Sharing of Data Using Privacy Preserving Public Auditing in Cloud

S.Monika
Department of Information Technology, Velammal Engineering College, Chennai.
Email: pavithrapt1998@gmail.com
S.Pavithra
Department of Information Technology, Velammal Engineering College, Chennai.
Email: monikadevi560gmail.com

ABSTRACT

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 data shared. With our mechanism, the identity of the user 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 was able to perform multiple auditing tasks simultaneously instead of verifying them one by one. The propose system, a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism 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.In order to improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing.Our future work will be based on these two interesting problems. One of them is traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations.

I. INTRODUCTION

In Cloud service providers offer users efficient and scalable data storage services with a much lower marginal cost than that traditional approaches. The shared file was divided into a number of small blocks and each block is independently signed by one of the two users

with existing public auditing solutions. Once a block in this shared file was modified by a user, this user needs to be signed by the new block using his/her private key. Eventually, different blocks are signed by different users due to the modification introduced by these two different users.In order to correctly audit the integrity of the entire data, a public verifier needs to be chosen the appropriate public key for each block (e.g., a block signed by Alice can only be correctly verified by Alice's public key). As a result, this public verifier will inevitably learn the identity of the signer on each block due to the unique binding between an identity and a public via digital certificates under public key infrastructure (PKI).

In this paper, to solve the above privacy issue on shared data, we propose Oruta,1 a novel privacy-preserving public auditing mechanism. Public verifier was able to verify the integrity of shared data without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier.

II. EXISTING SYSTEM

In the existing mechanism a new significant privacy issue introduced in the case of shared data with the use of the leakage of identity privacy to public verifiers. The traditional approach for checking data correctness was to retrieve the entire data from the cloud, and to verify data integrity by checking the correctness of signatures.

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met:

- TPA should be able to efficiently audit data storage in cloud without demanding the local copy of data, and introduce no additional on-line burden to the cloud data privacy.
- The third party auditing process should have no new vulnerabilities towards user

III. DISADVANTAGE OF THE EXISTING SYSTEM

- As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted.
- They do not perform the multiple auditing tasks in simultaneously.
- Loss of data's.
- Does not provide any privacy for private data's.
- Authentication time takes too long.

IV. PROPOSED SYSTEM

The propose system, a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism 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.

In order to improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. Our future work will be based on the following, One of them is traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations.

Stands for "Simple Mail Transfer Protocol." this can be the protocol used for causation e-mail over the web. Your e-mail shopper uses SMTP to send a message to the mail server, and also the mail server uses SMTP to relay that message to the proper receiving mail server. Basically, SMTP could be a set of commands that certify and direct the transfer of electronic message. Once configuring the settings for your e-mail program, you always ought to set the SMTP server to your native net Service Provider's SMTP settings. However, the incoming mail server (IMAP or POP3) ought to be set to your mail account's server, which can differ than the SMTP server.

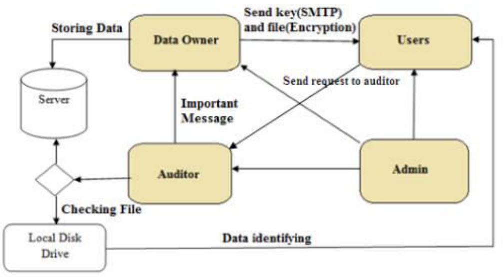


Fig 1-work flow of proposed system.

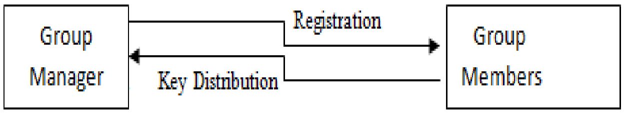
V. MODULES

Four modules are used in this system.

- User Registration.
- Public Auditing.
- Sharing Data.
- Integrity Checking.

5.1 User Registration

For the registration of user with identity ID the group manager randomly selects a number and the group manager adds into the group user list which will be used in the traceability phase. After the registration phase, user obtains a private key which will be used for group signature generation and file decryption.



5.2 Public Auditing

Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, we had proposed to uniquely integrate the Homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF). The proposed scheme is as follows:

- Setup phase
- Audit phase

5.3 Sharing Data

The canonical application is data sharing. The public auditing property is especially useful when we expect the delegation to be efficient and flexible. The schemes enable a content provider to share her data in a confidential and selective way, with a fixed and small ciphertext expansion, by distributing to each authorized user a single and small aggregate key.

5.4 Integrity Checking

Hence, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now we show how our main scheme can be adapted to build upon the existing work to support data dynamics, block level operations of modification, deletion and insertion. We can adapt this technique in our design to achieve privacy-preserving public auditing with support of data dynamics.

5.5 Advantages

- The proposed system can perform multiple auditing tasks simultaneously.
- They improve the efficiency of verification for multiple auditing tasks.
- High security provided for file sharing.
- Admin has control deleting users.
- Users can send request to auditor.

VI. CONCLUSION

We propose a privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute the verification of 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 secured 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 parallely instead of verifying them one by one.
The propose system, a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism 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 testing multiple auditing tasks, we further extend our mechanisms to support batch auditing. There are two interesting problems we will continue to study in our future work. One of them is traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations.

AES is associate degree unvarying instead of Feistel cipher. It's supported 'substitution–permutation network'. It contains of a series of joined operations, a number of that involve exchange inputs by specific outputs and other involve shuffling bits around.

Interestingly, AES performs all its computations on bytes instead of bits. Hence, AES treats the 128 bits of a plaintext block as sixteen bytes. These sixteen bytes square measure organized in four columns and 4 rows forthe process as a matrix.

VII. References

[1] The MD5 Message-Digest Algorithm (RFC1321). https://tools. ietf.org/html/rfc1321, 2014.

[2] B. Wang, B. Li, and H. Li, "Certificate less Public Auditing for Data Integrity in the Cloud," Proc. *IEEE Conf. Comm. and Network Security (CNS'13),* pp. 276-284, 2013.

[3] C. Wang, S.S. Chow, Q. Wang, K. Ren , and W. Lou, "*Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers,* vol. 62, no. 2, pp. 362-375, Feb. 2013.

[4] 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.