Abstract

Personal Health Record (PHR) service is an emerging model for health information exchange. It allows patients to create, update, and manage personal and medical information. Also they can control and share their medical information with other users as well as health care providers. PHR data is hosted to the third party cloud service providers in order to enhance its interoperability. However, there have been serious security and privacy issues in outsourcing these data to cloud server. For security, encrypt the PHRs before outsourcing. So many issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for client’s data, a novel patient-centric framework is used. This framework mainly focuses on the multiple data owner scenario. A high degree of patient privacy is guaranteed simultaneously by exploiting multi authority ABE. This scheme also enables dynamic modification of access policies or file attributes, support efficient on demand user/attribute revocation. However some practical limitations are in building PHR system. If consider the workflow based access control scenarios, the data access right could be given based on users identities rather than their attributes, while ABE does not handle that efficiently. For solving these problem in this thesis proposed PHR system, based on Attribute

References

- X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext Policy Attribute Based Encryption with Efficient Revocation", technical report, Univ. of Waterloo, 2010
- G. Wang, Q. Liu, and J. Wu, "Hierachical attribute-based encryption for fine-grained access control in cloud storage services", in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010
- Pascal Junod, Alexandre Karlov "An Efficient Public-Key Attribute-Based Broadcast Encryption Scheme Allowing Arbitrary Access Policies";
- D. Lubicz and T. Sirvent, "Attribute-based broadcast encryption scheme made efficient. First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008"

Index Terms

Computer Science
Security
Keywords
Cloud computing  Data privacy  Fine grained access control  Attribute based encryption