Chapter 77
A Cloud Based Solution for Collaborative and Secure Sharing of Medical Data

Mbarek Marwan
Chouaib Doukkali University, Morocco

Ali Kartit
Chouaib Doukkali University, Morocco

Hassan Ouahmane
Chouaib Doukkali University, El Jadida, Morocco

ABSTRACT

Healthcare sector is under pressure to reduce costs while delivering high quality of care services. This situation requires that clinical staff, equipment and IT tools to be used more equitably, judiciously and efficiently. In this sense, collaborative systems have the ability to provide opportunities for healthcare organizations to share resources and create a collaborative working environment. The lack of interoperability between dissimilar systems and operating costs are the major obstacle to the implementation of this concept. Fortunately, cloud computing has great potential for addressing interoperability issues and significantly reducing operating costs. Since the laws and regulations prohibit the disclosure of health information, it is necessary to carry out a comprehensive study on security and privacy issues in cloud computing. Based on their analysis of these constraints, the authors propose a simple and efficient method that enables secure collaboration between healthcare institutions. For this reason, they propose Secure Multi-party Computation (SMC) protocols to ensure compliance with data protection legislation. Specifically, the authors use Paillier scheme to protect medical data against unauthorized usage when outsourcing computations to a public cloud. Another useful feature of this algorithm is the possibility to perform arithmetic operations over encrypted data without access to the original data. In fact, the Paillier algorithm is an efficient homomorphic encryption that supports addition operations on ciphertexts. Based on the simulation results, the proposed framework helps healthcare organizations to successfully evaluate a public function directly on encrypted data without revealing their private inputs. Consequently, the proposed collaborative application ensures privacy of medical data while completing a task.

DOI: 10.4018/978-1-5225-8176-5.ch077

1. INTRODUCTION

The adoption of collaborative software or groupware in healthcare domain would inevitably improve patient services (Lee & Leu, 2016). Indeed, it allows healthcare ecosystem to share data and tools efficiently. The ability of this model to easily build a collaborative environment has significantly attracted the attention of healthcare institutions. Despite its remarkable ability to facilitate coordination and data exchange, this concept requires massive investment in hardware and software. In this respect, we propose a highly efficient approach and framework to encourage communication and effective teamwork among healthcare professionals. This can be achieved by using cloud technology which ensures cost reduction, greater flexibility, elasticity and optimal resource utilization (Mell & Grance, 2009; Shameem, Johnson, Shaji, & Arun, 2017). Additionally, customers take advantage of a flexible usage-based pricing system for an optimal use of cloud resources (Arinze & Anandarajan, 2010). More precisely, metering and reporting tools are generally based on real-time usage and the quality-of-service requirements of cloud services. The features and characteristics of cloud are summarized in the Figure 1.

Although cloud services offer significant potential and advantages, the utilization of off-site solutions raise numerous security issues (Marwan et al., 2018). In order to use cloud services safely, it is of paramount importance to explore and seriously address cloud security risks. The next step is to design and develop a cloud platform that enables secure collaboration among medical professionals. The primary contribution of this research consists in using Secure Multi-party Computation (SMC) protocol in conjunction with Pallier cryptosystem to protect patient privacy against unauthorized users. Concretely, this technique enables various parties to conduct operations over distributed data without revealing confidential information. In reality, SMC protocol is widely used to guarantee data privacy in various

Figure 1. Definition of cloud computing according to NIST