Abstract

Traditional system in cryptography allows just sharing of keys between the sender and receiver, for such a technique only the signature storage is provided for the user's public key. But as the number of users increases, it became a challenging job to have such a certificate storage as well as key distribution, to overcome this Identity Based Encryption (IBE) was proposed, but again it had created the time consuming environment as it was supporting only to one-to-one communication. After IBE Attribute Based encryption (ABE) made possibilities to provide multicast communication between users but it was limited to only key policy based encryption as well as could not provide the revocation phenomenon for keys. So this paper aims to develop an existing system using MAMM (Multiple Authority Multiple Mediator) with the use of distributed CP-ABE (Cipher Policy ABE) which enhances the revocation and improves the performance.

References

- Adi Shamir, "Identity Based Cryptosystems and Signature schemes," Departments of applied mathematics, 1998.
Improving Revocation Scheme to Enhance the Performance in Multi-Authority ABE

- Antoine Joux, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems"; Computer Science, Edited by G. Goos, J. Hartmanis, and J. van Leeuwen.


- S. D. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate pairing"; Springer-Verlag, 2002.
- Piyi Yang, Zhenfu Cao and Xiaolei Dong, "Fuzzy identity based signature"; 2008.


- Melissa chase "Multi-authority Attribute Based Encryption"; Computer Science Department Brown University Providence, RI 02912.
- Bethencourt John, Sahai Amit, Waters Brent, "Cipher-text-policy attribute- Based
- Sonia Jahid, Prateek Mittal, Nikita Borisov, "Easier: Encryption-based access
- Riddhi mankad, Devesh Jinwala "Investigating multi authority attribute-based
- M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for Designing
efficient protocols. In ACM conference on Computer and Communications Security (ACM
- Vipul Goyal, "Reducing Trust in the PKG in Identity Based
Cryptosystems," Department of Computer Science, University of California, Los Angeles,
- Sascha Müller, Stefan Katzenbeisser, "Distributed Attribute Based
Encryption," P. J. Lee and J. H. Cheon (Eds.): ICISC 2008, LNCS 5461, pp. 20–36,

Index Terms

Computer Science
Security

Keywords
Cipher-text Distributed Cipher-text policy Encryption Multi-Authority
Multi-Authority Single Mediator.