Secure Audit Service by using TPA

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 139
Number 4

Year of Publication: 2016

Authors:
Pradnya P. Kulkarni

10.5120/ijca2016909136

Abstract

Using Cloud Storage, users can remotely store their data and enjoy high quality applications and services from a shared pool of resources. However, users, when they don’t have the physical possession of the data, chances of raising data integrity issue are possible. Thus, verification of data integrity is the at most important for a user, who has outsourced data to the cloud. To make the integrity check, a public auditing must be made possible. For it, resort to a Third Party Auditor (TPA). Also, the auditing process should not bring in further more burdens to the user, a secure cloud storage for which integrate the technique of Homomorphic linear authenticator with random masking. Thereby, assure integrity of the user’s outsourced data in the cloud.

References

Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the Clouds: A Berkeley View of Cloud
5. M. Arrington, “Gmail Disaster: Reports of Mass Email Deletions,”
Apr.-June 2012.
8. F. Sebe, J. Domingo-Ferrer, A. Martínez-Balleste, Y. Deswarte, and J.-J. Quisquater,
“Efficient Remote Data Possession Checking in Critical Information Infrastructures,” IEEE
10. M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of
Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems
(HotOS '07), pp. 1-6, and 2007.

Index Terms

Computer Science Security

Keywords

Data integrity, Third Party Auditing, Public Auditing, Data storage, Cloud computing, Batch
verification, Zero knowledge.