Privacy Preserving Third Party Auditing for Secure Cloud Storage

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

Volume 181
Number 18

Year of Publication: 2018

Authors:
Swati B. Ghavle, B. M. Patil

10.5120/ijca2018917877
{bibtex}2018917877.bib{/bibtex}

Abstract

With cloud data services, it is possible to all or common place for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to misconception due to the existence of hardware/software failures and human errors. To allow both data owners and public verifiers several mechanisms have been designed for efficiently auditing cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these previously existing mechanisms will inevitably reveal confidential information, identity & privacy to public verifiers. In this work a novel privacy-preserving mechanism used to supports public auditing on shared data stored in the cloud. In particular, here exploit ring signatures is used which computes verification of metadata on user demand and audit the correctness of shared data.

References

1. B. Wang, B. Li, and H. Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in


Index Terms

Computer Science
Security

Keywords

Public auditing, privacy-preserving, shared data, cloud computing, ring signature, data integrity.