Survey on Privacy Preserving Auditing of Dynamic Shared Data in Cloud

Priyanka S. Tandale
ME Scholar
Department of Computer Engineering
PICT, Pune

Prof. Virendra Bagade
Assistant Professor
Department of Computer Engineering
PICT, Pune

Abstract

Cloud computing technology is increasingly patronized by both organizations and individuals because of its ability to provide users with on-demand, flexible, reliable and low-cost services. Cloud Storage has become popular because of the abundant benefits provided by it like ubiquity, elasticity, and scalability. Along with data security/privacy, ensuring data integrity of outsourced data is also one of the major concerns in adoption of the cloud services. This problem is also known as data auditing when the verification is conducted by a trusted third party. With cloud storage services, it is common place 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.

Keywords: Cloud computing, Security, Auditing, privacy-preserving, shared data, cloud computing
General Terms: Cloud computing, Security

I. INTRODUCTION

Cloud services are becoming indisputable parts of modern information and communication systems and step into our daily lives. Cloud service providers manage an enterprise-class Infra-structure 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 team, as data sharing becomes a standard feature in most cloud storage offerings, including Dropbox and Google Docs. 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.

A new privacy preserving public auditing mechanism for shared data in an untrusted cloud. We utilize ring signatures to construct holomorphic 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. In addition, we further extend our mechanism to support batch auditing, which can audit multiple shared data simultaneously in a single auditing task. To use random masking to support data privacy during public auditing, and leverage index hash tables to support fully dynamic operations on shared data. A dynamic operation indicates an insert, delete or update operation on a single block in shared data.

II. SECURITY AUDITING FRAMEWORK

Security auditing framework to establish the user trust by

1) Allowing the cloud service users (CSUs) to provide their security preferences with the desired cloud services
2) Providing a conceptual mechanism to validate the security controls and internal security policies of cloud service providers (CSPs) published in the CSA's (Cloud Security Alliance) Security Trust and Assurance Registry (STAR) database
3) Maintaining a database of CSPs along with their responses to the Consensus assessment Initiative Questionnaire (CAIQ) as well as the certificates issued by the certificate authorities.

III. THIRD PARTY AUDITOR BASED TRUST

A TPA is required to obtain an objective trust model. The role of the auditor is to total the predetermined criteria that is relevant to the CSP to establish trust. Key stakeholders of cloud computing, such as CSU, CSP and a TPA are involved to establish a trust model. If a CSP requests to enter the clouding computing market it must provide a set of information for registration into a TPA. This information would include basic material of services that the CSP can offer the CSUs. Not all of the services required by the CSU may be available from a given CSP. In proposed an analysis of problems that may arise for CSU using a CSP. The first

problem posed was the protection of data integrity. The data must be monitored so that CSU's data is not read or leaked and no new threats will be introduced to the data during auditing. To insure data integrity, one method that can be used is message authentication with a cryptographic technique of Message Authentication Code (MAC). Second presented problem is dynamic data support; data that is added, deleted or updated at any given time. The solution is implementing provable data possession (PDP). Support for access control is the third problem posed. This is permitting the CSU to have access to its resources and the TPA is able to verify identify of the CSU. The Trusted Computer System Evaluation Criteria is the accepted criterion that resolves the third problem. The fourth is support for batch auditing. The solution to this problem is called batch-processing mechanism. The final problem outlined by is to minimize the cost of auditing. There has not been a definite solution found to this drawback of cloud computing. A TPA is needed to protect the integrity of the data a user is storing in the cloud. A TPA should audit and log the user and CPS's behavior A process was proposed in to build a trusted and practical TPA. This process is called Trust Enhanced Third Party Auditor (TETPA). To implement this method certain requirements are necessary:-Trust identification, strict storage security, and Active challenging and notifying.

A. Provable data possession (PDP):

The first provable data possession (PDP) mechanism to perform public auditing is designed to check the correctness of data stored in an untrusted server, without retrieving the entire data. Moving a step forward is designed to construct a public auditing mechanism for cloud data, so that during public auditing, the content of private data belonging to a personal user is not disclosed to the third party auditor.

B. 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 members' private keys, but the verifier is not able to determine which one.

IV. THE ROLE OF CSA

In our proposed framework, we adopted the CAIQ which allows the CSPs to publish their security strength by choosing the appropriate security controls within each security domain. The CAIQ defines sixteen different security factors where each one has a varying numbers of security controls. We consider these security factors as top-level security domains (TLSD) as shown in Fig1.The TLSD covers a variety of different security, privacy, management, and auditing aspects ranging from applications security to threats and vulnerability management. The description of TLSD and the specific security controls are given in Appendix A. The role of CSA in our proposed framework is to regulate the collection and storage of the CSP's responses. A CSP that wants to publish its security information contacts the CSA to request non-validated security controls and policies of the CSPs. for the CAIQ. Once the response of the CAIQ is received from one particular CSP, it will be stored in the STAR database maintained by the CSA. Thus, the STAR database contains the information of non-validation security controls.

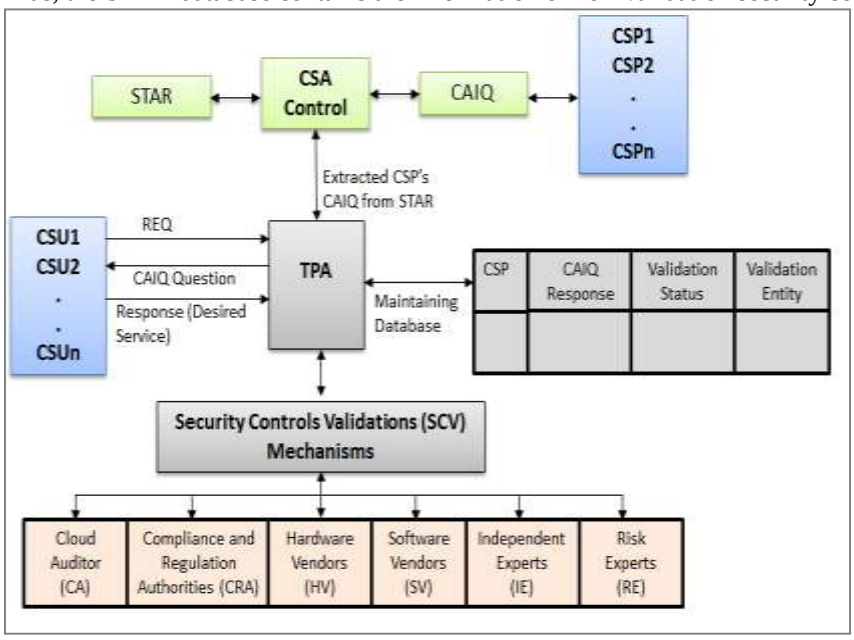

Fig. 1: TPA based Framework

V. SECURE CLOUD STORAGE MODEL

The Proposed system consists of following entities:

A. Client:

Client is an entity, who possesses data files that he/she may wish to store on cloud and relies on cloud for further maintenance and operations. Client can be an individual or any organization, or a group of organizations having same policies or objectives.

B. Cloud Storage Server:

It is an entity, which possess significant amount of storage space as well as computational and network resources to manage client's data stored on cloud.

Cloud storage server is managed by Cloud Service Provider (CSP).

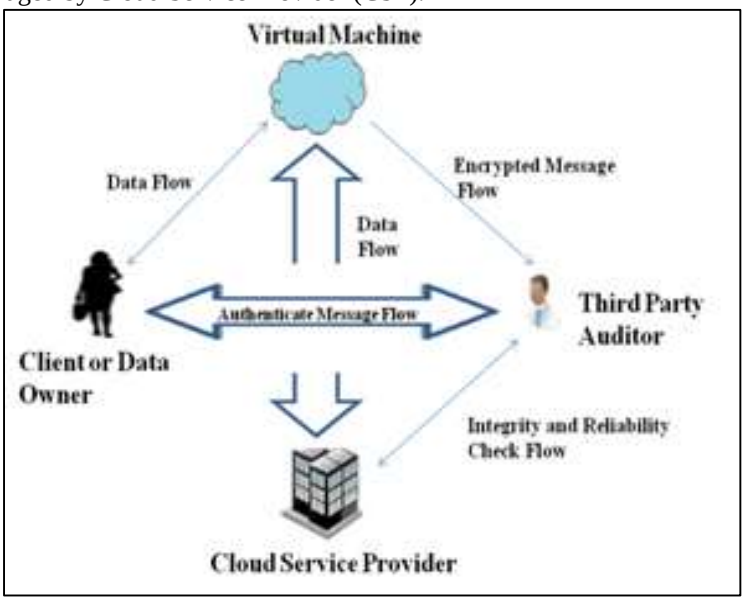

Fig. 2: Secure Cloud Storage Model

C. Third Party Auditor: (TPA)

It is a trusted entity which is having skills, expertise and capabilities and TPA is allowed to assess the integrity of data stored on cloud by the client. TPA performs auditing of client's data stored on cloud On behalf of client. It periodically notifies the status of client's data to client this work also supports the dynamic operations on data.

VI. RELATED WORK

Sr.no	*Author*	*Topic*	*Algorithm Applied*	*Advantages*	*Disadvantages*
1	*Q .wang [1]*	*Enabling public verifiability and data dynamics for storage in cloud computing*	*Merkle hash tree and Bilinear map*	*Support dynamic operations on data.*	*This Scheme is uses the concept of Third Party Auditor (TPA), whose failure can affect the entire scheme*
2	*K.D. Bowers*	*Proof of Retrievability: Theory and implementation.*	*Cryptographic Techniques With error correcting and spot checking codes.*	*Lower storage overhead.*	*Though this scheme provides possession and retrievability, but it fails to achieve auditing and dynamic operations on data.*
3	*C.Wang*	*Ensuring data storage security in cloud.*	*Erasure correcting code.*	*This scheme supports the dynamic operations on data like data update, delete and append.*	*Though this scheme supports dynamic operations on data, it Not supports insertion of data blocks in between the data.*
4	*G.Ateniese*	*Provable data possession at untrusted stores*	*RSA algo. & homomorphic verifiable Tags(HVT)*	*Allows a user whose data has been stored at untrusted server to verify that the server possesses the original data without retrieving it*	*Though this scheme supports auditing but it does not support dynamic operations on data as dynamic case may incur some design and security problems*
5	*Q.wang*	*Enabling public auditability and data dynamics for storage in cloud computing.*	*Merkle hash tree and homomorphic authenticators, with erasure coded data.*	*User's verification task on data stored on cloud is hand over to a Third Party Auditor (TPA), which reduces user's task and time.*	*This scheme may suffer if TPA fails during any failure events.*

VII. CONCLUSION

As TPA is going to perform number of auditing tasks simultaneously, it is essential for this scheme to manage the load on TPA, so that it can perform auditing properly. Hence this work proposes to provide simultaneous auditing tasks by using Third Party Auditor (TPA) with dynamic data support and sharing in cloud.

REFERENCES

[1] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE" Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" IEEE Transactions on Cloud Computing, Volume: 2,Issue:1,Issue Date :March 2014
[2] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE "Privacy-Preserving Public Auditing for Secure Cloud Storage"
[3] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Symp. Research in Computer Security (ESORICS '09),2009.
[4] 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), 2007.
[5] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Report 2008/175, Cryptology ePrint Archive, 2008
[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in CloudComputing,"Proc.17thInt'lWorkshop Quality of Service (IWQoS '09), 2009.
[7] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li "Enabling10. Qian Wang, Cong Wang, Kui Ren , Wenjing Lou And Jin Li " Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE transaction Paper on Parallel and Distributed Systems vol 22 No 5, May 2011 .
[8] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, ''Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage,''IEEE Trans. Parallel Distributed System. vol. 23, no. 12, Dec. 2012.
[9] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proc. In-ternational Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2003.
[10] 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.
[11] 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.
[12] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, "Practical Short Signature Batch Verification," in Proc. RSA Con-ference, the Cryptographers' Track (CT-RSA). Springer-Verlag, 2009.