ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Implementation of Privacy Preserving Model for Auditing Data in The cloud

Vinod Suryavanshi, B.S.Hambarde

M.E Student, Dept. of CSE, SRTM University, Nanded, India

HOD, Dept. of CSE, SRTM University, Nanded, India

ABSTRACT: Public auditing for cloud storage is of critical importance as the users relies on semi-trusted cloud storage service for data sharing which does not guarantee/assure the integrity of the data being stored. With public auditing of clouds, users resort to a third party auditor (TPA) who verify and assure the internal consistency/lack of corruption of their data in cloud storage services. Despite the good work previously done by researchers in auditing while preserving privacy, still available mechanisms do not efficiently conceal users' privacy from TPA during sharing of data and yet supporting data and group dynamics. In this paper, we propose privacy preserving auditing scheme that exploits the ring signature to calculate verifications needed to audit data integrity. In this proposed approach, the identities of the user are kept private from public verifier and dynamic groups are supported –that is a new user can be added into the group and an existing group member can be revoked during data sharing

KEYWORDS: Public Auditing, Cloud Storage, Privacy-preserving, shared data, cloud computing.

I. INTRODUCTION

Cloud computing is transforming the nature of how business and people uses information technology today. This computing paradigm shift provides a scalable environment for growing amounts of data and processes that work on various application and services by means of on demand self services. Particularly, the outsourced storage in clouds is a new profit generating area by providing a uniformly low cost, scalable, geographically location-independent platform for managing users' data. The cloud storage services lighten the burden for storage management and maintenance. Nowadays it is a routine for most users to leverage cloud storage services to share data with others in a group, as data sharing becomes a standard features in most cloud storage offerings including Google Drives, iClouds and Dropbox. However, the exciting advantages which are provided by cloud storage services, storing data in a cloud does not give any guarantee on data integrity and availability. Users' data is put at risk of losses or being incorrect during sharing as the cloud service providers are separate administrative distance, out of the control of users. These security risks can be caused by: the internal and external threats in clouds infrastructures, for example there are various motivations for cloud service providers to behave unfaithfully towards the clouds users as well as the dispute due to lack of trust on Cloud storage service. Cloud users may not be aware of this behaviour even if these disputes may results into users own's improper operation [1]. Following these and related challenges, public auditing, in particular privacy preserving one is suggested by researchers as trust worthy solution to be enhanced in cloud storage service so as to check for correctness of users data. In privacy preserving public auditing, the third party auditor is resorted to publicly verify the integrity of users' data stored in clouds before being shared among multiple users without knowing the data and users' identities privacy. A traditional approach provides only public auditing while preserving data privacy. This conventional approach will provide public auditing while keeping private users identities from third party auditor in a dynamic group data sharing environment.

II. EXISTING SYSTEM

Many mechanisms have been proposed to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud[2][3][4], which is referred to as public

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

auditing . In these mechanisms, data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking . A public verifier could be a data user (e.g., researcher) who would like to utilize the owner's data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking services. Moving a step forward, Wang et al. designed an advanced auditing mechanism .So that during public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers. Unfortunately, current public auditing solutions mentioned above only focus on personal data in the cloud .We believe that sharing data among multiple users is perhaps one of the most engaging features that motivates cloud storage. Therefore, it is also necessary to ensure the integrity of shared data in the cloud is correct. Existing public auditing mechanisms can actually be extended to verify shared data integrity. However, a new significant privacy issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to public verifiers. However, a new significant privacy issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to public verifiers.

DISADVANTAGES OF EXISTING SYSTEM**:**

1.Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information to public verifiers.

2.Protect these confidential information is essential and critical to preserve identity privacy from public verifiers during public auditing.

III.**PROPOSED SYSTEM**

To solve the above privacy issue on shared data,Privacy-preserving public auditing mechanism is proposed. More specifically,in this mchanism we utilize ring signatures to construct homomorphic authenticators, so that a public verifier is 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. In addition, we further extend our mechanism to support batch auditing, which can perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks. Meanwhile, this mechanism is compatible with random masking, which has been utilized in WWRL [5]and can preserve data privacy from public verifiers.A high-level comparison among model and existing mechanisms is presented.

ADVANTAGES OF PROPOSED SYSTEM**:**

1.A public verifier is able to correctly verify shared data integrity.

2.A public verifier cannot distinguish the identity of the signer on each block in shared data during the process of auditing.

3.The ring signatures generated for not only able to preserve identity privacy but also able to support blockless verifiability.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

IV .LITERATURE SURAVEY

Sr. No.	Title of the Paper	Methods	Pros	Cons
1.	Privacy Preserving Public Auditing for Secure Cloud Storage.[5]	Homomorphic Linear Authenticator , Random Masking	This method allow Safe public data auditing.	Privacy of data cannot preserve.
2.	Towards Secure and Dependable Storage Services in CloudComputing. [7]	Homomorphic Token along with Distributed Erasure-Coded Data	Audit cloud data with lightweight communication and computation cost	
3.	An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing. sep.[8]	Proof of Retriviabilitywithbilinearityproperty of bilinear paring	Lowcommunication and computation cost	This scheme does not support the efficient preserving privacy for public data auditing of store (shared) data.
4.	Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. May[9]	Message Authenticated code	It provide secure auditing of shared data	High communication and computation complexity.
5.	Oruta: Privacy Preserving Public Auditing for shared Data in the cloud. JanuaryMarch[7]	Homomorphic Authenticatoralong with ringsignature	Perform multiple document verification simultaneously rather than one by one	1. Traceability and data freshness could not check while preserving the identity privacy. 2. Data re-computation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

V. DESIGN OBJECTIVES

To enable the TPA efficiently and securely verify shared data for a group of users, This mechanism should be designed to achieve following properties:
(1) Public Auditing: The third party auditor is able to publicly verify the integrity of shared data for a group of users without retrieving the entire data.
(2) Correctness: The third party auditor is able to correctly detect whether there is any corrupted block in shared data.
(3) Unforgeability: Only a user in the group can generate valid verification information on shared data.
(4) Identity Privacy: During auditing, the TPA cannot distinguish the identity of the signer on each block in shared data.

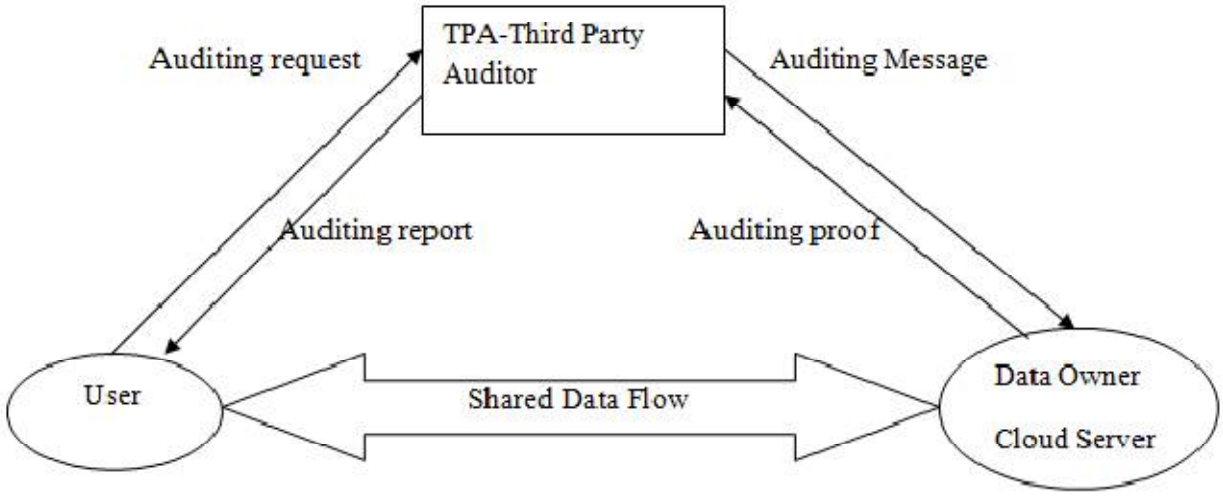

Fig.System Architecture

VI.RING SIGNATURES

Rivest et al. first proposed the concept of ring signatures [4] in 2001. Main core of this paper is ring signature.With ring signatures, a verifier is convinced that a signature is computed using one of group members' private keys, but the verifier is not able to determine which one. More concretely, given a ring signature and a group of d users, a verifier cannot distinguish the signer's identity with a probability more than 1=d. This property can be used to preserve the identity of the signer from a verifier.

Construction of Ring Signature:
It contains three algorithms: KeyGen, RingSignandRingVerify. In KeyGen, each user in the group generates his/her public key and private key. In 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. A verifier is able to check whether a given block is signed by a group member in RingVerify.

VII. CONSTRUCTION

Now, we present the details of our public auditing mechanism.It includes five algorithms: KeyGen, SigGen, Modify, ProofGen and ProofVerify.

1. KeyGen:In this users generate their own public/private key pairs.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

2. SigGen:In this a user (either the original user or a group user) is able to compute ring signatures on blocks in shared data by using its own private key and all the group members' public keys.
3. Modify:Each user in the group is able to perform an insert, delete or update operation on a block, and compute the new ring signature on this new block in Modify.
4. ProofGen:This is operated by a public verifier and the cloud server together to interactively generate a proof of possession of shared data[5].
5. ProofVerify:In this the public verifier audits the integrity of shared data by verifying the proof.

Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be multiplicative cyclic groups of order p, g_1 and g_2 be generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a bilinear map, and $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ be a computable isomorphism with $\psi(g_2) = g_1$. There is a public map-to-point hash function H_1: $\{0,1\}^* \to \mathbb{G}_1$, which can map a string $\{0,1\}^*$ into an element of $\mathbb{G}_1$ (i.e., an point on an elliptic curve). The total number of users in the group is d. The global parameters are $(e, \psi, p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, H_1, d)$.

KeyGen. For a user u_i, he/she randomly picks $x_i \overset{R}{\leftarrow} \mathbb{Z}_p$ and computes $w_i = g_2^{x_i} \in \mathbb{G}_2$. Then, user u_i's public key is $\mathbf{pk}_i = w_i$ and his/her private key is $\mathbf{sk}_i = x_i$.

RingSign. Given all the d users' public keys $(\mathbf{pk}_1, ..., \mathbf{pk}_d) = (w_1, ..., w_d)$, a block $m \in \mathbb{Z}_p$, the identifier of this block id and the private key $\mathbf{sk}_s$ for some s, user u_s randomly chooses $a_i \in \mathbb{Z}_p$ for all $i \neq s$, where $i \in [1, d]$, and let $\sigma_i = g_1^{a_i}$. Then, he/she computes

$$\beta = H_1(id) g_1^m \in \mathbb{G}_1, \quad (1)$$

and sets

$$\sigma_s = \left(\frac{\beta}{\psi(\prod_{i \neq s} w_i^{a_i})} \right)^{1/x_s} \in \mathbb{G}_1. \quad (2)$$

The ring signature of block m is $\boldsymbol{\sigma} = (\sigma_1, ..., \sigma_d) \in \mathbb{G}_1^d$.

RingVerify. Given all the d users' public keys $(\mathbf{pk}_1, ..., \mathbf{pk}_d) = (w_1, ..., w_d)$, a block m, an identifier id and a ring signature $\boldsymbol{\sigma} = (\sigma_1, ..., \sigma_d)$, a verifier first computes $\beta = H_1(id) g_1^m \in \mathbb{G}_1$, and then checks

$$e(\beta, g_2) \overset{?}{=} \prod_{i=1}^{d} e(\sigma_i, w_i). \quad (3)$$

If the above equation holds, then the given block m is signed by one of these d users in the group. Otherwise, it is not.

Fig. Mathematical Model

VIII. CONCLUSION

We propose privacy preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphic authenticators, so the TPA is able to audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can achieve identity privacy. To improve the efficiency of verification for multiple auditing tasks, we further extend our mechanism to support batch auditing. An interesting problem in our future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor.

REFERENCES

[1]B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.
[2]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.
[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]R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret,"Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01),pp. 552-565, 2001.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.
[6]Oruta : Privacy Preserving Public Auditing for shared Data in the cloud. B. Wang, Student Menber, IEEE ,Baochun Li, Senior Member, IEEE, IEEE Transaction On Cloud Computing Vol.2, No.1, JanuaryMarch 2014.
[7] Cong Wang, Student Member, IEEE, Qian Wang, Student Member,IEEE, Kui Ren, Member, IEEE, "Towards Secure and Dependable Storage Services in Cloud Computing"
[8] Kan Yang "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing ,"IEEE Transactions On Parallel and Distributed Systems, VOL. 24, NO. 9, SEPTEMBER 2013
[9] Qian Wang, IEEE, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, "IEEE Transactions On Parallel And Distributed Systems, VOL. 22, NO. 5, MAY 2011.