IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. III (Jul – Aug. 2014), PP 33-38
www.iosrjournals.org

Privacy-Preserving Public Auditing For Secure Cloud Storage

Salve Bhagyashri[1], Prof. Y.B.Gurav[2]
P.G Scholar, Department of Computer Engineering, PVPIT, Bavdhan, Pune[1].
Assistant Professor, Department of Computer Engineering, PVPIT, Bavdhan, Pune[2].

***Abstract*:** *By using Cloud storage, users can access applications, services, software whenever they requires over the internet. Users can put their data remotely to cloud storage and get benefit of on-demand services and application from the resources. The cloud must have to ensure data integrity and security of data of user. The issue about cloud storage is integrity and privacy of data of user can arise. To maintain to overkill this issue here, we are giving public auditing process for cloud storage that users can make use of a third-party auditor (TPA) to check the integrity of data.Not only verification of data integrity, the proposed system also supports data dynamics. The work that has been done in this line lacks data dynamics and true public auditability. The auditing task monitors data modifications, insertions and deletions. The proposed system is capable of supporting public auditability, data dynamics and Multiple TPA are used for the auditing process. We also extend our concept to ring signatures in which HARS scheme is used. Merkle Hash Tree is used to improve block level authentication.*
Further we extend our result to enable the TPA to perform audits for multiple users simultaneously through Batch auditing.
***Index Terms*:** *Cloud Storage, Data Dynamics, Public Auditing, Privacy Preserving, Ring Signatures.*

I. Introduction

CLOUD computing has been envisioned as the next- generation information technology (IT) architecture for enterprises. Cloud computing is extensively developed technology used in business, IT industries which provide services like network access, resources, infrastructure, platform, rapid resource elasticity as per user require [1]. The user can gain access of services anytime, anywhere on-demand. In cloud computing the data of user is centralized to the cloud storage. Cloud storage is a prototype of networked online storage in which the data is stored in virtualized pools of storage that are generally given by the TPA. NIST definition of cloud computing as:

"Cloud computing is a model for enabling convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[2]

Many users from remote location use services continuously so there may arise some issues like data security, data integrity, dynamic updates. Every time it is not possible for user to check the data is being consistent which is stored on cloud storage. So user always wants that cloud server must have to maintain data integrity and privacy. Cloud service providers are the separate entities that store data and provide services to the user. The security and data integrity issues arise due to following reasons:

1) The types of attackers like internal and external and their capability of attacking the cloud. 2) The security risks associated with the cloud, and where relevant considerations of attacks and Countermeasures. 3) Emerging cloud security risks.

Some other issues like lack of training and expertise, unauthorized secondary usage, complexity of regulatory compliance, lack of user control, addressing transborder data flow restrictions, legal uncertainty, compelled disclosure to the government, data accessibility, location of data, transfer and retention, data security and disclosure of breaches[3][4][5] .

The cloud server stores large amount of data which does not offer guarantee on data integrity and consistency. This problem is addressed and solve by giving public auditing for secure cloud.

To ensure the data security and integrity and to reduce online burden it is of importance to enable public auditing service for cloud storage, so that user may resort to third-party auditor (TPA) to audit the data. TPA does the auditing process on behalf of the user. The TPA who has capabilities and expertise that can periodically check the integrity of the data stored in cloud. The user does not have the capabilities that the TPA has. The TPA check the correctness of data stored in cloud on behalf of user and maintain the integrity of data. Enabling public auditing service will play an important role for privacy data security & minimizing the data risk from hackers. The proposed system supports data dynamics in which user performs update, insert, delete operation. For public auditing process we use the hashing technique in which hash function is applied on the user's data. So during the auditing process TPA would not learn any knowledge or users data. The user's data

get maintained from TPA. By using HARS scheme of ring signature the identity of the signer is gets preserved from the verifier.

II. Literature Survey

Ateniese et al. [6] are the first to consider public auditability in their defined "provable data possession" (PDP) model for ensuring possession of files on untrusted storages. In their scheme, utilize RSA based homomorphic tags for auditing outsourced data, thus public auditability is achieved. However, Ateniese et al. do not consider the case of dynamic data storage, and the direct extension of their scheme from static data storage to dynamic case may suffer design and security problems. In their subsequent work [7], Ateniese et al. propose a dynamic version of the prior PDP scheme. However, the system imposes a priori bound on the number of queries and does not support fully dynamic data operations, i.e., it only allows very basic block operations with limited functionality, and block insertions cannot be supported. In [17], Wang et al. consider dynamic data storage in a distributed scenario, and the proposed challenge-response protocol can both determine the data correctness and locate possible errors. Similar to [7], they only consider partial support for dynamic data operation. Juels et al. [10] describe a "proof of retrievability" (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrievability" of data files on archive service systems. Specifically, some special blocks called "sentinels" are randomly embedded into the data file F for detection purpose, and F is further encrypted to protect the positions of these special blocks. However, like [7], the number of queries a client can perform is also a fixed priori, and the introduction of precomputed "sentinels" prevents the development of realizing dynamic data updates.

Shacham et al. [16] design an improved PoR scheme with full proofs of security in the security model defined in [10].

They use publicly verifiable homomorphic authenticators built from BLS signatures , based on which the proofs can be aggregated into a small authenticator value, and public retrievability is achieved. Still, the authors only consider static data files. Erway et al. [9] was the first to explore constructions for dynamic provable data possession. They extend the PDP model in [6] to support provable updates to stored data files using rank-based authenticated skip lists. The scheme is essentially a fully dynamic version of the PDP solution. To support updates, especially for block insertion, they eliminate the index information in the "tag" computation in Ateniese's PDP model [6] and employ authenticated skip list data structure to authenticate the tag information of challenged or updated blocks first before the verification procedure. However, the efficiency of their scheme remains unclear. Shan et al.[13] introduce TPA concept to maintain data integrity and preserve privacy. It reduces online burden and keeps the privacy preserve. Chen et al.[8] gives mechanism for auditing the correctness of data with multiple server. Frenz et al.[11] introduce a new strategy ,an Oblivious out-sourced storage which is based on Oblivious RAM technique. This idea used to conceal user access pattern and preserve the identity.

Although the existing schemes aim at providing integrity verification for different data storage systems, the problem of supporting both public auditability and data dynamics has not been fully addressed. How to achieve a secure and efficient design to seamlessly integrate these two important components for data storage service remains an open challenging task in Cloud Computing. Two basic solutions (i.e., the MAC-based and signature based schemes) for realizing data auditability and discuss their demerits in supporting public auditability and data dynamics. Secondly, generalize the support of data dynamics to both proof of retrievability (PoR) and provable data possession (PDP) models and discuss the impact of dynamic data operations on the overall system efficiency both.

In particular, emphasize that while dynamic data updates can be performed efficiently in PDP models more efficient protocols need to be designed for the update of the encoded files in PoR models.

III. Problem Statement

As data integrity and the security is main important thing in cloud, to provide full security and data integrity we are giving public auditing process. Our scheme performs both public auditing and data dynamic operation. For public auditing process we are using here Hashing technique in which hash function is applied on the user's data. The data dynamic performs operation like insert, update, and delete in block wise manner. TPA does the auditing process. Again we extend our concept in which multiple user access cloud storage simultaneously through batch auditing. TPA batch multiple auditing task together and audit at one time. So it reduces the time for auditing process. In our proposed wok we are giving multiple TPA for auditing process. As there are problems like users load ,system crash , system failure at this situation multiple TPA do the auditing process in which if there is failure of one TPA another TPA do the auditing process by taking backup of first TPA.

Again we are giving here ring signature concept in which we are using HARS (Homomorphic Authenticable Ring Signature) scheme. In this scheme a group of users can access the CS and they share data in

group. Any user in group does the update, delete operations. The system model for our scheme is given below.

A. The System Model:

The system model consist three different entities: the cloud user, the cloud server (CS) and the third-party auditor (TPA).

As shown in fig. 1.The cloud user is the one who has large amount of data files that are stored in the cloud; the cloud server is the one who provides the data storage service like resources, software to the user. The cloud server is managed by cloud service provider; the third- party auditor is the one who has belief to access the cloud storage service for the benefit of user whenever user request for data access. The TPA has capabilities and competence that the user does not have. They can also interact with cloud server to access the stored data for different purpose in different style. Every time it is not possible for user to check the data which is stored on cloud server that arrives online burden to the user .so that's why to reduce online burden and maintain that integrity cloud

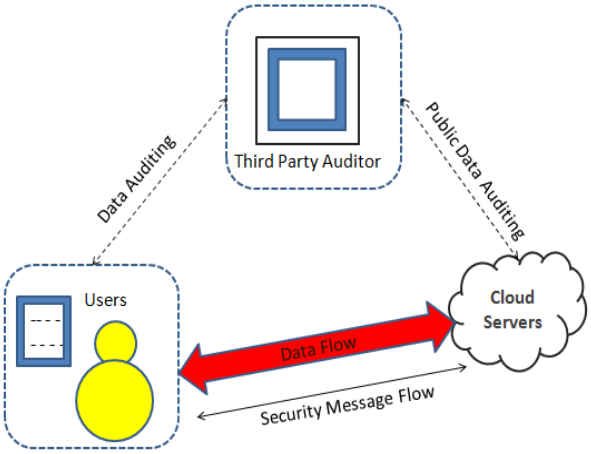


Fig.1. The architecture of cloud data storage.

user may resort to TPA. The data stored on cloud server is come from internal and external attacks ,which is having data integrity threads like hardware failure, software bug, hackers, and management errors. The Cloud Server can maintain reputation for its self-serving. The CS might even decide to hide these data correction incidents to user. So that's why here we are giving third-party auditing service for users to gain belief on cloud.

B. Design Goals:

The data integrity and security can be achieved by enabling privacy public auditing for cloud data storage as given below:

1. Privacy-preserving: TPA can't see the user's data content during the auditing process.
2. Public Auditability: To allow TPA to verify the correctness of cloud data without demanding the copy of whole data.
3. Batch Auditing: TPA handles multiple user's for multiple task during auditing process.
4. TPA performs auditing process with minimum communication.
5. Identity privacy: The TPA cannot identify the identity of the signer of each block when auditing process going on.

IV. The Proposed Schemes

In this section we are giving public auditing Scheme for ensuring the data integrity. Firstly giving the notation and preliminaries, after that the framework and later overview of public auditing system.

A. Notation and Preliminaries

1: F- The data file to be fetched, denoted as a sequence of n blocks $m_1,\ldots m_i\ldots,m_n \in Z_p$ for some large prime p.

2: MAC $_{(.)}$ $^{(.)}$– Message authentication code (MAC) function, given as : $K\times\{0,1\}^*\rightarrow\{0,1\}^l$

Where K denotes the key space.

3: H (.), h (.) - Hash function.

B. Framework

The framework for privacy-preserving public auditing system maintains the data integrity. Public auditing schemes consist of four algorithms. **KeyGen, SigGen, GenProof, VerifyProof.** In **KeyGen** the Key is generated called as Key generation algorithm, which is run by the user to set up scheme. In **SigGen** verification metadata is generated by the user which consists of digital signature. **GenProof** is run by the cloud server to generate a proof of data storage. **VerifyProof** algorithm is run by TPA to audit and verify the proof.
During the public auditing process, it consists of two phases as explain below:

- **Setup**: By executing KeyGen algorithm, the user initializes the public and secret parameters of the system .By using SigGen, it generate verification metadata by preprocessing the data file F. The data file F & verification metadata is stored at cloud server by the user and delete its local copy. User may also alter the data file F by expanding it.
- **Audit**: TPA send audit challenge or message to cloud server to become sure that the cloud server has keep data file F during the auditing process. By executing GenProof the cloud server gets response message by using file F and verification metadata as an input. And lastly the TPA verifies the response given by the cloud server by performing verifyproof algorithm.

C . How process Works?

Here we are given the block diagram for the process flow. Fig 2 show the process flow for multiple users by using multiple TPA.

Algorithm for Data Integrity Verification
1. Start
2. TPA generates a random set like public key p_k, private key s_k and signature σ on each block (Verification metadata).
3. CS computes root hash code based on the filename/blocks input.
4. CS computes the originally stored value.
5. TPA decrypts the given content and compares with generated root hash.
6. After verification, the TPA can determine whether the integrity is breached.
7. Stop

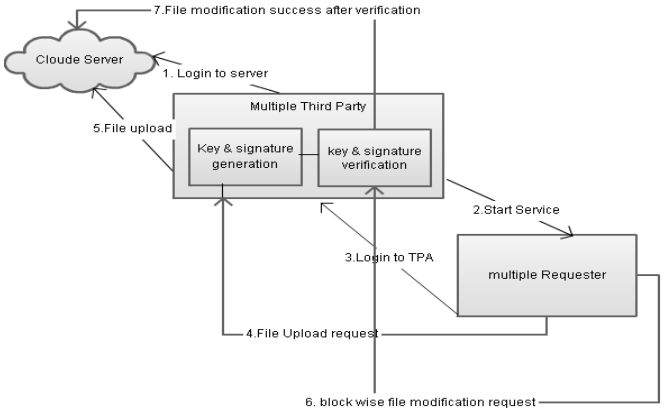


Fig 2. Process flow

D. Supports For Data Dynamics

In cloud computing, users update their data continuously for various application purposes. [14][15][16].So here privacy preserving public auditing supports for data dynamics in which user can do modifications on stored data. This data dynamics supports for update, delete, inert operation. For data dynamics we are using here Merkle Hash Tree (MHT). As data file F is divided into number of blocks m1,m2, . .,mn. Suppose user wants to modify the ith block mi to mi'. At that time client generates new signature on block σi' = (H(mi').umi')α. When the CS receives the request it runs ExecUpdate(F,ϕ,update). Specifically, the server 1) replaces mi with mi' and outputs F'; 2) replaces σi with σi' ; 3) replaces H(mi) with H(mi') in the MHT construction and generates the new root R'. On this new root hash signature is generated and that signature is stored newly.
For insert operation , data gets inserted block wise manner into the file. And if user wants to delete file or

particular block user can delete it by the same procedure.

E. Privacy-preserving Public Auditing Using Ring Signature scheme

As per existing work, public auditing scheme utilizes the technique of public key-based homomorphic linear authenticator (HLA), which allows TPA to perform the auditing without expecting the local copy of data and thus minimizes the communication. To maintain more data integrity and security Ring Signatures concept we are implementing here. The concept of ring signatures is first proposed by Rivest et al. in 2001[12]. The ring signature is the type of digital signature which can be performed by any group member of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. The best characteristic of a ring signature is that it should be difficult to identify which of the group members' keys was used to produce the signature. In this, the signature is computed using one of the group member's private key, but the verifier is not able to determine which one. This property can be used to preserve the identity of the signer from a verifier.

The ring signatures concept is used to hide the identity of singer on each block so that the private and sensitive information of group does not seen by the TPA. To reduce time and long verification, we are extending the ring concept by homomorphic authenticable ring signatures. This homomorphic authenticable ring signature not only maintains the identity but also reduce long verification with supporting to blockless verification.

The privacy-preserving public auditing using signatures consist of three algorithms as mentioned here: **KeyGen** , **RingSign**, **RingVerify**. In KeyGen algorithm each user in the group generates their public key and private key. In RingSign algorithm user in the group is related to sign a block with her private key and all group members' public keys. In Ring verify algorithm the verifier is used to check whether the given block is signed by the group member. The ring signatures for public auditing consist of following steps for auditing.

1: Each user generates its public and private key.
2: A user in the group sign a block with her private key and all group member's public key.
P_{k1} is public key of the user;
S_{k1} is private key of the user;
(P_{k1} ……P_{kd}) is 'd' number of users of data block m $\in Z_P$
3: User randomly selects data block m
Let id is identifier of data block m
4: User u_i encrypts with all user's public key, so only private key of the group user's i $\in$ [1,d] would be able to decrypt it. This ensures privacy of data.
5: To ensure auditing by third-party user (u_i), where
i $\in$ [1,d] signs the data block using his private key.
6: TPA (Third-party auditor) , using a P_{k1} ……P_{kd} Where d is number of users in the group.

TPA calculates signature of data blocks but unaware of who sign it .Therefore calculates signature using each given public key (P_{k1} ……P_{kd}) from this set.

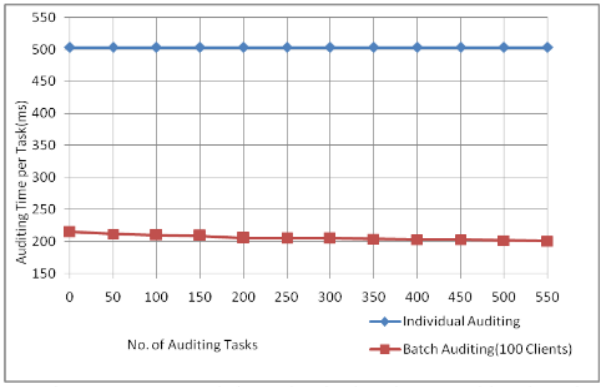
G_{sign} = signature set for (P_{k1} ……P_{kd})

If G_{sign} = {$sign_1$,$sign_2$,……$sign_d$} matches with original sign then data block is intact.

By using this scheme user can also do the data dynamic operation. As there is group of users which share their data to each other , they can do modification on data of CS.

F. Supports For Batch Auditing

In batch auditing multiple user can access CS simultaneously. The TPA may concurrently handle multiple auditing processes for multiple users. Multiple TPA are used for the auditing process. TPA batch all users task and audit it at one to time. The advantage of batch auditing is that it reduces the time for handling the multiple audits for multiple users. The graph shows the comparison of individual auditing and the batch auditing. The comparison is done on the basis of auditing time required to perform number o tasks.



V. Conclusion

Here in this paper, we are given the privacy –preserving public auditing scheme which supports data dynamic operations. Public auditing scheme supports hashing technique. The data dynamic operations can get performed by using Merkle Hash Tree(MHT). We use multiple TPA for the auditing process which handles multiple users through batch auditing. We utilize ring signature for secure cloud storage which ensures that during the auditing process the TPA would not learn any information or knowledge about data content of group stored on cloud server. Ring signature preserves the identity of the signer from the verifier. We use HARS scheme for group of users in which they share data to each other and update and delete data block wise manner.

References

[1]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.
[2]. P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloud- computing/index.html, June 2009.
[3]. Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing,3-42.
[4]. Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurityalliance.org, 2010
[5]. M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com/2006/12/28/gmail disasterreports- of-mass-email-deletions/, 2006.
[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. 598-609, 2007.
[7]. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10, 2008.
[8]. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Stroage Sys-tems," in Proc. ACM Cloud Computing Security Workshop (CCSW), 2010, pp.31– 42.
[9]. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. 16th ACM Conf.Computer and Comm. Security (CCS '09), 2009.
[10]. A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
[11]. M. Franz, P. Williams, B. Carbunar, S. Katzenbeisser, and R. Sion, "Oblivious Outsourced Storage with Delegation," in Proc. Finan-cial Cryptography and Data Security Conference (FC), 2011, pp. 127– 140.
[12]. R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc.International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2001, pp. 552– 565.
[13]. M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.
[14]. R. Curtmola, O. Khan, and R. Burns, "Robust Remote Data Checking," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS '08), pp. 63-68, 2008.
[15]. K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Proc. ACM Workshop Cloud Comput- ing Security (CCSW '09), pp. 43-54, 2009.
[16]. D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from The Weil Pairing," J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.
[17]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Service Computing, vol. 5, no. 2, 220-232, Apr.-June 2012.