International Journal of Innovative Technologies
WWW.IJITECH.ORG
ISSN 2321-8665
Vol.04,Issue.01,
January-2016,
Pages:0041-0047

Securing Shared Data in Public Cloud with User Revocation

SARA HAMEED[1], SARA ALI[2], SALEHA FARHA[3]

[1]PG Scholar, Dept of CSE, Shadan Women's College of Engineering and Technology, Khairtabad, Hyderabad, TS, India.
[2]Assoc Prof, Dept of CSE, Shadan Women's College of Engineering and Technology, Khairtabad, Hyderabad, TS, India.
[3]HOD, Dept of CSE, Shadan Women's College of Engineering and Technology, Khairtabad, Hyderabad, TS, India.

Abstract: In today's Computing world Cloud computing is one of the biggest innovation which uses advanced computational power and it improves data sharing and data storing capabilities. Main difficulty in cloud computing was issues of data integrity, data privacy and data access by un authorized users. Modification and sharing of data is quite simple as a group. To verify integrity of the shared data, members in the group needs to compute signatures on all shared data blocks. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. User revocation is one of the biggest security threats in data sharing in groups. During user revocation shared data block signed by revoked user needs to download and re-sign by existing user. This task is very inefficacious due to the large size of shared data blocks on cloud. PANDA Plus is the new public auditing mechanism for the maintaining integrity of shared data with efficient user revocation in the cloud. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Moreover, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

Keywords: Public Auditing, Shared Data, User Revocation, Cloud Computing.

I. INTRODUCTION

Cloud service providers manage an enterprise-class infrastructure that offers a scalable, secure and reliable environment for users, at a much lower marginal cost due to the sharing nature of resources. It is routine for users to use cloud storage services to share data with others in a team, as data sharing becomes a standard feature in most cloud storage offerings, including Drop box and Google Docs. The integrity of data in cloud storage, however, is subject to skepticism and scrutiny, as data stored in an untrusted cloud can easily be lost or corrupted, due to hardware failures and human errors. To protect the integrity of cloud data, it is best to perform public auditing by introducing a third party auditor (TPA), who offers its auditing service with more powerful computation and communication abilities than regular users. The first provable data possession (PDP) mechanism to perform public auditing is designed to check the correctness of data stored in an untrusted server, without retrieving the entire data. Moving a step forward, Wang et al. (referred to as WWRL in this paper) is designed to construct a public auditing mechanism for cloud data, so that during public auditing, the content of private data belonging to a personal user is not disclosed to the third party auditor.

We believe that sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage. A unique problem introduced during the process of public auditing for shared data in the cloud is how to preserve identity privacy from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a higher valuable target than others. For example, Alice and Bob work together as a group and share a file in the cloud. The shared file is divided into a number of small blocks, which are independently signed by users. Once a block in this shared file is modified by a user, this user needs to sign the new block using her public/private key pair. The TPA needs to know the identity of the signer on each block in this shared file, so that it is able to audit the integrity of the whole file based on requests from Alice or Bob. With shared data, once a user modifies a block, she also needs to compute a new signature for the modified block. Due to the modifications from different users, different blocks are signed by different users. For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group.

As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group. Therefore, although the content of shared data is not changed during user revocation, the blocks, which were previously

signed by the revoked user, still need to be re-signed by an existing user in the group. As a result, the integrity of the entire data can still be verified with the public keys of existing users only. Since shared data is outsourced to the cloud and users no longer store it on local devices, a straightforward method to re-compute these signatures during user revocation (as shown in Fig. 1) is to ask an existing user (i.e., Alice) to first download the blocks previously signed by the revoked user (i.e., Bob), verify the correctness of these blocks, then re-sign these blocks, and finally upload the new signatures to the cloud. However, this straightforward method may cost the existing user a huge amount of communication and computation resources by downloading and verifying blocks, and by re-computing and uploading signatures, especially when the number of re-signed blocks is quite large or the membership of the group is frequently changing. To make this matter even worse, existing users may access their data sharing services provided by the cloud with resource limited devices, such as mobile phones, which further prevents existing users from maintaining the correctness of shared data efficiently during user revocation.

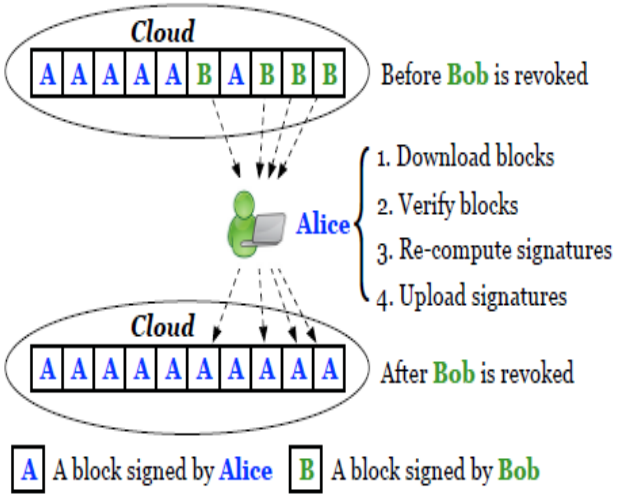

Fig.1. Alice and Bob share data in the cloud. When Bob is revoked, Alice re-signs the blocks that were previously signed by Bob with her private key.

As shown in Fig. 1, after performing several auditing tasks, some private and sensitive information may reveal to the TPA. On one hand, most of the blocks in shared file are signed by Alice, which may indicate that Alice is an important role in this group, such as a group leader. On the other hand, the 8-th block is frequently modified by different users. It means this block may contain high value data, such as a final bid in an auction, that Alice and Bob need to discuss and change it several times. As described in the example above, the identities of signers on shared data may indicate which user in the group or block in shared data is a higher valuable target than others. Such information is confidential to the group and should not be revealed to any third party. However, no existing mechanism in the literature is able to perform public auditing on shared data in the cloud while still preserving identity privacy. In this paper, we propose Panda, a novel public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. In our mechanism, by utilizing the idea of proxy re-signatures, once a user in the group is revoked, the cloud is able to resign the blocks, which were signed by the revoked user, with a re-signing key (as presented in Fig. 2). As a result, the efficiency of user revocation can be significantly improved, and computation and communication resources of existing users can be easily saved.

Meanwhile, the cloud, which is not in the same trusted domain with each user, is only able to convert a signature of the revoked user into a signature of an existing user on the same block, but it cannot sign arbitrary blocks on behalf of either the revoked user or an existing user. By designing a new proxy re-signature scheme with nice properties, which traditional proxy re-signatures do not have, our mechanism is always able to check the integrity of shared data without retrieving the entire data from the cloud. Moreover, our proposed mechanism is scalable, which indicates it is not only able to efficiently support a large number of users to share data and but also able to handle multiple auditing tasks simultaneously with batch auditing. In addition, by taking advantages of Shamir Secret Sharing, we can also extend our mechanism into the multi-proxy model to minimize the chance of the misuse on re-signing keys in the cloud and improve the reliability of the entire mechanism.

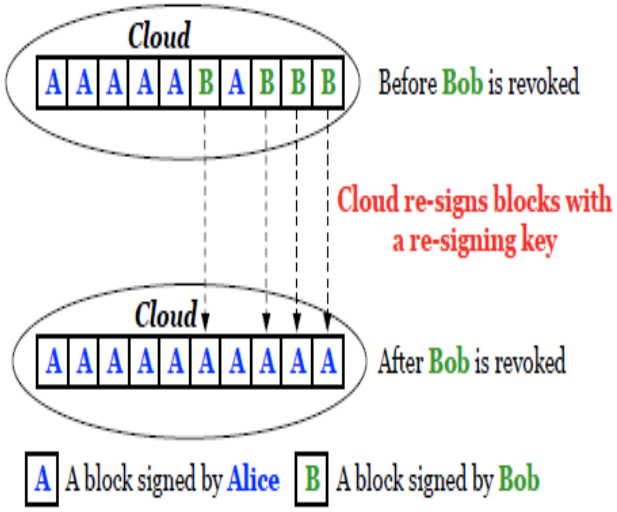

Fig.2. When Bob is revoked, the cloud re-signs the blocks that were previously signed by Bob with a resigning key.

The remainder of this paper is organized as follows: In Section 2, we present the Techniques Used for Public Auditing. Literature Survey in Section 3. Project Description in Section 4 and conclude this paper in Section 5.

II. TECHNIQUES USED FOR PUBLIC AUDITING

To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage so that users may resort to an independent

third-party auditor (TPA) to audit the outsourced data when needed. The TPA can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. Moreover, in addition to help users to evaluate the risk of their subscribed cloud data services, the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud-based service platform, and even serve for independent arbitration purposes. In a word, enabling public auditing services will play an important role for this cloud economy to become fully established; where users will need ways to assess risk and gain trust in the cloud. Recently, the notion of public audit ability has been proposed in the context of ensuring remotely stored data integrity under different system and security models. A brief survey of various techniques has been discussed further.

A Privacy Preserving Policy-Based Content Sharing in Public Clouds is implemented using a Broadcast Group Key Management (BGKM) scheme. An attribute based access control mechanism is developed whereby a user is able to decrypt the contents if and only if its identity attributes satisfy the content provider's policies, whereas the content provider and the cloud learn nothing about user's identity attributes. The mechanism is fine-grained in that different policies can be associated with different content portions. A user can derive only the encryption keys associated with the portions the user is entitled to access. But in this approach the size of the encrypted database is not constant with respect to the original database size. Redundant encryption of the same record is required to support attribute-based access control policies (acps) involving disjunctions. Another public auditing mechanism for shared data is implemented with efficient user revocation in the Cloud. This mechanism implements integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, the cloud can perform to re-signing of blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves.

In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, the mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. But with this mechanism if a revoked user is able to collude with the cloud, which possesses a re-signing key, then the cloud and that revoked user together can be able to easily reveal the private key of an existing user. To overcome this limitation, some proxy re-signature schemes with collusion resistance in which one can generate a re-signing key with a revoked user's public key and an existing user's private key, can be used. Unfortunately, how to design such type of collusion resistant proxy re-signature schemes while also supporting public auditing, that is, block less verifiability and non malleability remains to be seen. Yet another technique is where a secure multi-owner data sharing scheme is used for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of this scheme are independent with the number of revoked users. But unfortunately this mechanism is not highly efficient in terms of accuracy.

Public Audit ability and Data Dynamics for Storage Security in Cloud Computing can as well be enabled by identifying the difficulties and potential security problems with fully dynamic data updates. In particular, to achieve efficient data dynamics, proof of storage models can be enhanced by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, bilinear aggregate signatures can be used so that a TPA can perform multiple auditing tasks simultaneously. But unfortunately with this mechanism only private data can be verified and hence this mechanism is not efficient. Also high amount of storage space is required. Assurance to the users of the correctness of the data in cloud is an important concern to be addressed. As the data is physically not accessible to the user, the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. Also checking the integrity of data without downloading them, known as public auditing, is as well an effective method as shown in Fig.3. There are various techniques which are being used for privacy preservation and public auditing. Each one is better than other but at the same time all these mechanisms have both advantages as well as disadvantages. Hence it is very much public auditing so that efficient integrity check without losing the identity privacy can be done. A comparison study of these mechanisms will make it simple to choose the best mechanism to perform auditing as well as integrity check.

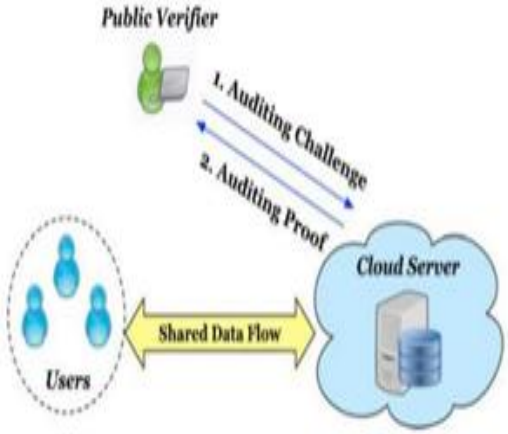

Fig.3. SystemArchitecture.

III. LITERATURE SURVEY

For some years, tools for defending against hackers have been in the form of software to be installed on each device being protected or appliances deployed on-premise.

However, to be effective, such protection needs to be constantly updated. Common methods for ensuring security of data in cloud consist of data encryption (cryptographic process) before storage, authentication process before storage or retrieval and constructing secure channels for data transmission. The protection methods find their routes in cryptographic algorithms and digital signature techniques. The cryptographic algorithms are classified into two categories: symmetric and asymmetric algorithms. Symmetric algorithm uses a single key known as secret key both for encryption and decryption process whereas asymmetric algorithm uses two keys; one is the public key made available publically and the other one is the private key, which is kept secret used to decrypt the data. Breaking the private key is rarely possible even if the corresponding public key is known well in advance. Examples of symmetric algorithm comprise of Data encryption standard (DES), International data encryption algorithm (IDEA), advanced encryption standard (AES) on the other hand asymmetric key algorithm include RSA algorithm. Asymmetric algorithms are best suited for real world use and provides undeniable advantages in terms of functionality whereas symmetric algorithms is ideally suited for security applications like remote authentication for restricted websites which do not require full-fledged asymmetric set up.

The use of passwords for authentication process is popular among the users but the transmission of messages containing password may be vulnerable to illegal recording by the hackers hence posing a security breach in the system. Some more advanced authentication techniques may employ the concept of single-usage-password where the system may generate challenge token expecting the user to respond with an encrypted message using his secret key which converts the password to some derived value enabling. While using the cryptographic techniques for ensuring data security care should be taken for storing encryption and decryption keys. Rigorous methods should be adopted to prevent insiders and privileged user from gaining access to the encrypted data and decryption key simultaneously. Thus, the importance of SLAs is recognized in this context. The policies responsible for user data protection must be clearly mentioned in the provider's contract. After reviewing the data security requirements following recommendations have been included in multiparty SLA suggested at the end to ensure data security in cloud:

- Encrypted data and decryption key must not be stored at the same place
- Access control techniques should be applicable for malicious insiders and privileged users
- Independent audits must be conducted to access the effectiveness of techniques employed for data storage
- Service providers must abide the ethics and legal laws and should be responsible for discrepancies if any
- Backup and reset methods against system crash and failures.

In many applications, it is desirable to work with signatures that are both short and yet where many messages from different signers are verified very quickly. RSA signatures satisfy the latter condition, but are generally thousands of bits in length. Recent developments in pairing based cryptography produced a number of short signatures which provide equivalent security in a fraction of the space. Unfortunately, verifying these signatures is computationally intensive due to the expensive pairing operation. In an attempt to simultaneously achieve short and fast signatures, it was proved how to batch verify two pairing-based schemes so that the total number of pairings was independent of the number of signatures to verify. On the theoretical side, we introduce new batch verifiers for a wide variety of regular, identity based, group, ring and aggregate signature schemes. Our goal is to test whether batching is practical; that is, whether the benefits of removing pairings significantly outweigh the cost of the additional operations required for batching, such as group membership testing, randomness generation, and additional modular exponentiations and multiplications.

IV. PROJCET DESCRIPTION

A. Implementation

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

B. Modules

- Registration
- File Upload
- Download
- Re-upload
- Unblock module

1. Registration: In this module each user registers his user details for using files. Only registered user can able to login in cloud server.

2. File Upload: In this module user upload a block of files in the cloud with encryption by using his secret key. This ensures the files to be protected from unauthorized user.

3. Download: This module allows the user to download the file using his secret key to decrypt the downloaded data of blocked user and verify the data and re-upload the block of file into cloud server with encryption .This ensure the files to be protected from unauthorized user.

4. Re-upload: This module allow the user to re-upload the downloaded files of blocked user into cloud server with resign the files(i.e) the files is uploaded with new signature

like new secret with encryption to protected the data from unauthorized user.

5. Unblock Module: This module allows the user to unblock his user account by answering his security question regarding to answer that provided by his at the time of registration. Once the answer is matched to the answer of registration time answer then only account will be unlocked.

C. Methodologies

Methodologies are the process of analyzing the principles or procedure for auditing process in shared data in public cloud with efficient user revocation.

D. Snapshots

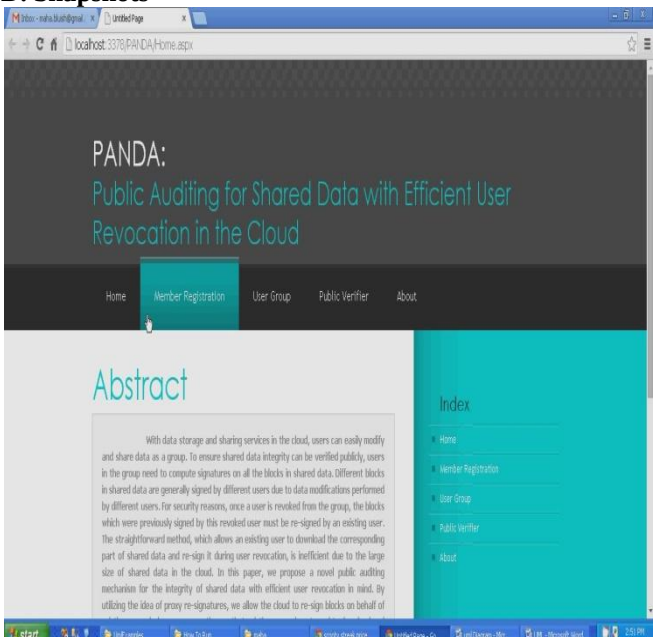

Fig.4.

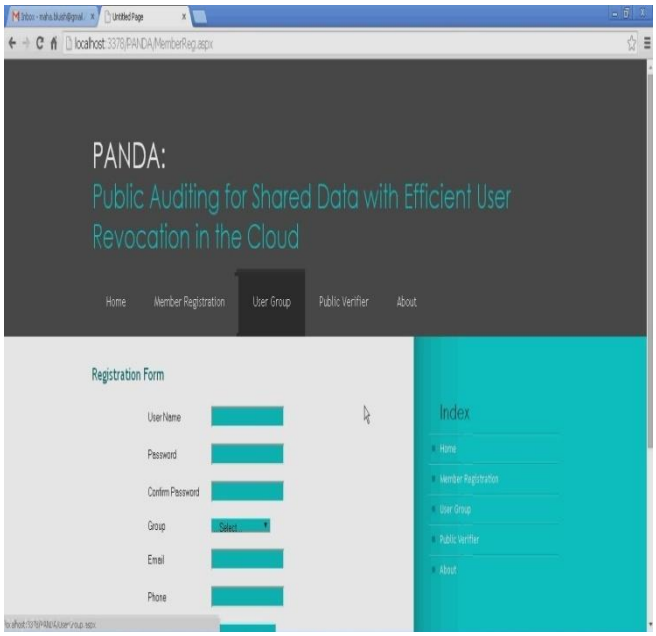

Fig.5.

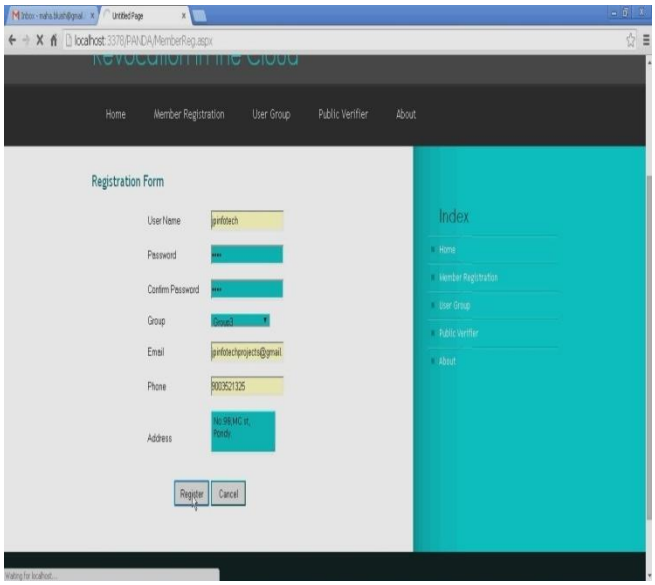

Fig.6.

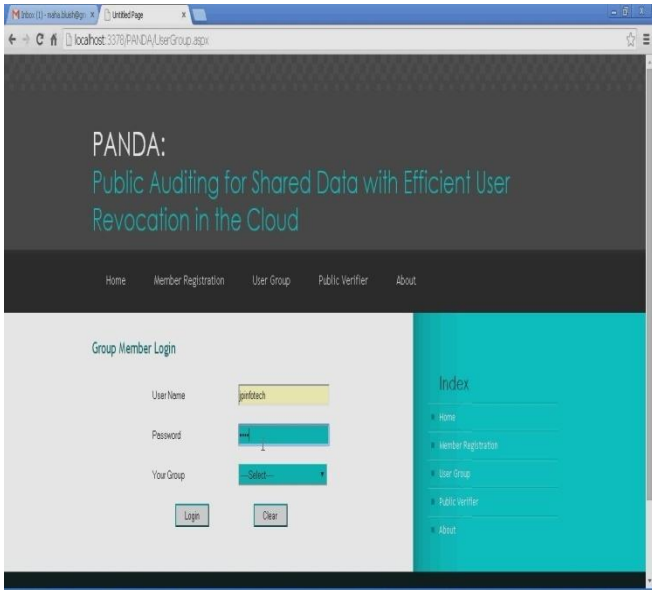

Fig.7.

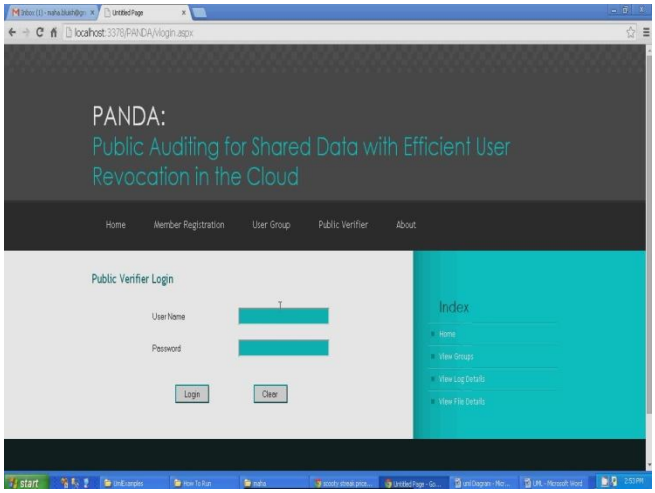

Fig.8.

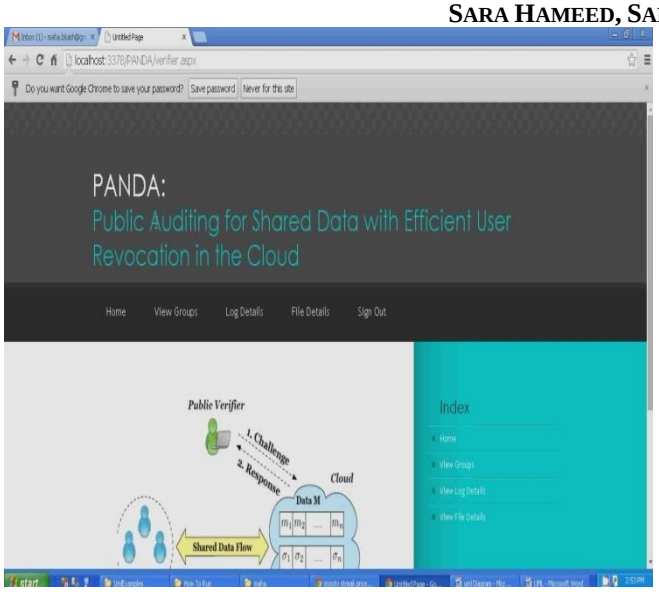

Fig.9.

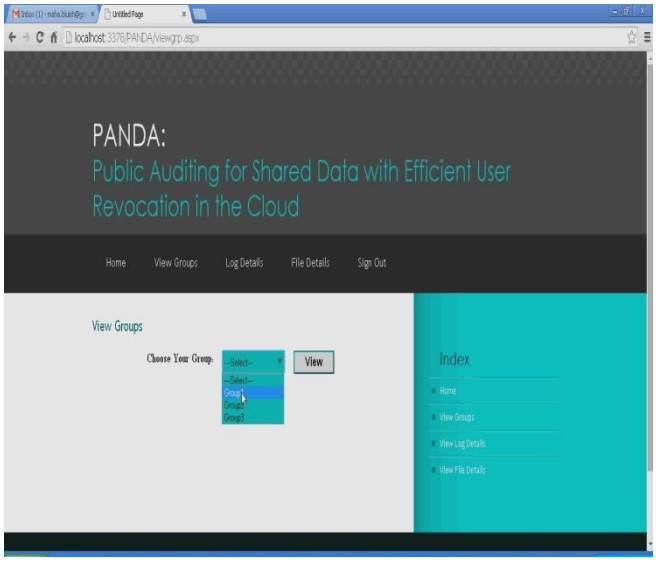

Fig.10.

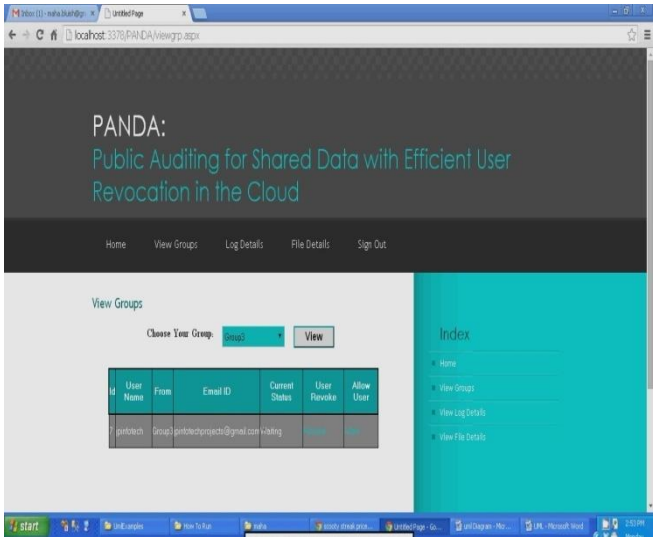

Fig.11.

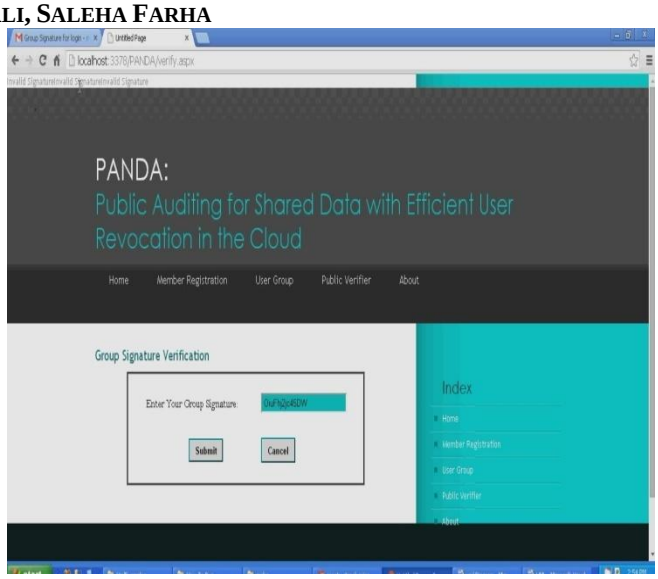

Fig.12.

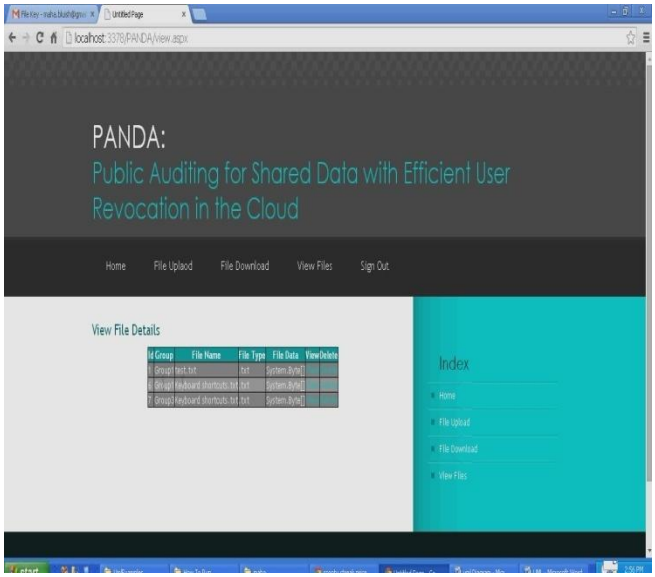

Fig.13.

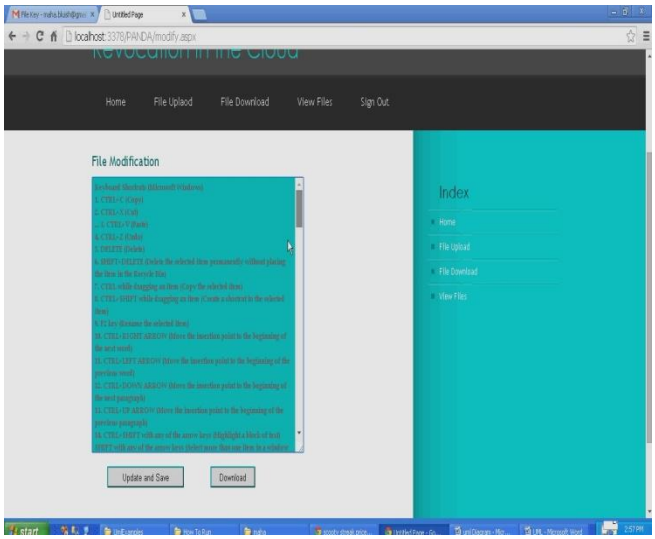

Fig.14.

V. CONCLUSION

In this paper we proposed a new public auditing mechanism for shared data with user revocation in the cloud. Cloud computing is world's biggest innovation which uses advanced computational power and improves data sharing and data storing capabilities. As every coin has two sides it also has some drawbacks. Privacy security is a main issue for cloud storage. To ensure that the risks of privacy have been mitigated a variety of techniques that may be used in order to achieve privacy. It increases the ease of usage by giving access through any kind of internet connection. When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Experimental results show that the cloud can improve the efficiency of user revocation, and existing users in the group can save a significant amount of computation and communication resources during user revocation.

VI. REFERENCES

[1] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE Transactions on Service Computing No: 99 Vol: Pp Year 2014.

[2] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.

[3] 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," Communications of the ACM, vol. 53, no. 4, pp. 50–58, April 2010.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in the Proceedings of ACM CCS 2007, 2007, pp. 598–610.

[5] H. Shacham and B. Waters, "Compact Proofs of Retrievability," in the Proceedings of ASIACRYPT 2008. Springer-Verlag, 2008, pp. 90–107.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IW QoS 2009, 2009, pp. 1–9.

[7] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533.

[9] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in the Proceedings of ACM SAC 2011, 2011, pp. 1550–1557.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.

[11] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, "Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Transactions on Services Computing, accepted.

[12] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.

Author's Profile:

Sara Hameed Presently pursuing Masters in Technology-Computer Science Engineering (JNTUH) from Shadan Women's College of Engineering and Technology, Khairtabad, Hyderabad, T.S, India. She is doing research work on "Securing Shared Data in Public Cloud with User Revocation." under the guidance of Sara Ali.

Ms. Sara Ali has completed her B.E (Computer Science Engineering) from Muffakham Jah College of Engineering &Technology and M.Tech (Information Technology) from IIT Bangalore. She worked in I.T industry for four years and has two years of experience in teaching field. Currently, she is working as the Associate professor in the I.T department in Shadan Women's College of Engineering & Technology, Khairtabad, Hyderabad, T.S, India.

Ms.Saleha Farha has completed her B.Tech (Computer Science Engineering) and M.Tech (Software Engineering) from JNTUH University, Hyderabad. She has five years of experience in teaching field. Currently, she is working as the Head of CSE Department in Shadan Women's College of Engineering and Technology, Hyderabad, T.S, India