Abstract

Cloud computing, is an emerging computing environment which allows users to remotely store the data in one centralized place. This facilitates on demand scalable services as well as efficient management and sharing of data. However, there have been wide privacy concerns as data is outsourced to third party servers and to unauthorized users. The best way to ensure confidentiality of the data in the cloud is to utilize encryption/decryption for data in transit and data at rest. Data encryption/decryption technique can be applied on both coarse-grained level and fine grained level but in both techniques it is required to give another party your private key. Hence Key management becomes a critical issue and the cloud provider require policies and procedures in place for storage, generation and archival of private keys. To achieve scalability in key management, flexible access and efficient user revocation an attribute based encryption (ABE) technique has been recently popularized. Using ABE records are encrypted at fine-grained level instead of coarse grain level which helps in scalable data access control. The paper discusses the use of cloud computing and cryptographic techniques i.e. (ABE) for Personal health record (PHR). PHR is an upcoming patient-centric model for storing patients’ e-record in one centralized place. It allows patients to create, manage, control and share their health information with other users as well as health care providers.
REFERENCES


Index Terms

Computer Science

Security
Keywords
Attribute based encryption  cloud computing  MA-ABE  fine-grained access control

Personal Health Record