International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Privacy Preserving For The Data Sharing In The Cloud

D.Yugandhar
MCA Sri Padmavathi College Of Computer Sciences And Technology Tiruchanoor, Tirupati,Andhra Pradesh, India

ABSTRACT

Online data exchange for increased productivity and efficiency is now one of the most important requirements for any business. The advent of cloud computing has pushed the boundaries of sharing beyond geographical boundaries, allowing a variety of users to collaborate and collaborate on shared data.In existing system first, theyintroduce the PDP model to ensure ownership of files on untrusted storage, and provide an RSA-based scheme for a static case that achieves communication costs. They also proposed a publicly verifiable version that would allow anyone, not just the owner, to challenge the server for data ownership. They proposed a lightweight PDP scheme based on cryptographic hash function and symmetric key encryption, but the servers can deceive the owners by using prior metadata or responses because the challenges are not challenging. The number of updates and challenges is limited and fixed in advance, and users cannot perform block inserts. With cloud storage services, it is commonplace for data to be not only stored within the cloud, but additionally shared across multipleusers. However, public auditing for such shared information — whereas protective identity privacy — remains to be associate degree open challenge. In thispaper, we tend to propose the primary privacy-preserving mechanism that permits public auditing on shared information keep within the cloud. aboveall,we exploit ring signatures to cypher the verification data required to audit the integrity of shared information. With our mechanism, the identity of the signer on every block in shared information is unbroken personal from a 3rd party auditor (TPA), World Health Organization continues to be ready to in public verify the integrity of shared information while not retrieving the whole file. Our experimental results demonstrate the effectiveness and potency of our proposed mechanism once auditing shared information.

Keywords: Public Auditing, Privacy-Preserving, Shared Data, Cloud Computing.

I. INTRODUCTION

Cloud Computing is that the new trend model for processing that uses the internet to communicate and store information. Key options of cloud computing embrace sharing information and firmly storing important information within the cloud.once it involves sharing and storing information, Cloud users are a little hesitant to place the data within the cloud and lookout of the confidentiality and security of the info. Cloud service suppliers manage an enterprise-class infrastructure that provides a scalable, secure and reliable environment for users, at a far lower marginal cost attributable to the sharing nature of resources. it's routine for users to use cloud storage services to share information with
others during a team, as information sharing becomes a regular feature in most cloud storage offerings, together with Dropboxand Google Docs. The integrity of information in cloud storage, however, is subject to skepticism and scrutiny, as information hold on in Associate in Nursinguntrusted cloud will simply be lost or corrupted, due to hardware failures and human errors. To protect the integrity of cloud information, it's best to perform publicauditing by introducing a third party auditor (TPA), who offers

its auditing service with a lot of powerful computation and communication skills than regular users. The first demonstrable information possession (PDP) mechanism to perform public auditing is meant to examine the correctness of information hold on in Associate in Nursing untrusted server, without retrieving the complete information. Moving a discovery, Wang is meant to construct a public auditing mechanism for cloud information, so that during public auditing, the content of personal data happiness to a private user isn't disclosed to the third party auditor. We believe that sharing information among multiple users is perhaps one amongst the foremost partaking options that motivates cloud storage. a unique drawback introduced throughout the method of public auditing for shared information within the cloud is how to preserve identity privacy from the TPA, because the identities of signers on shared information could indicate that a particular user within the cluster or a special block in shared data could be a higher valuable target than others.

With cloud storage services, it is commonplace for data to be not only stored in the cloud, but also shared across multipleusers. 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. Our experimental results demonstrate the effectiveness and efficiency of our proposed mechanism when auditing shared data.

With the usage of public auditing in the cloud, the TPA may receive amount of auditing requests from different users in a very short time. Unfortunately, allowing the
TPA to verify the integrity of shared data for these users in several separate auditing tasks would be very inefficient. Therefore, with the properties of bilinear maps, we further extend Oruta to support batch auditing, which can improve the efficiency of verification on multiple auditing tasks.

II. ALGORITHM

In this section we are going to know the algorithms used in this paper. The algorithm is oruta which is constructed by using HARS.WithOruta,the TPA can verify the integrity of shared data for a group of users without retrieving the entire data. Meanwhile, the identity of the signer on each block in shared data is kept private from the TPA during the auditing.

Oruta should also support dynamic operations on shared data. An dynamic operation includes an insert, delete or update operation on a single block. However, since the computation of a ring signature includes an identifier of a block (as presented in HARS), traditional methods, which only use the index of a block as its identifier, are not suitable for supporting dynamic operations on shared data. The reason is that, when a user modifies a single block in shared data by performing an insert or delete operation, the indices of blocks that after the modified block are all changedand the changes of these indices require users to re-compute the signatures of these blocks, even though the content of these blocks are not modified. we present the details of our public auditing mechanism, Oruta.

It includes five algorithms:
KeyGen,**SigGen**, **Modify**, **ProofGen**and **ProofVerify**. In Key- Gen, users generate their own public/private key pairs.

In SigGen, a user (either the original user or a group user) is able to compute ring signatures on blocks in

shared data. Each user in the group is able to perform an insert, delete or update operation on a block, and compute the new ring signature on this new block in Modify. ProofGenis operated by the TPA and the cloud server together to generate a proof of possession of shared data. In ProofVerify, the TPA verifies the proof and sends an auditing report to the user.

Note that the group is pre-defined before shared data is created in the cloud and the membership of the group is not changed during data sharing. Before the original user outsources shared data to the cloud, she decides all the group members, and computes all the initial ring signatures of all the blocks in shared data with her private key and all the group members' public keys.

After shared data is stored in the cloud, when a group member modifies a block in shared data, this group member also needs to compute a new ring signature on the modified block.

III. CONCLUSION

In this paper, we propose Oruta, the first privacypreserving public auditing mechanism for shared knowledge in the cloud. we tend to utilize ring signatures to construct homomorphic authenticators, that the TPA is ready to audit the integrity of shared knowledge, nevertheless cannot distinguish World Health Organization is the signer on every block, which may bring home the bacon identity privacy. to enhance the potency of verification for multiple auditing tasks, we tend to more extend our mechanism to support batch auditing. a remarkable downside in our future work is a way to expeditiously audit the integrity of shared knowledge with dynamic teams whereas still conserving the identity of the signer on every block from the third party auditor.

IV. 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). Springer- Verlag, 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). Springer- Verlag, 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.

[11]. A. L. Ferrara, M. Green, S. Hohenberger, and M. 0. Pedersen, "Practical Short Signature Batch Verification," in Proc. RSA Con- ference, the Cryptographers' Track (CT-RSA). Springer-Verlag, 2009, pp. 309-324.

[12]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in Proc. ACM Conference on Computer and Communications Security (CCS), 2006, pp. 89-98.

[13]. A. Juels and B. S. Kaliski, "PORs: Proofs pf Retrievability for Large Files," in Proc. ACM Conference on Computer and Communications Security (CCS), 2007, pp. 584-597.

[14]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proc. International Conference on Security and Privacy in Communication Networks (SecureComm), 2008.

[15]. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in Proc. ACM Conference on Computer and Communications Security (CCS), 2009, pp. 213-222.

Author's Profile:

Mr. Dhande Yugandhar has received his graduation degree in BSc. Bachelor of Science from Sri Vaishnavi Degree & PG College, Affiliated to Yogi Vemana University , Kadapa , AP in the year of 2012 – 2015. At Present he is Pursuing Post graduate degree MCA, Master of Computer Applications from Sri Padmavathi College of Computer Sciences and Technology Affiliated to Sri Venkateswara University , Tirupati, AP, India.