Chapter 4
Secure Health Monitoring in the Cloud Using Homomorphic Encryption: A Branching-Program Formulation

Scott Ames
University of Rochester, USA

Muthuramakrishnan Venkitasubramaniam
University of Rochester, USA

Alex Page
University of Rochester, USA

Ovunc Kocabas
University of Rochester, USA

Tolga Soyata
University of Rochester, USA

ABSTRACT

Extending cloud computing to medical software, where the hospitals rent the software from the provider sounds like a natural evolution for cloud computing. One problem with cloud computing, though, is ensuring the medical data privacy in applications such as long term health monitoring. Previously proposed solutions based on Fully Homomorphic Encryption (FHE) completely eliminate privacy concerns, but are extremely slow to be practical. Our key proposition in this paper is a new approach to applying FHE into the data that is stored in the cloud. Instead of using the existing circuit-based programming models, we propose a solution based on Branching Programs. While this restricts the type of data elements that FHE can be applied to, it achieves dramatic speed-up as compared to traditional circuit-based methods. Our claims are proven with simulations applied to real ECG data.

DOI: 10.4018/978-1-5225-9863-3.ch004

INTRODUCTION

Software as a Service (SaaS) provides an excellent alternative to any corporation looking to simplify their IT infrastructure. By renting Software as a Service (SaaS), rather than purchasing, the responsibility of software upgrades, as well as the infrastructure to run the software are transferred to the provider of the software. Upgrades on the software could be done instantly, since new patches and code improvements could be contained at the source, which resides within the servers of the provider of the software. While SaaS has been very successful in certain categories of applications, such as Salesforce.com (SalesForce.com, 2014), its adoption in the medical application arena has been very slow due to the strict rules and regulations introduced by Health Insurance Portability and Accountability Act - HIPAA (HIPAA, 2014). According to HIPAA regulations, private medical information should be treated with utmost care, and the penalties associated with the breach of HIPAA are steep and unacceptable. Despite the fact that a hospital can confidently switch its application hosting and file storage to cloud operators, save money, and simplify its IT infrastructure (Reichman, 2011; Good, 2013), this transition has been very slow.

A novel application introduced in (Kocabas, et al., 2013; Kocabas & Soyata, 2014)guarantees privacy of patient medical information during cloud computing. This technique owes its capability to using Fully Homomorphic Encryption (FHE) during its computations. FHE allows generalized operations on encrypted data (Gentry, 2009), without actually observing the underlying medical data, thereby completely eliminating privacy concerns due to processing sensitive medical information. While novel in theory, this technique is plagued by performance bottlenecks: FHE-based computations are orders of magnitude slower than their unencrypted counterparts, which confine the application space of FHE-based implementations to a very restricted set. Additionally, FHE-encrypted data takes up orders of magnitude larger storage space (Page, Kocabas, Soyata, Aktas, & Couderc, 2014). With this significant expansion in storage space, and extremely prolonged execution time, the cost-saving advantage of cloud outsourcing becomes questionable for FHE-based implementations.

This performance disadvantage of FHE motivated the launch of the large-scale DARPA PROCEED program (DARPA-PROCEED, n.d.) to improve FHE performance. While the privacy advantages of FHE-based implementations are clear, substantial work has to be done before FHE can be practical. In this chapter, a reformulation of the idea introduced in (Kocabas, et al., 2013) is discussed, where FHE is not applied to the problem in a generalized way. Instead, a meaningful trade-off is presented between performance and range of input data. It is shown through simulations that, when a medical application is performing operations on data elements that lie within a well-defined range (e.g., 0.4 and 0.6 in the case of the QT_c value extracted from an ECG as will be described shortly in this chapter), comparisons can be made drastically faster. While most of the existing FHE implementations treat the arithmetic operations within a computer application as a set of operations that can be represented as a *circuit*, the formulation in (Page, Kocabas, Ames, Venkitasubramaniam, & Soyata, 2014) takes a radically different approach and is described in detail in this chapter.

In (Page, Kocabas, Ames, Venkitasubramaniam, & Soyata, 2014), a study is provided on a set of arithmetic (and logical) operations required for the execution of a medical application. These operations primarily consist of integer comparisons to determine the health state of a patient. These comparisons are performed on the vitals of a patient, such as the heart rate, or certain other metrics extracted from an Electrocardiogram (ECG). Rather than using the usual circuit-based representation of the operations, a *branching program* approach is taken, where each comparison is represented as a set of decisions applied to the bits of the compared values. Allowing the medical application to be represented as a branching