from the same user in multi-user applications.

3.3 Key aggregate encryption for data sharing

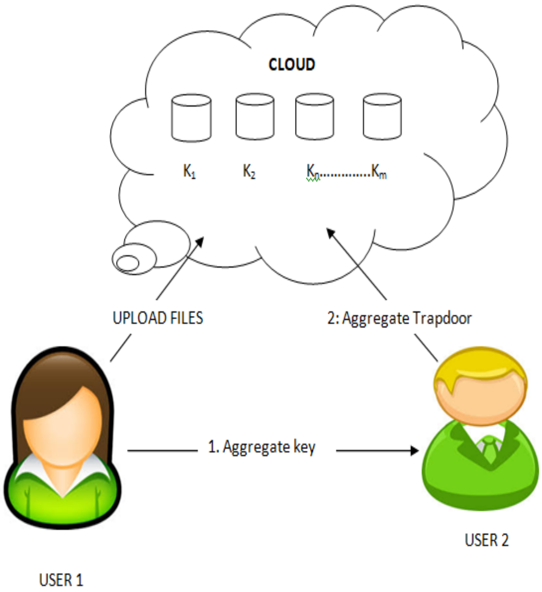
This aims at reduction in a number of distributed data encryption keys. In the traditional approach where several documents are to be shared with different encryption keys with the same user, the data owner will need to make the distribution of all such keys to the user which is usually impractical. Key aggregate encryption (KAE) overcomes this bad point in which a single aggregate key is produced for the user to decrypt multiple documents. In this user could encrypt a message not only under public-key but also the identifier of each document.

3.4 Disadvantages of existing systems

MUSE main hard question is that there is no control over which users can access which documents .i.e. Shared data will not be secured.
A number of keys and trapdoors generated are very large.
A very general way to perform a keyword search over a group of documents with single trapdoor is performed by MKSE.
With the increase in a number of decryption keys, there is an increase in cost and complexity.
Key aggregate encryption (KAE) doesn't support any search over the cloud, to get done the purpose of privacy-preserving data sharing keyword search is a very important point of view.

4. PROPOSED SYSTEM

In this paper, we address this challenge and offer a different idea of key-aggregate searchable encryption (KASE) as a better solution through a KASE scheme. The design of this scheme draws its attention from both the multi-key searchable encryption scheme as well as from key- aggregate data sharing scheme, in order to create aggregate searchable encryption key instead of many independent keys. This offered KASE scheme applies to hybrid cloud storage that supports group data sharing ability, which means any user can selectively share a group of selected files with a group of selected users while allowing the user to perform a keyword search over the cloud. To support searchable group data sharing the main requirement for efficient key management are twofold. Firstly, a data owner only needs to distribute a single aggregate key (instead of a group of keys) to a user for sharing any number of files. Secondly, the user needs to put forward a single aggregate trapdoor (instead of a group of trapdoors) to the cloud for performing a keyword search over any number of shared files. Each searchable encryption key is accompanied with a particular index of a document, and the aggregate key is created by embedding the owner's master secret key into a product of public keys associated with the documents. In order to perform a keyword search over different documents using the aggregate trapdoor. The cloud server can use this process to produce an adjusted trapdoor for each and every document.



5. KASE FRAMEWORK

We define a general framework of key aggregate searchable encryption (KASE) composed of seven polynomial algorithms for security parameter setup, key generation, encryption, key extraction, trapdoor generation, trapdoor adjustment, and trapdoor testing.

5.1 Setup (1λ, n)

To set up the scheme this algorithm is run by cloud service provider. Inputs given are 1λ and the maximum possible number of n documents which belongs to data owner., it gives public system parameter params as output, and these parameters can be reused by different data owners to share their files

5.2 Keygen

To generate random key pair (pk, msk), this algorithm is run by the data owner

5.3 Encrypt (pk, i)

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

5.4Extract (msk, S)

To generate an aggregate searchable encryption key for delegating the keyword search right for a certain set of documents to other users this algorithm is run by the data owner. On input of owner's master-secret key msk and a set S which contains the indices of documents,it generates the aggregate key kagg as a output.

5.5Trapdoor (kagg, w)

To perform search this algorithm is run by the user who has the aggregate key. Input taken are aggregate searchable encryption key kagg and a keyword w, and the output is only one trapdoor Tr.

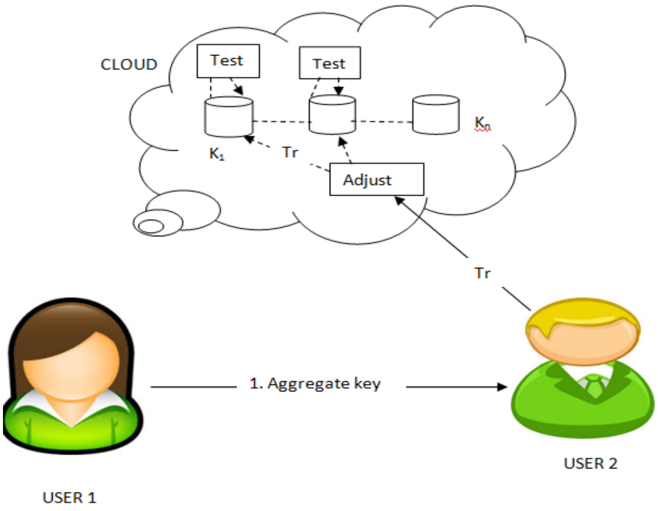
5.6Adjust (params, i, S, Tr)

To adjust the aggregate trapdoor to generate the right trapdoor for each different document this algorithm is run by cloud server. Input taken are system public parameters params, the set S of documents' indices, the index i of the target document and the aggregate trapdoor Tr, then it outputs each trapdoor Tri for the i-th target document in S.

5.7 Test (Tri, i)

To perform a keyword search over an encrypted document this algorithm is run by the cloud server. Input taken are trapdoor Tri and the document index i, then the outputs are true and false to signify whether the document doci contains the keyword w.

.



6. WORKFLOW

6.1 SYSTEM SETUP

when a data owner submits a request, the cloud will create a database. Moreover, it assigns an administrator account for the manager then the group data sharing system will work under control of manger.

6.2 USER REGISTRATION

In this new user do their registration

6.3 USER LOGIN

After registration user can login to their system

6.4 DATA UPLOADING

data owner uploads their respective documents.

6.5 DATA UPLOADING

data owner uploads their respective documents

6.6 DATA SHARING

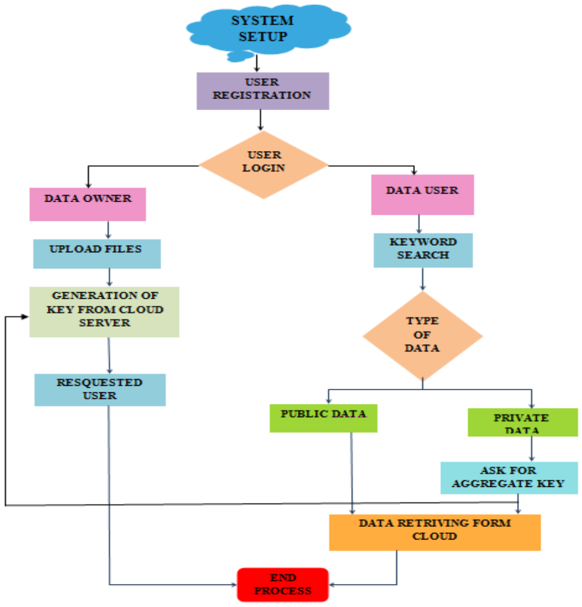
To share a group of documents with the group of users.

6.7 KEYWORD SEARCH

To retrieve the documents containing an expected keyword.

6.8 DATA RETRIEVING

After receiving a key user can get encrypted data from cloud depending on public or private data.



7. ADVANTAGES OF KASE

In a KASE design, when the owner wants to share lots of documents with the user then he/she needs to make the distribution of a single key to a user. And the user only needs to put forward a single trapdoor when he queries over all the documents shared by the same owner.

In a practical data sharing system based on cloud storage, the user can retrieve data from any possible devices and the mobile devices which are widely used now.

Even when the cloud server colludes with a malicious authorized user, they are not able to perform a keyword search over any document, not in the scope of user's aggregate key.

An attacker is unable to produce the new aggregate key for any new set of documents from the known aggregate key.

An attacker is unable to come out to a decision about a keyword in a query from the given trapdoor.

An attacker is unable to actuate a keyword in the document from the stored keyword cipher texts and the related public parameters

8. CONCLUSION

In this paper, practical problems of data sharing among a group of users are taken into consideration, without data leaks which usually occurs in cloud storage. A normal method performed is to share a large number of keys to all authorized data users from data owner, which gives the authorized user to access the set of documents shared to him/her. But due to some loop holes and security issues, this system is impractical for use.

In KASE scheme, the data owner needs to distribute a single key to data user while sharing lots of documents and the user only needs to submit a single trapdoor while retrieving all the documents shared by the same owner. However, if data user wants different documents shared by different data owner then he must generate multiple trapdoors to the cloud. However future work of this is how to reduce the number of keys in the multi-owner setting.KASE scheme has not been applied directly in federated clouds. Hence it can be a future work to provide the solution for KASE scheme in case of the federated cloud. The security analysis and performance evaluation both confirm that our proposed schemes are practically secured and efficient.

9. REFERENCES

[1] Baojiang Cui and Zheli liu "Key-Aggregate Searchable Encryption (KASE) for Group data sharing via Cloud Storage", IEEE Transactions on Computers, the year 2015.

[2] R.Rakesh and Anoop S. "Key-Aggregate Searchable Encryption for Group Data sharing", International Journal of Computer Applications, vol.139-no. 2nd April 2016.

[3] Dr.V.Goutham lalbahadur Kethavath and K.swetha "Key-Aggregate Searchable Encryption With Secure and efficient Data Sharing in Cloud", International Journal of Computer Engineering and Technology (IJCET) Volume 7,Issue 4th July 2016.

[4] K.Manohar,R.Anil Kumar,N.Parshuram, liu "Key-Aggregate Searchable Encryption for Group data sharing via Cloud Data Storage", ", International Journal of Computer Engineering and Research Trends(IJCERT) Volume 2,Issue 12 December 2015.

[5] Nikesh Pansare, Akash Somkuwar, Adil sheikh and Satyam Shrestha" Key-Aggregate Searchable Encryption(KASE) for User Revocation in Cloud Storage, ", International Journal of Engineering and techniques, Volume 2,Issue Jan-Feb 2016.

[6] https//youtu.be/6d3slX36LqA

.