Privacy Preserving in Shared Data using Third Party Auditing

Surendra Babu M S[1] Satish B Basapur[2] Vikas L Ghorade[3]

Abstract— providing security to data is one of the major challenges in cloud computing. As many users use cloud for storing their private data it is essential to provide privacy and security for it. Many approaches are present to handle these issues but lack in providing confidence in end users as they are unaware of the status of data. Due this reason of many big companies, users are not showing interest in cloud .So to provide transparency third party auditing is done as not only cloud service provider is assuring the security of the data but also third party auditor. This increases the confidence of the end users as well third party auditor informs end user about any data breach if happens which makes end user to have awareness about his data. this paper throws light on how third party auditing is a key factor in increasing the trust of end user, big companies on cloud computing.

Key words: Privacy Preserving, Shared Data, Third Party Auditing

I. INTRODUCTION

Cloud service providers manage an enterprise class infrastructure that offers a scalable, secure and reliable environment for users, at a much lower marginal cost due to the sharing nature of resources. It is routine for users to use cloud storage services to share data with others in a group, as data sharing becomes a standard feature in most cloud storage offerings, including Drop box and Google Docs.

The integrity of data in cloud storage, however, is subject to skepticism and scrutiny, as data stored in an entrusted cloud can easily be lost or corrupted, due to hardware failures and human errors. This a serious issue as it may lead for end users to stop having faith in cloud. So to protect the integrity to a personal user is not disclosed to the third party auditor. Sharing of data among multiple users is one of the important key feature which motivates the users to store data on cloud. A unique problem introduced during the process of public auditing for shared data in the cloud 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 more valuable target than others. Oruta, a new privacy-preserving public auditing mechanism for shared data in an untrusted cloud.

II. OBJECTIVES

A. Authentication

oruta provides authentication with the help of key. First of all the key is generated at cloud server using RSA algorithm. This generated key is given to end users based on data owner's permission. only these users with key can access the data.

B. Privacy

oruta provides privacy by allowing users to view only portion of data to which data owner has given permission. data owner can split data and form many portions of data .each portion has separate key so data owner is in control of situation he can limit any end user to which ever extent he wants.

C. Security

oruta provides security to data. If any hacker hacks into data the data owner is immediately intimated by oruta.

III. RELATED WORK

D Boneh et al[1] have used RSA to provide ata dynamics and BLS to provide audibility. It is difficult to remove sensitive information before auditing as it may be used by auditor for his personal benefits. So complete data is not provided to auditor. But restricting auditor to a limit does not allow to check data completely so to overcome these problems D Boneh proposed approach which allows clients themselves to check the integrity of data at any time.

R burns et al[2] have proposed PDP which is unique technique that enables the users to verify data without accessing it. Hence how much ever the data may be large it does not effect for the client to verify and also does not indulge any load on server. It also lessens the cost for client to verify as there is no need to load or access data. PDP fits for these purposes: They incur a low (or even constant) overhead at the server and require a small, constant amount of communication per challenge. Key components of proposed schemes are the homomorphic verifiable tags. They allow to verify data possession without having access to the actual data file.

H Xiong[3] introduced a concept known as cloudsafe which is a general and practical data-protection solution by integrating cryptographic techniques and systematic mechanisms that addresses the issue of Outsourced data processing on vulnerable cloud platforms .Data protection in public cloud remains a challenging problem. Outsourced data processing on vulnerable cloud platforms may suffer from cross-VM attacks, e.g. side-channel attacks that leak secrecy keys. CloudSafe puts special emphasis on new security issues raised from cross-VM side-channel attacks against secure data processing on the virtualized cloud platforms.

IV. CONCLUSION

Oruta is a efficient technique which not only provides facility for third party to audit but also preserves the privacy of data owners as block of data which is audited does not contain the signature of data owner there by making it resistant to leak of privacy.

REFERENCES

[1] 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.

[2] 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] H Xiong CloudSafe: Securing Data Processing within Vulnerable Virtualization Environments in the Cloud.

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Kon-winski, 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, April 2013.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in *Proc.* IEEE INFOCOM, 2012, pp. 525–533.

[6] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in Proc.ASIACRYPT. Springer-Verlag, 2011, pp. 552–565.

[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. Ø. Pedersen, "Practical Short Signature Batch Verification," in Proc. RSA Conference, 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.

