Secure Cloud based Medical Data exchange using Attribute based Encryption

IJCA Special Issue on Advanced Computing and Communication Technologies for HPC Applications

© 2012 by IJCA Journal

ACCTHPCA - Number 2

Year of Publication: 2012

Authors:

Shini S G

Chitharanjan K

{bibtex}accthpca1015.bib{/bibtex}

Abstract

Secure Management of medical data has become a major issue as there is an increase in need for medical data exchange among different healthcare providers. Cloud platform can form an exchange platform that all healthcare organizations use and can serve as storage centre of medical records. However, there had been wide security and privacy concerns as medical records are known to third-party server and unauthorized parties. The medical data residing on a cloud server are subjected to many inside and outside malicious attacks. To keep sensitive medical data confidential in cloud, existing solutions apply encryption methods by disclosing data decryption keys only to authorized users. Then also issues like risk of information
Secure Cloud based Medical Data exchange using Attribute based Encryption
disclosure, user revocation, scalability in key management are present which hinders to achieve fine grained data access control. To achieve fine grained and scalable access control for medical records, attribute based encryption techniques are used to encrypt medical data. The main method is to map an access control policy into a secret encryption key and then to encrypt the data under the encryption key such that only authorized users who possess the decryption key can access the data in cloud. The secret key is associated with a set of attributes which identify the particular user. The user can decrypt the data if and only if his attributes satisfy access control policies. The proposed method supports efficient user revocation and achieves break glass in emergency situations. The proposed scheme is implemented at real time cloud environment in Microsoft Azure.

References

- M. Atallah, K. Friken, and M. Blanton, "Dynamic and efficient key management for access hierarchies," in Proc. of CCS'05, 2005.
- G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS'06, 2005.
- Ran Canetti and Susan Hohenberger. Chosen-ciphertext secure proxy re-encryption.
Secure Cloud based Medical Data exchange using Attribute based Encryption


Index Terms

Computer Science
Hpc Applications

Keywords
Medical Records  cloud Computing  attribute Based Encryption  user Revocation.