Abstract

In today's world management of electronic documents is a very tedious job. As electronic documents are used for all the transactions the authentication of the document is very important. Digital signatures are the best methods to provide authenticity. Many existing schemes for digital signatures are proposed. In this paper a scheme which can be used to authenticate a group of members has been proposed. The proposed scheme uses RSA algorithm. The existing scheme provides group signatures which are static. But the proposed scheme is dynamic. It allows the group members to dynamically join the group and revoke the group. The proposed work is efficient and secure for electronic transactions and even for cloud environment where authenticity is essential.

References

- H. Zhu, D. Li, "Research on Digital Signature in Electronic Commerce," The 2008 IAENG International Conference on Internet Computing and Web Services, HongKong, 2008, pp. 8
- Kiayias and M. Yung, "Group signatures: Provable security, efficient constructions and anonymity from trapdoor-holders," IACR
- Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent? Patrick J. Flinn and James M. Jordan III (c) 1997 Alston & Bird LLP July 9, 1997 anonymity from trapdoor-holders, IACR

**Index Terms**

Computer Science

Security

**Keywords**

Digital signature, group signature, authentication, RSA, cryptography