International Journal of Advanced Engineering and Technology
ISSN: 2456-7655; Impact Factor: RJIF 5.54
www.newengineeringjournal.com
Volume 1; Issue 2; May 2017; Page No. 13-15

Efficient user revocation for dynamic groups using cloud

[1] VA Patil, [2] Pratiksha Kute, [3] Pritam Pardeshi, [4] Smrutigandha Pathare

[1] Assistant Professor, Department of Computer Engineering, SITS Narhe Pune, Maharashtra, India
[2, 3, 4] Students, Department of Computer Engineering, SITS Narhe Pune, Maharashtra, India

Abstract
The dawn of the cloud computing makes storage outsourcing become a rising trend, which promotes the secure data auditing a hot topic that appeared in the research literature. In recent times some research reflect on the problem of secure and efficient public data integrity auditing for secure active data. However previous schemes were not efficient for securing and sharing data among user and maintain the concept of Revocation. In this paper, we figure out the collusion attack in the exiting scheme and provide an efficient secure data auditing scheme with secure group user revocation based on SHA1 and user key generation algorithm revocation group signature. We design a tangible design based on the our scheme definition. Our schema supports the tight security for data and efficient Revocation with some very nice properties like secure sharing of data, choosing a particular group to make data secure, allowing member to upload data, confidentiality and traceability. Finally, the security and experimental exploration show that, compared with its relevant schemes our scheme is also secure and efficient.

Keywords: cloud computing, access control, dynamic groups, and data sharing

1. Introduction
In our proposed system, we will create a new idea; the user revocation problem is not considered and the audits cost is linear in the size of the group and data. To further improve the system and previous support group user revocation. However, the plan assumes that the private and authenticated channels exist between each pare entities and there is no collusion between them. Another attempt to improve the previous scheme efficient, scalable and collusion resistant is designed a dynamic public integrity auditing scheme with group user revocation. Many researchers have devoted considerable attention to the problems on how to securely outsource local store to remote cloud server. Among which, the problem of remote data integrity and availability auditing attacks the attestation of many researchers.
To give a facility to employees to provide a quick service and secure data storage with encryption which will provide employees with immediate access of cloud data with higher permissions to improve performance and fault tolerance Length of key is smaller and less time cost. There are two interesting problems we will continue to look to our future scope. One of them is traceability, which means the ability to group manager (e.g. the original user) to reveal the identity signer on the basis of verification of the metadata in some special situations

1.1 Aims & Objectives
- Describing cloud storage model of our system then providing threat model considered and security goals we want to achieve.
- Valid and efficient data is being shared among users in group which ensure security of public data integrity auditing with multi user modification and maintain the data after revocation of user
- To ensure safe storage of user data.
- To make the process handy and transparent.

1.2 Modular Approach
Our proposed system is divided into four distinct modules described as follows:
- User: User can able to share data on group with higher level permissions.
- Data Owner: A number of users who are authorized to access and modify the data by the data owner. Data Owner is responsible for creating group and sharing over cloud. Data owner could encrypt and upload its data to the remote cloud storage server.
- Admin: Admin provides permissions for data sharing and accepting data from different users TPA.
- TPA: TPA authenticate user then share user data via admin permissions also TPA will be able to conduct data integrity of the shared data store in cloud server.

2 Design Goals
2.1 Access control
Cloud Server allows only the authorized group member to store their private data in the cloud offered by cloud service providers.

2.2 Data confidentiality
Data owner will store their data in the cloud and share the data among the group members. Whoever uploads the information have rights to do modication like update and delete their data in the cloud.

2.3 Traceability
In case of any dispute occurs it can easily traceable. If other group member delete the other group members data can be easily noticeable

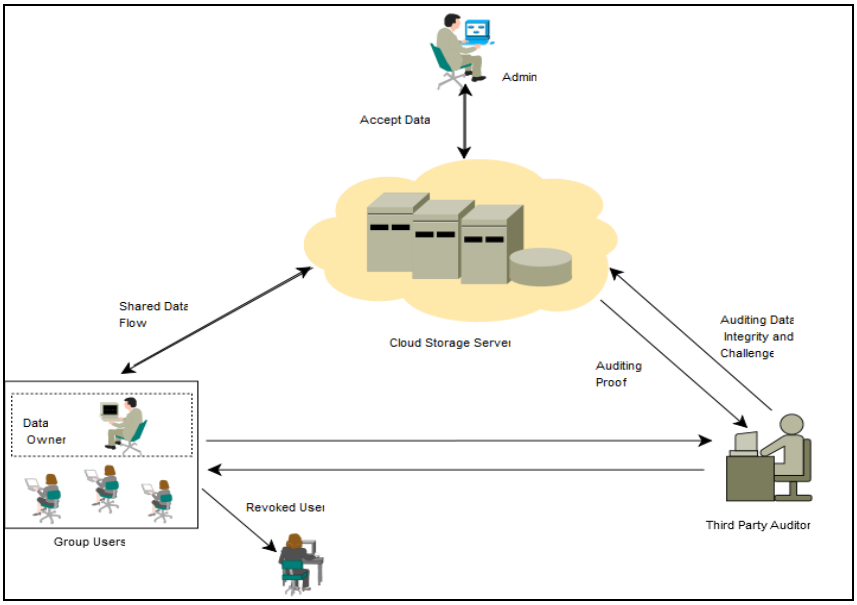

Fig 1: Architecture

3. Implementation Modules

3.1 Data Group sharing

Server can use this aggregate trapdoor and some public information to perform keyword search and return the result to Bob, but it remains an open problem to delegate the keyword search rights together with the decryption rights, which is the subject topic of this paper.

3.2 Public integrity auditing

Public integrity auditing for shared dynamic data with group user revocation. Our contributions are three folds:

a) We explore on the secure and efficient shared data integrate auditing for multi-user operation for cipher text database.
b) By incorporating the primitives of victor commitment, asymmetric group key agreement and group signature, we propose an efficient data auditing scheme while at the same time providing some new features, such as traceability and count ability.
c) We also gives security and efficiency analysis of our scheme, and results show that our scheme is secure and efficient.

3.3 Cloud Storage Model

It is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers, and the physical environment is typically owned and managed by a hosting company. The cloud storage keeps the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

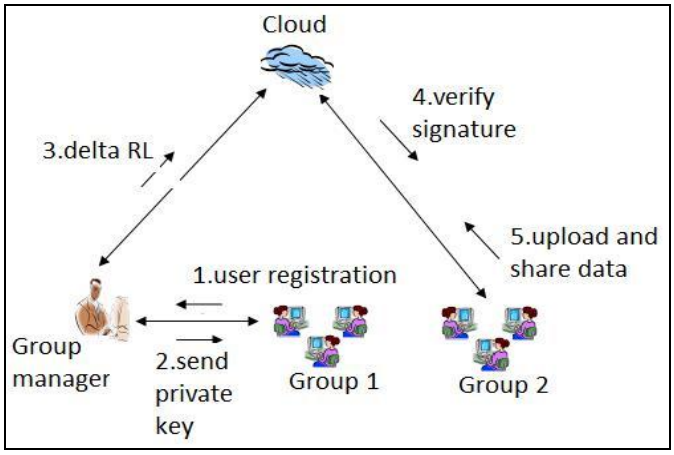

Fig 2

Who are authorized to access and modify the data by the data owner. The cloud storage server is semi-trusted, who provides data storage services for the group users. TPA could be any entity in the cloud, which will be able to conduct the data integrity of the shared data stored in the cloud server. In our system, the data owner could encrypt and upload its data to the remote cloud storage server. Also, he/she shares the privilege such as access and modify (compile and execute if necessary) to a number of group users.

3.4 Group signature

Group signature is introduced by Chaum and Heyst It provides anonymity for signers, where each group member has a private key that enables the user to sign messages. However, the resulting signature keeps the identity of the signer secret. Usually, there is a third party that can conduct the signature anonymity using a special trapdoor. Some systems support revocation where group membership can be disabled without affecting the signing ability of unrevoked users. Boneh and

Shacham proposed an efficient group signature with verifier-local revocation. The scheme provides the properties of group signature such as selfless-anonymity and traceability. Also, the scheme is a short signature scheme where user revocation only requires sending revocation information to signature verifiers. Libert et al. proposed a new scalable revocation method for group signature based on the broadcast encryption framework. However, the scheme introduces important storage overhead at group user side. Later, a scheme to enhance the former scheme which could obtain private key of constant size. In their scheme, the unrevoked members still do not need to update their keys at each revocation

4. Additional Formatting and Style Resources

The Success of this research work would have been uncertain without the help and guidance of a dedicated group of people. We would like to express my true and sincere acknowledgements as the appreciation for their contributions

5. Conclusions

The primitive of verifiable database with efficient updates is an important way to solve the problem of verifiable outsourcing of storage. We propose a scheme to realize efficient and secure data integrity auditing for share dynamic data with multi-user modification. The scheme vector commitment, Asymmetric Group Key Agreement (AGKA) and group signatures with user revocation are adopt to achieve the data integrity auditing of remote data. Beside the public data auditing, the combining of the three primitive enable our scheme to outsource cipher text database to remote cloud and support secure group users revocation to shared dynamic data. We provide security analysis of our scheme, and it shows that our scheme provide data confidentiality for group users, and it is also secure against the collusion attack from the cloud storage server and revoked group users. Also, the performance analysis shows that, compared with its relevant schemes, our scheme is also efficient in different phases.

6. Acknowledgment

The Success of this research work would have been uncertain without the help and guidance of a dedicated group of people. We would like to express my true and sincere acknowledgements as the appreciation for their contributions. Revoked users are updated for every one day. If any user revoked, they have a chance for accessing the cloud after the users revoked.

7. References

1. Boneh D, Boyen X, Shacham H. Short Group Signature Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO). 2004, 41-55.
2. Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO). 2001, 213-229.
3. Boneh B, Lynn, Shacham H. Short Signature from the Weil Pairing Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology. 2001, 514-532.
4. Chaum D, van Heyst E. Group Signatures Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT). 1991, 257-265.
5. Fiat A, Naor M. Broadcast Encryption Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO). 1993, 480-491.\
6. Kallahalla M, Riedel E, Swaminathan R, Wang Q, Fu K. Plutus: Scalable Secure File Sharing on Untrusted Storage Pro USENIX Conf. File and Storage Technologies. 2003, 29-42.
7. Kamara S, Lauter K. Cryptographic Cloud Storage Proc. Int'l Conf. Financial Cryptography and Data Security (FC). 2010, 136-149.
8. Kulkarni S, Bezawada Bruhadeshwar. Rekeying and Storage Cost for Multiple User Revocation Department of Computer Science and Engineering, Michigan State University, East Lansing, MI48824USA.