Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 127 (2018) 388–397

Procedia Computer Science

www.elsevier.com/locate/procedia

The First International Conference On Intelligent Computing in Data Sciences

Security Enhancement in Healthcare Cloud using Machine Learning

Mbarek Marwan*, Ali Kartit, Hassan Ouahmane

Chouaïb Doukkali University, LTI Laboratory, ENSA
Avenue Jabran Khalil Jabran, BP 299, El Jadida, Morocco

Abstract

Image processing requires sophisticated platform because it is usually very expensive in terms of memory space and computational time. Consequentely, it is important to adopt economical solutions to replace traditional systems. These considerations led us to use cloud computing to meet large-scale data processing requirements. Meanwhile, this approach provides rapid access to on-demand services with high availability and scalability. Therefore, using cloud services instead of in-house applications would undoubtedly help healthcare organizations outsource computations to an external party, thereby minimizing operating expenses. Nevertheless, strong data protection against both untrusted clouds and unauthorized users is required to prevent malicious data disclosure. Today, various frameworks are developed to enable users to store and process their data using cloud computing. In genaral, they are built up using cryptosystems, distributed systems and sometimes a combination of both. In particular, homomorphic cryptosystems, Service-Oriented Architecture (SOA), Secure Multi-party Computation (SMC) and Secret Share Schemes (SSS) are the major security mechanisms for almost all existing implementations. The main problem in the process of massive data analysis over cloud using these techniques is the computational costs associated with image processing tasks. The first and foremost challenge is to prevent unauthorized access to medical records and personal health information. In this regard, we propose a novel approach based on machnine learing techniques to secure data processing in cloud environement. Typically, we use Support Vector Machines (SVM) and Fuzzy C-means Clustering (FCM) to classify image pixels more efficiently. Additionally, we incorporate a further level, the CloudSec module, into the conventional two layered architecture to reduce the risk of the potential disclosure of medical information. We perform two sets of experiments to evaluate the proposed technique. The simulation results demonstrate that the use of Support Vector Machines (SVM) is an efficient concept for simultaneous image segmentation and data protection. In fact, we obtain some encouraging findings which reveal new insights so as to promote cloud services in the healthcare domain.

Keywords: Cloud computing; image processing; security; machine learning; SVM; FCM

* Corresponding author. Tel.: +212678418459.
E-mail address: marwan.mbarek@gmail.com

10.1016/j.procs.2018.01.136

1. Introduction

Cloud computing can offer the possibility of outsourcing computation operations, thereby allowing healthcare organizations to leverage the cost advantages. The use of this concept enables consumers to process patients' electronic health records remotely using cloud-based imaging solutions. The principal benefit of this concept is the ability to provide ubiquitous access to imaging applications without having to buy and maintain these tools. It is commonly agreed that cloud computing has completely revolutionized the way health records are being managed, stored, processed and used. In this model, cloud providers deliver a wide variety of Health Information Technology (HIT) solutions to support E-health systems and meet the growing need for healthcare services. Interestingly, the easy utilization of cloud applications, flexible resources management, a pay-per-use basis model for charging clients are some basic characteristics that define a cloud service [1]. This obviously implies that there will be a substantial growth in demand for cloud adoption since it offers enormous opportunities for healthcare organizations. Unlike a traditional model, the usage of cloud brings security issues because clients' data are commonly stored and processed on distant data centers. There is actually a large number of factors that can specifically affect cloud solution considerations, including virtualization security risks [2], data storage location challenges [3], potentially insecure storage web technology [4], systems interoperability issues [5], [6] and legal constraints [7]. For instance, homomorphic cryptosystems, Service-Oriented Architecture (SOA), Secure Multi-party Computation (SMC) and Secret Share Schemes (SSS) are widely used as a security mechanism to ensure a minimum level of confidentiality and privacy of patient's health records. However, in many cases, these techniques cannot guarantee the Quality of Service (QoS) requirements, which are expressed and well-defined in the Service Level Agreement (SLA). First, digital records are so large that they are time-consuming in the processing stage. Second, these mechanisms are still insufficient with regard to medical data protection compliance.

Our main objective is to provide healthcare organizations with a simple and efficient cloud framework to analyze digital records using only cloud resources. We are going to show how machine learning algorithms can be used to overcome security problems in data processing. Especially, we rely, in this study, on Support Vector Machine (SVM) classifiers because they have received a growing interest in multi-region segementation techniques. In addition to providing more secure operations, the proposal is a good distributed processing solution to noticeably improve the running time. The objective of the three-level architecture is to handle additional cloud security challenges and risks, especially anonymity and unlinkability.

The rest of this paper is organized as follows. Section 2 examines the related works in this field and discusses the limitations of existing approaches. In Section 3, we describe the fundamentals of the proposed solution to address security problems in cloud-based services. Section 4 provides details about techniques involved in data protection. Section 5 reports experimental results of our proposal. Conclusion and perspectives are given in Section 6.

2. Related work

In general, significant privacy concerns might emerge when outsourcing data storage and computation to cloud providers. The confidentiality of health records in cloud storage usually involves encrypting clients'data before transmitting them into off-site servers. In this sense, several techniques are available to help deal with this issue, including AES, RSA DES, 3DES, ECC, ECDH. These methods, unfortunately, do not provide the ability to achieve secure data processing because they cannot be used in encrypted domain. In response to this challenge, we provide and discuss, in this section, techniques for implementing a secure cloud-based image processing.

In [8], the authors developed a framework that uses XML standard and Service-Oriented Architecture (SOA) to build distributed software systems. In this approach, a block of many web services is created to process digital records. Accordingly, each node is responsible for performing a specific task. Technically, the process of image analysis is first decomposed into smaller tasks each of which is mapped to a distinct cloud provider. This method is meant to ensure collaboration between business components during data processing. However, privacy protection is the main disadvantage of this technique because it processes only raw images. In the same line, image processing as a service is developed in [9]. Chiang et al. use an APIs (Application Programming Interface) that integrates frontend services to analyze clients'data easily. Mainly, SOA and ImageJ tools are used to simplify the development and deployment processes on the cloud platform. The proposal is composed of various modules to process data