Original Research Paper

Volume : 5 | Issue : 11 | November 2016 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 69.48

A Survey on Auditing Shared Data in Cloud through Privacy Preserving Mechanisms

Engineering

KEYWORDS: Public-Auditing, Privacy-preserving, Shared data, Batch auditing, and cloud computing.

R.Vikram — Asst. Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyd,Telangana,India.

Kareemunnisa — Asst. Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyd,Telangana,India.

Y.Sowjanya — Asst. Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus,Hyd,Telangana India.

ABSTRACT

Cloud is a place where we can store a huge amount of data and access them across multiple users. This leads two major problems such as "security" and "privacy". Many mechanisms has been designed to allow both data owners and public verifiers who are also called as Third Party Auditors (TPA) to efficiently audit the integrity of data in cloud without retrieving the entire data from the server. Public or TP auditing on the integrated data may reveal the confidential information. The proposed system uses a novel privacy-preserving mechanism called ORUTA (One Ring to Rule Them All) support public auditing on shared data in the cloud and also exploits ring signatures to compute verification metadata (signature) needed to audit the correctness of shared data. The main scope of this project is to provide multiple auditing tasks simultaneously instead of verifying one by one.

1. INTRODUCTION:

Cloud service providers provide an efficient and scalable data storage services to the user with a low cost. Due to this the users purchase cloud storage services to share their data with others in a group. The accuracy of the data which is stored in the cloud cannot be believed and examined because the data stored in the cloud can be easily lost or corrupted due to the hardware or software failures or due to the human errors[3],[4]. Sometimes the cloud service provider does not inform users about the data errors in order to maintain the reputation of their services and avoid losing benefits. That is why the data in the cloud should be checked before utilization.

The existing approach [2] to make sure that the data is correct is to download the total data from cloud, and then find out the accuracy of the data by checking the correctness of signatures of the total data. Certainly, this current approach is successful in checking the correctness of cloud data but it is not so effective and efficient and may cause leakage of the confidential information.

The is because of the size of cloud is very large we can store a massive amount of data in cloud but for verifying the stored data we need to download the entire data this will cost more when the data is corrupted. Many mechanisms [6], [7], [8], [9], [10], [11], [12], [13], [14] have been introduced for efficiently auditing the shared data without downloading the entire data from the cloud, this is called public auditing. In the proposed mechanism the data is divided into small blocks, where each block is independently signed by the owner so, while auditing the integrity of this shared data random combination of these blocks are taken and verified. Here the public auditor or verifier who provides an expert integrity checking services to the users may utilize the users private data via cloud to avoid these Wang et al. proposed a public auditing mechanism so that during public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers. Unfortunately present public auditing solutions focus on personal data in cloud.

Shared Data: The ability to share same data resource with multiple applications or users. The data is stored in one or more servers in the network and that there is some software that prevents the same set of data from being changed by two people at the same time.

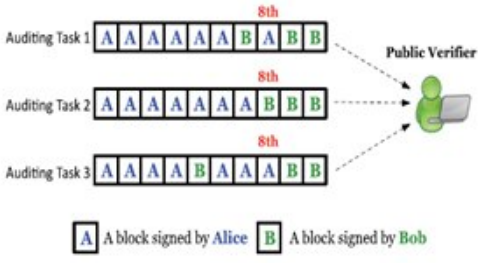


Fig.1: Alice and Bob share a data file in the cloud, and a public verifier audits shared data integrity with existing mechanisms.

For example, in Fig.1 Alice and Bob work together in a group and share a file in the cloud. When the file is shared in cloud the file is divided into small blocks where each block is independently signed by the two users with existing auditing mechanisms. Once a block is modified by a user, the user needs to sign the new block with his or her own private key. The data in the cloud is changed frequently by the different users. In order to correctly audit the integrity of the entire data public verifier needs to choose the appropriate public key for each block. i.e.a block signed by Alice can only be correctly verified by Alice's public key. After performing several auditing tasks, public verifier comes to a conclusion that Alice plays a more important role in the group than the Bob because most of the blocks in shared file are signed by Alice, public verifier can also easily identify that eighth block contain the confidential information because this block is frequently modified by different users. So, to protect this confidential information, it is essential to protect identity privacy from public verifiers during public auditing.

2. Related Work:-

The Cloud service providers offer users efficient and scalable data storage services with a much lower marginal cost than existing approaches [2].

The accuracy of data in cloud storage, however, is subject to skepticism and scrutiny, as data stored in the cloud can easily be lost or scorrupted due to the inevitable hardware/ software failures and human errors [3], [4].

Unfortunately current public auditing mechanisms focus only on personal data in cloud [1]. Wang et al. [10] leveraged homomorphic tokens to ensure the correctness of erasure codes-based data distributed on multiple servers. This mechanism is able not only to support dynamic data, but also to identify misbehaved servers. To minimize communication overhead in the phase of data
Repair.

Zhu et al. [12] exploited the fragment structure to reduce the storage of signatures in their public auditing mechanism. In addition, they also used index hash tables to provide dynamic operations on data.

The verifier challenges the untrusted server by specifying the positions of a collection of sentinels and asking the untrusted server to return the associated sentinel values. Shacham and Waters [7] designed two improved schemes. The first scheme is built from BLS signatures [21], and the second one is based on pseudo-random functions.

Juels and Kaliski [20] defined another similar model called Proofs of Retrievability (POR), which is also able to check the correctness of data on an untrusted server. The original file is added with a set of randomly-valued check blocks called sentinels. The verifier challenges the untrusted server by specifying the positions of a collection of sentinels and asking the untrusted server to return the associated sentinel values.

Wang et al. [9] utilized Merkle Hash Tree and BLS signatures [21] to support dynamic data in a public auditing mechanism. Erway et al. [8] introduced dynamic provable data possession (DPDP) by using authenticated dictionaries, which are based on rank information.

3. Proposed method :-

Public-auditing is one of the measures to check the integrity of the shared data in the cloud because if the auditing for the data in cloud is not done this may lead to many security and privacy problems, and the intruder may attack on the data and can be corrupted. To avoid all these problems a new privacy-preserving public auditing mechanism called ORUTA i.e One Ring to Rule Them All is proposed and in that ring signature are used to build a Homomorphic Authenticable Ring Signatures. So, that we can preserve the identity as well as the data of the user to others.

Objectives:-

- Support batch auditing
- It can perform multiple auditing tasks simultaneously
- Improve the efficiency of verification for multiple auditing tasks
- Preserve data privacy from public verifiers

4. Conclusion and future work :-

ORUTA One Ring to Rule Them All, is one of the public auditing mechanism to preserve the identity privacy of both the data and the data owners. By utilizing the ring signatures concept we construct the HARS called Homomorphic Authenticable Ring Signatures in ORUTA. By this mechanism public verifier can monitor the accuracy of the shared data without downloading the total data from cloud. So, by using this mechanism the public verifier cannot differentiate who is the actual owner for that particular block. In future we can prolong our mechanism to support batch auditing.

The two thought-provoking problems are traceability and another one is how to prove data freshness.

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. Zaharia, "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. 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.
7. 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.
8. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer
and Comm. Security (CCS'09), pp. 213-222, 2009.
9. 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.
10. 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.
11. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems,"
Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.
12. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau, "Dynamic Audit Services for Integrity Verification of Outsourced
Storages in Clouds," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.
13. N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based
Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM,
2012.
14. B. Wang, B. Li, and H. Li, "Certificateless Public Auditing for Data Integrity in the Cloud," Proc. IEEE Conf. Comm. and Network
Security (CNS'13), pp. 276-284, 2013.
15. C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.
16. B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp. 2904-2912, 2013.
17. B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Trans. Services Computing, 20 Dec. 2013, DOI: 10.1109/TSC.2013.2295611.
18. 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.
19. B. Wang, H. Li, and M. Li, "Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics," Proc. IEEE
20. A. Juels and B.S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597, 2007
21. D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 514-532, 2001.