PRIVACY-PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD

[1]KATAKAMSETTY NITHIN SAI KRISHNA,

[1]M. Tech Student, Department of CSE ,Nalanda Institute Of Engineering and Technology, Kantepudi Village, SattenapalliMandal. Guntur Dist, Andhra Pradesh, India.

[2] MODEM JEEVAN KUMAR,

[2] Assistant Professor, Department of CSE ,Nalanda Institute Of Engineering and Technology, Kantepudi Village, Sattenapalli Mandal. Guntur Dist, Andhra Pradesh, India.

ABSTRACT- Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data rather than a local server or a personal computer. The privacy preserving supports the public auditing without the retrieval access of entire data blocks. The integrity of data in cloud storage, however, is subject to skepticism and scrutiny, as data stored in an untrusted cloud can easily be lost or corrupted, due to hardware failures and human errors. To protect the integrity of cloud data, it is best to perform public auditing by introducing a third party auditor (TPA), who offers its auditing service with more powerful computation and communication abilities than regular users. In this paper, we propose Oruta, a new privacy preserving public auditing mechanism for shared data in an untrusted cloud. In Oruta, we utilize ring signatures to construct homomorphic authenticators , so that the third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data — while the identity of the signer on each block in shared data is kept private from the TPA. We only consider how to audit the integrity of shared data in the cloud with static groups.

1. INTRODUCTION

The cloud services mainly include sharing, online storage, Web-based email and database processing. By adapting the Cloud computing, it becomes easy to share the virtualized resources. Here Users do not need any background knowledge of the services and it's very easy to maintain when compared to any traditional technologies. Cloud computing is of three types named Infrastructure as Service, Platform as a Service, and Software as a service .By these three; it is possible to make complex things very easy.

Infrastructure as a Service delivers basic storage and computing capabilities as standardized services over the network. Third Party Auditor is kind of inspector. There are two categories: private audit ability and public audit ability. Although private audit ability can achieve higher scheme efficiency, public audit ability allows anyone, not just the client, to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform. Hence TPA will help data owner to make sure that his .data are safe in the cloud and management of data will be easy and less burdening to data owner.User will transfer their knowledge on cloud and might access those knowledge anytime anyplace with none further burden. The User doesn't have to worry regarding storage and maintenance of cloud knowledge. However as knowledge is hold on at the remote place however users can get the confirmation regarding hold on knowledge. Hence Cloud knowledge storage ought to have some mechanism which can specify storage correctness and integrity of knowledge stored on a cloud. The foremost drawback of cloud knowledge storage is security. Cloud is employed not just for storing knowledge, but also the hold on knowledge is shared by multiple users. Owing to this the integrity of cloud knowledge is subject to doubt. Thus, facultative public auditability for cloud storage is of vital importance so users will resort to a Third Party Auditor (TPA) to examine the integrity of outsourced knowledge and be doubt free. To firmly introduce an efficient TPA, the auditing method ought to usher in no new vulnerabilities toward user knowledge privacy, and introduce no further on-line burden to user .Sharing knowledge among multiple users is probably one in every of the foremost participating options that motivates cloud storage. a singular drawback introduced throughout the method of public auditing for shared knowledge within the cloud is the way to preserve identity privacy from the TPA, as a result of the identities of signers on shared knowledge could indicate that a selected user within the cluster or a special block in shared knowledge could be a higher valuable target than others. many mechanisms are designed to support public auditing on shared knowledge hold on within the cloud. Throughout auditing, the shared knowledge is unbroken personal from public verifiers, unagency are able to verify shared knowledge integrity exploitation ring signature while not downloading or retrieving the entire file. Ring signature is employed to reason verification data required to audit the correctness of shared knowledge. With this, the identity of the signer in shared knowledge is unbroken personal from public verifiers.

2. RELATED WORK

Cong Wang, Sherman S.M. Chow, Qian Wan, Kui Ren and Wenjing Lou, Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Boyang Wang, Baochun Li, and Hui Li,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.

R. Rajasaranyakumari, S.Velmurugan, K.J. Nithya, Cloud is used not only for storing data, but also the stored data can be shared by multiple users. Due to this the integrity of cloud data is subject to doubt. Several mechanisms have been designed to support public auditing on shared data stored in the cloud. During auditing, the shared data is kept private from public verifiers, who are able to verify shared data integrity using ring signature without downloading or retrieving the entire file. Ring signature is used to compute verification metadata needed to audit the correctness of shared data. With this, the identity of the signer in shared data is kept private from public verifiers. In this paper, we propose a traceability mechanism that improves Data Privacy by achieving traceability and the data freshness(the cloud possess the latest version of shared data) is also proved while still preserving identity privacy.

B.Banu priya, V.Sobhana, Prof.Mishmala Sushith, we have made a concise survey on various privacy preserving techniques in cloud. Homomorphic Authenticable Ring Signature (HARS), privacy-preserving public auditing System for data storage security are discussed. Public key cryptosystem, the MD5 Message-Digest Algorithm are depicted. Proof-Of- Retrievability system for public verifiability is described. Dynamic Provable Data Possession (DPDP) to enlarge the PDP model is discussed in detail. LT codes based cloud storage service (LTCS) to empower efficient decoding, Merkle Hash Tree (MHT) for the block tag Authentication is discussed. Cong Wang, Qian Wang, KuiRen, Wenjing Lou,[7] Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with woo salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s).Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks

C. Wang, Q. Wang, K. Ren, and W. Lou , Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability 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 (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacypreserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

2.1 CLOUD DATA ACCESSING

Cloud may be a wide network space, quite one user will store and access information at anyplace and anytime .so there's several chance to developing information privacy and security issues .Some of the privacy problems ar depleted user control , info speech act, Unauthorized secondary storage, Uncontrolled information proliferation , Dynamic Provision etc. depleted user management may be a information owner lacks control over their information within the cloud, particularly once their data ar accessed or processed within the cloud atmosphere. The information speech act may be a speech act of sensitive information while information moves across the cloud. Sensitive info may be user's identity, usage data, personal info, etc. Unauthorized storage device is that the risk of accessing and retrieving the sensitive info and backing up containing files. The uncontrolled information proliferation is outlined as flows of knowledge within the cloud are unpredictable and uncontrollable by the information owner. Dynamic Provision may be a methodology outlined because the legal responsible entity within the cloud to assure privacy that is remains unclear, attributable to the dynamic nature of the cloud. Also there's several security problems within the cloud information. Data proliferation is outlined because the flow of knowledge within the cloud is unpredictable and uncontrollable by the information owner . Dynamic Provision may be a methodology outlined because the legal responsible entity within the cloud to assure privacy that is remains unclear, attributable to the dynamic nature of the cloud. The system security problems ar access management, verification, the consumer will access device management,

information access, monitor, information deletion verification as follows Access control verification is guarantee solely approved user will access information from the cloud. The shopper access device management is management of consumer access device or points as mobile, PAD, personal computer ar secure enough. the information access monitor is ensuring whom, once and what information being accessed from Cloud by Cloud service supplier. information deletion verification is specifying information deleted should be the information owner rather than another user of Cloud. The cluster signature contains some properties ar traceability, excludability, anonymity, correctness. Traceability may be a cluster manager confirm valid signature and additionally confirm that member of cloud signed within the specific cloud cluster. The cluster signature created by a bunch member can't be attributed successfully to a different and cluster manager cannot generate signature behalf of another cluster member. obscurity may be a group signature on message unworkable to see that particular member of Cloud generated the signature. Correctness may be a properly generated cluster signature that must be accepted by verification by the cluster manager.

3. DIFFERENT MECHANISMS IN PRESERVING PRIVACY IDENTITY PUBLIC AUDITING

Oruta was introduced as a privacy conserving public auditing mechanism. It's a public auditing mechanism with identity privacy that doesn't reveal the identity of the user. Oruta uses the HARS (Homomorphic Authenticable Ring signature) theme that is that the digital signature supported bilinear map. Oruta can support dynamic operations on shared data, dynamic operation contains AN insert, delete, update operation on one block. Since the computation of a ring signature contains a symbol of block that use index of the block as its identifier. Reason is once user modifies single block in information shared by activity insert or delete operation, conjointly that content of those blocks not changed.

Homomorphic authenticators are employed to store blocks of knowledge which will have distinctive properties: correctness, block less verifiability, unforgeability, non plasticity and identity privacy. Oruta works on 5 algorithms:

- **KeyGen:** Here Users can generate their own public/private key pairs.
- **SigGen**: Here User must reckon the ring signatures on the blocks in shared information by mistreatment private key and cluster members' public keys.
- **Modify:** Here User of cluster square measure able to perform insert, delete or update operation within the block. It computes the new ring signature on the changed block.
- **ProofGen:** it's operated by a public protagonist, cloud server along interactively it generate proof of possession for shared information.
- **ProofVerify:** the general public protagonist audits the integrity of shared information by corroboratory the proof.

Whenever a user updates any block of the info, a ring signature is computed by mistreatment its personal key any public key. A signature on any block is computed by mistreatment SigGen algorithms. These signatures square measure verified by ProofVerify algorithm. Because it has achieved unforgeability, none of the user will generate the signature on the block except cluster user. Hence it provides security to the shared go into terms of authentication. However, Oruta isn't capable to trace the identity of any user on misdeed and revoke. It conjointly fails in providing the info freshness. Privacy protective auditing technique, it's conjointly supported homomorphic raincoat that reduces the area to store the verification knowledge, with cluster signature. Homomorphic raincoat used in this method uses pseudo-random perform.

Knox uses Homomorphic authenticable cluster Signature theme, which extends BBS cluster signature and BLS signature in terms of achieving block less verifiability and unforgeability. Knox is performed on the a gaggle of users that have a gaggle manager which might revoke the user on his misbehaviour. AFS-Authenticated Filing System is additionally a privacy protective mechanism that is that the fully same as Oruta except knowledge freshness. It works on documented filing system. It verifies the freshness of the information whereas playing the file operations. They guarantee knowledge freshness with 2 layers: Lower layer stores a raincoat for every block that allows random access. A version range is additionally related to the raincoat block that is incremented by every update. The higher layer consists of Markle tree. Block verions square measure hold on by its leaves whereas hashes of youngster's square measure hold on by internal nodes. The freshness of the file knowledge block is verified by the raincoat block and also the freshness of the block version.

4. HOMOMORPHIC AUTHENTICABLE RING SIGNATURES

In this section, we have a tendency to introduce a replacement ring signature scheme that is appropriate for public auditing. Then, we will show the way to build the privacy-preserving public auditing mechanism for shared information within the cloud based mostly on this new ring signature theme within the next section. As we have a tendency to introduce in previous sections, we have a tendency to will utilize ring signatures to cover the identity of the signer on every block, in order that personal and sensitive info of the cluster isn't disclosed to the TPA. However, traditional ring signatures cannot be directly used into public auditing mechanisms, as a result of these ring signature schemes don't support blockless verification. Without blockless verification, the TPA needs to transfer the whole record to verify the correctness of shared data that consumes excessive information measure and takes long verification times. Therefore, we have a tendency to initial construct a replacement homomorphic authenticable ring signature (HARS) theme, which is extended from a classic ring signature theme, denoted as BGLS. The ring signatures generated by HARS is able not solely to preserve identity privacy however additionally to support blockless verification.

5. PUBLIC AUDITING FOR PROTECTED DATA STORAGE

We consider a cloud data storage service involving three different entities: the cloud user, who has large amount of data files to be stored in the cloud; the cloud server, which is managed by the cloud service provider to provide data storage service and has significant storage. Space and computation resources (we will not differentiate CS and CSP hereafter); the third-party auditor, who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. As users no longer possess their data locally, it is of critical importance for users to ensure that their data are being correctly stored and maintained. In short, although outsourcing data to the cloud is economically attractive for long-term largescale storage, it does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the success of cloud architecture. To save the computation resource as well as the online burden potentially brought by the periodic storage correctness verification, cloud users may resort to TPA for ensuring the storage integrity of their out sourced data. Public auditability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data. However, most of these schemes, do not consider the privacy protection of users' data against external auditors.

6. PRIVACY-PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD

A. Support Dynamic Operations

To change every user within the cluster to simply modify data within the cloud and share the most recent version knowledge with the remainder of the cluster, Oruta ought to additionally support dynamic operations on shared information. Associate in nursing dynamic operation includes Associate in nursing insert, delete or update operation on a single block. Yet, since the computation of a hoop signature includes Associate in nursing symbol of a block (as bestowed in HARS), ancient strategies, that solely use the index of a block as its symbol, don't seem to be appropriate for supporting dynamic operations on shared information. The rationale is that, when a user modifies one block in shared information by performing Associate in Nursing insert or delete operation, the indices of blocks that when the changed block square measure all modified, and also the changes of those indices need users to re-compute the signatures of these blocks, even if the content of those blocks are not changed.

By applying index hash tables, our mechanism will allow a user to expeditiously perform a dynamic operation on one block, and avoid this sort of re-computation on different blocks.

B. Construction of Oruta

Now, we have a tendency to gift the main points of our public auditing mechanism, Oruta. It includes 5 algorithms: KeyGen, SigGen, Modify, ProofGen and ProofVerify. In KeyGen, users generate their own public/private key pairs. In SigGen, a user (either the initial user or a gaggle user) is in a position to reckon ring signatures on blocks in shared information. Every user within the cluster is in a position to perform an insert, delete or update operation on a block, and measure the new ring signature on this new block in Modify. ProofGen is operated by the TPA and therefore the cloud server along to get a symptom of possession of shared information.

In ProofVerify, the TPA verifies the proof and sends an auditing report back to the user. Note that the cluster is pre-defined before shared information is created within the cloud and therefore the membership of the cluster is not modified throughout information sharing. Before the initial user outsources shared information to the cloud, she decides all the cluster members, and computes all the first ring signatures of all the blocks in shared information together with her private key and every one the cluster members' public keys. After shared information is hold on within the cloud, once a gaggle member modifies a block in shared information, this group member additionally has to reckon a replacement ring signature on the changed block.

7. CONCLUSION

We consume ring signatures to create homomorphic authenticators so that a public verifier is able to audit shared data integrity without repossess the entire data yet it cannot differentiate who is the signer on each block. To get better the competence of verifying multiple auditing tasks we further lengthen our mechanism to hold up batch auditing. There are two interesting problems we will continue to study for our future work. One of them is traceability which means the capability for the group manager i.e., the original user to disclose the distinctiveness of the signer based on verification metadata in some special situations. Since Oruta is based on ring signatures where the individuality of the signer is unconditionally protected, the current design of ours does not support traceability.There are two intriguing issues we will keep on considering for our future work. One of them is traceability, which implies the capacity for the gathering administrator to uncover the identity of the signer based on verification metadata in some special situations. Another problem for our future work is how to prove data freshness while still preserving identity privacy.

REFERENCES

[1] 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,” Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl.2010.

[2] 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.

[3] 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.

[4] 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). SpringerVerlag, 2001, pp. 552–565.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,” in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2003, pp. 416–432.

[6] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). SpringerVerlag, 2008, pp. 90–107.

[7] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, “Dynamic Audit Services for Integrity Verification

of Outsourced Storage in Clouds," in Proc. ACM Symposium on Applied Computing (SAC), 2011, pp. 1550–1557.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 534–542.

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

[10] D. Boneh and D. M. Freeman, "Homomorphic Signatures for Polynomial Functions," in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2011, pp. 149–168.