Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 111 (2017) 145–153

Procedia Computer Science

www.elsevier.com/locate/procedia

8th International Conference on Advances in Information Technology, IAIT2016, 19-22 December 2016, Macau, China

An authentication and authorization mechanism for long-term electronic health records management

Nai-Wei Lo*, Chia-Yi Wu, Yo-Hsuan Chuang

Department of Information Management, National Taiwan University of Science Technology, Taipei, Taiwan

Abstract

In the past five decades, major improvement on sanitation, new invention on medicines, and novel development on medical technologies had been widely deployed and adopted in modern societies. In consequence, the average lifetime of human being is much longer than it was before. Therefore, to safely establish and manage personal health records for each individual during his/her lifetime within the electronic form has gradually become an interesting topic for individual citizens and social welfare departments; the reason is that a well-maintained health records document of an individual can help doctors and hospitals know important and necessary medical and body conditions of the targeted patient in time before conducting any therapy. In this paper, we proposed an authentication and authorization protocol to manage which organization (usually a hospital) is allowed to have the access right on the long-term historical electronic health records of a targeted individual. By using the proposed scheme, a person can migrate his/her health records to a specific organization along with access right authorization. In our protocol, the cumulatively notarized signature mechanism is introduced to preserve the evidence on the ownership transfer of targeted electronic health records between two organizations. A trusted notary is used to verify the management privilege of involved organizations on those health records of targeted individuals. In addition, we show that the protocol achieves data integrity, non-repudiation for data authorization and data availability.

Peer-review under responsibility of the organizing committee of the 8th International Conference on Advances in Information Technology

Keywords: Electronic health records; long-term electronic records management; cumulatively notarized signature; authentication, authorization.

* Corresponding author. Tel.: +886-2-27336778.
E-mail address: nwlo@cs.ntust.edu.tw

1877-0509
Peer-review under responsibility of the organizing committee of the 8th International Conference on Advances in Information Technology
10.1016/j.procs.2017.06.021

1. Introduction

In the past couple of years, monitoring personal health condition in real time has become a new movement in modern societies along with the deployment of body sensors and the development of body area network (BAN). In near future, those health-related sensed data generated from wearable devices such as smart watch or health bracelet will be stored as part of electronic medical records (EMR) or electronic health records (EHR). In addition, the average lifetime of human being through the past decade has further extended. Therefore, to safely establish and manage personal health records for each individual during his/her lifetime within the electronic form (e.g. EMR or EHR) has gradually become an important topic for individual citizens and social welfare departments. Well-maintained health records document of an individual can help doctors and hospitals know important and necessary medical and body conditions of the targeted patient in time before conducting any therapy.

As health-related records are highly sensitive and confidential to individuals, there are basic security requirements to be accomplished to protect those records. In general, health-related records should always be encrypted during transmission, even offline access. Nowadays personal privacy is a highly significant issue; therefore, health-related personal records, especially daily real-time records, become the focus of protection. In consequence, how to protect user (or individual) ownership for his/her health records is one of the important tasks. Authentication mechanisms [1][2][3] should be adopted between a health record owner and a record preserver (i.e., an organization stored the data). Authorization mechanisms [2][4][5][6] are also required for user ownership protection.

Another curial issue is how to preserve long-term health records and maintain availability and usability of those records at the same time [7][8][9][10][11]. Lekkas and Gritzalis [7] proposed a scheme to preserve data access capability and data integrity on long-term EHR data. Their scheme uses cumulatively notarized signature mechanism on EHR data such that the lifetime of applied digital signatures can be extended. In their scheme EHR data transfer mechanism between two notaries is also addressed. Carmela et al. [11] presented a Secure Long-Term Archival System (SLTAS), which is a server-client architecture. SLTAS can verify the authenticity of signatures generated in distinct time points to preserve data integrity. In the signature phase of SLTAS, two timestamps are recorded: one before generating the signature and the other after generating signature. In order to achieve authenticity reliability, the system uses the mechanism of re-timestamp in onion. When a client needs to retrieve the data, the system will verify the last timestamp in onion or all wrapped timestamps starting from the last timestamp. These clinical records should keep longer than average human lifespan. Through a person's lifetime, his/her health-related data may be distributed in different medical and health-related institutions such as hospitals, clinics, IoT service companies and healthcare centers. In [12], Vigil et al. roughly categorized four technical approaches for the preservation of digital documents, including hardware and programs, emulators, transcoding digital documents, and standard formats. However, these schemes cannot accomplish the management work for long-term document preservation.

To resolve the need of long-term health data preservation and the data controllability for users, a new management scheme is proposed in this study. The major techniques used in the proposed protocol is cumulative notarized signature [7][10] and PKI cryptosystem. For the proposed scheme, there are three major contributions. First of all, the proposed protocol utilizes trusted third party (notary) and PKI cryptosystem to secure user health records for a long period of time. Second, the protocol achieves data integrity, non-repudiation for data authorization and data availability to stored health records. Third, ours protocol supports user controllability for users to decide which organization can receive their health records and what actions to manipulate their records are granted.

2. The proposed protocol

2.1. Preliminary

Public Key Cryptosystem: Public key cryptosystems are based on asymmetric-key algorithms. These cryptosystems are derived from hard NP-complete mathematical problems such as integer factorization, discrete logarithm, and elliptic curve cryptography (ECC). Public key cryptosystem generates one private key and one corresponding public key and utilizes the key pair to encrypt and decrypt messages. Due to computational complexity, it is very hard for an adversary to compute and derive a private key based on its corresponding public key and other publicly known data such as encrypted messages.