Chapter 32
User Authentication Into Electronic Health Record Based on Reliable Lightweight Algorithms

Mishall Al-Zubaidie
https://orcid.org/0000-0002-3149-9129
Thi-Qar University, Iraq & University of Southern Queensland, Australia

Zhongwei Zhang
University of Southern Queensland, Australia

Ji Zhang
University of Southern Queensland, Australia

ABSTRACT

Supporting a mechanism to authenticate members in electronic health record (EHR) is a fundamental procedure to prevent different threats from penetrating patients' identities/data. Existing authentication schemes still suffer from security drawbacks. Exchanging medical-related information/data between clients and the servers leaves them compromised to breakthrough by intruders as they can transmit over an unreliable environment. To guarantee the protection of patient records, this chapter proposes a new scheme that provides authentication of patients/providers in EHR depending on the legitimate member identities and the device information. The scheme utilizes an elliptic curve cryptography and lightweight hash function to accomplish robust security with satisfying performance. Moreover, it depends on a set of techniques such as multi-pseudonyms to authenticate legitimate members. Additionally, concentrated theoretical and experimental analysis proves that the proposed provides elevated performance and security compared to existing research.

DOI: 10.4018/978-1-7998-5728-0.ch032

INTRODUCTION

An insufficiency of privacy and security of medical records applied by healthcare applications (HCA) stays the major drawback that reduces the prevalence of these applications. The healthcare (HC) systems demand reliable protection techniques to validate HC members via accomplishing the security requirements (He & Zeadally, 2015) and the obedience of the Health organizations standards to secure patient records from being modified and tampered. Protection procedures (confidentiality, integrity, and availability) should be achieved during exchanging medical records between clients (users) and server applications, as any alteration to this data affects both the patients' condition and medical decisions (Al-Zubaidie et al.,2020). Authentication is the most critical security procedure that performs the main role in constructing proper protection before the exchange of patients' records in HCA (Das et al., 2017; Li et al., 2016; Rajput et al., 2016). First, authentication can limit fatal/malicious errors caused by permeation threats on the authentication requests. Second, it mitigates errors in specifying dose, drug, timing, or procedure. Consequently, authentication protocols are significant countermeasure to prevent different threats. Commonly, the server should block all illegal and fake authentication requests (Shen, Gui, et al., 2018). It should safeguard personal identities (IDs), medical data, and physiological records such as blood pressure and sugar. Nonetheless, the authentication information can be simpler to penetrate if the information and data kept on the same server. Moreover, a sending of authentication requests in an unreliable channel (Internet/wireless sensor network (WSN)), can subject patients' records for destruction/alteration (Li et al., 2016). Many examples of real-world security threats implemented against user authentication in HCA as follows:

- In 2017, a patient's personal information was compromised at the AU Medical Centre, Children's Hospital and Clinics of Georgia. However, information database attacks were not detected until 2018 (Donovan, 2018).
- In 2018, according to the proofpoint report, more than 100 million authentication attacks were carried out around the world against clinics, hospitals and insurance companies (Proofpoint, 2018).
- In 2019, the Oregon Department of Human Services indicated that cyber-threats breached users' credentials (625000 patients' records) (Jessica Davis, 2019).

The conventional signature/encryption performs complex operations that exhaust server resources such as memory and time to process with big data of HC (Manogaran et al., 2018) and hence, which may cause them infeasible. The digital signature is utilized to verify the safety of the members' IDs within the authentication message (Giri et al., 2015). Many lightweight hash-function (PHOTON and ARMADILLO) are preferred to apply a digital signature that performs lightweight processes to reduce consumption of the server resources. HCA require encryption and signature secure, and high-speed techniques (Liu & Chung, 2017). To build an authentication scheme, many mechanisms, such as Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC), hash-function and fuzzy extractor (Chandrakar & Om, 2017), are implemented in HCA projects. Many modern HCA are depending on RSA and ECC, both supply the same protection strength, but ECC has performance better compared to RSA. The HCA authentication protocols should include countermeasures to various threats plus the efficiency of high-performance.