ABSTRACT

PHR System is a favorable platform for personal health information exchange. In order to ensure that the personal information is not falsified and leaked by malicious users, we use the attribute based signcryption technology to provide secure and reliable data protection. At the same time, in order to prevent users from accessing the data in the system by collusion of attributes, we proposes a revocable cloud-assisted attribute-based signcryption scheme which using the broadcast encryption technology and key segmentation technology realize user revocation function. Moreover, the proposed scheme is proven to be confidentiality and unforgetability under chosen plaintext attack in the random oracle model. And the experimental evaluation indicates that the proposed scheme is practical and feasible. With the development of medical information technology, Personal Health Record (PHR) system is gradually developing and improving. PHR system is a health record storage service system, which allows patients to create, control and share their HR data with a wide range of target users, including doctors, nurses, health insurance providers and family members. In order to improve the quality of PHR services at a lower cost, PHR service providers want to store PHR users' personal medical data on cloud servers.