Enabling Public Verifiability for Storage Security by Preserving Privacy in Cloud

Saravavan T[1] Priyadharsini C[2] Preethy R[3]
[1]Assistant Professor
[1, 2, 3]Department of Information Technology
[1, 2, 3]Jeppiaar Engineering College, Chennai, India

Abstract—*With cloud data services, it is common place not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information and identity privacy to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one.*

Keywords—Integrity, Auditing, Metadata, Ring signatures, Public verifier.

I. Introduction

Cloud service providers offer users efficient and scalable data storage services with a much lower marginal cost than traditional approaches .The integrity of data in cloud storage is subject to skepticism and scrutiny, as data stored in the cloud can easily be lost or corrupted due to the inevitable hardware/ software failures and human errors .The objective of this paper is to propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. Ring signatures is exploited to compute verification metadata needed to audit the correctness of shared data. With this mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, this mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one.

II. Related Work

In ”Privacy-Preserving Public Auditing for Secure Cloud Storage” [1] the homomorphism linear authenticator and random masking are used to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process. This eliminates the burden of cloud user from the tedious and possibly expensive auditing task and alleviates the users' fear of their outsourced data leakage. But the technique of public key based homomorphism linear authenticator drastically reduces the communication and computation overhead. In “Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud” [4] when a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. The group can save a significant amount of computation and communication resources during user revocation. But this revoked user should no longer be able to access and modify shared data. In addition, to operate multiple auditing tasks from different users efficiently, they extended their mechanism to enable batch auditing by leveraging aggregate signatures [7].

III. Proposed System

The propose system Oruta, a privacy-preserving public auditing mechanism for shared data in the cloud the ring signatures is utilized to construct homomorphism 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, batch auditing mechanism is used. There are two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations.

IV. System Model

As illustrated in Fig. 1, the system model in this paper involves three parties: the cloud server, a group of users and a public verifier. There are two types of users in a group: the original user and a number of group users. The original user initially creates shared data in the cloud, and shares it with group users. Both the original user and group users are members of the group. Every member of the group is allowed to access and modify shared data. Shared data and its verification metadata (i.e., signatures) are both stored in the cloud server. A public verifier, such as a third party auditor providing expert data auditing services or a data user outside the group intending to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server.

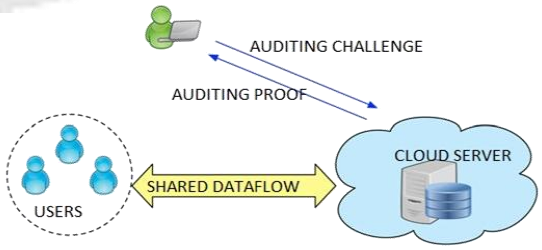
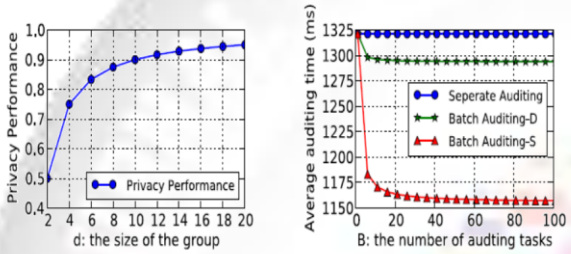


Fig. 1: Our system model includes the cloud server, a group of users and a public verifier

When a public verifier wishes to check the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the cloud server responds to the public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof.

V. Experimental Results

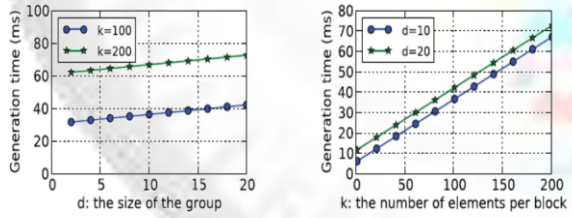
The privacy performance of our mechanism depends on the number of members in the group. Given a block in shared data, the probability that a public verifier fails to reveal the identity of the signer is 1 _ 1=d, where d = 2. Clearly, when the number of group members is larger, our mechanism has a better performance in terms of privacy. As we can see from Fig. 2a, this privacy performance increases with an increase of the size of the group.



(a) Impact of d on privacy performance. (b) Impact of B on the efficiency of batch auditing, where $k = 100$ and $d = 10$.

Fig. 2: Performance of Privacy and Batch Editing

As illustrated in Figs. 3a and 3b, when k is fixed, the generation time of a ring signature is linearly increasing with the size of the group; when d is fixed, the generation time of a ring signature is linearly increasing with the number of elements in each block. Specifically, when d ¼ 10 and k ¼ 100, a user in the group requires about 37 milliseconds to compute a ring signature on a block in shared data.



(a) Impact of d on signature generation time (ms). (b) Impact of k on signature generation time (ms).

Fig. 3: Performance of Signature generation

VI. Conclusion and Future Work

In this paper, we propose Oruta, the first privacy-preserving public auditing mechanism for shared data in the cloud. With Oruta, the public verifier is able to efficiently audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can preserve identity privacy for users. An interesting problem in our future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor.

There are two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager (i.e., the original user) to reveal the identity of the signer based on verification metadata in some special situations. Since Oruta is based on ring signatures, where the identity of the signer is unconditionally protected [12], the current design of ours does not support traceability. To the best of our knowledge, designing an efficient public auditing mechanism with the capabilities of preserving identity privacy and supporting traceability is still open. Another problem for our future work is how to prove data freshness (prove the cloud possesses the latest version of shared data) while still preserving identity privacy.

References

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.

[2] 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. Zachariah, "A View of Cloud Computing," Comm. ACM,vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[4] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[6] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[7] D. Boneh, C. Gentry, B. Lynn, and H.Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of cryptographic Techniques: Advances in Cryptology (EUROCRYPT'03), pp. 416-432, 2003

[8] 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), pp. 598-610, 2007.

[9] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008..

[10] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security.(ESORICS'09), pp. 355-370, 2009.

[11] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th

Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

[12] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT'03), pp. 416-432, 2003