JOURNAL OF APPLIED SECURITY RESEARCH
2017, VOL. 12, NO. 4, 463–477

Securing Private Keys in Electronic Health Records Using Session-Based Hierarchical Key Encryption

Adebayo Omotosho[a], Justice Emuoyibofarhe[b], and Alice Oke[b]
[a]Department of Computer Science, Landmark University, Omu-Aran, Kwara State, Nigeria; [b]Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria

ABSTRACT
Patients want the assurance that the confidentiality of their records accessed through Electronic Health Records (EHR) are safe. With increasing implementation of EHR for health care, privacy concern remains a barrier that limits patients' favorable judgment of this technology. Sensitive records can be compromised and this represents problems in EHRs, which are considered to be more efficient, less error prone, and of higher availability compared to traditional paper health records. In this article, a session based hierarchical key encryption system was developed that allows patient to have full control over certain nodes of their health records. Health records were organized in a hierarchical structure with records further broken down into subcategories. Cryptography was used to encrypt the health records in their different subcategories. Patients' generate a root keys using Blum Blum Shub Algorithm for pseudorandom number generator from which the session-based subkeys were derived, and only authorize users can access these records within a designated period marked as session. The system development demonstrates one way patients' privacy and security can improve using session based hierarchical key encryption system for EHR.

KEYWORDS
Health records; EHR; private keys; security, privacy