A Review of Research on An Aggregate Key Sharing Mechanism For Sharing Data Between Different Groups Via Cloud

[1]Sharayu.J.Lande, [2]Prof. N.B.Kadu
[1]PG Student, [2]Associate Professor
[1]Department of Computer Engineering
[1]Pravara Rural Engineering College, Loni, India

***Abstract* - One of the important functionality of cloud is Data sharing .It is possible to store data on data storage servers such as e- mail servers and files servers in encrypted form to decrease security and privacy threats. But this usually indicates that if we want to get increased amount of security we have to lose the functionality. For example, if a customer wants to retrieve only documents containing few words, it was not known how to data storage server perform the search and answer the query without loss of data and information. With the property of low maintenance cost, cloud computing provides an economically affordable and efficient way for sharing various information among cloud users. In this article, we show how to securely, efficiently, and flexibly we share data with others in cloud storage. Unfortunately, sharing data in a multi-user manner while preserving data and data privacy from an untrusted cloud is still a large limitation, due to the change of the membership. In this paper we are introducing an aggregate key for communication in different groups of cloud.**

***Index Terms* – Data sharing,Cloud storage,Data Privacy**

I. INTRODUCTION

Cloud storage is becoming more popular nowadays. In enterprise settings, we see the rise in demand for data outsourcing, which benefits in the field of corporate data and its management. It is also useful as a core technology for different online technologies for individual applications[2]. Cloud computing is known as an alternative to traditional technology due to its better resource-sharing and low-maintenance capabilities.The main aim of cloud computing is to provide high performance energy of computing for various field like military and reasearch organization for performing billions of computations at each second.It is also used in customer oriented areas like portfolios to transfer confidential information. In cloud computing, the cloud service providers (CSP), like Amazon, are able to provide various services to users with the help of powerful data servers. Moving the local data management systems into cloud servers, users can take advantage of high-quality services and store important investments on their local infrastructures. However, while sharing data through cloud storage, users are simultaneously aware about the data leakages in the cloud[5]. One of the most fundamental services delivered by cloud service providers is data storage. consider a data application. There is a company which permits its staffs in the same group or department to store and share documents or files in the cloud. Using the cloud, the staffs can be fully released from the local data storage and maintanance. However, it also creates a significant risk to the confidentiality of those stored documents. Specifically, the cloud servers controlled by cloud providers are not fully believed by users while the documents stored in the cloud may be s confidential, such as business ideas. Identification of privacy is most important problem for wide development of cloud computing.Without the proof of identity privacy users are not ready to utilize the cloud services because they dont want to expose their real identity.To maintain data privacy, a basic idea is to encrypt files, and then upload the encrypted data into the cloud. In this paper, we demonstrate cryptographic scenarios for the problem of searching on encrypted data and provide result of security for the resulting crypto systems[4].

II.BACKGROUND OF PROBLEM

Suppose that Client 1 uploads all her private pictures and videos on Dropbox, and she does not want to see her photos by everyone. Due to various data leakages in cloud there may be possibility that client 1 cannot feel satisfied by just relying on the privacy protection provided by Dropbox, so she encrypts all the pictures using her own keys before uploading. One day, Client 1's friend,say client 2, asks her to share her pictures taken during all these years which client 2 appeared in. client 1 then uses the share function of Dropbox, but the problem is how to delegate the decryption rights for these pictures to client 2. A possible option client 1 can choose is to securely send client 2 the secret keys included .Therefore there are two ways for her under the traditional encryption paradigm:

1)client 1 encrypts all files with a single encryption key and gives client 2 the corresponding secret key directly.

2)client 1encrypts files with distinct keys and sends client 2 the corresponding secret keys

surely, the first technique is inadequate since all data which is not yet choosen may be also leaked to client 2. For the second method, there are practical concerns on efficiency. The number of keys is equivalent to the number of the shared photos, say, a thousand.Sending these secret keys requires a more secure channel, and storage of these keys requires expensive secure storage.

The cost and complexities included generally rise with the number of the decryption keys to be shared. In short, it is much heavy and costly to do[2] .

III.VARIOUS SEARCHABLE ENCRYPTION SCHEMES AND THEIR RELATIONSHIP TO OUR WORK:

A.Multi-user Searchable Encryption(MUSE): There is a large amount of literature on searchable encryption, including SSE and PEKS 's schemes . In contrast to those existing schemes ,in the cloud storage, keyword search under the multi-tenancy is a more used scenario. In such a scenario, the data owner will to share a document with a group of authorized users ,and each user who has the access authority can provide a trapdoor to perform the process of keyword search over the shared document, namely, the multiple-users searchable encryption (MUSE) scenario[1]. schemes are created by sharing the documents searchable encryption key with all users who have access on it, and broadcast encryptions used to reach coarse-grained access control. As a result, in MUSE, the big problem is how to manage which users can access which documents, whereas how to decrease the number of shared keys and trapdoors is not taken in account. Key aggregate searchable encryption can provide efficient solution and it can make MUSE more efficient and practical.

B.Multi-Key Searchable Encryption(MKSE): In this ,the number of trapdoors is equivalent to the number of documents to search over the documents (if user provides to the server a keyword trapdoor under every key along which a matched document can be encrypted). The objective of MKSE is to assure the cloud service provider can perform keyword search by using only one trapdoor over different documents, whereas the objective of Key Aggregate Searchable Encryption is delegate the right of keyword search to any user by distributing the aggregate key to user in a group data sharing system[1].

C.Searchable symmetric encryption (SSE): It allows a client to encrypt its data in such a way that this data can get searched still. The most significant application of SSE ito the cloud storage is where it enables a client to securely transfer its data to an untrusted cloud provider without loosing the ability to search over it[1].SSE is active research and various functionalities of schemes can achieve various levels of security and effciency. Any practical SSE scheme, however, should satisfy the following properties: sublinear searching time, security,indexes and the ability to modify files effciently[7]. Previous existing-known SSE schemes cannot achieve all these properties at the simultaneously. This limits the practical value of SSE and reduces its chance of deployment in real-world cloud storage system.

D. Attribute Based encryption (ABE): It contains every ciphertext to be associated with an attribute, and the master-secret key holder can be extract a secret key for a policy of these attributes so that the ciphertext can be decrypted by this key if its associated attribute confirms to the policy.In this technique the user's secret key and ciphertext is dependent on attributes[2].

IV.CONTRIBUTON OF EXISTING TECHNIQUES TO OUR WORK:

Any user in the group is able to securely share data with others by the un trusted cloud is proposed. It is possible to support dynamic groups efficiently. Generally, newly granted users can directly decrypt documents and files uploaded before their interaction without communicating with data owners. User revocation can be easily done by managing novel revocation list without modifying the secret keys of the remaining users. The size and computation overhead of encryption are constant and not dependent with the number of revoked users.

To deliver secure and privacy-preserving access control to users, which guarantees any participant in a group to anonymously use the cloud resource. Moreover, the true identities of data owners can be exposed by the group manager when error occur. A rigorous security result, and perform extensive simulations to derive the efficiency of our scheme in terms of storage and computation overhead is provided[5].

A] COMPARISON ON SIZE BETWEEN DIFFERENT SEARCHABLE ENCRYPTION KEYS:

Searchable schemes	Size of decryption keys	Size of Cipher text	Type of encryption
Key assignment scheme	It is depend on hierachy and not constant	Constant	Public key or symmetric key encryption
Symmentric key encryption using compact key	Constant	Constant	Symmetric key encryption
Identity based encryption with compact key	Constant	Not Constant	Public key encryption
Attribute based encryption	Not constant	Constant	Public key encryption
KAC	constant	Constant	Public key encryption

Table 1.Comparison on size between different searchable encryption

V.SCOPE

1)This can be useful in cloud environment where large number of documents are need to share in a secure way.

2)There is the practical problem of privacy preserving data sharing system based on public cloud storage server which requires a data owner to distribute a huge number of keys to users to enable them to access their documents, here we for the first time proposing the concept of key-aggregate searchable encryption (KASE) and construct a concrete and efficirnt KASE scheme.

VI.ADVANTAGES

It provide provable security for encryption, that is the untrusted server cannot get any information about the plaintext when only the ciphertext is available. It provide query isolation for searching purpose, Means that is the untrusted server cannot get any information related the plaintext only than search result. It provide controlled searching, so that the untrusted server cannot find for an arbitrary word without the user's identification.It also enables to search for hidden queries, so that the user may ask the untrusted server to search for a secret word without exposing the word to the server[4].

VII.LIMITATIONS

As a result, in MUSE, the main issue is how to gain control on which users can access which documents, whereas how to decrease the number of shared keys and trapdoors is not taken in account[2].The above stated limitations mostly focus on the difficulties related to multiuser's searchable encryption. These drawbacks must be enhanced in the future that KASE scheme can be widely used in cloud. If proper facilities are available, the KASE scheme can be implemented of federated clouds.

VIII.PROPOSED SYSTEM

Nowadays Cloud storage is known as a promising solution for providing universal , convenient, and on-demand access to greater amounts of information shared on the Internet. Today, billions of users are sharing personal data such as photos, videos, confedential documents with their friends via social networking applications based on the cloud storage on a daily basis. Business users are also getting attracted by cloud storage due to its numerous advantages, including lower price, greater agility, and better resource utilization capabilities[1]. But there is the practical problem of preserving privacy of data sharing system based on public cloud storage which need a data owner to distribute a huge number of keys to users to enable them to access their documents, we are proposing first time the concept of key-aggregate searchable encryption (KASE) and built a concrete KASE scheme. As we discussed in limitations that how to reduce a number of shared keys ,here we are introducing a single aggregate key for all documents.

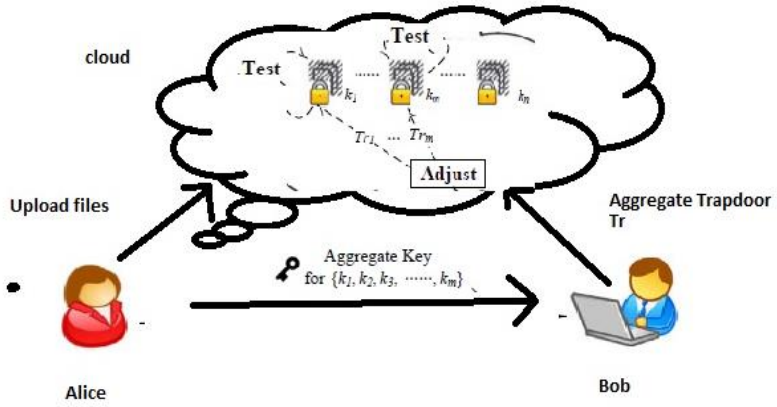

Fig.Aggregate Key sharing mechanism

IX.CONCLUSION

Due to the characteristic of low maintenance, cloud computing provides financially suitable and efficient solution for sharing group resource among cloud users. Our scheme is also very flexible, and it can be simply extended to support more advanced searching query . Here we conclude that this provides a tremendous building block for the construction of secure services in the cloud storage which are not trusted by user . As we will share only single key the storage space required will become less and more efficient.

REFERENCES

[1] Baojiang Cui, Zheli Liu_ and Lingyu Wang "Key-Aggregate Searchable Encryption (KASE)for Group Data Sharing via Cloud Storage" PP : 99 , 2015.
[2] 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.
[3] 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 2007, LNCS, pp. 2-22, 2007.
[4] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.
[5] 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.
[6] 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.
[7] S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965- 976, 2012.

[8]J. Li, Q. Wang, C. Wang. “Fuzzy keyword search over encrypted data in cloud computing”, Proc. IEEE INFOCOM, pp. 1-5, 2010.
[9] C. Bosch, R. Brinkma, P. Hartel. “Conjunctive wildcard search over encrypted data”, Secure Data Management. LNCS, pp. 114- 127, 2011.
[10] C. Dong, G. Russello, N. Dulay. “Shared and searchable encrypted data for untrusted servers”, Journal of Computer Security, pp. 367-397, 2011.
[11] 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.
[12] J. W. Li, J. Li, X. F. Chen, et al. “Efficient Keyword Search over Encrypted Data with Fine-Grained Access Control in Hybrid Cloud”, In: Network and System Security 2012, LNCS, pp. 490- 502, 2012.
[13] J. Li, K. Kim. “Hidden attribute-based signatures without anonymity revocation”, Information Sciences, 180(9): 1681-1689, Elsevier, 2010.
[14] X.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.
[15] 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.