IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

# A Review of Certificate-less Cryptographic Approaches for Public Auditing of Cloud Data Integrity

**Harshal Chaudhari, Rushikesh Rajput, Gaurav Kadam, Rushikesh Shelar**
**Prof. Purushottam R. Patil**
Department of Computer Sciences & Engineering
Sandip University, Nashik, India
harshalschaudhari769@gmail.com, rushirajput1414@gmail.com, gauravkadam493@gmail.com,
rushikesh3108@gmail.com, purupatil7@gmail.com

**Abstract:** *With the rise of cloud computing for collaborative data storage, ensuring data integrity in group-shared environments has become critical. Traditional integrity verification methods rely on Public Key Infrastructure (PKI), which, while effective, introduces complexities and administrative overhead due to certificate management. This project proposes a certificate-less public integrity-checking mechanism specifically designed for verifying group-shared data on cloud platforms without the need for certificates. By leveraging certificate-less cryptography, the protocol streamlines key management, reducing computational and storage overhead while maintaining robust security. Authorized group members or third-party auditors can verify data integrity without directly accessing the data, preserving confidentiality. The protocol also supports dynamic group management, allowing seamless addition or removal of members without compromising data integrity. Experimental results demonstrate that this certificate-less approach achieves comparable or improved performance over traditional PKI-based systems, offering a scalable and efficient solution for public integrity verification in cloud-based collaborative settings.*

**Keywords:** Certificate-less cryptography, public integrity checking, cloud storage security, group-shared data, data integrity verification.


DOI: 10.48175/568