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

An Efficient Privacy Preserving Mechanism of Shared Data in Cloud by Supporting Traceability

B. Sarvani
M.Tech, Software Engineering,
Andhra University College of Engineering,
Visakhapatnam, AP, India.

Dr.K.Venkata Rao
Associate Professor,
Department of Computer Science and Systems
Engineering, A. U. College of Engineering,
Visakhapatnam, AP, India.

ABSTRACT:

Ever since the phenomenon of cloud computing was proposed, has been seen as unitary of the technology that poses the next-generation computing revolution. The popularity and rapid growth of cloud storage services to impart information to others has prompted an uncertainty in the integrity of data in cloud storage, as data stored in the cloud can easily be lost or undermined because of the inescapable hardware/software failures and human errors. A public verifier or a third party auditor provides expert integrity checking services. Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information to public verifiers. Hence we propose a technique called group key generation (gkg) to hide confidential details of user and his data. For this purpose, ring signatures are implemented 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 the public verifier, yet is able to efficiently audit the integrity of shared data within dynamic groups, without being able to distinguish who is the signer on each block. Traceability, a new feature is implemented that allows group manager(i.e., real user) to reveal the identity of signer based on verification metadata, in some special situations.

Index Terms:

cloud computing, storage services, integrity, public verifier, auditor, group key.

INTRODUCTION:

In a cloud model, “customers” plug into the “cloud- to access IT resources which are priced and provided “on-demand”. Delivered over an Internet connection, the “cloud” replaces the company data center or server providing the same service. Cloud computing[3] is a recently evolved computing terminology or metaphor based on utility and-consumption of computing resources. Cloud computing involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer services or resources. Clouds can be classified as public, private or hybrid.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[5] 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 arc giving public auditing process for cloud storage that users can make use of a third-party auditor (TPA)[1] to check the integrity of data. The auditing task monitors data modifications, insertions and deletions.

PROBLEM STATEMENT:

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:

•The types of attackers like internal and external and their capability of attacking the cloud.

•The security risks associated with the cloud, and where relevant considerations of attacks and Countermeasures.
•Emerging cloud security risks.

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[6] will play an important role for privacy data security & minimizing the data risk from hackers.A unique problem introduced during the process of public auditing for shared data in the cloud[8] is how to preserve identity privacy from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a higher valuable target than others.

Alice and Bob work together as a group and share a file in the cloud. The shared file is divided into a number of small blocks, which are independently signed by users. Once a block in this shared file is modified by a user, this user needs to sign the new block using her public/private key pair. The TPA needs to know the identity of the signer on each block in this shared file, so that it is able to audit the integrity of the whole file based on requests from Alice or Bob. After performing several auditing tasks, some private and sensitive information may reveal to the TPA. On one hand, most of the blocks in shared file are signed by Alice, which may indicate that Alice is a important role in this group, such as a group leader. On the other hand, the 8-th block is frequently modified by different users. It means this block may contain high value data.

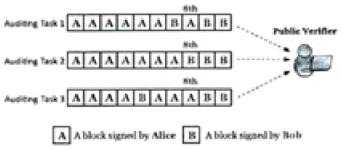


Fig. 1.1 Sample auditing scenario

Alice and Bob share a data file in the cloud, and a public verifier audits shared data integrity with existing mechanisms.Another interesting problem is how to audit the integrity of shared data in the cloud with dynamic groups[7] — a new user can be added into the group and an existing group member can be revoked during data sharing — while still preserving identity privacy. We will leave this problem to our future work. When a user (either the original user or a group user) wishes to check the integrity of shared data, she first sends an auditing request to the TPA. After receiving the auditing request, the TPA generates an auditing message to the cloud server, and retrieves an auditing proof of shared data from the cloud server. Then the TPA verifies the correctness of the auditing proof. Finally, the TPA sends an auditing report to the user based on the result of the verification.

DESIGN OBJECTIVES:

The proposed system is capable of supporting public audit ability and data dynamics.
•In this paper, to solve the above privacy issue on shared data, we propose GKG, a novel privacy-preserving public auditing mechanism.
•More specifically, we utilize ring signatures to construct homomorphism 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 dynamic groups.
•We also extend our concept to ring signatures in which HARS[4] scheme is used.

PROPOSED SYSTEM:
Traceability (Tracking the user):

•All the attributes and points of interest of the general customer are kept up in the log files, by verifier.
•When the client login; the verifier checks the log files with the existing log files. If the details matches with existing records then it allow the users, and if the detail does not coordinate with existing files then some security questions are asked.
•If the answer of security questions is right, then it permits the users and if the answer isn't right, it is considered as fake users and it block that users from getting to the information from the cloud.
•In cloud if it is found that the unauthorized user is trying to access data of any other authorized user then the third party comes in picture, the third party auditor gives the notification to the authorized user that some unauthorized user is trying to access its private data.

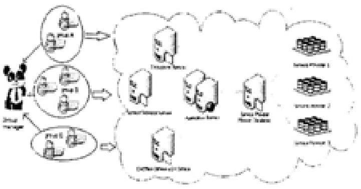


Fig 2. Proposed system Architecture

Group Manager:

This new module is introduced in this paper, which plays important role in implementing traceability. A group manager is the one who handles the entire activities on the client side.

•The group manager maintains the original audit of tasks performed by each group member of all the groups present.
•He can expose the identity the signer based on verification metadata in some special situations.
•Every new user to e group is registered with the group manager, and group manager generates a key for a new member in a group. The key is generated based group into which the user enrolls.
•The GkG mechanism helps the group manager to identify to which group a signer on the block belongs, whenever a block is modified.
•These details are kept privately with the manager, hence the identity of group members is hidden from third party auditor(TPA)

PRELIMINARIES:
Ring Signatures:

The concept of ring signatures is first proposed by Rivest et al. in 2001. With ring signatures, a verifier is convinced that a signature is computed using one of group member's private keys, 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 signature scheme introduced by Boneh et al. (Referred to as BGLS in this paper) is constructed on bilinear maps.

We will extend this ring signature scheme to construct our public auditing mechanism. The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures (e.g., RSA) or hash values (e.g., MD5) of the entire data. However, the size of cloud data is large in general and downloading the entire cloud data to verify data integrity will cost or even waste users' resources and time.Hence verifier should efficiently perform integrity checking without downloading the entire data from the cloud and its critical to preserve identity privacy from public verifiers during public auditing. To solve the above privacy issue, we utilize ring signatures to construct homomorphism authenticators.

Homomorphism Authenticable Ring Signature (LIARS):

As we introduced in previous sections, we intend to utilize ring signatures to hide the identity of the signer on each block, so that private and sensitive information of the group is not disclosed to the TPA. However, traditional ring signatures cannot be directly used into public auditing mechanisms, because these ring signature schemes do not support block-less verification. Without block-less verification, the TPA has to download the whole data file to verify the correctness of shared data, which consumes excessive bandwidth and takes long Verification times. Therefore, we first construct a new homomorphism authenticable ring signature (HARS) scheme, which is extended from a classic ring signature scheme.

Construction of HARS[2]:

HARS contains KeyGen, RingSign and RingVerify algorithm. Every client/user in the group creates his/her public key and private key combines in KeyGen. In RingSign, a user signs a block with his/her private key and all the gathering group members' public keys. In RingVerify, a public verifier has the capacity check whether a given block is marked by a gathering part or not.

a.KeyGen: It is a key generation algorithm which is controlled by the users to make the keys.

b.SingGen: It is utilized by the client to create verification metadata which may comprise of signature.

c.GenProof: it is utilized by Cloud Server to deliver an evidence of data storage correctness.

d.VerifyProof: Used by TPA to audit the proofs. It is separated into two areas as setup phase and review phase.

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

Setup Phase:

Public and private key variables are assigned by using KeyGen and points of details are preprocesses by using SingGen to deliver verification metadata at Cloud Server & deleted its regional duplicate.

Review Phase:

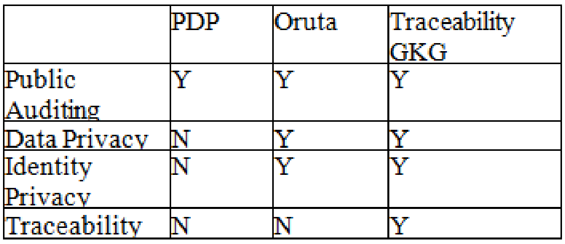
TPA issues a review idea to Cloud Server. The Cloud Server will acquire a response idea by executing GenProof. TPA conforms the reaction utilizing and its verification meta-data.

Scheme:

Let Consider G I , G2, GT are the multiplicative cyclic-groups of order p. g I , g2 are the generators of G I and G2 respectively. Let bilinear map as c: GI x G2 —* GT, and NI:G2 GI be a computable isomorphism with xi/ (g2) = gl.There is a public map-to-point hash function HI: 10, I} * I .(e, yr, p. G I, G2. GT, g I , g2, H 1) these are the global parameters. d be the total numbers of users in group. Let U denote the group which contains all the d users.

RESULTS:

Efficiency of Traceability GKG is evaluated in the below experiments:Performance of Batch Auditing: at the point when there are different auditing verifications, public in general verifier can enhance the efficiency of confirmation by performing batch auditing. The following Table I shows the comparison between Separate auditing and batch auditing and the Figure 2 show the graphical representation of Table I. (ii).Traceability GKG: Table below shows the comparison between Provable Data Possession (PDP), Oruta and Traceability GKG techniques.



	PDP	Oruta	Traceability GKG
Public Auditing	Y	Y	Y
Data Privacy	N	Y	Y
Identity Privacy	N	Y	Y
Traceability	N	N	Y

CONCLUSION:

In this paper, we propose GkG, a privacy-preserving public auditing mechanism for shared data in the cloud, that can also support traceability. We utilize ring signatures to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support dynamic groups.

REFERENCES:

[1]Boyang Wang, Baochun Li and Hui Li, Oruta: Privacy-Preserving Public Auditingfor Shared Data in the Cloud" in IEEE Transactions on Cloud Computing,Volume:2,Issue:1,Issue Date :March 2014.

[2]Boyang Wang, Baochun Li and Hui Li Privacy-Preserving Public Auditing for Shared Data in the Cloud", published in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on 24-29 June 2012.

[3]Deepak Puthal, B. P. S. Sahoo, Sambit Mishra, and Satyabrata Swain, "Cloud Computing Features, Issues and Challenges:A Big Picture" in 2015 International Conference on Computational Intelligence & Networks (CINE 2015).

[4]Ms.Sonam and M. Kamble, Prof.A.C.Lomte. Homomorphic Authenticable Ring Signature (HARS) mechanism for Public Auditing on Shared Data in the cloud (Oruta)" in International Journal of Engineering Research and General Science Volume 2,Issue 6, October-November, 2014.

[5]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.

[6]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.

[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.

[8]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

Author's Details:

Ms.Sarvani Bhogireddi, Student, received M.Tech in 2015 with specialization in Software Engineering from department of Computer Science and Systems Engineering, Andhra University College of Engineering, Visakhapatnam, AP, India.

Dr.K.Venkata Rao,Associate Professor, Department of Computer Science and Systems .Engineering ,A. U. College of Engineering,Visakhapatnam, AP,India. Also worked as former Webmaster of Andhra University Soon after B.Tech served as a Software Engineer for 2 years, and later out of passion towards teaching worked in various positions as a Lecturer, Assistant Professor, Associate Professor and taught for various levels of students of different courses like B.Sc(Computers),BCA, M.Sc(Computers),M.S(IS), M.C.A, B.Tech and M.Tech.