An Efficient and Secure Solution for Attribute Revocation Problem Utilizing CP-ABE Scheme in Mobile Cloud Computing

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 129
Number 1

Year of Publication: 2015

Authors:
Vijay H. Kalmani, Dinesh Goyal, Sanjay Singla

10.5120/ijca2015906807

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


Index Terms

Computer Science Information Sciences

Keywords

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