**ENHANCED ATTRIBUTE BASED ENCRYPTION TECHNIQUE FOR SECURING PERSONAL HEALTH RECORDS IN CLOUD COMPUTING**

**ABSTRACT**

Personal Health Record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers and unauthorized parties. To ensure the patients control over access to their own PHRs, it’s a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have been remained the most important challenges towards achieving fine-grained cryptographically enforced data access control. A novel patient centric framework and a suite of mechanisms for data access control to PHRs are stored in semi-structured format. To achieve fine grained and scalable data access control for PHRs, leverage attributes based encryption techniques are used for encrypting each patient PHR file. Apart from the traditional approaches the multiple data owner’s scenario and partition among the users in the PHR system into multiple security domains has been greatly reduced the key management complexity for owners as well as users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi authority Enhanced Attribute Based Encryption (EABE).