Chapter 6
Efficient Healthcare Integrity Assurance in the Cloud with Incremental Cryptography and Trusted Computing

Wassim Itani
Beirut Arab University, Lebanon

Ayman Kayssi
American University of Beirut, Lebanon

Ali Chehab
American University of Beirut, Lebanon

ABSTRACT

In this chapter, the authors propose the design and implementation of an integrity-enforcement protocol for detecting malicious modification on Electronic Healthcare Records (EHRs) stored and processed in the cloud. The proposed protocol leverages incremental cryptography premises and trusted computing building blocks to support secure integrity data structures that protect the medical records while: (1) complying with the specifications of regulatory policies and recommendations, (2) highly reducing the mobile client energy consumption, (3) considerably enhancing the performance of the applied cryptographic mechanisms on the mobile client as well as on the cloud servers, and (4) efficiently supporting dynamic data operations on the EHRs.

INTRODUCTION

The healthcare industry is considered one of the main sectors that can take advantage of the services offered by the cloud computing model. By outsourcing the storage and processing of EHRs to remote cloud providers, healthcare institutions are guaranteed unlimited opportunities summarized in the following points:

1. On-demand abundance in fault-tolerant storage capacities.

DOI: 10.4018/978-1-4666-6118-9.ch006

2. Powerful processing on clusters of commodity computing machinery.This contributes toreducing the physicians' practice times as well as the patient's waiting times.
3. Better compliance with regulatory policies such as HIPAA (Annas, 2003) by migrating the EHRs to HIPAA-compliant cloud providers.
4. Mobile universal access that enhances the seamless sharing of medical information among physicians, patients, and insurance companies. This results in better dissemination of medicalexpertise among physicians and in major time and cost savings.
5. Adaptable pay-as-you-go pricing schemes that ensure the cost-effective management of the ever-growing patient data.

Despite the manifold advantages inherently provided by cloud computing in the healthcare field, several challenges are hindering its widespread adoption and impeding the process of medical data and software migration to the cloud. A chief concern is represented in safeguarding the integrity of the patient medical information as it is stored and processed in the cloud. The integrity assurance of patients' data should be given exceptional attention since any malicious modification on EHRs may result in fallacious medical decisions and hence life-threatening consequences. The patients concern about the integrity of their medical records is highly justified and has its roots in the intrinsic structure of the cloud computing modelwhere everything is under the jurisdiction of the cloud provider. In cloud computing, EHRs are stored and processed on top of, possibly, untrusted servers that are not owned, controlled, or even managed by the respective healthcare institution. If the cloud service provider happens to have malicious intentions, it may undetectably jeopardize the integrity of the patients' medical records.

In addition to the integrity threats posed by malicious and "misbehaving" cloud providers, other sources of risk on healthcare cloud data include traditional internal and external attacks on the cloud network.

EHRs are characterized by a set of security, regulatory, and operational constraints that distinguish them from generic cloud data as far as integrity assurance is concerned:

1. EHRs are governed by strict regulatory policies, such as HIPAA, that all medical institutions must comply with by law. HIPAA specifies the administrative, technical, and physical protection mechanisms that need to be applied to safeguard the privacy and integrity of medical records.
2. Individual EHRs consist of relatively large data sets represented in medical imagery (X-Rays, CT scans, MRIs, radiology scans), lab test reports, physician diagnosis and transcripts, etc. that increase continuously over the life span of the respective patient subject. The healthcare integrity enforcement system should be designed to operate efficiently on large data records.
3. Individual EHRs may be modified and updated frequently depending on the respective patient case. The healthcare integrity enforcement system should be able to securely support dynamic operations on cloud data as it is stored and processed in the cloud.
4. A considerable portion of EHRs is, currently, generated, analyzed, and updated using battery-powered mobile and portable devices on the client side. The healthcare integrity enforcement system should be designed with energy-awareness in mind to preserve the battery resources of energy-limited devices operated by physicians and medical personnel.
5. EHRs should be preserved in storage and kept accessible for relatively long periods of time (minimum EHR retention periods can reach up tothirty years in the majority of medical institutions in the US.). This fact stresses