RECORD MAINTENANCE AND SECURE PRESERVING OF SHARED DATA IN PUBLIC AUDITING

Abstract

In this paper we believe that sharing data among multiple users enhances cloud storage we provide security among multiple users for sharing integrity of data. Here we are using ring signatures for providing hash values and also to check the hash values where the data canbe divided into number of blocks. Hash values providing public verifier and HARS for authenticated ring signatures also provides meta decryption for correctness of data or scalable data. public cloud will provide logical and physical servers which store large amount of data .it uses authorized and also provides Saas for service providers. Largest storage device provided by cloud computing.

Keywords: *Secure Preserving, Public Auditing, Shared Data, Cloud Computing, TPA*

----------***----------

1. INTRODUCTION

cloud computing provides services like Iaas, Paas, Saas, DBaas for providing the integrity of shared data for cloud users. I cloud provides authorized users for accessing the Saas to compute large amount of data. this cloud also provides skepticism and scrutiny. In record maintenance and secure preserving of shared data for public auditing providing oruta i.e one ring to rule them all for providing hash values. data can be lost due to hardware or software failures. integrity of data in cloud storage is subject to uncertainly. here we are using user, owner ,tpa for public auditing of shared data. cloud service providers may be unwilling to inform users about these data errors in order to maintain the good status of services and avoid profit loss. Therefore the integrity of data should be verified before any utilization of data. The comparison among different mechanisms as shown in table1.where public auditing can be used as provable data possession and also checked for WWRL it is also used as one ring rule them all for checking the correctness of data. Identity privacy and data privacy can be provided for different mechanism of the secure preserving of public auditing.

TABLE 1
Comparison among Different Mechanisms

	PDP [9]	WWRL [5]	Oruta
Public Auditing	√	√	√
Data Privacy	X	√	√
Identity Privacy	X	X	√

2. ARCHITECTURE

2.1 System Model

In this model we introduce three parties: the cloud server, a group of users and a public verifier. and also it uses two types of users which creates shared data in the cloud and shares it with cloud servers and group users. tpa checking services for publicly verify it first sends an auditing challenge i.e. response from pv to cs and after receiving auditing challenge the cloud server will send request to pv to verify and learn that it is the proxy signs the data.

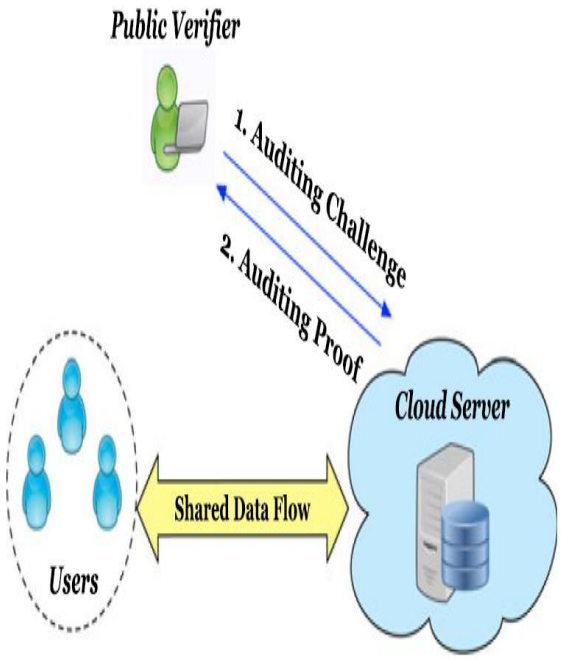

Fig 1: System model

2.2 Threat Model

2.2.1 Integrity Threats

In this model the software or hardware failures and human errors can be corrupted.

2.2.2 Privacy Threats

The data can be divided into blocks that can be signer on each block for providing integrity of shared data in cloud storage and hence it provides confidential data for the users.

3. DESIGN OBJECTIVES

Our mechanism is to provide without loss of data providing security (1) Public Auditing: without modifying the data for public checking the data can be retrieved. (2) Correctness: public verifier should provide scalable data for correctness of data (3) Enforceability: user in the group data can be used as signatures. (4) security: A public verifier cannot differentiate the identity of the signer on each block for public checking.

4. CONSTRUCTION OF HARS

 HARS contains three algorithms: Key Gen, Ring Sign and Ring Verify.
KeyGen: this key provides public and private key for authorization of users.

 Ring Sign: users in the group will provide private key for generation of block verification.

 Ring Verify: It is used to verify the signer on each block to check ring signatures**.**

5. PUBLIC AUDITING MECHANISM

The public verifier can check the integrity of shared data without modifying the entire data, for users. it also reduce ring signature for the block to be verified where the group users are cyclic. This mechanism can also support the dynamic operations on secure preserving of shared data for the update operations of the blocks for ring signatures which use the index for the identifier. It also includes security analysis of one ring rule them all for public auditing.

5.1 Batch Auditing

In this mechanism, this can verify the correctness to allow most of auditing proofs to still pass the verification when there exists only a small number of incorrect auditing proofs, we can utilize binary search during batch auditing. sharing a file in the cloud, and a public verifier audits the integrity of shared data with Oruta.

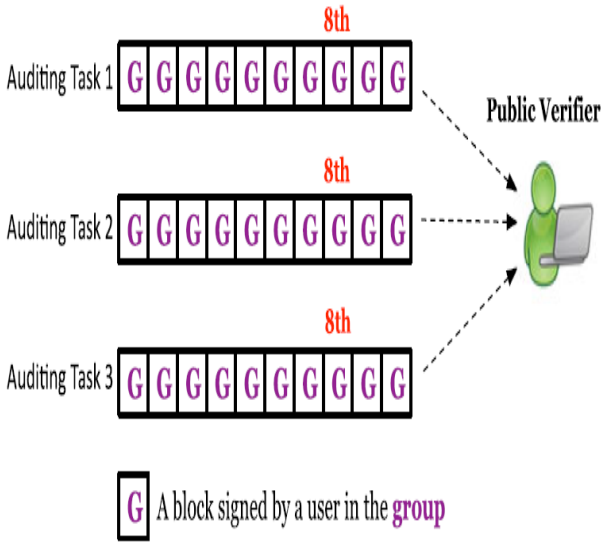

Fig 2: Auditing tasks

Authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. public auditor may share multiple auditing tasks for scalable data .batch auditing better improves the efficiency.

REFERENCES

[1] 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.

[2] Juels and B.S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597, 2007.

[3] 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.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

[5] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.

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

[7] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 514-532, 2001.