Volume 6, Issue 10, October 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhanced Key Aggregate Searchable Encryption For Group Data Sharing Via Cloud Data Storage

[1] Darshnam Prathyusha, [2] Shaik Khaja Mohiddin
[1] (M.Tech) –CSE, Vasireddy Venkatadri Institute of Technology (VVIT), Namburu, Guntur, Andhra Pradesh, India
[2] Assistant Professor, Dept of CSE, Vasireddy Venkatadri Institute of Technology (VVIT), Namburu, Guntur, Andhra Pradesh, India

Abstract: ***In this paper we 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 key aggregate searchable encryption (KASE) and construct a concrete KASE scheme. It can provide an efficient solution to building practical data sharing system based on public cloud storage. In a KASE scheme, the owner needs to distribute a single key to a user when contributing a more no of documents with the user and the user needs to submit a single trapdoor when they query 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 trapdoors to the cloud. as a proposed work we suggested STMO-KASE(SingleTrapdormany owners-KASE)schemes which leads to decrease the number of trapdoors under manyowners setting by attaining the security.***

Keywords: ***searchable encryption (SE) scheme,CloudComputing,Group data sharing,Cloud Data Storage,STMO-KASE(SingleTrapdor many owners-KASE)***

I. INTRODUCTION

In cloud computing communication cloud has three primitive services i.eSaaS,IaaS and PaaS, where IaaS Consist of Cloud storage services whichare a solution for sharing and accessing large amounts of data, which is shared by various users by means of internet. Today, many users are mostly sharing huge no of unique documents, which are considered to be under several categories like photos, videos and documents via various social networking based applications on aday-to-day basis. There are massivepaybacks of using cloud storage like lower cost, greater swiftness and better resource utilization has added more attraction from plenty number of business users toward using the cloud storageCloud computing which is built on parallel, distributed computing, utility computing and service-oriented architecture. Generally, speaking about cloud storages, we all are enjoying the comfort of sharing all kinds of data. But all users are more bothered about the data leaks which usually happen in the cloud storage. Such type of data leaks occurs due to reason like an untrusted cloud provider and by hackers who decrypt the files using various types of software. A common approach usually used is to encrypt all the types of data available to him/her. Which are to be uploaded to the cloud by the data owner. The encrypted data obtained shall be retrieved and then performing decryption by persons who have theright set of access keys. This type of cloud storage is known as Cryptographic cloud storage.

searchable encryption (SE) scheme. In this scheme, the data owner encrypts all the keywords which were used to encrypt the data and both the encrypted keyword and encrypted data were outsourced to the cloud organized. In order to access the real data, theuserneeds to passonkeyword trapdoor on the public cloud which will be used to match a data with a keyword. If a match is found then the related document will be retrieved, otherwise the keyword based searching continues, until all the keyword trapdoor have been tested on the document collection available on the cloud server,.

By combining both the cryptographic cloud storage along with the searchable encryption scheme, the essential basic security requirements can be attained. Also, management of keys is a serious problem.. Usually uploaded data is encrypted with a different encryption key. The number of key generated will be proportional to the number of document files to be encrypted. Also, how to send these set of different keys among the various kind of users. So, has to perform the searching and decryption over the set of documents. These keys must be sent to a user using a secure communication channel, also how can a user store and manage these keys in their devices like mobile phones, PCs, laptops, removable devices etc.

II. RELATED WORKS

Multi-User Searchable Encryption (MUSE): In thedescription of cloud storage, a most common scenario is keyword search which is performed by various users and it is known as multiuser setting. In this MUSE, the data owner shares a document with a number of authorized users and each authorized user who has the right set of access rights can perform searching over the document using trapdoor mechanism. Most recent developed works included in [3],.

Speaking about which mainly focus on MUSE, in this implementation is done by single key combined with various access controls.

In the construction of MUSE scheme [3] and [2], which is developed for first of all share the searchable encryption key which is used for document encryption to all the users. The users who have the keys can access these documents, also by using broadcast encryption. It achieves the access control for all the documents shared. In the description [4-5], by applying the attribute based encryption, it achieves more fine access control which is based on keyword searching.

The main goals of both i.e. KASE and MKSE are completely different ideas. The goal of MKSE: when akeyword search is performed by the cloud server with only one trapdoor on different types of user owned documents, that of KASE: by mainly providing the generated single aggregate key to data users in a group sharing based system. Speaking more about the MKSE, thedata user can store public data information which is known as Delta on acloud server. This public information is relevant to data user key and used anencryption key. Data user can perform searching for a word on all the documents, for doing this he/she needs the data user key to calculate the trapdoor for the word and directly submit this generated trapdoor value to thecloud server.

Searchable Encryption: Searchable encryption schemes categorized into two categories, i.e., searchable symmetric encryption (SSE) and public key encryption with keyword search (PEKS). Both SSE and PEKS can be described as the tuple SE= (Setup, Encrypt, Trapdoor(Trpdr),Test):

1. Setup(1λ): This algorithm is run by the owner to set up the scheme. It takes as input a security parameter 1λ and outputs the necessary keys.

2. Encrypt(l;n): This algorithm is run by the owner to encrypt the data and generate its keyword ciphertexts. It takes as input the data n, owner's necessary keys including searchable encryption key l and data encryption key, outputs data ciphertext and keyword ciphertextsCn.

3. Trpdr(l;x): This algorithm is run by a user to generate a trapdoor Trd for a keyword w using key 4.Test(Trd, Cn): This algorithm is run by the cloud server to perform a keyword search over encrypted data. It takes as input trapdoor Trd and the keyword ciphertextsCn, outputs whether Cn contains the specified keyword. For exactness, it is required that, for a message n containing keyword x and a searchable encryption key l, if (Cn⇐-Encrypt(l;n) and Tr⇐Trpdr(l;x)), then Test(Trd, Cn)=true.

Key-Aggregate Encryption (KAE): Recently more attention has been created around the cloud storage, which is based on data sharing systems [6]-[7]. By considering the paper [7] which points out that how to decrease the number of keys used for data encryption. In thetraditional approach, all used encryption keys must be distributed among the concerned authorized users. This challenge is solved by KAE, where it generates an aggregate key which will be used by the user to decrypt all the documents shared with him/her. The concept of KAE is to obtain the original document by decrypting with a single aggregate key, which was encrypted with different keys. To perform this data owner, not only needs the public key but also the identity of each document. This is concept is adapted from the broadcast encryption scheme. In thedevelopment of KAE scheme, the data owner is designed as abroadcaster. Broadcaster will be having the public key and master secret key. The data user is designed as the receivers, who are listening to this secure broadcast channel. Generally, speaking about public information which consists of various relevant information like data owner's master secret key and encryption key. Here, data encryption is performed using the symmetric encryption in broadcast encryption. But the key aggregation and data decryption is done by the algorithms like BE.Encrypt and BE.Decrypt respectively. By using scheme [7], which delegates all the decryption rights to the data users. The problem with KAE, we can't perform searching over the encrypted documents. So, the development of new scheme is needed, which will provide us to perform keyword-based searching, trapdoor generation and also more complex procedure to obtain keyword matching in more efficient way. So, KASE scheme was designed and developed by the researchers in the field of research and development.

III. SYSTEM STUDY

3.1. MultiKey for data Sharing and Searching over Cloud:

A huge amount of data will be stored in cloud servers by the distinct data owners , and every single document is given different keys. This infers the amount of keys that need to be scattered to users, both for them to search for the encrypted files and to decrypt the files, will be proportional to the number of such files. Such a large number of keysmust not only be spread 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.The advanced work over this is that, 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. Second, the user only needs to submit a single aggregate trapdoor (instead of a group of trapdoors) to the cloud for performing akeyword search over any number of shared files.

As our proposed system we suggested STMO-KASE(SingleTrapdor many owners-KASE)schemes which lead to decrease the number of trapdoors under manyowners setting by attaining the security

In the above-proposed scenario our system consists of three entity i.e

1. Data owner
2. User
3. Cloud Server

Initially all data owners outsource their data onto public cloud in encrypted form for the sake of data privacy,in order to improve the searching performance Owner append effective data retrieval a search index over an encrypted data, to make convenient search usability a set of keywords has set.

3.2. Single Trapdoor and Aggregated Key:

To reduce thecomplexity of increase in a number of trapdoorsproportional to a numberoffilesshared.We propose schemes where single trapdoorisprovided by user and server gets thecapability to search for that trapdoor's keyword in shared documents even their encryption keys are different. Further to reduce the number of encryption keys we use the concept of Key aggregate Encryption which flexibility to decrypt any number of acipher text with constantsize decryption key. Our model further enhances this concept by providing keyword search over encrypted data to achieve goal of privacy

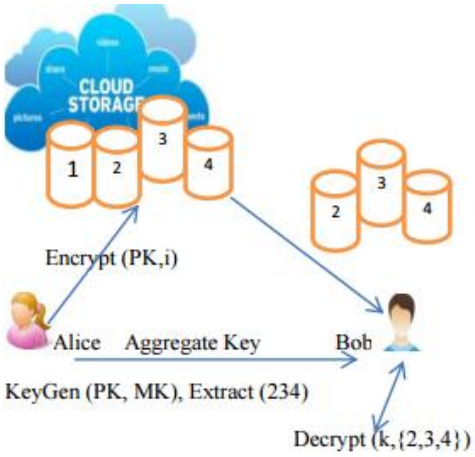

Fig 1.Single Trapdoor and Aggregated Key

For sharing selected data on the server Alice first performs the Setup. Later the public/master key pair (pk, me) is generated by executing theKeyGen. The msk master key is kept secret and the public key pk and param are made public. Anyone can encrypt the data m and this data is uploaded to theserver. With the decrypting authority the other users can access those data. If Alice wants to share a set S of her data with a friend Bob then she can perform the aggregate key KS for Bob by executing Extract (MK, S). As kSis a constant size key and the key can be shared through secure email. When the aggregate key has got Bob can download the data and access it.The following encryption schemes are followed.

3.3. Searchable Encryption Scheme:

1) Multiuser Searchable Encryption(MUSE): It works under multitenancy operations where data owner shares documents with agroup of users and users can receive them by submitting trapdoor for keyword search on shared content.

2) Multi-key Searchable Encryption: A single trapdoor for multiple different keys is provided which reduces the number of trapdoors used for each document separately.

Multi-User Searchable Encryption (MUSE): In thedescription of cloud storage, a most common scenario is keyword search which is performed by various users and it is known as multiuser setting. In this MUSE, the data owner shares a document with a number of authorized users and each authorized user who has the right set of access rights can perform searching over the document using trapdoor mechanism.It achieves the access control for all the documents shared

Multi-Key Searchable Encryption (MKSE). Considering the multi-user based applications, the ratio of a number of trapdoors is directly equivalent to the number of searched documents.This algorithm is explained as a data user to give a single trapdoor which consists of a single keyword to the cloud server. But on another hand, the cloud server gives provision to search over the keyword trapdoor by using different keys. it consists of a Multi-Key Searchable Encryption (MKSE) which shows that a data user is submitting his/her generated trapdoor(Tr) to acloud server and the cloud server performing the adjust and test thealgorithm on the document collection.. In MKSE the adjusting process is an approach to perform searching on the group of documents shared by means of thesingle trapdoor. This adjusts process can't be applied directly to the development of KASE scheme.

3.4. KASE(KEY-AGGREGATE SEARCHABLE ENCRYPTION) Scheme:

The KASE construction is composed of several algorithms. Especially, to set up the method, the cloud server would generate public parameters of the system during the Setup algorithm, and these public parameters can be reprocessed by contradictory data owners to consign their files. For each data owner, they should produce a public/mastersecret key pair through the Keygen algorithm. Keywords of each document can be encrypted through the Encrypt algorithm with the exclusive searchable encryption key. In that case, the data owner can apply the mastersecret key to produce an aggregate searchable encryption key for a group of selected documents through the Extract algorithm.

The aggregate key can be spread securely to approve users who need to access those documents. a certified user can create a keyword trapdoor via the Trapdoor algorithm using this aggregate key, and submit the trapdoor to the cloud. After getting the trapdoor, to carry out the keyword search over the particular set of documents, the cloud server will run the Adjust algorithm to produce the right trapdoor for each document, and then run the Test algorithm to test whether the document contains the keyword. This construction is summarized in the following.

1. Setup(1λ, n): This algorithm is run by the cloud service provider to set up the scheme. On input of a security parameter 1λ and the maximum possible number n of documents which belongs to a data owner, it outputs the public system parameter params.

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

3.Encrypt(pk, i): This algorithm is run by the data owner to encrypt the ith 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 ciphertextsCi.

3. Extract(msk, S): This algorithm is run by the data owner to generate an aggregate searchable encryption key for hand over the keyword search right for a certain set of documents to other users. It takes as input the owner's mastersecret key msk and a set S which enclose the directory of documents, and then outputs the aggregate key.

4. Trapdoor(kagg, x): This algorithm is run by the user who has the aggregate key to perform a search. It takes as input the aggregate searchable encryption key kagg and a keyword w, then outputs only one trapdoor Ted.

5. Adjust(params, i, S, Trd): this algorithm is run by cloud server to adjust the aggregate trapdoor to generate the right trapdoor for each different document. It takes as input the system public parameters params, the set S of documents' indices, the index I of the target document and the aggregate trapdoor Tr, then outputs each trapdoor Tri for the ith target document in S.

6.Test(Tri, i): this algorithm is run by the cloud server to perform a keyword search over an encrypted document. It takes as input the trapdoor Tri and the document index i, then outputs true or false to denote whether the document does contains the keyword.

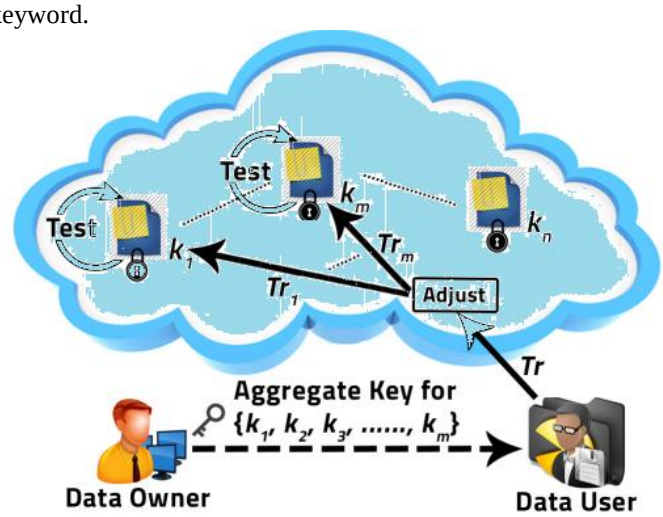

Fig 2.key-aggregate searchable encryption Framework

In Fig.2 it consists of a data owner generates a single aggregate key which was created by using the data owner public key and master secret key for encrypting the shared documents. This single aggregate key produced is sent to the data user through a secure communication channel. Then, the data user can perform searching over the shared documents by generating single aggregate trapdoor, submitted this trapdoor to the cloud server. Cloud server performs the adjusting algorithm/process by using the aggregate trapdoor over the collection of documents. Then, test algorithm is performed to ensure that the respective requester has the right to access them. If a match occurs, then cloud server will return all the shared documents to the respective data user.

The Key-Aggregate Searchable Encryption (KASE), it is a public key encryption scheme which is adapted from key-aggregate cryptosystem scheme [7] and Multi-key searchable encryption scheme. The advantage is that in place of sharing the documents, data owner sends the single aggregate key. By using this key, he/she can access all the documents will is meant for him/her.the data owner will generate a single aggregate key and transmit it to the user. Data user can submit generated single aggregate trapdoors to the cloud server. Cloud server than perform adjust and test algorithms to retrieve the relevant documents shared with him/her.

IV. PRAPOSED SYSTEM DESIGN

The system is designed to use the following algorithm.

4.1.STMO-KASE Algorithm:

1. Setup (1, n): this algorithm is run by the cloud service provider to set up the scheme. On input of a security parameter 1 and the maximum possible number n of documents which belongs to a data owner, it outputs the public system parameter params.

2. Encrypt (k; m): this algorithm is run by the ownerto encrypt the data and generate its keyword ciphertexts. It takes as input the data m, owner's necessary keys including searchable encryption key k and data encryption key, outputs data cipher text and keyword cipher texts Cm.

3. MultiOwner (a, o): In the group of owners a find the relevant owners o providing documents for the same group of users or asingle user with the same parameter and generates master key msk.

4. Extract (msk,S): this algorithm is run by thedata owner to generate an aggregate 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 mastersecret key and generates kagg.

5. Trapdoor(kagg,w): This algorithm is run by theuser who has the aggregate key to perform a search. It takes as input the aggregate searchable encryption key kagg and a keyword w, and then outputs only one trapdoor T r.

6. Test (T r,i): This algorithm is run by the cloud server to perform akeyword search over an encrypted document. It takes as input the trapdoor T r and the document index i, then outputs true or false to denote whether the document does contains the keyword w.

4.2. System Setup:

The System is set up with the following tables.

Group→groupID, groupName, parameters
Member→memberID,membeName, password, publicKey
docs→docID, docName,OwnerID, EncKey, SEKey, filePath>
sharedDocs→SID, memberID, OwnerID, do-cIDSet.

4.3.Working model:

User registration. When adding a new member, themanager assigns memberID, membeName, password and a key pair generated by any public key encryption (PKE) scheme for him, then stores the necessary data into the table member. A user's private key should be distributed through a secure channel.

User login. As in general it involves Password authentication

Data uploading. To upload a document, theowner runs Encryption algorithm to encrypt the keyword ciphertexts, then uploads them to the cloud. The cloud assigns a docID for this document and stores the encrypted data in the path filePath, then inserts a record into the table docs.

KeywordSearch. To retrieve the documents containing an expected keyword, a member runs searching algorithm, Based on the requirement single or multiple Trapdoors are generated. Data retrieving. After receiving the encrypted document, the member will decrypt the data

V. CONCLUSSION

In this paper we have been demonstrated how to make flexible data sharing over cloud server among multiowner manner using singletrapdoorkeysharingsystem,users prefer to upload there data on cloud and among different users. Outsourcing of data to server may lead to leak the private data of user to everyone. Encryption is a one Solution which provides to share selected data with desired Applicant. But the millions of files uploading require that many keys and trapdoors and lacks in performance. So we propose the new concept of Single Trapdoor Many Owner Key Aggregated Searching Encryption(STMO-KASE) for Cloud Storage, which needs an aggregated key and a single trapdoor to access same kind of files from multiple owners. It's proven as the efficient method.

REFERENCES

[1] K.Manohar vet al., International Journal of Computer Engineering In Research Trends Volume 2, Issue 12, December-2015, pp. 1132-1136.

[2] Z. Liu, Z. Wang, X. Cheng, et al. "Multi-user Searchable Encryption with Coarser-Grained Access Control in Hybrid Cloud", Fourth International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), IEEE, pp. 249- 255, 2013.

[3] 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.

[4] C. Dong, G. Russello, N. Dulay."Shared and searchable encrypted data for untrusted servers", Journal of Computer Security, pp. 367-397, 2011.

[5] J.Li, X.F. Chen, M.Q. Li, J.W. Li, P. Lee, Wenjing Lou. "Secure Deduplication with Efficient and Reliable Convergent Key Management", IEEE Transactions on Parallel and Distributed Systems, 25(6): 1615-1625, 2014.

[6] 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.

[7] 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.

