Self-Protecting Electronic Medical Records Using Attribute-Based Encryption

http://www.firstlight.cn 2010-11-05

We provide a design and implementation of self-protecting electronic medical records (EMRs) using attribute-based encryption. Our system allows healthcare organizations to export EMRs to storage locations outside of their trust boundary, including mobile devices, Regional Health Information Organizations (RHIOs), and cloud systems such as Google Health. In contrast to some previous approaches to this problem, our solution is designed to maintain EMR availability even when providers are offline, i.e., where network connectivity is not available (for example, during a natural disaster). To balance the needs of emergency care and patient privacy, our system is designed to provide for fine-grained encryption and is able to protect individual items within an EMR, where each encrypted item may have its own access control policy. To validate our architecture, we implemented a prototype system using a new dual-policy attribute-based encryption library that we developed. Our implementation, which includes an iPhone app for storing and managing EMRs offline, allows for flexible and automatic policy generation. An evaluation of our design shows that our ABE library performs well, has acceptable storage requirements, and is practical and usable on modern smartphones.

存档文本