International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

A Novel Key Aggregate Searchable Encryption for Group Data Sharing Using Cloud Data Storage

[1]Vulloji Raja, [2]P. Ashok Kumar
[1]M.Tech student, Dept of CSE, Vijaya Engineering college, , Ammapalem, Khammam,Telangana, India
[2]Associate professor, Dept of CSE,Vijaya Engineering college, , Ammapalem, Khammam,Telangana, India

Abstract: The capacity of preferentially sharing encrypted data with in contrast to clients by means of public cloud storage would quite ease safety depression, by means of likelihood data expose within the cloud. A key experiment to design such encryption notion lies within the good-organized management encryption keys. The preferred flexibility of allocating any group records with any group of clients by way of achieving weightage exclusive encryption keys to be used for exclusive files. However, this involves the need of securely distributing to clients through a large quantity of keys for both encryption and search, and people users have got to development to store the received keys. The indirect want for comfortable communique, storage, and complexity obviously purpose the unreasonable procedure. In this paper, we pay attention to this useful problem, through suggesting the novel thought of key combination searchable encryption (KASE) and instantiating the inspiration through an actual KASE scheme, where a knowledge proprietor desires to share out a single key to a consumer for distributing a massive number of records, and the person wants to reward a single trapdoor to the cloud for questioning the shared files.

Keywords-data sharing, Searchable encryption, data privacy, cloud storage.

I. INTRODUCTION

Cloud storage is a solution for sharing and accessing large amountsof data, which is shared for various users by means of internet.Today, a number of users are mainly sharing a large number of various kinds of documents, which are considered to be under variouscategories like photos, videos and documents via various social networking based applications on daily basis. There are huge benefitsof using cloud storage like lower cost, greater agility and better resource utilization has add more attraction from plenty number ofbusiness users toward using the cloud storage.Cloud 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 ofsharing all kinds of data. But all users are more bothered about thedata leaks which usually happen in the cloud storage. Such type ofdata leaks occur due to reason like an untrusted cloud provider andby hackers who decrypt the files using various types of software. Acommon approach usually used is to encrypt all the types of dataavailable with him/her. Which are to be uploaded to the cloud bythe data owner. The encrypted data obtained shall be retrieved andthen performing decryption by persons who have right set of accesskeys. This type of cloud storage is known as Cryptographic cloudstorage.

However, there are two challenging tasks:

(1) How can a user perform searching over the documents shared?

(2) How to retrieve only the data which can be retrieved by a givenkeywords?

Above stated two challenges can be solved by the implementation of searchable encryption (SE) scheme. In this scheme, thedata owner encrypts all the keywords which were used to encryptthe data and both the encrypted keyword and encrypted data areuploaded to the cloud together. To obtain the original data back,the user will need to send a keyword trapdoor which will be usedto match a data with a keyword. If a match is obtained than thedocument belonging to a data user can be retrieved, otherwise thekeyword based searching continues, until all the keyword trapdoorhave been tested on the document collection available on the cloudserver.

By combining both the cryptographic cloud storage along with thesearchable encryption scheme, the essential basic security requirements can be attained. Also, management of keys is a serious problem. How to efficiently manage the encryption keys is generallyneglected in case of survey based on

literature. First requirement ofa data owner is to share the selected set of data with types of different users. For example, sharing a photo and videos is a commonfashion now with the help social network applications like Facebook, WhatsApp etc. Generally, users share various types of documents through cloud storage social networking application likeGoogle drive, Dropbox, Citrix etc. Also Cloud service providersexamples like Amazons EC2 and S3 [2], Google App Engine [3],and Microsoft Azure [4], these provide us all the resources requiredas per our needs. We can pay them as we use these services. 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 differentkeys among the various kind of users. So, has to perform the searching and decryption over the set of documents. These keys must besend to a user using a secure communication channel, also howcan a user store and manage these keys in their devices like mobilephones, PCs, laptops, removable devices etc.Speaking about the traditional method of data sharing through various cloud storage providers, in Fig.1 it consists of two types ofusers: Data owner and Data user. Data owner is uploading n numbers of documents to cloud server which are shared with the datauser. Generally, each document is encrypted with a separate key, i.e.if n documents are to be encrypted than n keys are required to perform encryption using them. The key produced is send to the datauser via a secure communication channel by the data owner. Thanafter performing all these actions, data user can perform searching over the shared documents by generating keyword trapdoors.If a match is obtained, the cloud server returns the original files which were shared by the data owner to corresponding requesteddata user.

II. RELATED WORKS

A. Achieving Secure, Scalable, and Fine-grained DataAccess Control in Cloud Computing.

Cloud computing is develop computing paradigm inwhich resourcesof the computing infrastructure areprovided as services over the Internet. As to assureas it is, this paradigm also brings forth many newchallenges fordata security and access control whenusers outsource annoyed data for sharing on cloudservers, which are not within the same trustedinfluence, as data owners.To keep sensitive userdata confidential against untrusted servers, existingsolutionsusually apply cryptographic methods by tocause to appear data decryption keys only toauthorized users. The problem of simultaneouslyaccomplish fine grained access,scalability, and dataconfidentiality of access control actually stillremains not resolved.

B. Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing.

Success of data forensics in cloud computing isbased on secure place that records ownership andprocess history of data objects. But it is the stillchallenging issue in this paper. In this paper, theyproposed a new secure provenance scheme basedon the bilinear pairing techniques.As the essentialbread and butter of data forensics andpostinvestigation in cloud computing, the proposedscheme is characterized by providingtheinformation confidentiality on sensitivedocuments stored in cloud.Secure authentication onuser access,and place tracking ondisputeddocuments is provided in this paper. Withthe provable security techniques, this paperformally demonstrate the proposed scheme issecure in the standard model.

C. Mona: Secure Multi-Owner Data Sharingfor Dynamic Groups in the Cloud.

In this paper character of low maintenance, cloudcomputing provides an economical and efficientsolution for sharing group resource among cloudusers.Due to the frequent change of membershipsharing data in multi-owner manner whilepreserving data and identify privacy from untrustedcloud is still a challenging issue.

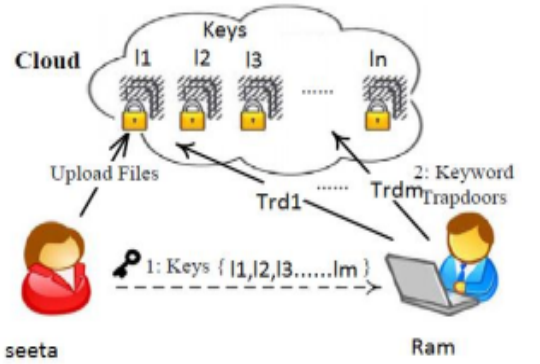
D. Key-Aggregate Crypto system for Scalable Data Sharingin Cloud Storage.

Data sharing is large functionality in cloud storageIn this article, weshow how to securely, efficiently,and adaptable share data with others in cloudstorage.The novelty is that one can aggregate any setofsecret keys and make them as compact as a singlekey, but to enclose the power of all the keys beingaggregated. In

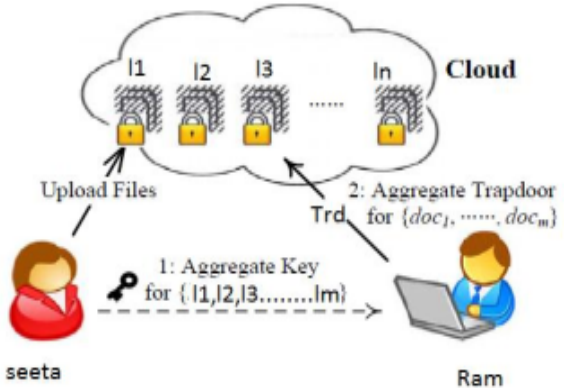
other words, the secret keysomething that holds or secures can release aconstant-size aggregate key for flexible choices ofciphertext set in cloud storage, but the otherencrypted files not inside the set unchangedconfidential.This compact aggregate key can besuitable sent to others or be stored in a smart cardwith very limited secure storage.

III. THE PROPOSED APPROACH

In this paper, we propose the novel approach ofKey-aggregate searchable encryption (KASE) as aenhanced solution, as depicted in Fig.1(b). , inKASE, seeta needs to issue a single aggregatekey, instead of {ki}mi=1 for sharing m documentswith Ram, and ram needs to issue a singleaggregate trapdoor, instead of { Tri }mi=1, to thecloud server. The cloud server can utilize thisaggregate trapdoor and some public data to carryout keyword search and revisit the result to Ram.As a result, in KASE, the delegation of keywordsearch right can be achieved by sharing the singleaggregate key.



(a) Tradational approach



(b) Key-aggregate searchable encryption

Fig.1 keywordsearch in group data sharing system

To design a key-aggregate searchable encryptionmethod under which any subset of the keywordciphertexts from any set of documents issearchable with a constant-size trapdoorgenerated by a constant size aggregate key.

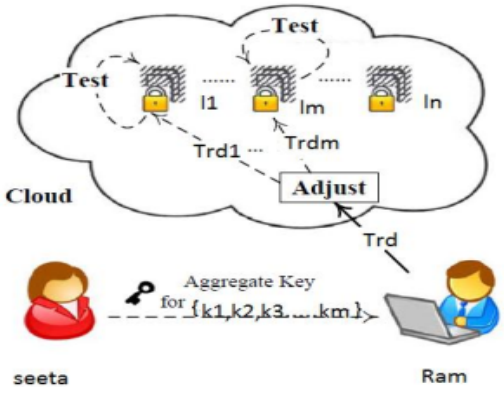


Fig.2 Framework for Key-aggregate searchable encryption

The KASE construction is composed of severalalgorithms. Specially, to set up the method, thecloud server would generate public parametersof the system during the Setup algorithm, andthese public parameters can be reprocess bydissimilar data owners to distribute their files.For each data owner, they should produce apublic/master-secret key pair through theKeygen algorithm. Keywords of each documentcan be encrypted through the Encrypt algorithmwith the exclusive searchable encryption key. Inthat case, the data owner can apply the mastersecret key to produce an aggregate searchableencryption key for a group of selected documentsthrough the Extract algorithm. The aggregate keycan be spread securely to approve users whoneed to access those documents. After that, asshown in Fig.2, an certified user can create akeyword trapdoor via the Trapdoor algorithmusing this aggregate key, and submit thetrapdoor to the cloud. After getting the trapdoor,to carry out the keyword search over theparticular set of documents, the cloud server willrun the Adjust algorithm to produce the righttrapdoor for each document, and

then run theTest algorithm to test whether the documentcontains the keyword.

This construction is summarized in the following.

1. Setup(1λ, n): This algorithm is run by the cloudservice provider to set up the scheme. On inputof a security parameter 1λ and the maximumpossible number n of documents which belongsto a data owner, it outputs the public systemparameter params.

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

3.Encrypt(pk, i): This algorithm is run by the dataowner to encrypt the i-th document and generateits keywords' ciphertexts. For each document,this algorithm will create a delta Дi for itssearchable encryption key ki. On input of theowner's public key pk and the file index i, thisalgorithm outputs data ciphertext and keywordciphertexts Ci.

3. Extract(msk, S): This algorithm is run by thedata owner to generate an aggregate searchableencryption key for hand over the keyword searchright for a certain set of documents to other users.It takes as input the owner's master-secret keymsk and a set S which enclose the directory ofdocuments, and then outputs the aggregate keykagg.

4. Trapdoor(kagg, x): This algorithm is run by theuser who has the aggregate key to perform asearch. It takes as input the aggregate searchableencryption key kagg and a keyword w, thenoutputs only one trapdoor Trd.

5. Adjust(params, i, S, Trd): this algorithm is runby cloud server to adjust the aggregate trapdoorto generate the right trapdoor for each differentdocument. It takes as input the system publicparameters params, the set S of documents'indices, the index i of target document and theaggregate trapdoor Tr, then outputs eachtrapdoor Tri for the i-th target document in S.

6.Test(Tri, i): this algorithm is run by the cloudserver to perform keyword search over anencrypted document. It takes as input thetrapdoor Tri and the document index i, thenoutputs true or false to denote whether thedocument doci contains the keyword w.

IV. CONCLUSION

In thisproposed concept of key-aggregate searchableencryption (KASE) and construct a concreteKASE scheme. It can provide an efficient solutionto building practical data sharing system basedon public cloud storage. In a KASE scheme, theowner needs to distribute a single key to a userwhen contributing a lot of documents with theuser, and the user needs to submit a singletrapdoor when they queries over all documentsshared by the same owner. On the other hand, ifa user wants to question over documents sharedby multiple owners, that user must producemultiple trapdoors to the cloud. The futureenhancement for this proposed work is to findout how to decrease the number of trapdoorsunder multi-owners setting by attaining thesecurity.

REFERENCES

[1] Cloud-Storage, http://www.thetop10besonlinebackup.com/cloudstorage.

[2] Amazon Web Services (AWS), http://aws.amazon.com.

[3] Google App Engine, http://code.google.com/appengine/.

[4] Microsoft Azure, http://www.microsoft.com/azure/. 00.

[5] X. Song, D.Wagner, A. Perrig. "Practicaltechniques for searches on encrypted data", IEEESymposium on Security and Privacy,IEEE Press, pp. 44C55, 2000.

[6] R. Curtmola, J. Garay, S. Kamara, R.Ostrovsky. "Searchable symmetric encryption:improved definitions and efficientconstructions", In: Proceedings of the 13th ACMconference on Computer and CommunicationsSecurity, ACM Press, pp. 79-88, 2006.

[7] P. Van,S. Sedghi, JM. Doumen."Computationally efficient searchable symmetricencryption", Secure Data Management, pp.87-100, 2010.

[8] S. Kamara, C. Papamanthou, T. Roeder."Dynamic searchable symmetric encryption",Proceedings of the 2012 ACM conferenceon Computer and communications security(CCS), ACM, pp. 965- 976, 2012.

[9] D. Boneh, C. G, R. Ostrovsky, G. Persiano."Public Key Encryption with Keyword Search",EUROCRYPT 2004, pp. 506C522,2004.

[10] Y. Hwang, P. Lee. "Public Key Encryptionwith Conjunctive Keyword Search and Its , Extension to a Multi-user System", In: PairingBased Cryptography C Pairing 2007, LNCS, pp.2-22, 2007.

[11] J. Li, Q. Wang, C. Wang. "Fuzzy keywordsearch over encrypted data in cloud computing",Proc. IEEE INFOCOM, pp. 1-5, 2010.

[12] C. Bosch, R. Brinkma, P. Hartel. "Conjunctivewildcard search over encrypted data", SecureData Management. LNCS, pp. 114- 127, 2011.

BIODATA

Vulloji Rajacurrently pusuing his M.Tech(cyber forensic &information security) from Vijaya Engineering College, Ammapalem, Khammam,Telangana, India.

P.Ashok Kumar completed his M.Tech(CSE) in 2009. Presently working as Associate Professor and HOD in Dept of CSE, Vijaya Engineering College, Ammapalem, Khammam,Telangana, India.