International Journal of Advanced Technology in Engineering and Science
Vol. No.08, Issue No. 03, March 2020
www.ijates.com
ijates
ISSN 2348 - 7550

# ENABLING EFFICIENT USER REVOCATION IN IDENTITY-BASED CLOUD STORAGE AUDITING FOR SHARED BIG DATA

**M.Aishwariya, J.Kokila, K.Gowri –Final year CSE Dr.S.Radha AP/CSE**

*Sengunthar Engineering College-(Autonomous)*

## Abstract

*Cloud storage auditing schemes for shared data refer to checking the integrity of cloud data shared by a group of users. User revocation is commonly supported in such schemes ,as users may be subject to group membership changes for various reasons. Thus, how to reduce the computational overhead caused by user revocations becomes a key research challenge for achieving practical cloud data auditing. In this paper, we propose a novel storage auditing scheme that achieves highly-efficient user revocation independent of the total number of file blocks possessed by the revoked user in the cloud. This is achieved by exploring a novel strategy for key generation and a new private key update technique. Using this strategy and the technique, we realize user revocation by just updating the non revoked group users' private keys rather than authenticators of the revoked user. The integrity auditing of the revoked user's data can still be correctly performed when the authenticators are not updated. The security and efficiency of the proposed scheme are validated via both analysis and experimental results.*

## 1. Introduction

Cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet. The cloud computing benefits individual users and enterprises with convenient access, increased operational efficiencies and rich storage resources by combining a set of existing and new techniques from research areas such as service-oriented architectures and virtualization. Although the great benefits brought by cloud computing are exciting for users, security problems may somehow impede its quick development. Currently, more and more users would outsource their data to cloud service provider (CSP) for sharing. These security matters existing in public cloud motivate the requirement to appropriately keep data confidential. Several schemes exploiting cryptographic mechanisms to settle the security problems have been proposed. The data owners could broadcast their encrypted data to a group of receivers at one time and the public key of the user can be regarded as email, unique id and username. Hence, by using an identity, data owner can share data with other group users in a convenient and secure manner.

Data sharing is the important service in the cloud. In data sharing service user share the data with group of user. User does not have physical control when the data is in cloud. Any mistake can cause loss of data. To check integrity of data some scheme is used, when user cheat or leaves the group, the user should be revoked from group. Therefore user revocation is important in cloud storage. The cloud data owner uses his private key to generate signature for file blocks. When user is removed the user private key should also be removed .In previous scheme all signatures generated should get transfer to non-revoked user. In such case the non-revoked user download all revoked user block resign and upload new one. This cause lots of computation of resources. Once user is removed from group, there is lots of burden of user revocation for large cloud. The situation will be more difficult when membership changes frequently.

The data sharing is one of the most widely used services that the cloud storage provides. With data sharing service, users can share their data in the cloud with a group of users, and reduce the burden of local data storage. Users, however, will lose the physical control over their data when they share them in the cloud. .Any error (the carelessness of human or the failure of hardware/software) might cause loss or damage to the data . In order to check the data integrity, some cloud storage auditing schemes for shared data are proposed .When a group user misbehaves or leaves the group, the user should be revoked from the group. Therefore, user revocation is a common realistic necessity in cloud storage auditing for shared data.

In cloud storage auditing schemes, the data owner needs to use his/her private key to generate authenticators (signatures) for file blocks. These authenticators are used to prove that the cloud truly possesses these file blocks. When a user is revoked, the user's private key should also be revoked. For traditional cloud storage auditing schemes for share data all of authenticators generated by the revoked user should be transformed into the authenticators of one designated non -revoked group user. In this case, this non-revoked group user needs to download all of revoked user's blocks, re-sign these blocks, and upload new authenticators to the cloud. Obviously, it costs huge amount of computation resource and communication resource due to the large size of shared data in the cloud. In order to solve this problem, recently, some auditing schemes for shared data with user revocation have been proposed. When a user is revoked, the cloud will transform the authenticators of the revoked user's blocks into the authenticators of one non-revoked group user corresponding to these blocks, with a re-signing key.

The computation overhead of user revocation is still linear with the total number of file blocks stored by the revoked user in the cloud. Although this method relieves the burden on the non-revoked group user, it transfers the burden to the cloud. There was over 1 byte of data stored in the cloud. In reality, people might share extensive amount of file blocks with others on the cloud. Once a user is revoked from the group, the burden of user revocation might be huge, even for the computationally powerful cloud. The matter will be even worse when the membership of the group frequently alters. Therefore, how to design a cloud storage auditing scheme for shared data supporting real efficient user revocation is very worthwhile.

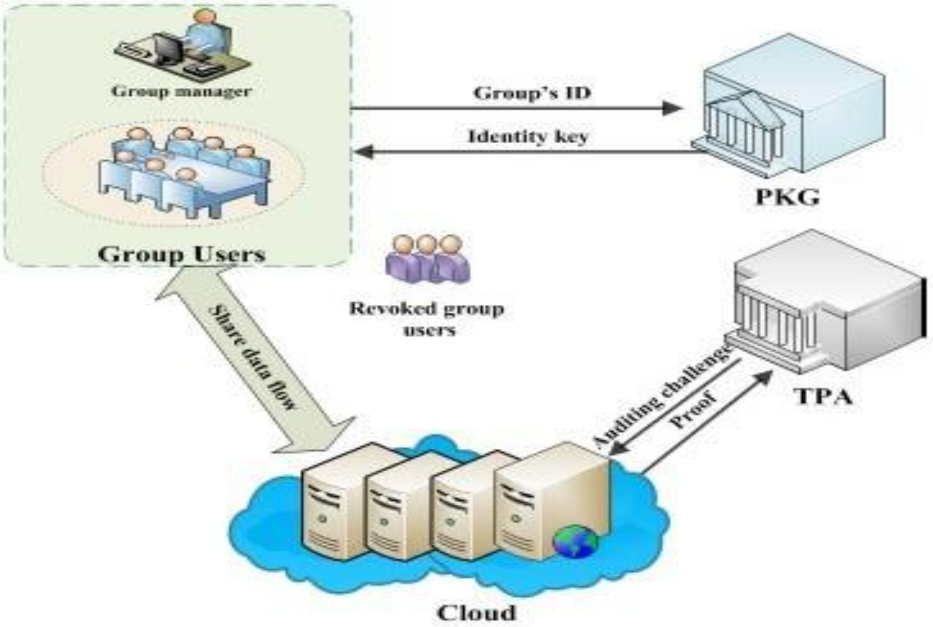
## 2. Proposed System

In existing approaches, when group users are revoked, the authenticators of revoked users' blocks will be transformed into those of some designated non-revoked group user to make the cloud storage auditing still work. It will incur huge computation overhead because the number of revoked users' blocks is usually enormous in big data storage scenario. Our basic idea of solving this problem is to update the non-revoked group users' private keys rather than update authenticators for realizing user revocation. One challenge we face is how to achieve the integrity checking of the revoked user's data under the condition that the revoked user's authenticators are not updated. In addition, we need to be able to detect and refuse the uploading request from the revoked user once he/she is revoked.

We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.

We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. We provide rigorous security analysis, and perform extensive Remote Access to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

### 2.1 .Architecture Diagram



The system model in our scheme includes five entities: the group user, the group manager, the cloud, the Private Key Generator (PKG), and the Third Party Auditor (TPA).

(1) Group user: There are multiple group users in a group. Each group user can share data with others through the cloud storage. Group users can join or leave the group. The legal group users are honest and will not leak any private information to others.

(2) Group manager: The group manager is a powerful entity. It can be viewed as an administrator of the group. When a user leaves the group, the manager is in charge of revoking this user. The revoked user cannot upload data to the cloud any more.

(3) Cloud: The cloud provides enormous storage space and computing resources for group users. Through the cloud storage, group users can enjoy the data sharing service.

(4) PKG: The PKG is trusted by other entities. It is in charge of generating system public parameters and the identity key of the group according to the group's identity (ID).

(5) TPA: The TPA is responsible for auditing the integrity of cloud data on behalf of group users. When the TPA wants to audit the data integrity, it will send an auditing challenge to the cloud. After receiving the auditing challenge, the cloud will respond to the TPA with a proof of data possession.

Finally, the TPA will verify the data integrity by checking the correctness of the proof. The TPA is a powerful party and it is honest.

In our system model, the shared data belong to the dynamic group composed of non-revoked users. Everyone in this dynamic group can upload data and share them with other group users. When a user is revoked, these data uploaded by it are still shared by the dynamic group.

The owner of these data still are this group. However, the revoked user would not be able to upload data and the corresponding authenticators to the cloud any more.

### 2.2. Working Model Generating Keys

In this module owner alone can have access to generate keys to their group useThere will be different group owners, for their users he/she need to generate group key an secretkey to their users in their group. Once owner generated keys it will send to user's registered mobile numbers.

### File Uploading

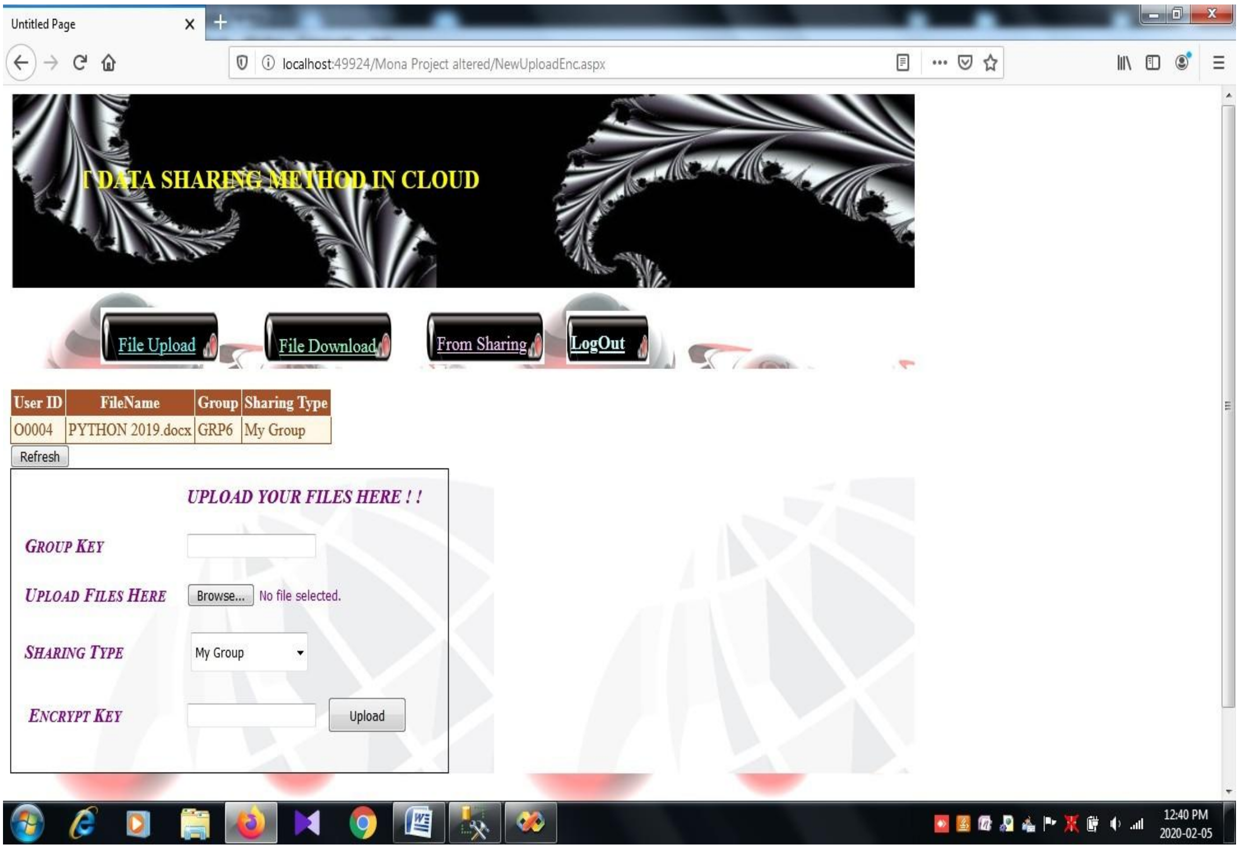
In this module, uploading of files will be done, while uploading file they need to enter the group key which they received from group owner once they registered. They can upload file only when the group key is valid otherwise they can't upload file. Additionally they need to set encrypt key to the file for security purpose and they need to select sharing option in this module

### File Downloading

In this module downloading of files will be processed, while downloading file they need to enter the book id and get corresponding decrypt key to their registered mobile number and they need to enter both the group key and decrypt key for downloading file, it will be downloaded only when the keys are valid.

### Sharing of Files

In this module common shared files will be listed, any group users can download files from these modules. Once they downloading they need to enter verification code and secret key which they received in their registered mobile number. Files will be downloaded only when their entered values are valid.



| User ID | FileName | Group | Sharing Type |
|---|---|---|---|
| O0004 | PYTHON 2019.docx | GRP6 | My Group |

UPLOAD YOUR FILES HERE ! !

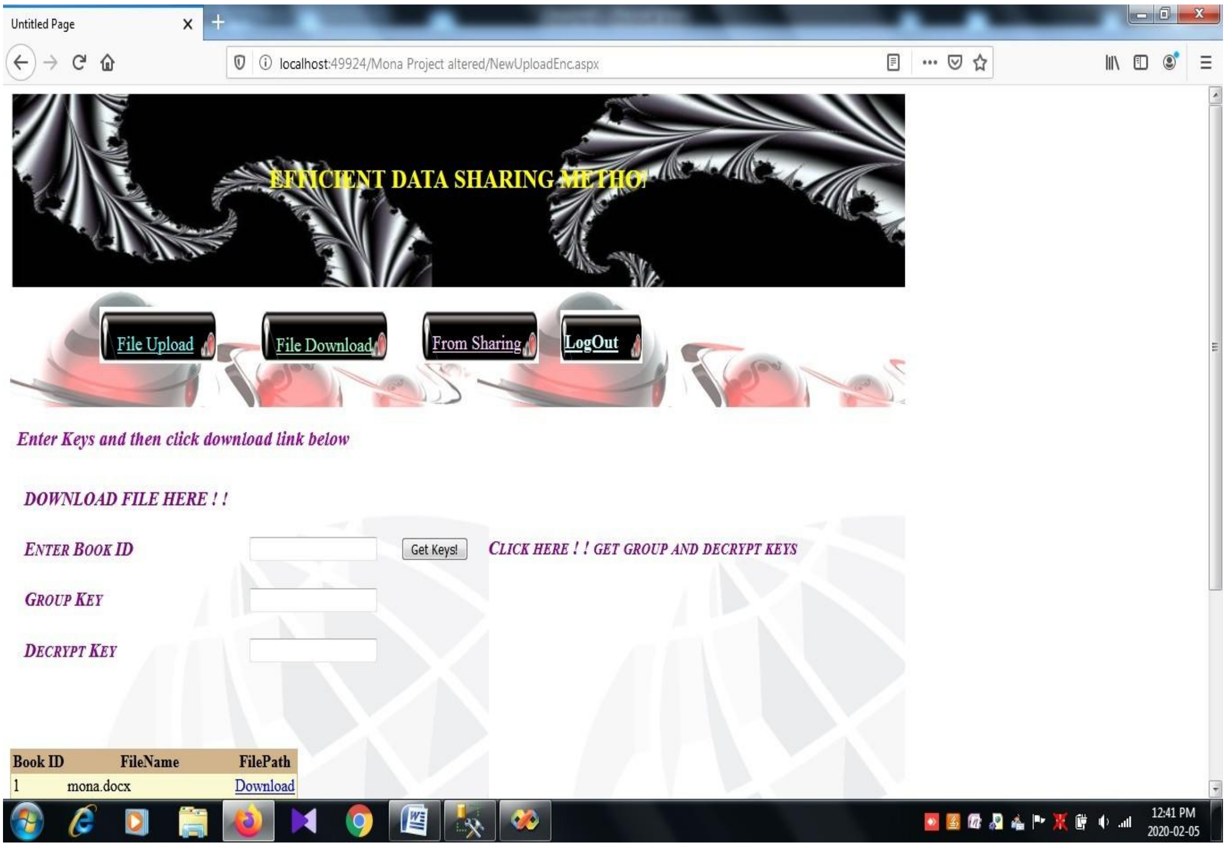
GROUP KEY

UPLOAD FILES HERE No file selected.

SHARING TYPE My Group

ENCRYPT KEY

## 3. Result


Untitled Page
localhost:49924/Mona Project altered/NewUploadEnc.aspx
EFFICIENT DATA SHARING METHO!
File Upload
File Download
From Sharing
LogOut
Get Keys!
12:41 PM
2020-02-05

*Enter Keys and then click download link below*

*DOWNLOAD FILE HERE ! !*

ENTER BOOK ID

CLICK HERE ! ! GET GROUP AND DECRYPT KEYS

GROUP KEY

DECRYPT KEY

| Book ID | FileName | FilePath |
|---|---|---|
| 1 | mona.docx | Download |

## 4. Conclusion

In this paper, we propose an identity-based cloud storage auditing scheme for shared data, which supports real efficient user revocation. In our scheme, the cloud or the non-revoked user does not need to re-sign any file blocks of the revoked user. The overhead of user revocation in our scheme is fully independent of the number of the revoked user's blocks. Security proof and experimental results show that our proposed scheme is secure and efficient.

A new public auditing mechanism for the shared data with an efficient user revocation in the cloud are been concluded when a user in the group is revoked, it allows the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Thus the cloud can improve the efficiency of user revocation, and existing users in this group can save a lot of their computation and communication resources during the user revocation

## 5. References

1.J. Yu, H. Rong, H. Xia, H. Zhang, X. Cheng, and F.Kong, “Intrusion-resilient identity based signatures: Concrete scheme in the standard model and generic construction, ”Information Sciences, vol. 442-443, pp. 158-172,2018.

2. J. Yu and H. Wang, “Strong Key-Exposure Resilient Auditing for Secure Cloud Storage,” IEEE Transaction son Information Forensics and Security, vol. 12, no.8, pp.1931-1940, 2017.

3.W. Shen, G. Yang, J. Yu , H. Zhang, F. Kong, and R. Hao, “Remote data possession checking with privacy-preserving authenticators for cloud storage,” Future Generation Computer Systems, vol. 76, pp. 136-145, 2017.

4. Yu, M. Au, G. Ateniese, X. Huang, W. Susilo, Y.Dai, and G. Min, “Identity-based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage,” IEEE Transactions on Information Forensics and Security, vol.12, no.4, pp. 767-778, 2016.

5. H. Wang, D. He, and S. Tang, “Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud,” IEEE Transactions on Information Forensics and Security. vol. 11, no. 6, pp. 1165-1176, 2016.

6. Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, “Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation,” IEEE Trustcom /BigDataSE /ISP, pp. 434-442, 2015.

7.J. Yuan and S. Yu, “Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification,” IEEE Transaction son Information Forensics and Security, vol. 10, no. 8, pp. 17171726, Aug. 2015.

8. H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, “Identity-based Remote Data Possession Checking in Public Clouds,” IET Information Security, vol.8, no.2, pp. 114-121, 2014.

9. K. Yang and X. Jia, “An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, ”IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1717-1726, 2013.

10. D. Cash, A. K ¨upc¸ ¨u, and D. Wichs, “Dynamic Proofs of Retrievability via Oblivious Ram,” In Proc. 32nd Intl Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT 13), pp. 279-295, 2013.

11. K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no.1, pp. 69-73, 2012.

12. B. Wang, B. Li, and H. Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,” In Proc.of IEEE Cloud 2012, pp. 295-302, 2012.