Int. J. Electronic Healthcare, Vol. 9, No. 4, 2017

Ensuring patients' privacy in a cryptographic-based electronic health records using bio-cryptography

Adebayo Omotosho*
Department of Computer Science,
Landmark University,
P.M.B 1001, Omu-Aran, Kwara State, Nigeria
Email: bayotosho@gmail.com
*Corresponding author
Justice Emuoyibofarhe
Department of Computer Science and Engineering,
Ladoke Akintola University of Technology,
P.M.B 4000, Ogbomoso, Oyo State, Nigeria
Email: eojustice@gmail.com
Christoph Meinel
Hasso Plattner Institute (HPI) for IT Systems Engineering,
University of Potsdam,
Potsdam, 14482, Germany
Email: meinel@hpi.de

Abstract: Several recent works have proposed and implemented cryptography as a means to preserve privacy and security of patient's health data. Nevertheless, the weakest point of electronic health record (EHR) systems that relied on these cryptographic schemes is key management. Thus, this paper presents the development of privacy and security system for cryptography-based-EHR by taking advantage of the uniqueness of fingerprint and iris characteristic features to secure cryptographic keys in a bio-cryptography framework. The results of the system evaluation showed significant improvements in terms of time efficiency of this approach to cryptographic-based-EHR. Both the fuzzy vault and fuzzy commitment demonstrated false acceptance rate (FAR) of 0%, which reduces the likelihood of imposters gaining successful access to the keys protecting patients' protected health information. This result also justifies the feasibility of implementing fuzzy key binding scheme in real applications, especially fuzzy vault which demonstrated a better performance during key reconstruction.

Keywords: EHR; electronic health record; biometrics; cryptography; privacy; accountability.