RESEARCH ARTICLE OPEN ACCESS

Key-Aggregate Searchable Encryption (KASE) for User Revocation in Cloud Storage

Nikesh Pansare[1], Akash Somkuwar[2] , Adil Shaikh[3] and Satyam Shrestha[4]
[1,2,3,4]*(Computer Department, SPPU, Pimpri)*

Abstract:

The capability of involving the selection sharing encrypted data with different users via public cloud storage may greatly ease security concerns over not intended data leaks in the cloud. A key challenge to designing such encryption schemes to be sustainable in the efficient management of encryption keys. The desired flexibility of sharing any group of selected documents with any group of users need for something different encryption keys to be used for different documents. However, this also implies the urgent need of securely distributing to users a large number of keys for both encryption and search, and those users will have to protected from danger 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 implied need for secure communication, storage, and complexity clearly to give to someone the approach impractical. In this work a data owner only needs to distribute a single key to a user for sharing a very large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents. User Revocation is used for Key Updation. Forward Secrecy and Backward Secrecy is used.

Keywords — **Cloud Computing, Encryption, Decryption, Cipher text, Data Encryption, Information Storage & Retrieval.**

I. INTRODUCTION

Cloud storage has emerged as a promising solving a problem for providing ubiquitous, convenient, and on-demand accesses to large amounts of data shared over the Internet. nowadays, millions of users are sharing personal data, such as photos and videos, with their friends through a dedicated website or other application which enables users to communicate with each and every other by posting information, messages,images based on cloud storage on a daily basis.

Business users are also being attracted by cloud storage due to its many benets, including lower cost, greater agility, and better resource utilization. However, while enjoying the quality of being useful, easy, of sharing data via cloud storage, users are also increasingly worried about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious a misbehaving cloud operator, can usually lead to behave badly break or fail to observe of personal privacy or business secrets (e.g., the recent high prole incident of a famous person photos being leaked in iCloud).

To address users relate to protect potential data leaks in cloud storage, a prevalent way of dealing with a situation is for the data owner to encrypt all the data before upload to cloud.

II. LITERATURE SURVEY

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

Cloud computing is develop computing paradigm in which resourcesof the computing infrastructure are provided as services over the Internet. As to assure as it is, this paradigm also brings forth many new challenges fordata security and access control when users outsource annoyed data for sharing on cloud servers, which are not within the same trusted

influence, as data owners.To keep sensitive user data confidential against untrusted servers, existing solutionsusually apply cryptographic methods by to cause to appear data decryption keys only to authorized users. The problem of simultaneously accomplish fine grained access,scalability, and data confidentiality of access control actually still remains not resolved.

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

Success of data forensics in cloud computing is based on secure place that records ownership and process history of data objects. But it is the still challenging issue in this paper. In this paper, they proposed a new secure provenance scheme based on the bilinear pairing techniques.As the essential bread and butter of data forensics and postinvestigation in cloud computing, the proposed scheme is characterized by providing theinformation confidentiality on sensitive documents stored in cloud.Secure authentication on user access,and place tracking on disputeddocuments is provided in this paper. With the provable security techniques, this paper formally demonstrate the proposed scheme is secure in the standard model.

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

In this paper character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users.Due to the frequent change of membership sharing data in multi-owner manner while preserving data and identify privacy from untrusted cloud is still a challenging issue.

D. *Key-Aggregate Crypto system for Scalable Data Sharing in Cloud Storage.*

Data sharing is large functionality in cloud storage In this article, weshow how to securely, efficiently, and adaptable share data with others in cloudstorage. The novelty is that one can aggregate any set ofsecret keys and make them as compact as a single key, but to enclose the power of all the keys being aggregated. In other words, the secret key something that holds or secures can release a constant-size aggregate key for flexible choices of ciphertext set in cloud storage, but the other encrypted files not inside the set unchanged confidential.This compact aggregate key can be suitable sent to others or be stored in a smart card with very limited secure storage.

III. METHODOLOGY

Through the concrete KASE scheme we address the challenges by proposing the new concept of key aggregate searchable encryption (KASE). By applying proposed KASE scheme to any cloud storage any user may selectively share group of selected files with a group of selected users.

User revocation is used in the proposed system. In user revocation forward secrecy and backward secrecy is used. User revocation is used for the key updation in the cloud storage. Forward secrecy means if any user is added into the group theaggregate is forward to the new member of the group.

Backward secrecy is if any group member is leaves from the group the aggragate key is updated in the server.And the new aggregate key is informed to the existing group members. Because ofthe user revocation the data is more secure in the cloud.

In the concrete KASE scheme user only needs to submit a single trapdoor to the cloud for querying the shared documents. And data owner only needs to distribute a single key to user for sharing a large number of documents Maintaining aggregate key is easy in server and for the group members. KASE alice only need to distribute a single aggregate key instead of multiple keys. It is an efficient public-key encryption scheme which supports flexible delegation. In this work we uses the AES algorithm for the encryption and decryption of data.

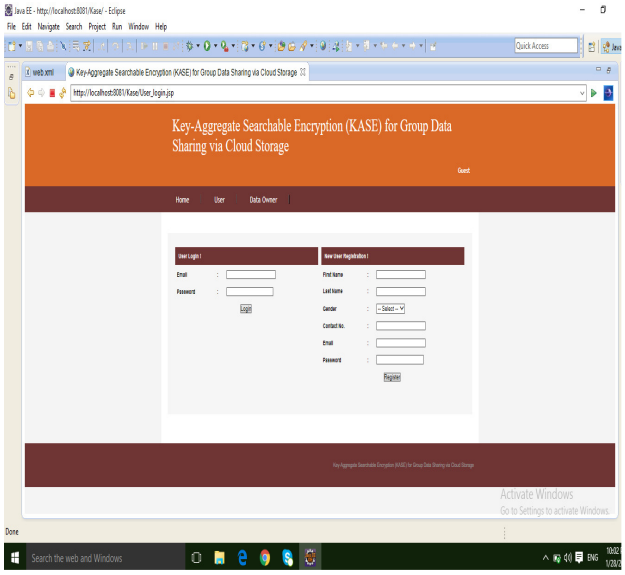

Fig 1 Login Page For the User

IV. CONCLUSIONS

Considering the practical problem of privacy maintain 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 . Analysis and assessmentresults confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage. When sharing a lots of documents with the user the owner only to distribute a single key.

User only need to submit a single trapdoor when all documents are shared by the same owner. In spite of that, if a user wants to query over documents shared by multiple owners, he must generate multiple trapdoors to the cloud. The future work is to reduce the number of trapdoors undermulti-owners setting. The inter clouds have attracted a lot of attention nowadays. But the KASE cannot be applied in this kind of case directly. In case of inter clouds and federated clouds to provide a solution for these is a future work.

REFERENCES

1. 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.

2. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010

3. X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multi- owner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182- 1191..

4. C.Chu,S.Chow,W.Tzeng,etal."Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477..

5. X.Song,D.Wagner,A.Perrig."Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.

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.