

## Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability

### Abstract:

Motivated by the privacy issues, curbing the adoption of electronic healthcare systems and the wild success of cloud service models, we propose to build privacy into mobile healthcare systems with the help of the private cloud. Our system offers salient features including efficient key management, privacy-preserving data storage, and retrieval, especially for retrieval at emergencies, and auditability for misusing health data. Specifically, we propose to integrate key management from pseudorandom number generator for unlinkability, a secure indexing method for privacy-preserving keyword search which hides both search and access patterns based on redundancy, and integrate the concept of attribute-based encryption with threshold signing for providing role-based access control with auditability to prevent potential misbehavior, in both normal and emergency cases.