A Survey on Group Data Sharing over Cloud in Multi-owner Environment using Key Aggregation and Trapdoor

Prajakta Salunkhe
Department of Computer Engineering
Marathwada Mitra Mandal's College of
Engineering, Pune.

Geetha R. Chillarge
Department of Computer Engineering
Marathwada Mitra Mandal's College of
Engineering, Pune.

ABSTRACT

Cloud is being used by different type of users to fulfil their storage needs and sharing requirements. Public cloud storage provides virtually unlimited capacity to its users for sharing encrypted data. The main challenge is to design the encryption scheme which is efficient in management of encryption keys. Numbers of keys are required in the sharing of group data scenario as well as it needs to distribute those keys in secure manner to the user and user has to store them securely again. Also user needs to create equally large number of trapdoors with keywords to access data. This project gives solution on this problem by providing a concrete scheme of key aggregate searchable encryption. In this, data owner needs to distribute a single key for sharing large number of documents and user required to submit a single trapdoor to the cloud for downloading multiple documents over the cloud. It also provides a solution for a situation where user searches for the documents shared by multiple owners and user needs to generate multiple trapdoors. In the proposed system, user needs to generate a single trapdoor for searching the files shared by multiple data owners.

Keywords

Cloud storage, Data privacy, Data sharing, Key aggregation, Searchable Encryption

1. INTRODUCTION

Now-a-days, cloud storage is gaining much popularity due to its benefits like it stores, manages, backed up and monitors data remotely. It costs only for the storage space leased by or purchased by the user rather than capital expenses. All types of users are using cloud storage tremendously based on social networking applications to share or store their pictures, videos, music flies, documents that mean all type of data.

Though, every user is enjoying the benefits of cloud services, they worry about data confidentiality and unintended data leakage which generally happens in the cloud environment. More often, these data security threats caused by a disloyal cloud operators or an attacker usually results in serious violation of personal or professional privacy.

Using cryptographic cloud storage is solution these cases which is the most common approach. In this, data owner stores all his data in encrypted format over a cloud. So this data can be decrypted by only those users who have decryption keys provided by data owner. Cryptography also becomes challenging for users to search required data as all data are stored in encrypted format and user submits keywords in plaintext. By applying searchable encryption schemes, this problem can be handled. For this, data owner needs to encrypt documents keywords as well as documents and then upload it on the cloud. At the time of searching those documents by user, he makes a keyword trapdoor over a cloud containing keywords which does keyword matching with the stored data.

Figure 1 shows the conventional approach of data sharing in a group.

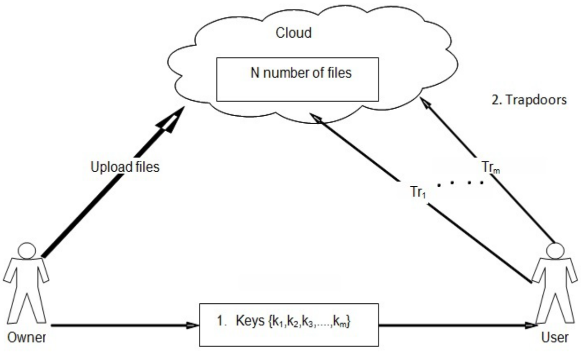

Fig. 1: Conventional approach of data sharing

This is very basic achievement in terms of security needs. There is huge data in cloud storage and n number of users accessing this data. So management of encryption keys becomes crucial part of searchable encryption. Provider has to assign encryption, decryption keys each time to each user for every file. It increases computational cost and storage overhead. This main issue is not taken into consideration in the literature.

Many times business organizations need to share the confidential data within the organization or to the other organizations. Consider a scenario where a manager wants to share multiple confidential documents with one of the employee then manager will upload suppose n number of documents on cloud storage and will provide n number of encryption keys to the employee. The employee will store all the keys securely. Then using these keys, the employee will generate the keyword trapdoor for accessing those documents. So for n number of documents, it is not efficient to provide n number of keys, store them securely and then generate trapdoors for each document. It becomes very expensive at the employees side server. This practical problem motivates to construct a scheme which will provide a single aggregated key to the employee and will allow access to the cloud by generating single trapdoor by the employee to access any number of documents. This scheme will work in multi-owner environment too where multiple owners share multiple documents. User will required to submit single trapdoors instead of multiple trapdoors to the cloud.

2. REVIEW OF LITERATURE

In this section, we will review several existing searchable encryption schemes and key management solutions proposed by various authors. There is a great literature available on searchable encryption.

Jun Yang et al. [2] first analysed outsourced server with multi-users. Then they classified the data sharing into two types which are data sharing using Searchable encryption among users and the goal of corresponding security. They proposed that ciphertext can be generated from parameter by authorized user for searchable encryption. The homomorphism and one-way function concepts are used to model the proposed scheme.

Database-as-a-Service (DaaS) is another trending service by cloud and organisations outsourcing their local database to the cloud database due to its facilities. Confidentiality is the issue so Kurra Mallaiah at al. [3] stored their data in encrypted form and used keyword search over it for searching of data. They proposed Multi user multi-key Encryption Search schemes. If multiple users are searching data, multiple keywords will be generated. They used trusted proxy which keeps record of users and encrypted files. This scheme supports searching when data is encrypted by multiple users and their different encryption keys.

Cheng-Kang Chu et al. [4] describes the mechanism to share data efficiently, flexibly and securely in cloud storage. They proposed a scheme which produces constant size ciphertext. They called it public-key cryptosystem. For any set of ciphertext, delegation of decryption rights is efficient due to constant size of ciphertext. They also described the system which will aggregate number of keys in a compact key or a single key. Their work predefines boundary for the number of maximum ciphertext classes and generally in cloud storage, number of ciphertext grows at a high speed. So this system needs to reserve sufficient ciphertext classes for future use. It is the limitation for the efficiency of the proposed scheme.

Zhiquan Lv et al. [5] stated that Ciphertext Policy Attribute Based Encryption (CP-ABE) is a rising technique to solve the issue of access control in multiuser environment. But it also has some challenges like inefficiency of decryptable files search, attributes verification and decryption. So they proposed a system using CP-ABE with proxy server in which proxy server is used to generate keyword index and trapdoor. A new method to verify each user's attributes is also designed by the authors. This method works without disclosing the relation of his identity and attributes.

Xuefeng Liu et al. [6] worked on problem where multiple owners want to share data to the dynamic groups in the cloud environment. Groups can be dynamic as they will be formed at the time when similar data need to share with users. So when data for sharing will change, users groups will dynamically change. For providing security, they combined group signature and broadcast encryption techniques are used. But when any user leaves, each user has to compute revocation parameters for this. It is necessary for the confidentiality of their data. This leads to the increased computation overhead. So authors assigned group manager to calculate revocation parameters.

R. A. Popa and N. Zeldovich [7] described a promising approach to prevent the exposure of confidential data. They stated that attackers compromise the servers, so at the server side, only encrypted data has to be stored and at the client side both encryption and decryption of documents should happen. In a multi-user scenario, each user may have access to different documents. To achieve this, each document has to be encrypted with separated per document key and user's client machine should have access to those keys. Authors cryptographic scheme provides a single search token to the servers and allows server to search for that tokens words in documents which are encrypted with different keys.

According to Z. L. Liu et al. [8] fine grained access control system increases the management complexity. So the coarse-grained access control concept is presented for the first time in this paper. Authors used this concept in hybrid cloud for the construction of multi-user searchable encryption model. They used two typical schemes which are broadcast encryption scheme and single-user searchable encryption scheme. Improved searchable symmetric encryption scheme is also used to implement the practical scheme.

Sebastian Graf et al. [9] introduced stream-based Key Graph-approaches in the cloud environment. Their proposed architecture does not need re-encryption of any data. Streambased key approach is used by authors to make key management flexible and scalable. They represented access rights in a graph form. For this they differentiated between keys used for data encryption and the encrypted updates on the keys. These updates are called as key-trails which represents the edges within the key graph. Key trails are also encrypted and stored.

Somchart Fugkeaw [10] proposed a model for privacy enhancing access control. This scheme is for multi-owner cloud environment. In this, multi-agent system is employed to accommodate multi-policy enforcement. It also supports parallel processing of authorization request. The main solution includes a combination of public key infrastructure key management and his proposed web access control infrastructure.

Shucheng Yu et al. [11] states that existing system usually uses cryptographic solutions to keep user data confidential. It results in increased heavy computation overhead as data owner needs to manage key distribution and management. This is not suitable when there is requirement of fine-grained data access control. This paper defines and enforces access policies based on data attributes. The proposed system allows data owner to assign computation task involved in fine-grained data access control to unreliable cloud server. It does not allow disclosing the contents of the data. This is achieved by combining three techniques which are attribute-based encryption, proxy re-encryption and lazy re-encryption.

The next table shows the study of above papers in brief manners. Which techniques are used and how they support the system is also given.

Table 1: Comparative Study

Sr. No	Author and Title	Method	Comment
1	Jun Yang, Chuan Fu, Nan Shen, Zheli Liu, Chunfu Jia, Jin Li, ``General Multi-Key Searchable Encryption", 29th International Conference on Advanced Information Networking and Applications Workshops, 2015.	Homomorphism and One-way function are used	• Parameters of authorized users are used for ciphertext generation • Supports Multi-key Searchable Encryption
2	Kurra Mallaiah, Prof. S Ramachandram , Rishi Kumar Gandhi, ``Multi User Searchable Encryption Schemes using Trusted Proxy for Cloud based Relational Databases", 2015 IEEE.	Use of trusted proxy	• Schemes for Multi user multi key Encryption Search for cloud Relational Databases (MES-RD) • System for Database-as-a-service cloud model • Supports Multi-user searchable encryption
3	Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, ``Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.	Ciphertext classes are used to associate with plain text	• Size of ciphertext, public-key, master-secret key, and aggregate key is constant • Key-aggregation is provided • It is public-key cryptosystem
4	Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, ``Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.	Group signature and Broadcast Encryption Technique is used	• User revocation is easily achieved • Multi-owner data sharing scheme • Supports dynamic groups in cloud efficiently
5	Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, ``Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", in Proc. IEEE Conf. Comput. Commun., 2010, pp. 534–542.	Proxy Re-encryption, Attribute-Based Encryption (ABE), and Lazy Re-encryption Techniques are used	• First paper which achieves fine-grainedness, scalability and data confidentiality for data access control in cloud computing • Supports user accountability

The systems explained above face many issues and challenges in terms of key management, security and efficiency of systems. These types of systems are not suitable to handle large data sharing. It also cost more for key storage as it has to store large number of keys. These systems are developed to provide a search on encrypted data. But it costs heavy computational overhead to provide information security and low computational power to the user side servers.

3. CONCLUSION

Due to the features of low maintenance, cloud computing provides economically suitable and powerful solution for distributing group data among cloud users. This survey paper gives the overview of existing systems which are developed for securely sharing of data in cloud environment. After analysing the problem of key management and key distribution, we concluded that there is a need of a system which will use key aggregation searchable encryption scheme. The further work is to develop a single system in both single owner and multi owner environment.

4. REFERENCES

[1] Baojiang Cui, Zheli Liu and Lingyu Wang,“Key-aggregate searchable encryption (KASE) for group data sharing via cloud storage”, IEEE transactions on computer vol. 65, No. 8, August 2016.

[2] Jun Yang, Chuan Fu, Nan Shen, Zheli Liu, Chunfu Jia, Jin Li, “General Multi-Key Searchable Encryption”, 29th International Conference on Advanced Information Networking and Applications Workshops,2015.

[3] Kurra Mallaiah, Prof. S Ramachandram , Rishi Kumar Gandhi, “Multi User Searchable Encryption Schemes using Trusted Proxy for Cloud based Relational Databases”, 2015 IEEE

[4] Cheng-Kang Chu, Sherman S. M. Chow,Wen-Guey Tzeng, Jianying Zhou and Robert H. Deng, “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”, IEEE TRANSACTIONS ON

PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.

[5] Zhiquan Lv, Min Zhang, Dengguo Feng,“ Multi-User Searchable Encryption with Efficient Access Control for Cloud Storage”, 6th International Conference on Cloud Computing Technology and Science IEEE 2014.

[6] Xuefeng Liu, Yuqing 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, VOL. 24, NO. 6, JUNE 2013

[7] R. A. Popa and N. Zeldovich, “Multi-key searchable encryption”, Cryptol. ePrint Archive, Rep. 2013/508, 2013.

[8] Z. L. Liu, Z. Wang, X. C. Cheng, and , C. F. Jia, K. Yuan, “Multiuser searchable encryption with coarser-grained access control in hybrid cloud”, in Proc. 4th Int. Conf. Emerging Intell. Data Web Technol., 2013, pp. 249255.

[9] Sebastian Graf, Patrick Lang,“Versatile Key Management for Secure Cloud”, 2012 31st International Symposium on Reliable Distributed Systems Storage.

[10] Somchart Fugkeaw, “Achieving Privacy and Security in Multi-Owner Data Outsourcing”, 2012 IEEE.

[11] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, in Proc. IEEE Conf. Comput. Commun., 2010, pp. 534542.