Abstract

The key feature of cloud computing is one can access information any place, anywhere, at any time. So basically cloud computing is subscription based service where one can obtain network storage space and computer resources for data storage as well as data sharing. Due to high fame of cloud for data storage and sharing, large number of participants gets attracted to it but it leads to issue related to efficiency, Data integrity, privacy and authentication. To overcome these issues, concept of ring signature has been introduced for data sharing amongst large number of users. Ring signatures are used to provide user’s anonymity and signer’s privacy. Use of ID-based ring signature, removes the need of certificate verification which was done using public key infrastructure, hence reduce cost as well as introduction of forward security, further strengthen this system more. Use of weil pairing, keeps even shorter keys secure and it also requires less processing power. So the motivation of this paper is to propose a secure data reading and sharing scheme using above mentioned scheme.

2. Javier Herranz IIIA, “Identity-Based Ring Signatures From RSA” Artificial Intelligence Research Institute, CSIC, Spanish National Research Council, Campus UAB s/n, E-08193 Bellaterra, Spain


4. Mihir Bellare and Sara K. Miner “A Forward-Secure Digital Signature Scheme” Dept. of Computer Science, & Engineering University of California at San Diego, 9500 Gilman Drive La Jolla, CA 92093, USA.


6. Gene Itkis Boston University Computer Science Dept.111 Cumming ton St. Boston, “Forward security: Adaptive cryptography-time evolution” MA 02215, USAitkis@bu.edu


Index Terms

Computer Science

Databases

Keywords

Authentication, data sharing, ring signature, forward security, cloud computing.