Abstract

Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computers with internet access. Personal Health Record (PHR) is an emerging patient centric model of health information exchange, which is outsourced to be stored at a third party, such as cloud providers. Issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation have remained the most important challenges towards fine-grained, cryptographically enforced data access control. In the proposed work, a novel patient centric framework and a mechanism for data access control to PHRs stored in semi structured servers. A high degree of patient privacy is ensured by exploiting Homomorphic Encryption technique. It also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break glass access under emergency scenarios without revealing the content of original data. For secure data outsourcing, the users are divided in the PHR system into multiple security domains that greatly reduces the key management for owners and users.
References

- Michael N, Kristin Lauter, Vinod Vaikuntanathan, &quot;Can Homomorphic Encryption be Practical?&quot; Proceedings of the 3rd ACM workshop on Cloud computing security workshop, CCSW &apos;11
- MD. Nurul Huda, Noboru Sonehara, Shigeki Yamada., &quot;A Privacy Management
A Homomorphic Encryption Technique for Scalable and Secure Sharing of Personal Health Record in Cloud Computing


Index Terms

Computer Science Information Systems

Keywords

Personal Health Record (PHR) Cloud Computing Homomorphic Encryption (HE)