Enhancing the Security of Exchanging and Storing DICOM Medical Images on the Cloud

O. Dorgham, Prince Abdullah Ben Ghazi Faculty of Information Technology, Al-Balqa Applied University, Al Salt, Jordan
Banan Al-Rahmaneh, Prince Abdullah Ben Ghazi Faculty of Information Technology, Al-Balqa Applied University, Al Salt, Jordan
Ammar Almomani, IT-Department, Al-Huson University College, Al-Balqa Applied University, Irbid, Jordan
Moh’d Al-Hadidi, Prince Abdullah Ben Ghazi Faculty of Information Technology, Al-Balqa Applied University, Al Salt, Jordan
Khalaf F. Khattatneh, Prince Abdullah Ben Ghazi Faculty of Information Technology, Al-Balqa Applied University, Al Salt, Jordan

ABSTRACT

Medical image information can be exchanged remotely through cloud-based medical imaging services. Digital Imaging and Communication in Medicine (DICOM) is considered to be the most commonly used medical image format among hospitals. The objective of this article is to enhance the secure transfer and storage of medical images on the cloud by using hybrid encryption algorithms, which are a combination of symmetric encryption algorithms and asymmetric encryption algorithms that make the encryption process faster and more secure. To this end, three different algorithms are chosen to build the framework. These algorithms are simple and suitable for hardware or software implementation because they require low memory and low computational power yet provide high security. Also, security was increased by using a digital signature technique. The results of the analyses showed that for a DICOM file with size 12.5 Mb, 2.957 minutes was required to complete the process. This was totaled from the encryption process took 1.898 minutes, and the decryption process took 1.059 minutes.

KEYWORDS

Cloud Computing, DICOM Images, Elliptic Curve Cryptography, Security

INTRODUCTION

Securing the information stored in cloud data centers is one today’s most pressing issues. All sensitive information, such as medical images, needs to be handled with great care to ensure its security when it is uploaded or exchanged on the cloud. Currently, many applications are being used to archive and store medical images. Telemedicine applications are considered to be one type of application that facilitates the transfer of medical images across networks. On the other side, cloud computing provides encapsulation for resources via the Internet in the form of either dynamic, scalable, or virtualized services. Medical imaging departments in hospitals continuously generate many different medical images. These images need to be stored and exchanged between different specialists in hospitals across the world for the purpose of diagnosis. Hence, it is necessary to provide a high level of data protection when transferring a patient’s data over the cloud environment in order to overcome any attacks that

DOI: 10.4018/IJCAC.2018010108

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
the data may encounter during transmission. Various security mechanisms such as authentication, cryptographic algorithms, and digital signatures are used to protect images from unauthorized attacks.

However, although there are many benefits, some risks may arise when circulating medical data in open networks which are easily accessible to intruders. Hence, more care is required to hide patient information in medical images and to protect them from different security threats, without affecting the quality of the images (Ashley 2002; McEvoy & Svalastoga 2009). Security issues to consider include confidentiality, integrity, availability, authentication, access control and privacy (Anuja & Jeyamala 2015).

The necessity of using cloud computing for medical data storage and transmission arises from the importance of needing a large repository for and continuous access to medical data. In this regard, cloud computing is a better solution for handling medical images than other available options. Due to the large and increasing number of medical images, the activities of storing and exchanging them has become a daily routine in hospitals around the world. So, it is vital to find a secure way to transmit them over the cloud. Not only medical applications need image security, there are other applications that need it, too, such as confidential communications, video surveillance materials, and military applications (Bernarding et al. 2001). On May 2017, one of the most infamous threats that the world has faced thus far was the disruption of the information technology (IT) systems of the National Health Service in the UK due to cyber-attacks. The hospitals affected were located in London, Blackburn, Nottingham, Cambridge and Hertfordshire.

There are many applications that are used to archive and store medical images. Telemedicine applications as in (Dorgham et al., 2017; Dorgham et al., 2012; Fisher et al., 2013) are considered to be one such type of application that facilitates the transfer of medical images across networks. On the other side, cloud computing provides resource encapsulation on the Internet in the form of dynamic, scalable, and virtualized services (Ulutas et al., 2011). However, cloud computing is an environment that works solely online and there is no full or robust security in many cases. This makes transferring medical images in cloud computing insecure. Data security is considered to be a weakness of cloud computing, especially when users outsource their data to distributed storage systems instead of using local storage (Rathi & Inamdar, 2012; Wu et al., 2017). Medical data contains sensitive and crucial data about a patient’s case. Hence, it is necessary to provide a high level of protection when transferring this type of data. Moreover, it is necessary to protect the system from any attack that may appear when transmitting medical data over a network.

Therefore, in the light of the above we propose a new framework based on different types of algorithms to secure medical data and reduce the execution time of the encryption process. The standards of Digital Imaging and Communication in Medicine (DICOM) are not just for images; they are for patient records, studies, reports and other data groupings, too. DICOM files contain sensitive information (such as the patient’s name, date of birth, diagnosis, name of doctor, etc.). They consist of one or more compressed images and cannot be viewed on a computer; they must be stored in a database. Thus, the information can be viewed anytime. Hence, the importance of ensuring data preservation and denial of access by unauthorized persons arises.

In addition, some further challenge faces developers when managing DICOM images because this process requires direct communication between the imaging device and another one in order to compile all the patients’ data. It is difficult to achieve high security and privacy for medical care data, in addition to meeting the general requirements of the cloud (such as confidentiality, authenticity, and integrity) (Furht & Escalante 2010; Khan & Al-Yasiri 2016; Patra & Barik 2014).

This research focuses on these challenges and intends to develop a secure method to transfer medical images using Elliptic Curve Cryptography (ECC), eXtended Tiny Encryption Algorithm (XTEA) and Secure Hash Algorithm 3 (SHA-3), which are chosen because they have a low memory requirement, provide high security, and are simple, fast and suitable for hardware or software implementation.
Information Technology Governance Barriers, Drivers, IT/Business Alignment, and Maturity in Ghanaian Universities

An Improved Secure SIP Registration Mechanism to Avoid VoIP Threats
[www.igi-global.com/article/an-improved-secure-sip-registration-mechanism-to-avoid-voip-threats/159849?camid=4v1a](www.igi-global.com/article/an-improved-secure-sip-registration-mechanism-to-avoid-voip-threats/159849?camid=4v1a)

Marketing and Reputation in the Services Sector: Higher Education in South Africa and Singapore
[www.igi-global.com/article/marketing-reputation-services-sector/45880?camid=4v1a](www.igi-global.com/article/marketing-reputation-services-sector/45880?camid=4v1a)