ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Efficient User Revocation with Public Auditing for Shared Data in the Cloud

Priyada Murali[*] , Jinta Mary Skariah[+] , Surekha Mariam Varghese[%]

Student, Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam , Kochi, Kerala, India[*-]

Student, Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam , Kochi, Kerala, India[+-]

Professor, Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam , Kochi, Kerala, India[%-]

ABSTRACT: With the advent of data storage in the cloud, users are now able to easily share and modify data in a group. Users of a particular group generate signature for each blocks in shared data to ensure data integrity. Since different blocks are updated and modified by different users of a group, the signature on each block tend to be different. To achieve security, once a user is revoked from a group due to misbehaviour, all the blocks which contains the revoked users signature must be re-signed by an existing user of the group. The upright method suggests an existing user to download the data previously signed by the revoked user and re-sign it. But due to its inefficiency this method is not preferred. In this paper, we propose an efficient method to perform user revocation along with a public auditing mechanism to ensure the integrity of shared data. By applying proxy re-signature mechanisms, the cloud is allowed to re-sign blocks during user revocation on behalf of existing users. This is so that the existing users does not have to download the data and then upload again. The paper also supports public auditing which lets a public verifier audit the integrity of shared data without having to retrieve entire data from cloud, even though some data are re-signed by the cloud. Experimental results indicate that this mechanism can improve the efficiency of user revocation significantly.

I. INTRODUCTION

With the advent of cloud, several services are being provided which makes working in group easier. Once a user creates a shared data in cloud, members of the group are not only modify and access the data, but also update and share it with the group. Although the services provided by the cloud are reliable and secure, data integrity can still be a worry due to human errors or hardware/software failures. A number of mechanisms have been provided to protect the integrity of data [1], [2], [3], [4], [5], [6], [7], [8]. Usually a signature is attached at the end of each data and the correctness of all signature implies the integrity of data. A common feature of this mechanism is to let a public verifier to check data integrity efficiently without having to download the entire data, called as public auditing. A public verifier can be a client who make use of the cloud data or it could be a third-party auditor (TPA) who provides verification services. Previous works done focus on auditing personal information. The present work focus on preserving identity privacy from verifiers while performing auditing on the shared data. But none of these mechanisms consider the efficiency in user revocation while auditing the shared data in cloud. Once a user updates a block, the user's signature needs to be computed on the block. This is mandatory especially when a user is revoked from a group due to misbehaviour. At this point, the revoked user's signature is replaced with an existing user's signature. Due to this, the revoked user can no longer update or access the shared data and neither the revoked user's signature is valid in the group. Therefore the integrity of the entire data could be verified by using public keys of existing users of the group.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

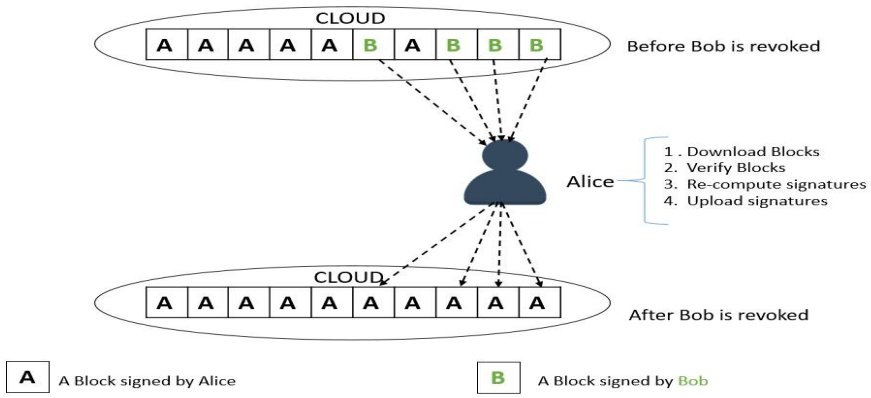

Fig 1. Alice and Bob share data in the cloud. When Bob is revoked, Alice re-signs the blocks that were previously signed by Bob with her private key

The earlier method included the existing user to download the entire data previously signed by the revoked user, perform the required modification and upload the data with the existing user's signature. This method would be really time consuming if the block size was huge or if the membership of the group changed frequently. Clearly, if the cloud had access to the private key of every user in a group, the re-signing task could be easily finished. But outsourcing every users private key gives raise to new security issues. Another important aspect which should not be compromised is the public auditing. Hence it is important to device a method that allows efficient user revocation along with the attractive property of public auditing. In this paper, we propose a novel method to perform efficient user revocation with public auditing for shared data in the cloud. In our method, we use the idea of proxy re-signature and once a user is revoked from a group, the cloud re-sign the blocks which were previously signed by the revoked user by using a re-signing key. This enhances the efficiency significantly and improves the communication and computation resource utilization. Meanwhile, the cloud can only convert the signature of a revoked user into an existing user's signature and by using the properties of proxy re-signature we are able to provide checking of data integrity without retrieving entire data from cloud.

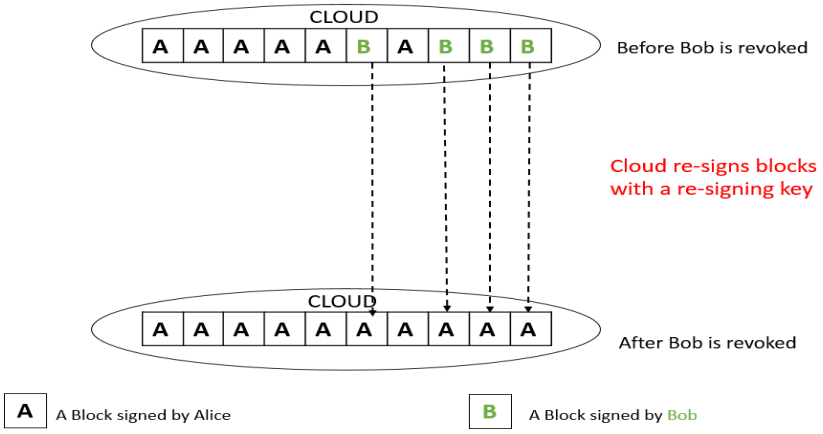

Fig 2. When Bob is revoked , the cloud re-signs the blocks that were previously signed by Bob with a re-signing key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

II. PROBLEM STATEMENT

We describe the security and system model used in our proposed model

A .SYSTEM AND SECURITY MODEL

The system model consists of three entities- the cloud, the users and the public verifier. The cloud provides data storage and sharing services in the group. These are the essential services used by the user entity. The users include the original user who is the creator of the group, also known as the manager of the group and the rest of the users who are the members of the group. Both the original users and group users are able create and share data in the group through the cloud. They can also modify and download the shared data. The public verifier can be the one who utilizes the cloud for several purposes or a third party auditor who performs auditing work. This is achieved by checking the integrity of shared data using a challenge-and-response protocol with the cloud. In this paper we follow certain assumptions. Cloud is considered to be semi-trusted. We also assume that there is no collusion between the cloud and any members of the group. To protect the integrity of shared data, a signature is attached to each block of shared data. Usually when a group is created all the data will be signed by the manager. When the data is modified by a particular user his signature will now be attached with that block of data. Because the data is being shared amongst several users, different blocks of data are signed by different users. When a user misbehaves or leaves the group, the user needs to be revoked from the group. Usually the manager is able to revoke a user on behalf of the group. Once a user is revoked from a group, the user's signature is considered to be invalid in that group.

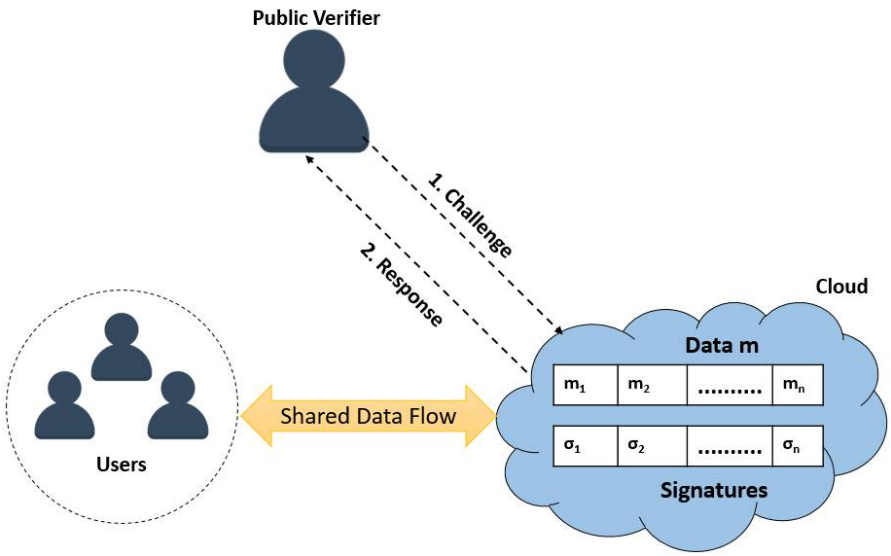

Fig 3. The system model includes the cloud, the public verifier and the users

As mentioned earlier, the locks previously signed by a revoked user must be re-signed by the manager. Hence by doing so the correctness of the entire data can be done by performing public auditing.

B. DESIGN OBJECTIVES

The main objective of this mechanism is to achieve the following properties:-

1) Correctness- Just by accessing a few data the public verifier must be able to check the integrity of data correctly.

2) Efficient User revocation- Once a user is revoked from the group, revoked users signature must be invalid in that group and also the data previously signed by revoked user must be re-signed by an existing user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

3) Public auditing- Without retrieving the entire data from the cloud the public verifier should be able to audit the integrity of shared data even though some blocks have been re-signed.
4) Scalability- The mechanism must support large number of users in the most efficient manner and also handle all the auditing tasks along with it.

III. IMPLEMENTATION

Based on proxy re-signature scheme, we present panda, a novel public auditing mechanics for shared data with efficient user revocation. In this scheme, a group consist of a number of users, with one user being the manager or owner of the group. He can revoke users from the group whenever necessary. Here cloud acts as a semi-trusted proxy and it translates signatures with re-signing keys. Practically the data and keys are placed on separate servers inside the cloud due to security reasons. So in our mechanism, it is based on the assumption that cloud has two servers, one for storing shared data and other for re-signing keys. This paper is focused on auditing the cloud shared data integrity. Another issue in this mechanism is handling dynamic data during public auditing. In conventional methods we compute the signature of a block based on the block identifier which is the index of a block. But this method is not efficient in terms of dynamic data. More specifically, when a user inserts or deletes a single block, the indices of blocks after this modified block will change, so the user need to re-compute the signature on such blocks, even if the contents of the block are not changed. Using the concepts of index hash tables, it is possible to modify individual blocks even without changing the block identifiers. Each block is attached with a signature, identifier for the block, and a signer identifier. The purpose of the signer identifier is that it allows the verifier to use the signer id to determine which key to use during auditing and the cloud uses it to determine the re-signing key during user revocation.

A. ALGORITHMS

Panda consist of six algorithms: KeyGen, ReKey, Sign, Resign, ProofGen, ProofVerify.
KeyGen: Every user generates his own private and public keys when the user joins the group. It can be viewed along with the other details of the user. Random function is used to generate the private and public key.
ReKey: Cloud itself computes a re-signing key for each pair of users. This is based on the assumption that there is no collusion.
Sign: When a user creates shared data in cloud, a signature of the user is attached with each block. And this changes when some other user modifies a block. This helps in identifying which user modified the data block last. The signature is generated using the public and private key of the user who uploaded the data as well as the path of the uploaded file.
ReSign: When a user is revoked from a group, the cloud re-signs the blocks with a re-signing key. The data integrity is verified using challenge-and-response protocol.
ProofGen: Cloud can generate a proof of possession of shared data under the challenge of a public auditor.
ProofVerify: Public verifier can verify the correctness of a proof obtained from the cloud.
Resign: Here we assume that the cloud converts the signature of a revoked user into signature of the original user, which is the group manager. An alternate strategy to determine the re-signing key is to ask the user to make a priority list (PL) based on the order of re-signing priority. Cloud substitutes the signature of the revoked user with the first user in the PL.
The correctness of **ProofVerify** can be well explained using the properties of bilinear maps as follows:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

$$
\begin{aligned}
e\left(\prod_{i=1}^{d}\beta_i, g\right) &= \prod_{i=1}^{d} e\left(\prod_{l\in L_i}\sigma_l^{\eta_l}, g\right) \\
&= \prod_{i=1}^{d} e\left(\prod_{l\in L_i}(H(id_l)w^{m_l})^{\pi_i\eta_l}, g\right) \\
&= \prod_{i=1}^{d} e\left(\prod_{l\in L_i}H(id_l)^{\eta_l}\cdot\prod_{l\in L_i}w^{m_l\eta_l}, g^{\pi_i}\right) \\
&= \prod_{i=1}^{d} e\left(\prod_{l\in L_i}H(id_l)^{\eta_l}\cdot w^{\alpha_i}, \mathtt{pk}_i\right).
\end{aligned}
$$

B. PROPOSED SYSTEM

Architecture of proposed cloud public auditor is shown in the figure. It consists of different modules which are responsible for different process which are required for efficient user revocation and to check correctness of data.

1) User Module: This module consist of several sub-modules such as Registration, Group creation, File upload, Download. A new member in order to use the proposed system has to register in by giving the required details. Then the user may log in further on. A user may create groups in order to share data. The creator of the group is assumed to be the manager of the group. Files are uploaded and shared amongst various members of the group. The integrity of shared data can be achieved by checking the validity of signature appended along with it. The signatures are generated using the DSA algorithm.

2) Database: For every registered user, a private and public key is generated. The public key is stored in the database. This module is also used to access and retrieve data when used for auditing. All the important information of the user and some information related to the files uploaded are stored here.

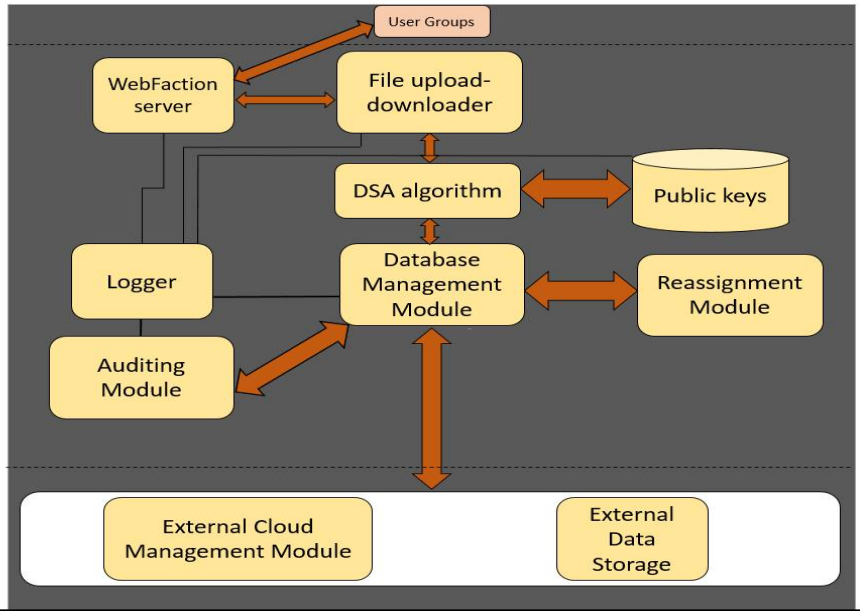

Fig 4: Different modules of the proposed system architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

4) Auditing Module: A user does not need to be a registered user in-order to perform auditing. The auditing can be easily performed by using a very efficient and easy method proposed by this system. Each file uploaded has a unique identifier. If a valid identifier is given as input, this system generates a signature corresponding to that file. If the real signature appended to this file matches the newly generated signature, then the file is valid.
5) External Cloud Storage Management: For security reasons, it is better to store the shared data and keys in different servers provided by WebFaction. Therefore, in this system, we assume that the data is stored in one server and the key in another.

C. SYSTEM DESIGN
This paper is implemented in such a way that the user can register himself onto the cloud and share data amongst several users. The creator of the group is assumed to be the manager of the group. The manager can add members to the group as well as remove users who misbehave. Any member of the group can upload files which can be accessed and downloaded by every member of that group

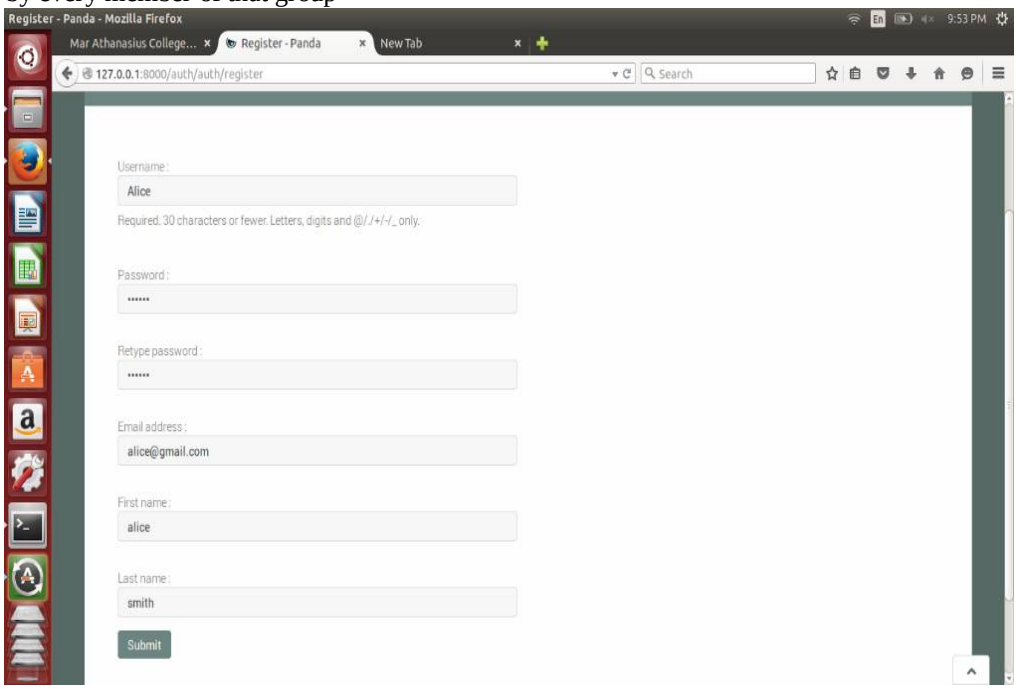

Fig 5: Screenshot showing the registration page

The special feature of this mechanism is that, along with every files uploaded by a specific user, his signature is also attached along for maintaining the integrity of data. This signature is computed using the public and private key of the user along with the path of file uploaded. So the signature will vary from person to person. Also if the same person who uploads two different files will have different keys.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

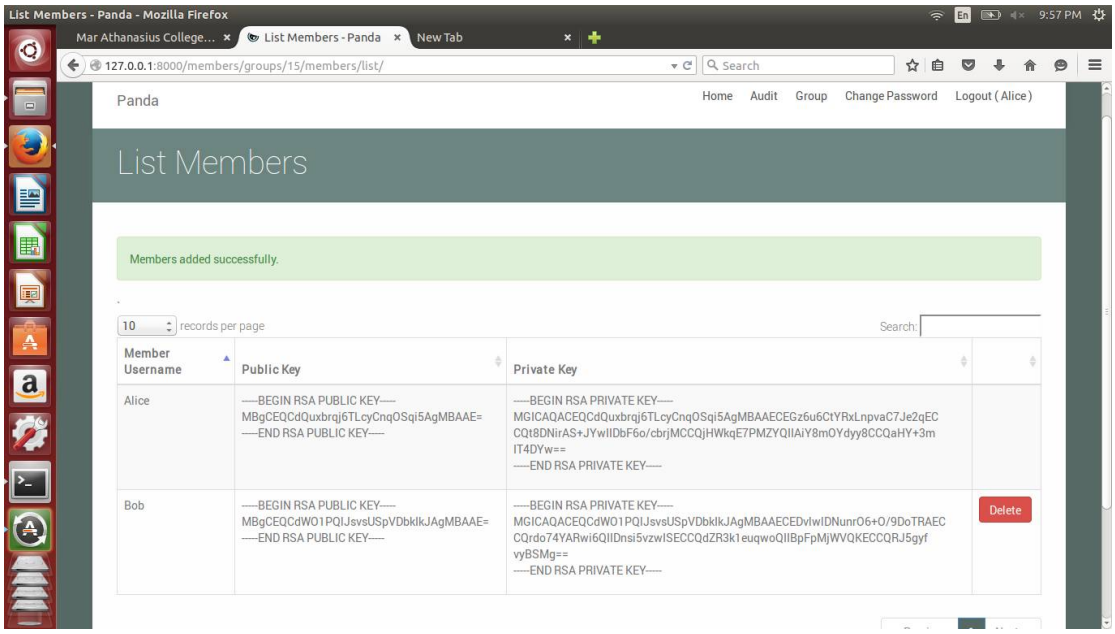

Fig 6: Screenshot showing the List Members

There is list showing the details of the file uploaded in the group. The details include an identification number which is used for auditing purpose, the name of the user who uploaded the file, name of the file, download option and the signature of the user who uploaded the file.

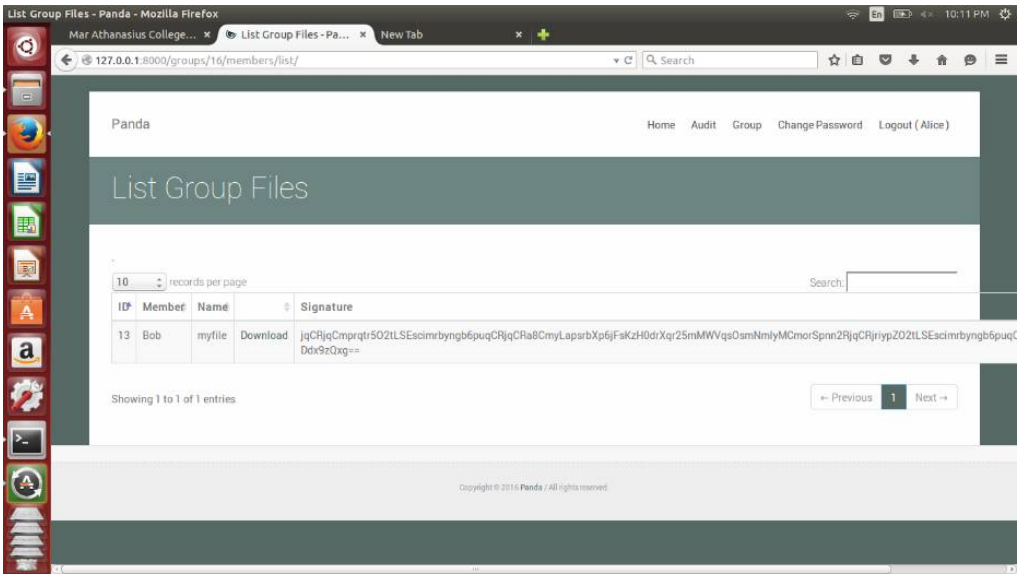

Fig 7: Screenshot showing List Group Files.

There are certain privileges possessed by the manager of the group. The manager is the only person who can delete any member of the group. If the manager itself leaves the group, automatically the group will no longer exist. The manager

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

can also delete the file uploaded by other users whereas the other group members can only delete those files uploaded by themselves.

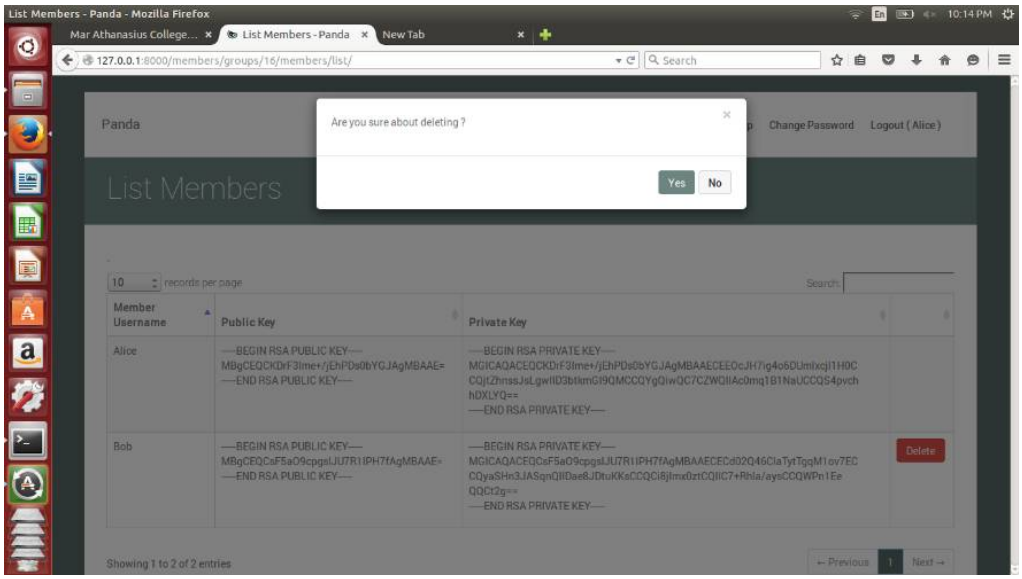

Fig 8: Screenshot showing User Revocation.

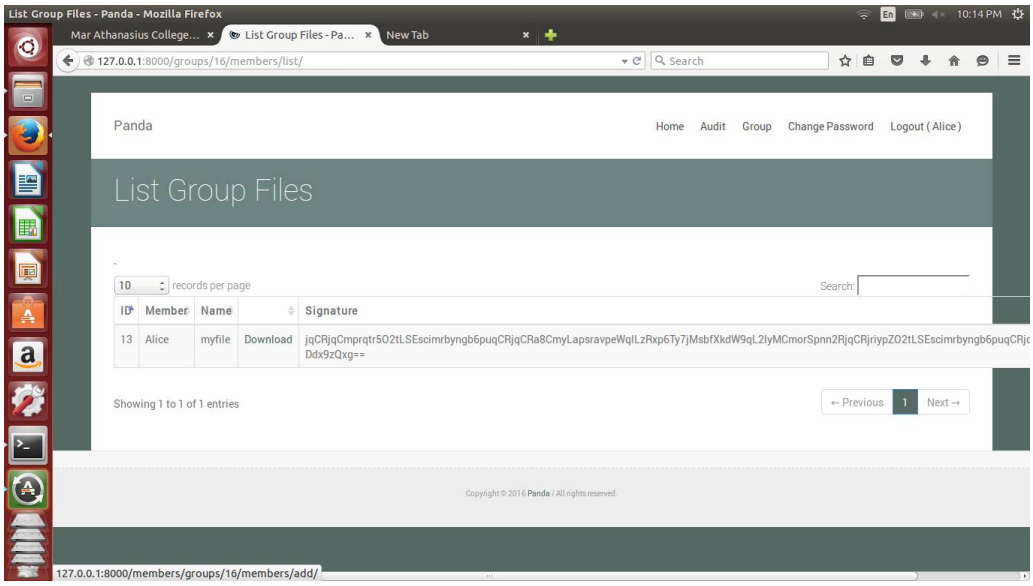

Fig 9: Screenshot showing List Group Files after User Revocation.

When a user misbehaves in the group, the manager of that group has the right to revoke the misbehaved user from the group. While performing user revocation, the files which were previously signed by a revoked user must now be signed by the manager. For this purpose the paper uses the concept of new proxy re-signature schemes wherein the cloud itself performs the resigning during user revocation. This increases the efficiency by great means.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

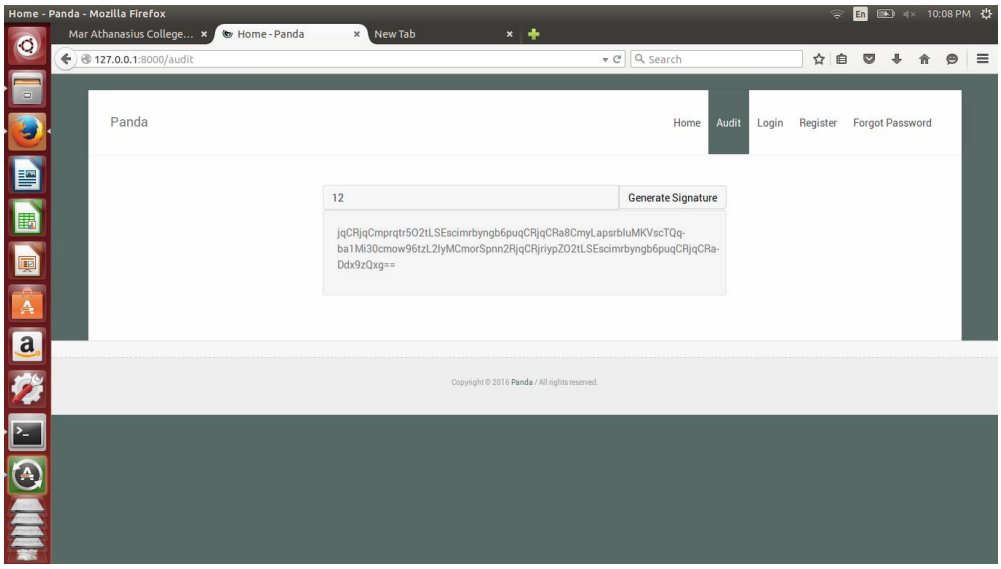

Fig 10: Screenshot showing the process of auditing.

Another major aspect of this paper is the ability to perform public auditing. Just by providing very few information, the integrity of shared data can be verified. The public verifier can either a member of the group or it can be a third party auditor. The third party auditor does not need to register in-order to perform auditing. In this paper, for performing auditing, the identification number of the file to be audited is to be entered on the space provided. On clicking the generate signature button, if the file is valid, a signature is generated which is similar to the signature present of the file on which auditing was performed. If there does not exist such a file, no signature will be generated.

D. EFFICIENT AND SECURE USER REVOCATION

This method is efficient because during user revocation the cloud is able to re-sign the blocks which were previously signed by the revoked user. Therefore the existing user need not have to download the blocks, re-compute the signatures and upload new signatures. Since the cloud itself performs the re-signing, this scheme improves the efficiency of user revocation thereby reducing the communication and computational overhead. Theorem: For the cloud, it is computationally infeasible to generate a forgery of an auditing proof in Panda as long as the DL assumption holds. Based on the theorem, cloud is not able to generate a valid signature for a block, even with a re-signing key. In addition, once a user is revoked from a group, he/she can no longer generate valid signatures on the common shared data.

IV. LIMITATIONS AND FUTURE WORKS

In the design phase, we make an assumption that there is no collusion between cloud and any user in the group. In our mechanism, cloud possesses a re-signing key. So if the revoked user collude with the cloud, then he can easily access the private key of an existing user. In order to overcome this limitation, a collusion resistant proxy re-signature scheme should be adopted [11]. It can generate re-signing key using the private key of the existing user and public key of the revoked user. This prevents the revoked user from accessing the private key of an existing user by colluding with the cloud. However, designing such collusion resistant scheme which supports public auditing at the same time remains to be seen. Generally these schemes have two levels of signatures. First level is signed by an existing user, whereas the second level is resigned by the proxy. The format of two levels of signatures are different and they need to be verified differently. But verifying them together in a public auditing scheme is a challenging one. This is left for our future work.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

V. CONCLUSION

In this paper, we proposed a new mechanism that allows efficient user revocation with public auditing for shared data in the cloud. When a user is removed from the group, we allow the cloud to re-sign the block which were previously signed by the revoked user by using the proxy re-signature schemes. This helps to improve the performance of the system by reducing the communication and computation resources required.

REFERENCES

[1] B. Wang, B. Li, and H. Li, Public Auditing for Shared Data with Efficient User Revocation in the Cloud, Proc. IEEE INFOCOM, pp.2904-2912, 2013.
[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, A View of Cloud Computing, Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, Provable Data Possession at Untrusted Stores, Proc. 14th ACM Conf. Computer and Comm. Security (CCS07), pp. 598-610, 2007.
[4] H. Shacham and B. Waters, Compact Proofs of Retrievability, Proc. 14th Intl Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT08), pp. 90- 107, 2008.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, Ensuring Data Storage Security in Cloud Computing, Proc. 17th ACM/IEEE Intl Workshop Quality of Service (IWQoS09), pp. 1-9, 2009.
[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing, Proc. 14th European Conf. Research in Computer Security (ESORICS09), pp. 355-370, 2009.
[7] C. Wang, Q. Wang, K. Ren, and W. Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, Proc. IEEE INFOCOM, pp. 525-533, 2010.
[8] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds, Proc. ACM Symp. Applied Computing (SAC11), pp. 1550-1557, 2011.