ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

# Privacy Preserving Public Auditing System for Data Sharing in Cloud

R.Chermalatha, M.Dhivya, Ms.P.Saranya,M.E,

IV Year, Dept. of CSE, Angel College of Engineering and Technology, Tamilnadu, India

IV Year, Dept. of CSE, Angel College of Engineering and Technology, Tamilnadu, India

Assistant Professor, Dept. of CSE, Angel College of Engineering and Technology, Tamilnadu, India

**ABSTRACT:** Cloud computing is the long dream vision of computing as a utility where users can remotely share the data into the cloud.By data outsourcing users can be relieved from burden of maintenance and security of data. For a protective data outsourcing , In this paper, we securely introduce an effective third party auditor to get the shared data by meeting the fundamental requirements . TPA should be able to efficiently audit the cloud data storage andintroduceno on-line burden to the cloud user we provide a homomorphicauthenticableringsignaturemechanism for public auditing on shared data in the cloud. Our scheme supports external auditor to audit user's outsourced data in the cloud and supports scalable and efficient data auditing in the cloud computing . we achieve auditing tasks from different users can be performed simultaneously by the TPA. we are providing better security for clients.User uses TPA to maintain and check integrity data. It improves the data privacy by achieving traceability and the data freshness. The Proposed system will perform audit for multiple users efficiently.

**KEYWORDS:** Privacy preserving, HARS, Data storage

## I.INTRODUCTION

The data storage and sharing services provided by the cloud, people can easily work together as a group by sharing data with each other. more specifically, once a user creates shared data in the cloud, every user in the group is able to not only access and modify shared data, but also share the latest version of the shared data with the rest of the group. Although cloud providers promise a more secure and reliable environment to the users, the integrity of data in the cloud may still be compromised, due to the existence of hardware/software failures and human errors In these mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures. One of the most significant and common features of these mechanisms is to allow a public verifier to efficiently check data integrity in the cloud without downloading the entire data, referred to as public auditing would like to utilize cloud data for particular purposes (e.g., search, computation, data mining, etc.) or a trusted party auditor (TPA) who is able to provide verification services on data integrity to users. Most of the previous works focus on auditing the integrity of personal data. Different from these works, several recent works focus on how to preserve identity privacy from public verifiers when auditing the integrity of shared data. Unfortunately, none of the above mechanisms considers the efficiency of user revocation when auditing the correctness of shared data in the cloud.With shared data, once a user modifies a block, she also needs to compute a new signature for the modified block. Due to the modifications from different users, different blocks are signed by different users. For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group. As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group. Therefore, although the content of shared data is not changed during user revocation, the blocks, which were previously signed by the revoked user, still need to be re-signed by an existing user in the group. As a result, the integrity of the entire data can still be verified with the public keys of existing users only.

Public Auditing is being used to allow data owners and public verifiers to check the integrity of the data without the need to download the entire data from cloud. This mechanism divides data into many small blocks, where each

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

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. However this approach leads to an issue where the identity of the signer is revealed to public verifier leading to situation of leaked identity privacy. The public verifier will 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). As a result, public auditing may put various confidential data at risk. In order to protect the confidential information, it is essential and critical to preserve identity privacy from public verifiers during public auditing.

## II. RELATED WORKS

The purpose of this review is to report, evaluate, and discuss the findings from research. A particular focus of this review is to facilitating privacy-preserving public auditing for secure shared data in cloud storage.

Boyang Wang, et.al With cloud storage services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. However, public auditing for such shared data — while preserving identity privacy — remains to be an open challenge. In this paper, we propose the first privacy-preserving mechanism that allows public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to publicly verify the integrity of shared data without retrieving the entire file.

Qian Wang,,etal. proposedthe techniques which achieve both the public auditing and also dynamic data operations. To achieve effective data dynamic, use Merkle Hash Tree construction for block label authentication. And to handle effective auditing task bilinear aggregate signature would be used and extend over multiuser settings, where TPA can do multiple auditing tasks simultaneously.Client: can be individual user or organization how has large number of data files to store on cloud and relies for data maintenance and computation. Cloud Storage Server: cloud service provider can managed it,which maintain client data and has storage space and computation resources. Third Party Auditor : On the behalf of client request it can manage all cloud storage services. To support effectively public auditing system resort on homomorphic authenticator, which is unforgettable metadata which generated from individual data blocks.

Jia Xu, et.al introduced Lightweight and Privacy-Preserving Delegatable Proofs of Storage, this proof allows to audit the integrity of the data stored on cloud without keeping the local copy back of the data. The slowness of all existing proof of storage (POS) has made the systems to bottleneck. They proposed a new variant formulation that is able to construct a POS scheme, which on one side is as efficient as private key POS schemes, and on the other side can support third party auditor and can switch auditors at any time, close to the functionalities of publicly verifiable POS schemes.

## III.PROPOSED MODEL

In this proposed work, we are providing better security in owner's upload side as well as on the download side.For better security client splitting that single file into nine different blocks and providing a unique identification number for each block.we are converting a block tag into secret value using ASCII value.

**Client**: An entity, which has large data files to be stored in the cloud computing and relies on the cloud computing for data maintenance and computation, During login for a client here an OTP was generated and that was sent to the registered mail id using that OTP only a client can login.

**Trusted Party Auditor (TPA):** We are using a public auditing in proposed an entity, which has expertise and capabilities that clients do not have, is trustedto assess and expose risk of cloud computing storage services on behalf of the clients upon request.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

**A,ARCHITECTURE DIAGRAM**

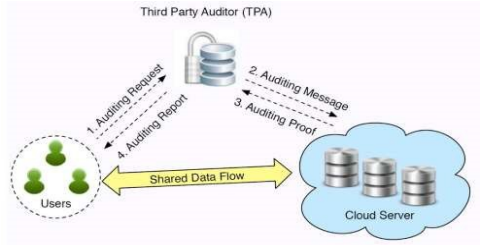


**Fig 1 :SYSTEM ARCHITECTURE**

**B. ARCHITECTURE DESCRIPTION**

Architecture involves three parties, the cloud server, a group of users and a TPA. There are two types of users ina group, the original user and a number of groups of users. The original annually shared data in the cloud, and shares it with group of users. Both the original user and group users are members of group. Every members of group is grant to access and modify the shared data. Shared data and its verification metadata are both stored in the cloud server. A TPA, such as a Third Part Auditor providing expert data auditing services or a data user outside the group attempt to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server. When TPA intended to check the integrity of shared data, it sends an auditing challenge to the cloud server. After receiving the auditing challenge, the cloud server responds to the TPA with an auditing proof of the tenancy of the shared data. Then, this TPA checks the exactness of the entire data by verifying the exactness of auditing proof. Essentially, the process of public auditing is a challenge and response protocol between a TPA and the cloud server. The identity of the signer on each block in the shared data is kept secret from the third part auditor.

**C. RING SIGNATURE SCHEME**

The design of the new homomorphic authenticable ring signature (HARS) scheme, which is extended from the standard ring signature scheme. The ring signature is developed by HARS mechanism are not only able to preserve identity privacy but also able to support block less verifiability.HARS contains three algorithms: KeyGen, RingSign and Ring Verify.

KeyGen: Each user in the group develops their private key and public key. RingSign: A user in a group is able to develop a signature on a block and its block identifier with his/her private key and all group members' public keys. A block identifier is a string that can characterize the comparable block from others. Ring Verify: A verifier is able to check whether a given block is signed by a group of member.

**D. PUBLIC AUDITING SCHEME**

Privacy preserving public auditing mechanism for shared data in the cloud.TPA can verify integrity of shared data without retrieving the entire data. Meanwhile, the identity of the signer on each block in shared data is kept private from public TPA during the auditing. We present the details of our public auditing mechanism. It includes five algorithms: KeyGen, SigGen, ProofGen, and ProofVerify. In KeyGen, users develop their own public/private key pairs. In SignGen, a user is able to compute ring signatures and blocks in shared data by using its own private key and all group members' public keys. ProofGen is operated by a TPA and the cloud server together to indicatively generate a proof of possession of shared data. In ProofVerify, the TPA audits the integrity of shared data by verifying the proof.

## IV.TECHNIQUES OF ALGORITHMS

Homomorphic Authenticator Ring Signature managed suppose that a group of entities each have public/private key pairs, (PK1, SK1), (PK2, SK2), ... ,(PKn, SKn). Party i can compute a ring signature σ on a message m, on input (m, SKi, PK1, ... , PKn). Anyone can check the validity of a ring signature given σ, m, and the public keys involved, PK1,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

... , PKn. If a ring signature is properly computed, it should pass the check. On the other hand, it should be hard for anyone to create a valid ring signature on any message for any group without knowing any of the secret keys for that group Ring signatures, rst introduced by Rivest, Shamir, and Tauman, enable a user to sign a message so that a ring of possible signers (of which the user is a member) is identified, without revealing exactly which member of that ring actually generated the signature. In contrast to group signatures, ring signatures are completely ad-hoc" and do not require any central authority or coordination among the various users (indeed, users do not even need to be aware of each other); furthermore, ring signature schemes grant users ne-grained control over the level of anonymity associated with any particular signature.

## V. MODULE IMPLEMENTATION

The security and privacy for shared data in the cloud using ring signature are consists of following modules:

A. Cloud User
B. Ring Signature
C. Third Party Auditor
D. Cloud Server

### A.CLOUD USER

A public verifier would be a data user who can like to utilize the owner data via Tpa or cloud who can provides the expert integrity checking services.During login for a client here an OTP was generated and that was sent to the registered mail id using that OTP only a client can login.

### B.RING SIGNATURE

Ring signature to construct homomorphic authentication.so that public verifier is able to audit shared data without downloading the entire data,and yet it cannot differentiate who is the signer on each block.Ring signature is computed by one of the team member private key,but the verifier is cannot able to identify which one this.

### C.THIRD PARTY AUDITOR

Third party auditor to verify the integrity of data that data are stored in cloud. Trusted third party view the user datas and upload into the distributed cloud[11]. If any modification by cloud owner message send to the third party auditor.Third party auditor check the correctness of data stored in the cloud.

### D.CLOUD SERVER

Cloud server provide key response to TPA to get requested file to client. Before sending requested file it generate a genProof key for a file and then it transfer files to TPA.

## VI. RESULTS & DISCUSSION

This results provide a more security in data auditing improves the security level of uploading and downloading the files. This result is executed using the enhanced HARS.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

## VII. RESULT SNAPSHOTS


**Fig 2 : OTP Generation**


**Fig 3 : File Uploading**

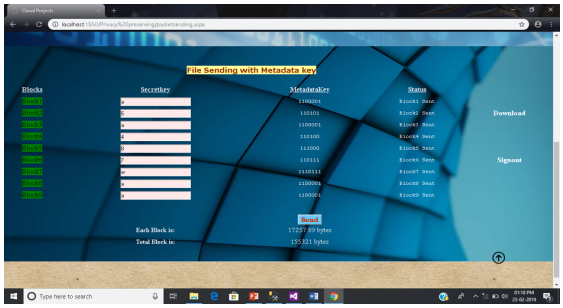


**Fig 4 : File Encryption**

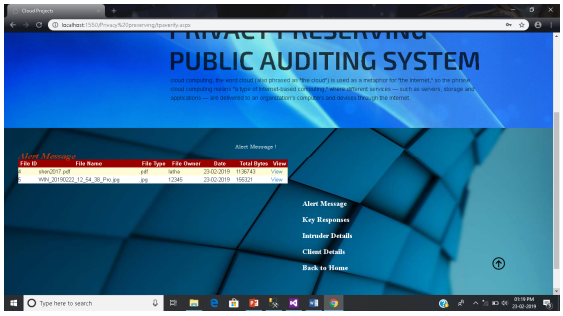


**Fig 5 : File sent to server**

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

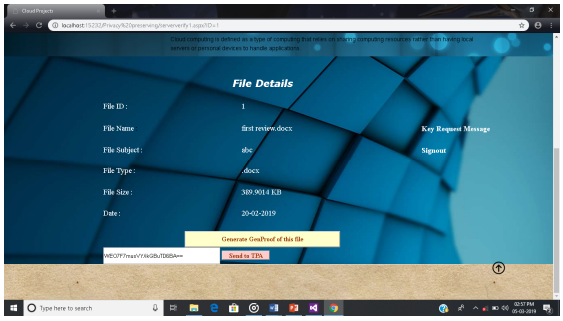


**Fig 6 : Server generate a Genproof key**

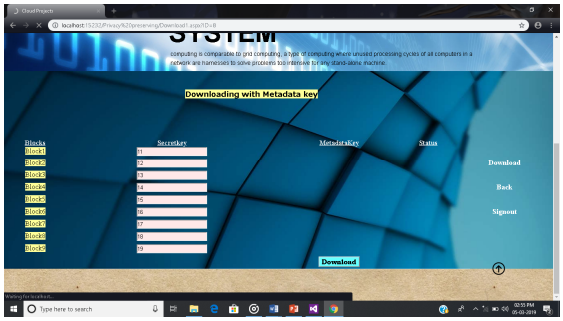


**Fig 7 : File Decryption**

## VIII. CONCLUSION & FUTURE WORK

Assumptions and without random oracles, and with short group signatures. Even less ambitious would be an efficient scheme that supports some subset of these properties (e.g., a fully dynamic scheme with a group manager) but meets the strongest definitions of security, as the only schemes we have seen that come close to achieving this level of edibility provide only CPA-style anonymity. we propose a privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphic authenticator and random masking to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminatesthe burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner.

## REFERENCES

1) Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011. Cloud Computing, pp. 295-302, 2012.
2)M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
3)K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.
4)D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.
5) B. Wang, M. Li, S.S. Chow, and H. Li,"Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013. .
6)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.
7)Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Visit: www.ijirset.com*

**Vol. 8, Issue 3, March 2019**

8)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.
9) 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.
10) B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Trans. Services Computing, 20 Dec. 2013, DOI: 10.1109/TSC.2013.229 5611.