Cloud Computing is one of the best platform which provides huge data storage and data sharing all over the time and also easily available to the users. Data sharing in the cloud contains the several issues such as data integrity, authenticity, anonymity and privacy of data owner. Identity based (ID-based) ring signature gives anonymous and authentic data sharing system, by using this there is no need of costly certificate verification in the traditional public key infrastructure (PKI). This work, enhances the security of ID-based ring signature with forward security. Using forward security, if private key of the signer is compromised then all the previously generated signatures of that signer remains valid. Using forward security, one of the user may revoke access of file to the other members of the group.

References

Optimal Data Sharing with Forward Security


Index Terms

Computer Science

Distributed Systems

Keywords

Cloud Computing, data sharing, data integrity, data authenticity, ring signature, anonymity, forward security.