Paper ID:CSEIT20

VERIFICATION OF MULTI-OWNER SHARED DATA WITH USER REVOCATION AND COLLUSION RESISTANCE IN CLOUD COMPUTING

Dipali S. Kasunde
Ms. A. A. Manjrekar
Computer Science and technology Department of Technology, Shivaji University, Kolhapur, India

Abstract—Cloud enables its users to easily store and share the data with each other. Due to the security threats in a cloud, users are not assured about the integrity of their data. Users are recommended to compute the signatures on their data for the verification of integrity. Many mechanisms are proposed to verify the integrity of the single owner shared data rather than multi-owner data. Proposed system provides public auditing on multi-owner shared data. When user is revoked from the group, blocks signed by revoked user must be resigned. Proposed system also provides efficient user revocation with collusion resistance i.e. even if cloud colludes with any users; it is not able to learn the contents of the stored data.

Keywords—Cloud computing; data integrity; user revocation; collusion.

I. INTRODUCTION

Cloud is the latest and fast growing technology which provides the resources to its users dynamically via the internet. NIST provides most widely used definition of cloud computing as "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. network, servers, storage, application and services) that can be rapidly provisioned and released with minimal management effort and service provider interaction".

Cloud storage is one of its services which provide a logical pool to store the digital data. It provides easy, cost effective and reliable way to manage the data. With cloud storage and sharing services (e.g. Google Drive, Dropbox) people can work together as a group and share the data with each other. Cloud computing enables its users to store the data as well as share the data with each other. When user creates the shared data, user not only accesses and modifies the data but also shares the data with other users. Since shared data accessed and modified by multiple users, it faces the challenges of maintaining the integrity of shared data. Various techniques are proposed to check the integrity of shared data [3], [4]. These techniques recommends to attach the signature to each block of data and their integrity depends on the correctness of the all the signatures. These mechanisms allow public verifier or third party auditor (TPA) to check the integrity of shared data.

Most of the work proposes techniques to verify the integrity of single owner shared data rather than multi-owner data. Multi-owner data is the data where each block is signed by the multiple users. Multi-owner shared data can be found in many real situations such as checking correctness of the financial records stored in cloud is valid only if all members of board committee are confirmed, patient's e-health records are further utilized only if both patient and his doctor(s) are approved and signed. In a group of users sharing the data, when user modifies a block, he/she needs to compute the signature on that modified block. So with multiple owners blocks are signed by multiple owners in the group. When any user leaves the group he/she must be revoked from the group and blocks signed by this revoked user must be resigned. Most of the previous work assumed that the cloud is semi-honest i.e. cannot be colluded with any untrusted or revoked user. In collusion attack, cloud is able to learn the contents of the shared data conspiring with revoked user.

II. LITERATURE REVIEW

Cloud storage a significant service of cloud computing which provides to its users an easy, cost effective and reliable way to manage the data. It also enables the users to share the data with each other by working as a group. Since shared data can be accessed and modified by multiple users and the group membership can be changed frequently, it faces the challenge of maintaining the integrity of shared data. Several schemes are proposed to ensure the integrity of the shared data.

G. Ateniese et al. [3] proposed a model for Provable Data Possession scheme which 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 the proofs of possession by sampling random sets of blocks from the server. The client maintains the verification metadata to verify the proof.

H. Shacham [4] et al. provides a provably secure proof of irretrievability system. This system allows compact proofs with one authenticator value. It provides two solutions; first one is privately verifiable and built on pseudorandom functions; second allows public verifiable proofs and based on the signature scheme.

B. Wang et al. [6] proposed a novel public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. This system utilizes the concept of proxy re-signature, once a user in the group is revoked; the cloud is able to resign the blocks, which were signed by the revoked user with resigning key. This method assumes single owner data rather than multi-owner data.

T. Jiang et al. [7] figured out the collusion attack in the existing scheme and provided an efficient public auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature. This scheme considers single owner data than a multi-owner data.

B. Wang et al. [10] proposed a novel public verification to audit the integrity of multi-owner data in an untrusted cloud by taking advantage of multi-signatures. It proposes a novel multi-signature scheme with blockless verifiability and then utilizes as a building block to construct the public verification mechanism on the integrity of multi-owner data in the cloud.

X. Liu et al. [2] presented a secure multi-owner data sharing scheme named Mona. It achieves fine grained access control and revoked users will not be able to access the sharing data again once they are revoked. However, the scheme will easily suffer from collusion attack by the revoked user and cloud.

III. SYSTEM PRELIMINARIES

The following basic equations and concepts will be used in system implementation.

A. Bilinear Mapping

Let be a multiplicative cyclic group of prime order p and g be its generator. The bilinear map e is defined as follows: e: . The bilinear map e has the following properties:

- Computability

There exists an efficient algorithm for computing map e

- Bi-linearity

, e(,)=e (3)

- Non-degeneracy

e(g, g)≠1 (4)

B. Computational Diffie-Hellman (CDH)Assumption

For any probabilistic polynomial time adversary , the advantage of adversary on solving the CDH problem in is negligible, which is defined as

Pr[(g, ,) = ( ): a,b ≤e (5)

It is also said that computing the CDH problem in is computationally infeasible or hard under the CDH assumption.

C. Descrete Logarithmic(DL) Assumption

For any probabilistic polynomial time adversary , the advantage of adversary on solving the DL problem in is negligible, which is defined as

Pr[(g,) = (a): a ≤e (6)

Similarly, we can also say computing the DL problem in G1 is computationally infeasible or hard under the DL assumption.

IV. PROPOSED SYSTEM

Proposed system will consist of the three main entities: group of multiple users, public verifier and the cloud. Group consists of multiple users which will share the data with each other; they can be multi-owner of the data. It consists of one group manager which is responsible for the system parameter generation, user registration and user revocation. Remained users in the group are the set of registered users that will store their own data into the cloud and share them with each other. Public verifier could be a client which utilizes the data for specific purpose or a third party auditor (TPA) which provides verification services on data integrity to users using challenge and response protocol with users. Cloud provides data storage and sharing services to the group users. Proposed system model for auditing with user revocation is as shown in fig.1: Figure 1 describes the following modules:

- Key Generation and Authentication
- Signature generation
- Data sharing
- Public auditing
- User revocation and collusion resistance

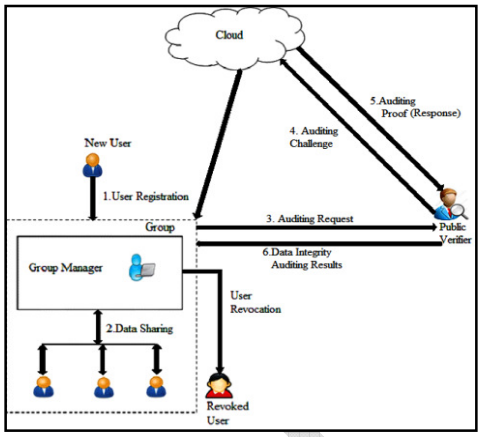

Fig.1. Proposed System Model which provides public auditing with user revocation

A. Key Generation and Authentication

Assuming the security parameters based on the bilinear mapping each user will generate a pair of public key and private key. Authentication includes new user registration.

New User Registration: In this step user will send its identifier and public key as a request to the group manager for group membership. On receiving the request from user, group manager will reply it with the verification message. After few verification steps group manager will add the user in the user list (UL). Group manager will sign the user list with its own signature and send it to the cloud. Cloud verifies and stores the list. After successful registration user will become the group member.

B. Signature Generation

Let d be the total number of owners which can also be group members. Data M is divided into n blocks as { ,…, } and each block has an identifier , for j ∈ [1,n]. Given block m and its identifier id, each owner will compute individual signature and upload to the cloud. After receiving d individual signatures { ,.., } on block m, the cloud will output

= (1)

and attach it to the block as in fig 2.

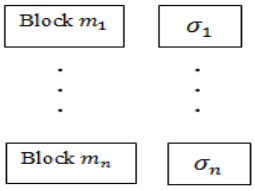

Fig. 2. Blocks signed with multi-signature[10]

Block identifier identifies index of the block in data file. Public keys will be used in the computation and verification of signatures.

C. Data Sharing

Here owner of the data will share data with its group members. Google cloud storage service will be used to store the files and share with the group. It includes the file uploading, file downloading and modification.

When group members will upload the file, it will sign with its own signature and will send this signed file to the group manager. Group manager will decrypt and check whether it is legal user. Group manager selects random re-encryption key, encrypts the ciphertext and sends it to the cloud along with its own signature. Cloud will also verify the group manager.

When group user wants to download the file, it will send the request to the cloud along with identifier of the data file which is encrypted with its own key. As cloud receives the request it will verify the user and if it is, it will send the data file to the respective user.

In modification of data file user will attach its own signature with the block of a file.

D. Public Auditing

Any group member in the group can generate the request to verify the integrity of shared data to the public verifier. Public verifier will generate an auditing request (challenge) and send it to the cloud server. After receiving an auditing message the cloud server will return a proof of verification to the public verifier as auditing response. Public verifier will make the use of all the public keys $\{PK_1,\ldots, PK_d\}$ and verification proof sent by the cloud server, compute the

$$PK_S = \prod_{i=1}^{d} PK_i \qquad (2)$$

It will output 1 for the correctness and 0 otherwise. Public verifier will send this data integrity result to the requestor who wants to verify the integrity.

E. User revocation and Collusion Resistance

When user is revoked from the group, there should be re-computation of signatures on blocks of data which are signed by the revoked user. This module will use the idea of proxy multi-signature [13, 14]. The proxy signer will take all the public keys of the users (except revoked user) and re-compute the proxy signature.

System will protect the collusion attack i.e. cloud will not get the original data file even if they compromise with the revoked user. When user will be revoked from the group, group manager will remove this user from the list and update the data files to the cloud encrypted with new re-encryption key. As the revoked user could not recover re-encryption key cloud will not be able to learn the content of the stored data file. Even if they will recover or collude it contradicts with the Computational Diffie Hellman Assumption (CDH) and Discrete Logarithm (DL) assumption [6]. So the system will be collusion resistant.

System will be analyzed based on the security preliminaries such as Computational Diffie-Hellman (CDH) assumption and Discrete Logarithm assumption (DL).

V. CONCLUSION

Cloud storage is one of the most prominent service of Cloud computing. But with advantages of cloud storage it has some problems related to the integrity of data in the cloud.

This paper proposes the system which will verify the integrity of multi-owner shared data. When users are working as a group, there should be mechanism to revoke the users. This paper proposes the novel user revocation method while auditing the integrity of shared data. In collusion attack cloud is able to learn the contents of shared data colluding with untrusted or revoked user. It also discusses the method to avoid collusion attack with efficient user revocation.

REFERENCES

[1] Meena, S. ; Karunya Univ., Coimbatore, India ; Daniel, E. ; Vasanthi, N.A.,"Survey on various data integrity attacks in cloud environment and the solutions" Circuits, Power and comp. Techno.(ICCPCT), 2013 Int. Conf.,Mar 2013.

[2] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems (TPDS'13), vol. 24, no. 6, pp. 1182-1191, June 2013.

[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] B.Wang, B. Li, H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE Trans. On Services Computing, Vol. 8, No. 1, Jan/Feb 2015.

[7] T. Jiang, X. Chen, and J. Ma,"Public Integrity Auditing for shared Dynamic Cloud Data with Group User Revocation", IEEE Trans on Computers, 2015.

[8] J. Yuan, S. Yu, "Public Integrity Auditing for Dynamic Data Sharing with Multi-User Modifiaction", IEEE Trans. On Infor. Forens. And Sec., 2015.

[9] Jingwei Li, Jin Li, Dongqing Xie and Zhang Cai,"Secure Auditing and Deduplicating Data in Cloud", IEEE Trans. on Computers, 2015.

[10] Boyang Wang, Hui Li, Xuefeng Liu,Fenghua Li, and Xiaoqing Li, "Efficient Public Verification on the Integrity of Multi-Owner Data in the Cloud", IEEE Jour. Of Comm. And Netw.,Vol. 16, No. 6, Dec 2014

[11] Boyang Wang, Baochun Li, and Hui Li, "Oruta: Privacy preserving Public Auditing for Shared Data In the Cloud", IEEE Trans. On Cloud Computing, Vol.2, Issue:1,Issue Date:March2014

[12] Boyang Wang, Sherman S. M. Chow, Ming Li and Hui Li," Storing Shared Data on the Cloud via Security-Mediator",IEEE 33rd Inter. Conf. on Distributed Computing System, 2013.

[13] Feng Cao, Zengfu Cao, "A Secure Identity Based multi-proxy Signature scheme", Elsevier, computers and Electrical engineering 35 (2009) 86-95.

[14] Xiangxue Li *, Kefei Chen, "ID-Based multi-proxy signature, multi-signature and multi-proxy multi-signature schemes from bilinear pairings", Elsevier-Applied Mathematics and Computation 169 (2005) 437-450.

Zhongma Zhu, Rui Jiang, "A secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Trans. On Parallel and Distributed Systems, 2013.