Department of Electrical and Computer Engineering
University of Rochester, Rochester, NY
Ph.D. Public Defense

Tuesday, December 15, 2015
1:30 PM
Computer Studies Building, Room 426

Design and Analysis of Privacy-Preserving Medical Cloud Computing Systems

Ovunc Kocabas

Supervised by
Professor Tolga Soyata

Abstract

Current financial and regulatory pressure has provided strong incentives to institute better disease prevention, improved patient monitoring, and push U.S. healthcare into the digital era. Outsourcing medical applications to a cloud operator helps healthcare organizations (HCO) to provide better patient care without increasing the associated costs. Despite these advantages, the adoption of medical cloud computing by HCO's has been slow due to the strict regulations on the privacy of Personal Health Information (PHI) dictated by The Health Insurance Portability and Accountability Act (HIPAA).

In this dissertation, we propose a novel privacy-preserving medical cloud computing system with an emphasis on "secure computation." The proposed system enables monitoring patients remotely outside the HCO using ECG signals. To eliminate privacy concerns associated with the public cloud providers, we utilize Fully Homomorphic Encryption (FHE) to enable computations on encrypted PHI data. Despite well-known performance penalties associated with FHE, we propose two methods for an efficient implementation. Specifically, we model our applications using two computational models: circuit and branching program, and propose optimizations to improve run-time performance. We compare our FHE-based solution with conventional and Attribute Based Encryption schemes for secure a) storage, b) computation, and c) sharing of the medical data. We show that despite the overhead compared to existing encryption schemes, our system can be implemented with a reasonable budget with major public cloud service providers. With the recent advances on FHE coupled with the decreasing costs of cloud services, we argue that our study is a novel step towards privacy-preserving cloud-based health monitoring that can improve the diagnosis of cardiac diseases, which are responsible for the highest percentage of deaths in the United States.