Abstract

Personal Health Record (PHR) is a web based set of tools that provides the facility to exchange and maintain a complete electronic health record of a patient. Third-party service providers are available to maintain PHRs like HealthVault, Google Health or Web MD. These applications allow individuals to enter, store and share their own health data, upload health measurements from their devices or from hospital EHR systems. Another alternative is to outsource PHR to third party cloud service providers or on semi trusted servers. It helps to increase PHR efficiency and to overcome problems associated with maintaining own specialized data centers. However, serious privacy concern arises as data are exposed to unauthorized users. The potential solution to this problem is to encrypt the data before outsourcing, however while encrypting data the issue of key management, data privacy and fine grained access remains a major concern. Taking these issues into consideration the paper proposes a model for securing PHR stored in semi-trusted third party servers by adopting attribute-based encryption (ABE). The advantage of ABE is, the complexity of encryption and decryption linearly increases with the increase number of attributes which are desired for large systems, although the challenge to make system collusion resistant need to be handled efficiently. To overcome these challenges the model proposes the use of dual system encryption methodology. The encryption techniques from Multi-authority ABE and Key-Policy ABE are combined. Use of MA-ABE
technique proves beneficial for key management and flexible access and potential security threat of colluding users is handled by KP-ABE. To this end, proposed framework has attempted to achieve data security by MA-ABE and data privacy by KP-ABE scheme thus improving overall security of the system.

References

- S. Yu, C. Wang, K. Ren, and W. Lou; Achieving secure, scalable, and fine-grained data access control in cloud computing; in IEEE INFOCOM; 10, May 12-15, pp. 73, 2010.
- V. Goyal, O. Pandey, A. Sahai, and B. Waters; Attribute-based encryption for fine-grained access control of encrypted data; in CCS; 06, October 30–November 3, pp. 89–98, 2006.
- X. Liang, R. Lu, X. Lin, and X. S. Shen; Patient self-controllable access policy on phi in ehealthcare systems; in AHIC; 10, vol. 6, Dec 7, pp 1-5, 2010.

Index Terms

Computer Science

Security
Keywords

Attribute based encryption  Attribute Authority cloud computing  MA-ABE  KP-ABE

data security

fine-grained access control

Personal Health Record.