Chapter 16
A Framework to Secure Medical Image Storage in Cloud Computing Environment

Mbarek Marwan
Chouaib Doukkali University, Morocco

Ali Kartit
Chouaib Doukkali University, Morocco

Hassan Ouahmane
Chouaib Doukkali University, Morocco

ABSTRACT

Nowadays, modern healthcare providers create massive medical images every day because of the recent progress in imaging tools. This is generally due to the increasing number of patients demanding medical services. This has resulted in a continuous demand of a large storage space. Unfortunately, healthcare domains still use local data centers for storing medical data and managing business processes. This has significant negative impacts on operating costs associated with licensing fees and maintenance. To overcome these challenges, healthcare organizations are interested in adopting cloud storage rather than on-premise hosted solutions. This is mainly justified by the scalability, cost savings and availability of cloud services. The primary objective of this model is to outsource data and delegate IT computations to an external party. The latter delivers needed storage systems via the Internet to fulfill client's demands. Even though this model provides significant cost advantages, using cloud storage raises security challenges. To this aim, this article describes several solutions which were proposed to ensure data protection. The existing implementations suffer from many limitations. The authors propose a framework to secure the storage of medical images over cloud computing. In this regard, they use multi-region segmentation and watermarking techniques to maintain both confidentiality and integrity. In addition, they rely on an ABAC model to ensure access control to cloud storage. This solution mainly includes four functions, i.e., (1) split data for privacy protection, (2) authentication for medical dataset accessing, (3) integrity checking, and (4) access control to enforce security measures. Hence, the proposal is an appropriate solution to meet privacy requirements.

DOI: 10.4018/978-1-5225-8176-5.ch016

1. INTRODUCTION

In the field of medicine, medical imaging constitutes an essential element in the diagnostic process. This is due mainly to the continuous development of biomedical imaging technology. In fact, these tools are considered as a clinical Diagnostic Support Tool (DST) to improve the quality of medical services. That is, hospitals and imaging centers produce large quantities of digital data to meet increasing demands. Therefore, scalable platforms along with software are required to manage patients' medical data. Traditionally, healthcare organizations build and maintain local data centers to achieve this objective. Although Electronic Medical Record (EMR) systems are very beneficial for healthcare domain, they necessitate large investments in in-house applications and computational resources. Unfortunately, this has a negative impact on operating costs related to maintenance and license. To remedy this problem, cloud storage is a new way of delivering on-demand computing resources over the Internet. The primary aim of this concept is to facilitate the implementation and usage of the storage systems. More precisely, this model is designed to deliver a shared pool of configurable computing resources via the Internet. With this technology, the needed storage systems are provisioned and released to the clients with minimum management effort (Mell et al., 2009). At the same time, cloud storage relies on pay-per-use pricing model in which the consumers are charged based on cloud services utilization. Hence, cloud storage is an adequate solution to cut costs and increasing profits.

For these reasons, there has been a continuous demand for cloud services in the healthcare domain. Though cloud storage has many advantages, the adoption of this technology brings several security problems (Fabian et al., 2015; Anuja et al., 2015; Diago et al., 2014). In this regard, ensuring the confidentiality of medical data in the cloud environment is the major challenge facing this new paradigm, especially in healthcare sector. For instance, many frameworks and solutions have been proposed recently to meet security requirements. The main contribution of this paper is twofold. First, we present the state-of-the-art cloud storage implementation as well as techniques involved in data security. Second, we propose a framework that uses segmentation and watermarking techniques to secure medical images. Additionally, we use ABAC model to enforce data security policies.

The rest of this paper is organized as follows: Section 2 and 3 are meant to present and discuss existing solution to ensure the security of cloud storage. Section 4 and 5 provide a deep insight into privacy-preserving requirements to meet healthcare needs, especially data security. In section 6 and 7, we present the proposed framework as well as method used in data protection process. We end this paper in section 8 and 9 by concluding remarks and future work.

2. RELATED WORK

Bastião et al. (2012) develop a novel architecture to safely implement an outsourcing solution of PACS (Picture Archiving and Communication System). The proposal is designed to support a multi-cloud system, which incorporates more than one cloud providers. Typically, two major components of a common PACS are used in this framework, i.e., DICOM object, Repository and Relational Database (RDBMS). In the same line, blobsore and database are commonly used for storing and archiving medical records. It uses three additional components to address security risks: Gateway, MasterIndex and Cloud Slaves. The MasterIndex module protects the patient's information, especially name and referring physician in order to ensure anonymity. Furthermore, it keeps different keys that are used during encryption and