PUBLIC AUDITING FOR SHARED DATA WITH EFFECTIVE USER REVOCATION IN THE CLOUD STORAGE

I.Arockia Antonysamy

Assistant Professor, Department of M.C.A.,St.Xavier's College (Autonomous),
Tamil Nadu - India

ABSTRACT: With data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straight forward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, the author proposes a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, the author allows the cloud to resign 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, 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.

1. INTRODUCTION

With data storage and sharing services (such as Dropbox and Google Drive) provided by the cloud, people can easily work together as a group by sharing data with each other. More specifically, once a user creates shared data in the cloud, every user in the group is able to not only access and modify shared data, but also share the latest version of the shared data with the rest of the group. Although cloud providers promise a more secure and reliable environment to the users, the integrity of data in the cloud may still be compromised, due to the existence of hardware/ software failures and human errors [2], [3]. To protect the integrity of data in the cloud, a number of mechanisms [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15] have been proposed. In these mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures. One of the most significant and common features of these mechanisms is to allow a public verifier to efficiently check data integrity in the cloud without downloading the entire data, referred to as public auditing (or denoted as Provable Data Possession [3]).

This public verifier could be a client who would like to utilize cloud data for particular purposes (e.g., search, computation, data mining, etc.) or a third-party auditor (TPA) who is able to provide verification services on data integrity to users. Most of the previous works [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13] focus on auditing the integrity of personal data. Different from these works, several recent works [14], [15] focus on how to preserve identity privacy from public verifiers when auditing the integrity of shared data. Unfortunately, none of the above mechanisms considers the efficiency of user revocation when auditing the correctness of shared data in the cloud. With shared data, once a user modifies a block, he/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 [16]. 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.

2. LITERATURE SURVEY

Cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about overprovisioning or underprovisioning. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1,000 servers for one hour costs no more than using one server for 1,000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT [2].

G. Ateniese et.al, proposed Provable Data Possession at untrusted Stores**.** They introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. They verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation [3].

In [6] Q. Wang et.al, discussed about Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing. They first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for seamless integration of these two salient features in their protocol design. In particular, to achieve efficient data dynamics, they improve the Proof of Retrievability model [1] by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication.

In existing mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures. One of the most significant and common features of these mechanisms is to allow a public verifier to efficiently check data integrity in the cloud without downloading the entire data, referred to as public auditing. This public verifier could be a client who would like to utilize cloud data for particular purposes or a third party auditor (TPA) who is able to provide verification services on data

integrity to users. 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.

Disadvantages of Existing System

- Straightforward method may cost the existing user a huge amount of communication and computation resources.
- The number of re-signed blocks is quite large or the membership of the group is frequently changing.

3. PROPOSED SYSTEM

In this paper, the author proposes 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 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. The overall system architecture is shown in the Fig 1.

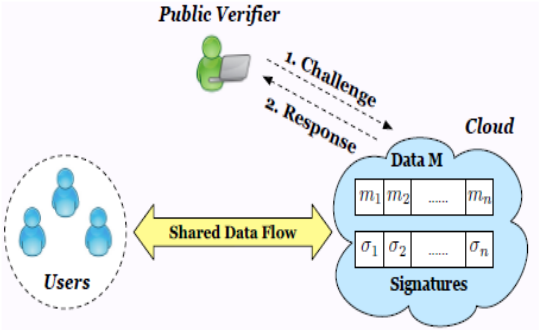

Fig.1 System Architecture

The System Modules are

A. Authorization and Authentication
B. Cloud Data Sharing
C. Data Utilization
D. User Revocation
E. Public Auditing

A. Authentication and Authorization

In this module the User have to register first, then only he/she has to access the data base. After registration the user can login to the site. The authorization and authentication process facilitates the system to protect itself and besides it protects the whole mechanism from unauthorized usage. The Registration involves in getting the details of the users who wants to use this application.

B. Cloud Data Sharing

The Admin initially creates shared data in the cloud, and shares it with groups. All the members of the group can view the shared data. Every member of the group is allowed to access and modify their shared data. Shared data and its verification metadata (i.e., signatures) are both stored in the cloud server. The original user (i.e., admin) shares cloud data to group users.

C. Data Utilization

Each user in the group is able to perform an insert, delete or update operation on a block, and compute the new ring signature on this new block in Modify. They can view others data as well. But they cannot modify the data.

D. User Revocation

Users can revocate the group. 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.

E. Public Auditing

The public auditing system of data storage security in cloud computing and provide a privacy-preserving auditing protocol. Our scheme enables an external auditor to audit user's cloud data without retrieving the entire data from the cloud. Shared data and its verification metadata (i.e., signatures) are both stored in the cloud server. A public verifier, such as a third party auditor providing expert data auditing services or a data user outside the group intending to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server.

Advantages of Proposed System:

- It follows protocols and does not pollute data integrity actively as a malicious adversary.
- Cloud data can be efficiently shared among a large number of users, and the public verifier is able to handle a large number of auditing tasks simultaneously and efficiently.

4. RESULTS

The author implements PANDA using java and jsp. First the Admin in PANDA is register with username and password. After registration the admin can login into the cloud.

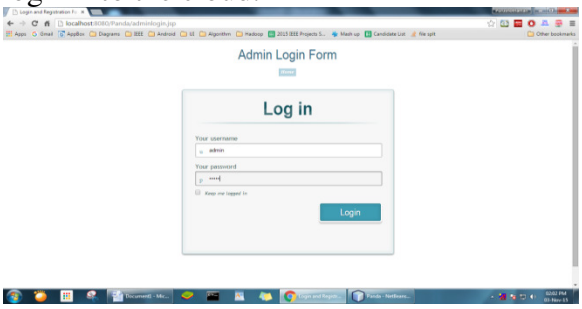

Fig.2 Login Form

Admin can create the group as shown in the Fig.3.

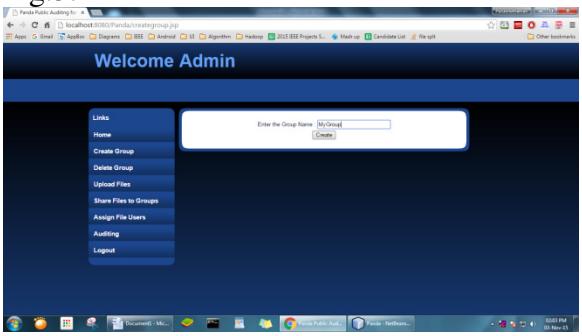

Fig.3 Group Creation

Admin can also delete the group as shown in the Fig.4.

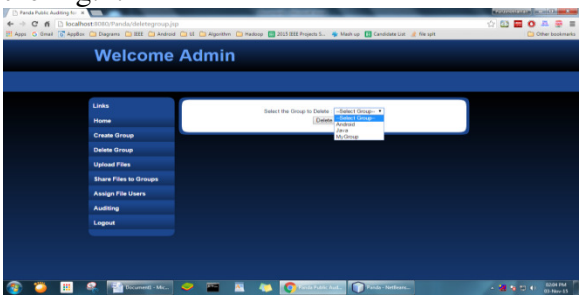

Fig.4 Group Deletion

The Admin can upload files in the group as shown in the figure Fig.5.

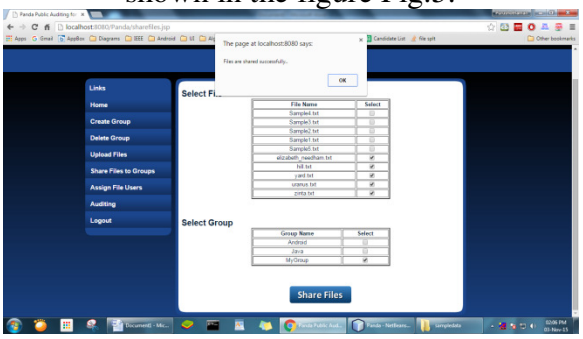

Fig.5 Upload Files

Now the user can register with the mail id. Then login with the user name and the password during the registration.

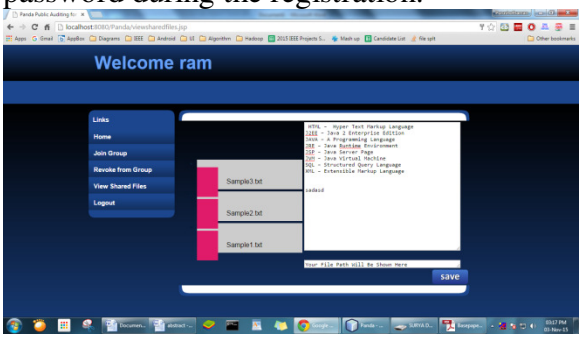

Fig.6 User View the Uploaded File

Then the user can join any group and select the file to view. The user may also revoke from the group when they want.

5. CONCLUSION AND FUTURE WORK

In this paper, the author proposed a new public auditing mechanism for shared data with efficient user revocation in the cloud. 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. Since this project is all about sharing files to friends perform computer actions the project has been designed keeping in mind the future scopes. What we have aimed and achieved creating is not a product but a tool to a better automotive environment, a tool can be used to shape many things in the future, thus this project will give rise to many future modifications forking in all directions.

REFERENCE

[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 (CCS'07), pp. 598-610, 2007.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'08), 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 Int'l Workshop Quality of Service (IWQoS'09), 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. esearch in Computer Security (ESORICS'09), 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 (SAC'11), pp. 1550-1557, 2011.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Jan. 2012.

[10] Y. Zhu, G.-J. Ahn, H. Hu, S.S. Yau, H.G. An, and C.-J. Hu "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Trans. Services Computing, vol. 6, no. 2, pp. 227-238, Apr.- June 2013.

[11] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, pp. 693-701, 2012.

[12] J. Yuan and S. Yu, "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud," Proc. ACM Int'l Workshop Security in Cloud Computing (ASIACCS-SCC'13), pp. 19- 26, 2013.

[13] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing, vol. 6, no. 4, pp. 551-559, Oct.- Dec. 2013.

[14] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE CLOUD, pp. 295-302, 2012.

[15] S.R. Tate, R. Vishwanathan, and L. Everhart, "Multi-User Dynamic Proofs of Data Possession Using Trusted Hardware," Proc. Third ACM Conf. Data and Application Security and Privacy (CODASPY'13), pp. 353-364, 2013.