ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Efficient Mechanism for Maintaining Privacy-Public Auditing to the Shared Data in the Cloud

Ch. Saikumar
M.Tech Student,
Department of CSE,
ASIT, Gudur.

K.Phalguna Rao
Professor,
Department of CSE,
ASIT, Gudur.

Abstract:

The cloud data services mainly provides the data storage to the users, this data storage services also shared the data to the different users. During sharing of data in the cloud, there is a chance of data integrity in the cloud it will be occurs due to the corrupted or damaged or failure of hardware/software or due to human errors. In early we have designed different mechanisms to allow the third party auditor (TPA or public verifier) and data owners to effectively audit the data integrity without receiving whole data from server.In the available mechanisms reveals the confidential information and identity of users to TPA during the public auditing on the shared data in the cloud. To overcome the above problems we introduce new public auditing mechanism that supports the identity privacy and does not reveal confidential information to public verifiers and it is effectively perform auditing on integrity to the shared data. And also supports the multiple auditing tasks at a time. It will reduces the computational cost.

key words:

cloud computing , identity-privacy, ring signatures, shared data, auditing.

1.INTRODUCTION:

Now a day's cloud computing goes most popular in sharing the data or resources to the users. Cloud computing is a next generation IT infrastructure to the internet. These cloud data storage services are provided by the cloud service providers such Amazon, Google drive, cloud front etc. CSP's provide services with low cost, scalable and highly efficient data storage services to the users.

Most common feature of the cloud storage services is data sharing. Verifying the data integrity in the cloud is some time difficult. The integrity of cloud data will occur due to the human errors or damaged or failure of software/ hardware. For the above reasons data can be easily corrupted or lost. When this situation occurred CSP's unwillingly to intimate to the users because of reputation of the services will be damaged. Before using of data from the cloud server we need to verify the cloud data integrity. Cloud data has the large amount of different types of data. To verify the data integrity in cloud data it's a difficult task and it will be wastage of time, resources and cost. Important thing is if data is lost or damaged in the cloud, users no need to save the whole data to their remote or local devices. Because of CSP's provide more computation services to users straightly on big scale data. In previous mechanisms, the data owner and TPA (public verifier) both are involved. TPA is able to check the data integrity efficiently on shared data without retrieving the whole data from the cloud server. During the public auditing, TPA can reveal confidential data of the users. They focus only on users data but not on the confidential data.We introducing new auditing mechanism and new ring signature scheme.We use ring signatures to design the new ring signature scheme called HVT ring signature (HVT means homomorphic verifiable tags) in new public auditing mechanism. It supports public verifier can be check the integrity of shared data without downloading the whole data from the cloud server and it can hide identity of signer to the public verifiers. It can perform multiple auditing tasks.

2.SYSTEM ARCHITECTURE:

In our system architecture have three members they are cloud server, public verifier (TPA), users.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The cloud server contains the different types of data like shared data or meta data or private data. The TPA provide auditing services and checking any data integrity in the cloud server and also watching any unauthorized users are accessing the shared data. In this architecture we have two types of users they are owner (original user) of the data and group users. The original user will shares the data to the group users. Group users will access or modify the shared data from the cloud server but who are registered in the group only.

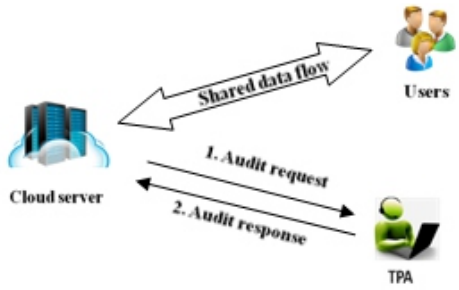

Fig 1: System Architecture.

public auditing mechanism looks like a challenge - response protocol model. If TPA wants to verify the data integrity in the shared data. TPA will send a audit request to cloud server and after request received by the cloud server it will send a auditing response (proof of possession of data) to TPA. Based on this TPA will verify the faultless of the whole data by checking the faultless of auditing response.

3.NEW RING SIGNATURE:

A ring signature is one of the digital signature. Ring signature can be generated by any one of the group users having keys. This ring signature is introduced by Ron Rivest, Adi Shamir, and Yael Tauman in 2001. Thereis no way to revoke the anonymity of an individual signature. Group users do not know who are generated the signature in the group. Here TPA is verified the signature using any one of the group users private keys but TPA is not able to find who are generated the signature in the group. So that identity of signer will be hide to the TPA.

3.1.Homomorphic Verifiable Ring Signature:

We improve the ring signature using homomorphic verifiable tags. It is normal tool to designing the public auditing mechanism. HVT hasthe two properties are block less verification and non-malleablity.

Blockless verification that supports to audit the faultless data stored in cloud server with special block. Special block is verifier is took different combination of blocks in data, If integrity of special block is correct then whole data in the server is correct and verifier will confirm there is no damage or lost data on the shared data. Non –malleabilty represents that who has no private key and is not able to generate the signature on blocks. In traditional ring signature, it does not support the blockless verification. If blockless verification is not exist in public auditing mechanism then TPA will retrieve entire data file to check the faultless of shared data. It takes more bandwidth and verification will take more time. We develop the new ring signature called homomorphic verifiable ring signature (HVRS). It supports the blockless verification and also maintains identity of signer. User's confidential information it will not reveal to the TPA and hides the identity of signer. HVRS consists of three methods are KyG, RgS, RgV. In KyG generate the public and private keys by every user in group. In Rgv, verifier is check whether user in the group is signed on the block or not. In RgS, produce a signature and identifier on block using with private key and group users public keys.

4 PUBLIC AUDITING MECHANISM:

In the previous auditing mechanisms, verifier will download entire data to check the integrity of shared data. To overcome this we introduce new public auditing mechanism called ORUTA (one ring use them all) auditing mechanism. It hides the identity of signer to TPA. TPA will not be receive the whole data from the server to verify the integrity of shared data.The conventional public auditing mechanism supports the dynamic operations like insert, update, and delete operations on blocks. In previous mechanisms use the index for identifying the block. Using the index as identifier, if a user performed the one of the dynamic operation on a single block in shared data and then index of blocks all are changed due to this we will verify the signatures again on the blocks and who are sharing data. In the new mechanism uses the hash values for identifying the index of blocks. In our public auditing mechanism has the five algorithms are keyGeneration, signatureGeneration, modify, proofVerify, proofGeneration. In the signatureGeneration, one of the user in the group using its own private key and all group users key computes signature on blocks of the shared data. keyGeneration that represents the public/private keys are generated by the users.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In proofGeneration, both TPA and cloud server generates the proof. TPA will verify the proof to check the integrity of shared data.

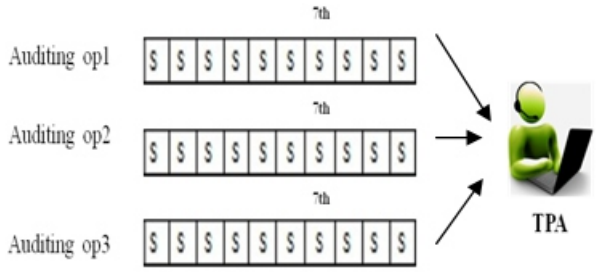

Fig 2: TPA audits the integrity of shared data using with oruta. A and B share a file in the cloud

Let us consider example fig 2. A and B share a file in to cloud and both are in same group. The shared file is split into small blocks and both are independently signed on each block. Where S is a block signed by the one of the user in the group. In our mechanism, to verify the integrity of shared data then TPA wants both public keys because every block on shared data signed by the any one of the user in the group and TPA cannot determine who signed on the block. Therefore there is no chance for revealing the confidential information by the TPA.And our auditing mechanism supports the dynamic groups. Dynamic group means new user can be added in to the group or existing user can be removed from the user. When changes are occurred in group TPA will again compute signature using with all users public key in the groups and signer private key. Finally, our new auditing mechanism that supports the multiple auditing tasks at a time and reduces the computation cost. In earlier mechanisms has no multiple auditing feature and did not hide the identity of signer.

5. CONCLUSION AND FUTURE WORK:

In this paper, we proposed the public auditing mechanism that audits the integrity of shared data in cloud. TPA will perform auditing for shared data and TPA cannot distinguish who is signer on the block. We utilize the homomorphic verifiable tag ring signature (HVRS) that hides the user identity on blocks and TPA will audit the integrity of shared data without downloading the entire data from the cloud. In future, We extend this mechanism to support the batch auditing effectively but here two problems are there one is traceability and data freshness.

6.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] 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.

[3] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[4] 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.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT'03), pp. 416-432, 2003.

[6] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," Proc. 24th Ann. Int'l Cryptology Conf. (CRYPTO'04), pp. 41-55, 2004.

[7] 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.

[8]https://en.wikipedia.org/wiki/Ring_signature.