International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 10: October 2015, pp 41-42. www.aetsjournal.com ISSN (Online) : 2394-6237

Differential Correlation Based Shared Data Repository Document Auditing In Cloud

Kasthuripriya S, Dhiyanesh B

Abstract— In this paper, we discuss the different public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing idea of proxy re-signatures, we allow the cloud to resign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves.

Keywords— Public auditing, Shared data, User revocation, Cloud computing.

I. INTRODUCTION

This public verifier could be a client who would like to utilize cloud data for particular purposes or a Third-Party Auditor (TPA) who is able to provide verification services on data integrity to users. Most of the previous works focus on auditing the integrity of personal data. shared data is outsourced to the cloud and users no longer store it on local devices, a straightforward method to re-compute these signatures during user revocation is to ask an existing user to first download the blocks previously signed by the revoked user, verify the correctness of these

blocks, then re-sign these blocks, and finally upload the new signatures to the cloud. The content of shared data is not changed during user revocation, the blocks, which were previously signed by the revoked user, still need to be re-signed by an existing user in the group.

II. VARIOUS AUTHENTICATION METHODS

The various authentication methods are as given in the table1.

Table 1 Analysis of Authentication methods

S. No	Title	Description
1.	Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud [2]	Propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation
2.	A View of Cloud Computing," Communications of the ACM [3]	Clearing the clouds away from the true potential and obstacles posed by this computing capability.
3.	Provable Data Possession at Untrusted Stores [4]	It allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it.
4.	Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds [5]	we propose a dynamic audit service for verifying the integrity of untrusted and outsourced storage.
5.	Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud [6]	It supports public auditing on shared data stored in the cloud. Exploit to compute verification metadata needed to audit the correctness of shared data.
6.	FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networks [7]	An initiating user can find from a group of users the one whose profile best matches with the limit of privacy exposure, only necessary and minimal information about the private attributes of the participating users is exchanged.
7.	Proxy Re-signatures: New Definitions, Algorithms and Applications [8]	To translate, the proxy converts a signature from Alice into a signature from Bob on the same message
8.	Hourglass Schemes: How to Prove that Cloud Files Are Encrypted [9]	we propose hourglass schemes, protocols that prove correct encryption of a resource requirement on the process of translating from one encoding domain to a target domain
9.	Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud [10]	To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud.
10.	POSTER: A Certificateless Proxy Re-Encryption Scheme for Cloud-based Data Sharing [11]	In CL-PRE, a data owner encrypts shared data in cloud with an encryption key, which is further encrypted and transformed by cloud, and then distributed to legitimate recipients for access control.

III. CONCLUSION

In this paper, we proposed a new public auditing mechanism for shared data with efficient user revocation in the cloud. 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.Experimental results show that the cloud can improve the efficiency of user revocation, and existing users in the group can save a significant amount of computation and communication resources during user revocation.

Kasthuripriya S, PG scholar, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India. (Email: kasthuripriyaa@gmail.com)

Dhiyanesh B, Assistant Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India. (Email: dhiyanu87hcet@gmail.com)

REFERENCES

[1] http://en.wikipedia.org/wiki/

[2] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud" in the Proceedings of IEEE INFOCOM 2013, 2013, pp.2904-2912.

[3] 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, April2010.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable Data Possesssion at Untrusted Stores," in the proceedings of ACM CCS 2007, 2007, pp. 598-610.

[5] 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 the preceedings of ACM SAC 2011, 2011, pp. 1550-1557.

[6] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing forShared Data in the cloud," in the proceedings of IEEE cloud 2012,2012,pp.295-302.

[7] M. li, N. Cao, S. Yu, and W. Lou, "FindU: Private-Preserving personal Profile Matching in Mobile Social Networks," in Proceedings of IEEE I NFOCOM, 2011, pp.2435-2443.

[8] G. Ateniese and S. Hohenberger, "Proxy Re-signatures: New Definitions, Algorithms and Applications," in the Proceedings of ACM CCS 2005, 2005, pp. 310-319.

[9] M. Van Dijk, A. Jules, A. Oprea, R. L. Rivest, E. Stefanov, and N. triandopoulos, "Hourglass schemas: how to prove that cloud files are encrypted," in the Proceedings of ACM CCS 2012, 2012, pp. 265-280.

[10] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the cloud," IEEE Transactions on parallel and Distributed System(TPDS), vol.24, no. 6,pp.1182-1191, 2013.

[11] L. Xu, X. Wu, and X. Zhang, "CL-PRE:a Certificateless proxy Re-Encryption Scheme for Secure Data Sharing with Public Cloud," in the Proceedings of ACM ASIACCS 2012, 2012.