A Novel Approach for Public Auditing for Shared Data using Cloud

Miss. Pooja R. Mandal[1] Mr. Nikhil P. Jadhav[2] Prof. Archana H. Renushe[3]
[1,2,3]Department of Computer Science and Engineering
[1,2,3]DACOE Karad, Satara, Maharastra, India

Abstract— With sharing services and data storage in the cloud, the users in group can easily modify the data and restore in the cloud. Users are working in a specific groups, as project are different the users working in different groups respectively. No users can share or access data through different groups, users can share data and access the data belongs to same group. When a user register for the cloud its generate a signature which divide into blocks. For security reasons once a user revoked from the group by public verifier, the blocks which were previously signed by this revoked user must be resigned by a existing user. In this paper, we propose the mechanism of public auditing mechanism to maintain integrity of Data as well as security of shared data user efficient user revocation. In addition public verifier can audit the integrity of shared data. Experimental results show that our mechanism can significantly improves efficiency of user revocation.

Keywords: shared Data, User revocation, cloud computing

I. Introduction

With the sharing services and storage data in the cloud, users can share and modify data within a group. User have to register to cloud with unique id. After registration of user, user's account will be activated when the public verifier will activated the user after that only a user can shared or modify the data through the cloud in a group. User can upload and download data, user can view the shared data of other users which are shared in that group.

To ensure the integrity of data in the cloud a number of mechanisms have been proposed. In these mechanisms, the signature were devoted to the each blocks in data, the integrity of data relies on correctness of all signatures. The most common features of these mechanisms is the public verifier have to check the data integrity efficiently without downloading the entire data. Different from these works, several recent works concentrate on how to preserve identity privacy from public verifiers when auditing the integrity of shared information. Unfortunately, none of above mechanism, consider the efficiency of user revocation when auditing the correctness of shared data in the cloud.

Based on the new proxy re-signature scheme and its properties in the existing System, we now present Public Auditing Shared Data using ECSDA and RSA-PKCS Algorithm. In our project, the original user acts as the group manager, who is able to revoke users from the group when it is necessary. Meanwhile, the cloud is allow to perform as the semi-trusted proxy and convert signatures for users in the group with resigning keys. As emphasized in recent work, for security reasons, it is necessary for the cloud service providers to store data and keys separately on different servers inside the cloud in practice. Therefore, it is assume that the cloud has a server to store shared data, and has another server to manage resigning keys. To ensure the privacy of cloud shared data at the same time, additional mechanisms can be utilized. The main focus of this project is to audit the integrity of cloud shared data.

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 Figure. 1 is to verify an a existing user i.e., Alice to download the blocks previously signed by the revoked user i.e., Bob, verify the correctness of these blocks, then re-sign the blocks, and finally upload the new generated signatures to the cloud. This straightforward method may cost the existing user a large amount of transmission and computation resources by downloading and verifying blocks, and by re-computing and uploading signatures, especially when the large number of re-signed blocks or the membership of the group is frequently changing. To create 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 information efficiently during user revocation.

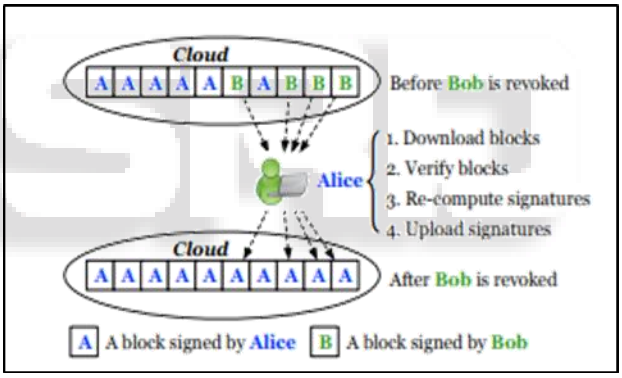

Fig. 1: Alice and Bob share data in the cloud. When Bob is revoked, Alice re-signs the blocks that were previously signed by Bob with her private key.

Apparently, if the could carry each user's private key, it can easily complete the re-signing task for existing users beyond asking them to download and re-sign blocks. However, since the cloud is not in the similar faithful domain with each user in the group, utilize every user's private key to the cloud would introduce denoting security issues. Another important issue we need to consider is that the re-computation of any signature during user revocation should not disturb the most interesting property of public auditing — auditing data integrity publicly without retrieving the whole information. Therefore, how to efficiently overcome the significant load to existing users introduced by user cancellation, and still allow a public verifier to check the integrity of shared data without downloading the entire data from the cloud, is a face off work. In this paper, we propose, a novel public auditing mechanism for shared data with efficient user revocation using cloud. In our mechanism, by applying the concept 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 Figure. 2). As a conclusion, the efficiency of user revocation can be significantly enhanced, and computation and communication resources of existing users can be easily saved. Concurrently, the cloud, who is not in the similarly 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 similar block, but it cannot sign random blocks on behalf of either the revoked user or an existing user. By designing a new proxy re-signature scheme with good properties, which traditional proxy re-signatures do no 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

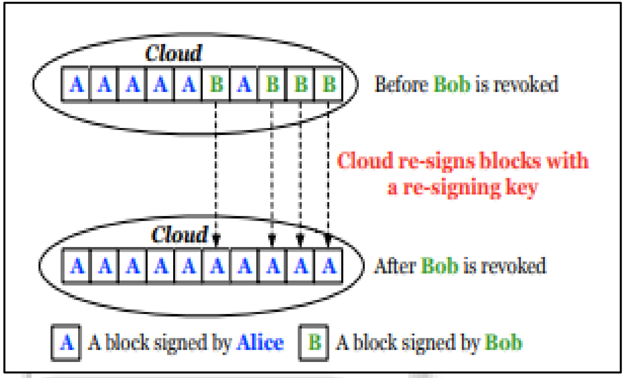

Fig. 2: When Bob is revoked, the cloud re-signs the blocks that were previously signed by Bob with a resigning key

II. PROBLEM STATEMENT

To ensure integrity of shared data with efficient user revocation, there is no efficient technique to resign block automatically and maintain its integrity. By applying the concept of proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation i.e. we can avoid download and re-sign blocks by themselves. We propose a novel public auditing mechanism for shared data with efficient user revocation in cloud.

III. PROPOSED SYSTEM ARCHITECTURE

As shown in figure 3, the system model has 3 entities user, public verifier, cloud. In this system architecture the user are working in a group they are sharing data using cloud. The data which are shared by other users in that group can be viewed by other user who belongs to that group. When data is uploaded in the cloud the data is splitted into 3 blocks and generates the signature and stored in the cloud. When data is uploaded it is uploaded by using private key and when the data want to download it uses a public key. A user cannot view or access data of other user which belongs to another group. Public verifier can check consistency of each file/data on cloud using respective user's public key ie it checks each files blocks for consistency.

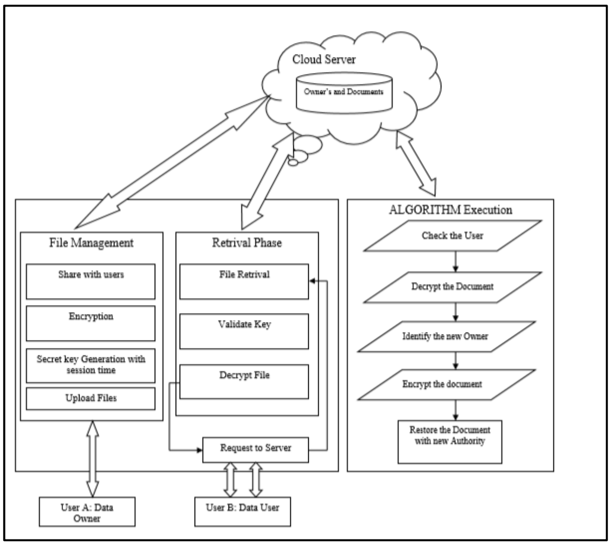

Fig. 3: System Architecture of Public Auditing for Shared Data using Cloud.

In user Revocation, User will download file and make changes and resign data and update to cloud Once user revoked by verifier or owner, verifier or owner will automatically resign their modified blocks with new signature i.e. revoked user cannot access previous unauthorized/inaccessible data.

IV. DESIGN OBJECTIVES

Our proposed mechanism must achieve the following properties: (1) Correctness: The public verifier is able to correctly check the purity of shared data. (2)Efficient and Secure User Revocation: On one hand, once a user is removed from the group, the blocks signed by the revoked user can be efficiently re-signed. On the other hand, only existing users in the group can create legal signatures on shared data, and the revoked user can no longer figure out legal signatures on shared data. (3) Public Auditing: The public verifier can analyze the purity of shared data without retrieving the whole data from the cloud, even if a few blocks in shared data have been re-signed by the cloud. (4) Scalability: Cloud data can be efficiently shared among a huge number of users, and the public verifier is able to handle a huge number of auditing event concurrently and efficiently.

V. IMPLEMENTATION DETAILS

A. Algorithm 1: ECDSA

1) Elliptic Curve Digital Signature Algorithm (ECDSA)

Elliptic Curve Digital Signature Algorithm is a one of the algorithm used for cryptography by Bitcoin to make sure that treasure can only be spent by their appropriate owners.

2) A few concepts related to ECDSA:

- Private Key: The person who generate it and keeps secret for its own purpose. In Bitcoin, someone with the private key that corresponds to treasure on the block chain can spend the treasure.
- Public key: Public key is used by anyone to encrypt data so that on other side it can be decrypted by other user by using its private key but it cannot be vise versa.

- Signature: Signature is a mathematical calculation which is generated to identify the authority of user. To ensure that authorized user is accessing the data.

B. Algorithm 2: RSA Algorithm

RSA Algorithm is an asymmetric cryptography algorithm which uses two different keys but mathematically linked keys. As it uses two different keys for cryptography it becomes more secure, one is public key and another is private key public key is shared by everyone and the private key must kept secret. It provides a method to ensure the confidentiality, integrity, authenticity, and non-repudiation of communications and data storage.

VI. Conclusion

In this project, we proposed a novel public auditing mechanism for the integrity of shared data with efficient user revocation using two secure algorithm ECDSA and RSA-PSS algorithm. To protect the integrity of shared data, each block in shared data is attached with a signature, once a user modifies a block, he/she must resign the modified block. When a user in the group is removed, we allow the semi-trusted cloud to re-sign blocks that were signed by the removed user with proxy re-signatures. Cloud can improve the efficiency of user revocation so that existing users in the group can save a significant amount of computation and communication resources during user revocation.

Acknowledgment

I take this opportunity to express my gratitude to my guide Prof. Archana H. Renushe, Co-ordinator Prof. Sayali P. Shinde, and the head of the department Prof. Ashish N. Patil, Department of Computer Science and Engineering, DACOE Karad, Shivaji University, for their kind cooperation and guidance during the entire research work.

References

[1] 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.

[2] M. Armburst, A. Fox, R. Griffith, A. D. Joseph, R. H. Kartz, A. Knowinski, G.Lee, D. A. Patterson, A. Rabkin, I. Stocia, and M. Zaharia, "A view of Cloud Computing," Communication of the ACM, vol.53,no. 4,pp. 50-58. April 2010.

[3] 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.

[4] B. Wang, S. S. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via SecurityMediator," in Proceedings of IEEE ICDCS 2013, 2013

[5] The Java Pairing Based Cryptography (jPBC) Library Benchmark. [Online]. Available: http://gas.dia.unisa.it/projects/ jpbc/benchmark.html

[6] J. Yuan and S. Yu. Efficient Public Integrity Checking for Cloud Data Sharing with Multi-User Modification. [Online]. Available: http://eprint.iacr.org/2013/484

[7] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," in the Proceedings of ASIACRYPT 2001. SpringerVerlag, 2001, pp. 514– 532.

[8] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in the Proceedings of ICST SecureComm 2008, 2008.

[9] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in the Proceedings of ACM CCS 2009, 2009, pp. 213–222.