Chapter 5
Towards Privacy-Preserving Medical Cloud Computing Using Homomorphic Encryption

Ovunc Kocabas
University of Rochester, USA

Tolga Soyata
University of Rochester, USA

ABSTRACT

Personal health monitoring tools, such as commercially available wireless ECG patches, can significantly reduce healthcare costs by allowing patient monitoring outside the healthcare organizations. These tools transmit the acquired medical data into the cloud, which could provide an invaluable diagnosis tool for healthcare professionals. Despite the potential of such systems to revolutionize the medical field, the adoption of medical cloud computing in general has been slow due to the strict privacy regulations on patient health information. We present a novel medical cloud computing approach that eliminates privacy concerns associated with the cloud provider. Our approach capitalizes on Fully Homomorphic Encryption (FHE), which enables computations on private health information without actually observing the underlying data. For a feasibility study, we present a working implementation of a long-term cardiac health monitoring application using a well-established open source FHE library.

INTRODUCTION

The Patient Protection and Affordable Care Act (US Government Printing Office) is one of the most significant government efforts to generalize the use of electronic medical records (EMRs) and to incentivize the development of innovative technologies that can help curb rising US healthcare costs. Cloud computing is a viable option to reduce healthcare costs associated with EMRs by outsourcing the storage of medical data to cloud operators (Amazon Web Services; Google Cloud Platform; Microsoft Windows Azure), however, Personal Health Information (PHI) privacy is strictly mandated by the Health Insurance Portability and Accountability Act (HIPAA) (US Department of Health and Human Services, 2014) and

DOI: 10.4018/978-1-5225-9863-3.ch005

the risks associated with a breach of PHI are steep (up to $1.5M depending on the type of violation). Signing a Business Associate Agreement (BAA) (US-HHS) authorizes cloud storage operators (e.g., (CareCloud, 2013) and (Dr Chrono, 2013)) to store PHI data. These offerings are all based on encrypted data storage, however, there is currently no service that offers secure long-term patient monitoring, which would imply computation on encrypted data.

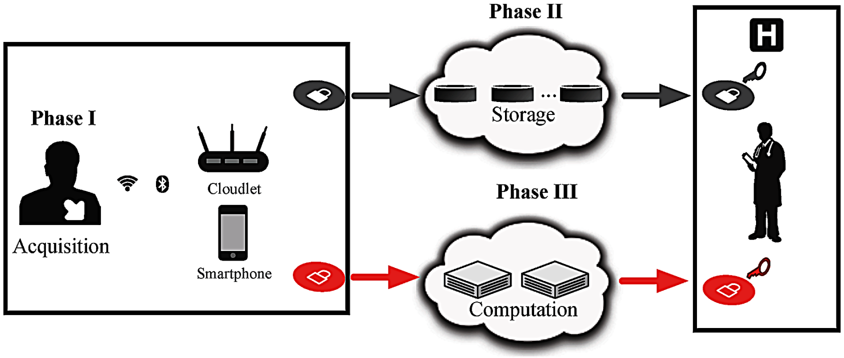
This chapter proposes a novel approach to eliminate privacy concerns. Our proposed Fully Homomorphic Encryption (FHE) based cloud computing solution allows the cloud to perform computations on encrypted data, without actually observing the data (i.e., patient private health information). While this method holds the promise to completely eliminate the cloud-based privacy concerns, it comes at a steep price: FHE-based operations are orders of magnitude slower than regular operations, rendering FHE impractical for generic applications (Bos, Lauter, & Naehrig, 2014; Naehrig, Lauter, & Vaikuntanathan, 2011; Kocabas, Soyata, Couderc, Aktas, Xia, & Huang, 2013; Wang, Hu, Chen, Huang, & Sunar, 2013; Dai, Doroz, & Sunar, 2014). In this chapter, one type of computation is shown to be a promising candidate for FHE-based medical applications: long-term patient monitoring.

Contributions of this chapter are: 1) implementation of a well-known ECG algorithm (Couderc, et al., 2011) using an open source FHE library (Halevi & Shoup, 2014), 2) detailed description of the steps required for such an implementation, which are far from trivial, 3) presentation of a proof-of-concept study on a restricted set of computations for long-term patient health monitoring using real data: specifically, the computation of the average heart rate, minimum and maximum heart rate, and the detection of a cardiac hazard called the drug-induced long QT syndrome (LQTS) (Aktas, Shah, & Akiyama, 2007; Brenyo, Huang, & Aktas, 2011), 4) demonstration of the potential for FHE-based generalized secure medical cloud computing.

Our claims are proven on test data taken from the University of Rochester THEW ECG database (Couderc J.-P., 2010), and it is shown that such operations can be performed homomorphically, thereby guaranteeing information security. Given that cardiac diseases are the #1 cause for deaths in the United States (Hoyert & Xu, 2012), our study is an important and novel step in the development of generalized secure medical cloud computing.

This chapter is organized as follows: We provide background information on FHE, followed by a system- and application-level introduction to our proposed solution. A description of the nature of the acquired medical data and the operations performed on this data are described in the next section and a

Figure 1. Proposed Cloud-based secure long-term patient monitoring system.
Adapted from (Page, Kocabas, Ames, Venkitasubramaniam, & Soyata, 2014).


Phase I
Acquisition
Cloudlet
Smartphone
Phase II
Storage
Phase III
Computation
H