Abstract

With the advent of business apps which allow users to form dynamic groups so that they can store data on cloud servers and share the data within their user groups through their mobile devices. A major concern comes here that mobile users need the security of their group data which should not be accessible to other group users. To solve the issue, ABE or Attribute Based Encryption techniques are employed as they are vastly recognized as a valid and robust mechanism to provide fine access control over the data to legitimate users. At the same time, as there are complex computations involved in key issuing and data encryption by AAs’ (Attribute Authorities) and decryption by legitimate users, there exist some efficiency issues. Rekeying plays a major role in dynamic systems where nodes come-in and move-out. As revocation of user rights requires the system to secure data from moved out users, rekeying has to be done on entire data set belonging to that attribute users in the group. However, the cost of re-keying is another concern for system efficiency which should not be compensated with a compromise on data security. There are many research works carried out earlier on data security for web applications using ABE, but there are limited studies on CP-ABE in mobile
computing with multi-authority data storage system. A system is implemented which allows user
groups to register, CAs’ (Certificate Authorities) to allow registrations of Users and AAs and
assign public Keys, AAs to manage attributes and revoke user access with re-keying and a
centralized server for data persistence. Experimental results show the effectiveness of
proposed solution and efficiency of re-keying mechanism while evoking user access rights on
system architecture.

References

Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.
3. B. Waters, “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and
Provably Secure Realization,” in Proc. 4th Int’l Conf. Practice and Theory in Public Key
Cryptography (PKC’11), 2011, pp. 53-70.
4. V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded Ciphertext-Policy Attribute-Based
Encryption,” in Proc. 35th Int’l Colloquium on Automata, Languages, and Programming
Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,”
6. Jin Li 0002, Jingwei Li, Xiaofeng Chen, Xinyi Huang and Yang Xiang, "Securely
Outsourcing Attribute-based Encryption with Checkability", in IEEE Trans. Parallel Distributed
7. M. Chase, “Multi-Authority Attribute-Based Encryption,” in Proc. 4th Theory of
Attribute-Based Encryption,” in Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09),
2009, pp. 121-130.
10. S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute
Revocation,” in Proc. 5th ACM Symp. Information, Computer, and Comm. Security
(ASIACCS’10), 2010, pp. 261-270.
12. Hur and D.K. Noh, “Attribute-Based Access Control with Efficient Revocation in Data
July 2011.
Networks with Efficient Revocation,” in Proc. 6th ACM Symp. Information, Computer, and


**Index Terms**

Computer Science

Information Sciences

**Keywords**

Attribute-Based Encryption, CP-ABE, Mobile Data Security, Re-Keying, User Access Control