SURVEY ONPRIVACY PRESERVING PUBLIC AUDITING MECHANISM FOR SHARED DATA IN CLOUD COMPUTING ENVIRONMENT

Dr. SuvarnaNandyal[1], Suvarna L. Kattimani[2], Aniruddha A. Atwadkar[3]

[1]Prof &Head of Department of CSE, P. D. A. College of Engineering, Gulbarga, (India)
[2]Assistant Professor, [3]PG Scholar(MTech), Department of CSE,
BLDEA's Dr.P.G.Halakatti College of Engineering &Technology, Vijaypur, (India)

ABSTRACT

In Cloud Computing Environment, data is stored and shared among multiple users. It is very important as well as very challenging job to maintain the integrity of the data. The data stored in the cloud is considered as subject of skepticism and scrutiny as the data is stored in the untrusted cloud. This survey, proposes the new mechanism for public auditing of shared data in the cloud computing environment. This mechanism takes advantage of the ring signatures to compute the signatures used by the users. the correctness of the data is audited using ring signatures and the identity of signer on each block is hidden from the third party auditor(TPA).this mechanism shows the effective auditing on various user's data, who are members of group. This survey shows effectiveness and coherence of auditing the data publicly.

Keywords: Cloud Environment, Dynamic Groups, Public Auditing, Privacy Preserving, Shared Data.

I. INTRODUCTION

1.1 Defining a Cloud Computing

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS).a Some vendors use terms such as IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) to describe their products.

1.2 Classes of Utility Computing

Any application needs a model of computation, a model of storage, and a model of communication. The statistical multiplexing necessary to achieve elasticity and the appearance of infinite capacity available on demand requires automatic allocation and management**.**

1.3 Cloud Storage Integrity

Cloud computing requires comprehensive security solutions based upon many aspects of a large and loosely integrated system. The application software and databases in cloud computing are moved to the centralized large data centers, where the management of the data and services may not be fully trustworthy.A data integrity checking algorithm which eliminates the third party auditing, to protect static and dynamic data from unauthorized observation, modification, or interference.

1.4 Data Correctness in Cloud Environment

The traditional approach for checking data correctness in cloud includes two steps. The first step is to retrieve the entire data from the cloud, and the second step is to verify data integrity by checking the correctness of signatures by RSA or hash values by MD5 of the entire data. Advantage of this approach is able to successfully check the correctness of cloud data. The disadvantage of this approach is efficiency decreased while using this traditional approach on cloud data.

1.5 Cloud Computing Economics

There are two particularly compelling use cases that favor utility computing over conventional hosting. A first case is when demand for a service varies with time. For example, provisioning a data center for the peak load it must sustain a few days per month leads to under-utilization at other times. Instead, cloud computing lets an organization pay by the hour for computing resources, potentially leading to cost savings even if the hourly rate to rent a machine from a cloud provider is higher than the rate to own one. A second case is when demand is unknown in advance.

For example, a Web startup will need to support a spike in demand when it becomes popular.

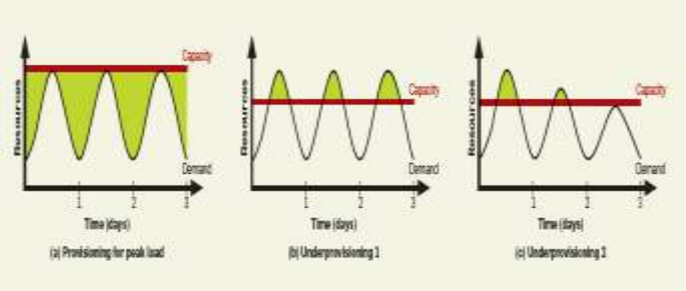

Fig. 1. (A) Waste of Resources Without Elasticity (B) Potential Revenue From Users Not Served. (C) Experiencing Poor Service.

1.6 Public Key Infrastructure

The shared file is divided into a number of small individual blocks, where each block is independently signed by one of the two users with Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing scheme. Once a block in this shared file is modified by a user, that particular user needs to sign the new block using his/her secret private key. Finally, different blocks are signed by various users due to the modification introduced by these different users. Then, in order to correctly audit the integrity or correctness of the entire data, a public verifier needs to choose the suitable public key for each block. Specifically, as shown in Fig. 2, after performing several auditing tasks, thethird party auditor can first learn that Alice may be a more important role in the group because most of the blocks in the shared file are always signed by Alice, on the other hand, this public verifier can also easily deduce that the eighth block may contain data of a higher value (e.g., a final bid in an auction), because this block is frequently modified by the two different users. In order to protect this confidential information, it is essential and critical to preserve identity privacy from third party auditor during public auditing.

As a result, thethird party auditor will inevitably learn the identity of the signer on each block due to the unique binding between an identity and a public key via digital certificates under public key infrastructure (PKI).

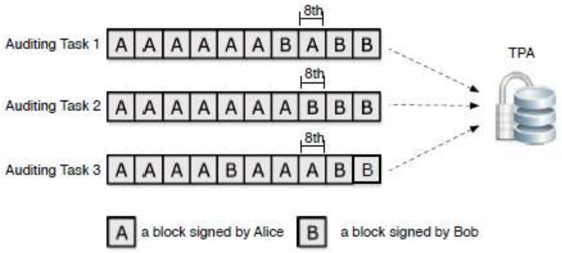

Fig. 2.Alice and Bob Share A File in the Cloud. the TPA Audits the Integrity of Shared Data With Existing Mechanisms.

II. EXISTING MECHANISM

In [1], thedescriptionis about framework for provable data possession. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs.Verifying the authenticity of data has emerged as a critical issue in storing data on untrustedservers. The client maintains a constant amount of metadata to verify the proof.The advantage of this scheme is the verifier is able to publicly audit the integrity of data without retrieving the entire data, which is referred to as public auditing.

Drawback

This mechanism is only suitable for auditing the integrity of personal data.

In [2], author describes about the security challenges cloud computing presents the burden of local data storage and maintenance. Public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor to check the integrity of shared data. The advantage of this mechanism is it eliminates the burden of cloud user from the tedious and possibly expensive auditing task.

Drawback

This mechanism only holds good for single user public auditing task.

In [3], author describes about a dynamic audit service for verifying the integrity of an untrusted and outsourced storage. The audit service is constructed based on the techniques,fragment structure, random sampling and index-hash table,supportingprovable updates to outsourced data, andtimely abnormal detection. Theresults not only validate the effectiveness of approaches, but also show audit system and verifies the integrity with lower computation overhead, requiring less extra storage for audit metadata.

Drawback

Less frequent activities may not detect in a timely manner.

In [4], the author describes about POR’s scheme which is also able to check the correctness of data on an untrusted server. The original file is added with a set of randomly-valued check blocks called sentinels. The verifier challenges the untrusted server by specifying the positions of a collection of sentinels and asking the untrusted server to return the associated sentinel values. Sentinel Based POR protocol is amenable to real-world application.

Drawback

- **Integrity Threats**

First, an adversary may try to corrupt the integrity of shared data. Second, the cloud service provider may inadvertently corrupt (or even remove) data in its storage due to hardware failures and human errors. Making matters worse, the cloud service provider is economically motivated, which means it may be unwilling to inform users about such corruption of data.

- **Privacy Threats**

The identity of the signer on each block in shared data is private and confidential to the group. During the process of auditing, a public verifier, who is only allowed to verify the correctness of shared data integrity, may try to reveal the identity of the signer on each block in shared data based on verification metadata.

In [5], author describes about an efficient PDP mechanism based on symmetric keys. This mechanism can support update and delete operations on data; however, insert operations are not available in this mechanism. It exploits symmetric keys to verify the integrity of data, it is not public verifiable.

Drawback

This scheme provides a user with a limited number of verification requests.

In [6], the author describes about leveraged homomorphic tokens to ensure the correctness of erasure codes-based data distributed on multiple servers. The major contribution of this mechanism is able support dynamic data, identify misbehaved servers.

Drawback

The leakage of identity privacy to public verifiers.

In [7], the author describes about a mechanism for auditing the correctness of data under the multi-server scenario, where these data are encoded by network coding instead of using erasure codes. This scheme minimizes communication overhead in the phase of data repair.

Drawback

This scheme requires bothBoneh–Lynn–Shacham (BLS) signatures and pseudo-random function.

In [8], the author describes about the problem of simultaneously achieving fine grainedness, scalability, and data confidentiality of access control. On one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents.

Drawback

This scheme has computing overhead complexity for cloud servers.

III. ARCHTECTURE

The architecture of proposed system is as shown in fig.3.

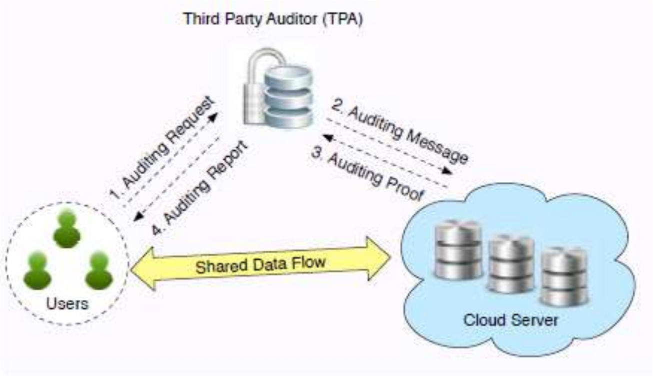

Fig. 3 Verification from TPA to Share the Data to Cloud Users

The proposed model architecture includes users, third party auditor(TPA), cloud server. The user requests for auditing the shared data in cloud by keeping the identity privacy to third party auditor.

The proposed system uses the HARS algorithm, which includes

KeyGen

Each user in the group generates his/her public key and private key.

RingSign

A user in the group is able to generate a signature on a block and its block identifier with his/her private key and all the group members public keys. A block identifier is a string that can distinguish the corresponding block from others.

RingVerify

A verifier is able to check whether a given block is signed by a group.

IV. SUMMARY OF CHARACTERISTICS BETWEENEXISTING SYSTEM AND PROPOSED SYSTEM.

SL. NO	METHODS	EXISTING (Privacy Preserving Public Auditing Scheme)	PROPOSED(ORUTA)
1	Technique	• Provable data possession (PDP) • Proofs of Retrievability (POR) • Dynamic Provable data possession (PDP)	ORUTA(One Ring to Rule Them All)
2	Identity of signer	Kept public to third party auditor	Kept private to third party auditor
3	Auditing task	Single auditing task	Multiple auditing task

V. CONCLUSION

In this paper, the proposed method is used to share data in the cloud. Privacy-preserving public auditing mechanism utilize ring signatures to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data. The scheme cannot differentiate the signer on each block. Our mechanism is used to audit the dynamic groups. To improve the efficiency of verifying multiple auditing tasks.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” in Proc. ACM Conference on Computer and Communications Security(CCS), 2007, pp. 598–610.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.

[3] Y. Zhu, H.Wang, Z. Hu, G.-J.Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage inClouds," in Proc. ACM Symposium on Applied Computing (SAC), 2011, pp. 1550–1557.

[4] A. 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.

[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proc. InternationalConference on Security and Privacy in Communication Networks(SecureComm), 2008.

[6] 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.

[7] 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.

[8] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," in Proc. International Conference on the Theory andApplication of Cryptology and Information Security (ASIACRYPT).Springer-Verlag, 2001, pp. 514–532.