ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Securing DICOM content in a public cloud using Transposition based AES

P.Subhasri [1], Dr. A. Padmapriya [2]

[1] Research scholar, [2] Associate professor,
Department of Computer science and Engineering,
Alagappa University, Karaikudi.
[1] swarnasubha91@gmail.com
[2] mailtopadhu@yahoo.co.in

Abstract - **Medical image processing is one of the rapidly growing areas in the healthcare systems. So the sharing of medical records in a secured way is very essential. In many hospital management systems, CD is used to share the patient report details among multiple health care services. But it was not a secured way of sharing patients reports. In this paper, a new mechanism is proposed for storing and sharing of medical images through public cloud. With the help of cloud we can store huge amount of data as well as avoid redundancy by sharing them. Here the DICOM encrypted contents are stored in a public cloud and it can be shared with the registered users who wants to access it. A novel transposition based AES encryption method is used to encrypt the DICOM contents and encrypted contents alone are stored on public cloud. Only authenticated users can access the contents. So the DICOM contents can be shared in secured way with the help of this proposed method.**

Keywords— **Cloud computing, Security, DICOM contents, Public cloud.**

I. INTRODUCTION

EMR (Electronic Medical Records) refers to a paperless, digital and computerized system of maintaining the entire medical details within hospital management system (5). It helps to reduce storage space and some errors which were appeared on its documentation transmissions. The fast growth of e-healthcare management system increases the medical data management challenges such as share, manage and process those data with minimum cost and secured access. The DICOM (Digital Imaging and Communication in Medicine) has been the universal standard for secured communications of medical images over networks. It was invented by National Electrical Manufacturers Association (NEMA) in 1983 (5). It contains four security profiles namely; secure usage profiles, secure transport connection profiles, digital signature profiles, and media storage security profiles to conform whether the health records are protected during its transmissions (6).

Cloud computing offers internet based technologies on virtualized storage and telemedicine services. Over cloud environment the hospital management system processed various computer paradigms like transmission, storage and further retrieval of patient details based on the user needs (8). While the transmissions of medical records on cloud it have some disadvantages also, data security considered a main problem on distributed storage systems. Therefore, when transferring the medical records over cloud, confidentiality and integrity are the main security issues to overcome (3). One solution to achieve the required trust management between the cloud computing and user, cryptographic techniques used to encrypt and decrypt the storage contents before transferring it.

The paper is organized as follows. Section 1 provides a general description of electronic medical records with cloud computing characteristics including DICOM details and cloud computing services. Section 2 presents a brief review of the related work and challenges about cloud computing security. Section 3 includes two phases of the proposed work which is the proposed algorithm methodology and cloud configuration. Section 4 illustrates the results and discussions of the proposed methodology. The efficiency and contributions of this paper are concluded in section 5.

1.1 DICOM Viewer

A DICOM file contains the details of the image pixel and also the explanation of the patient record in same file. For example, consider X-ray knee image, it actually contains the image details and patient records within the file. So a special

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

type of viewer is required to view the entire DICOM file. Various DICOM file viewer software is available in internet. This new type of DICOM viewer (9) is implemented in c#, this will be split the .dcm file into image and tag. The split .dcm image is stored in Jpeg, Png & Bmp image format and the tags are stored in text format.

1.2 Cloud computing Services

Sharing the data from provider to end users through internet is the important concept in cloud computing. It provides various types of services to share the medical records rather than a unit of product. These services will make is flexible and easy to share records. The basic types of services (4) as follows,

Web based cloud services: These services exploit certain web service functionality, rather than using fully developed applications. It includes an application programming interchange for Google maps, and also the payroll or credit card processing.

Saas (software as a service): It is one of the ideas to providing a given application to multiple tenants, typically using the browser saas solutions are common in sales, HR and ERP.

Paas (Platform as a service): This is different types of saas. The user runs their own application but they do it on the cloud provider's infrastructure.

Utility cloud services: There are virtual storage and server options that organizations can access on demand, even allowing the creation of a virtual data centre.

Managed services: This is maybe the oldest iteration of cloud solutions. In this concept, a cloud provider utilizes an application rather than end users. Anti-spam services or even application monitoring services is one of the managed services.

Service commerce: These types of cloud solutions are a mix of saas and managed services. This type of services includes expense tracking, travel ordering or even virtual assistant services.

II. RELATED WORK

The following papers motivated the proposed work for sharing DICOM contents over cloud computing environment.

Fatma E.-Z. A. Elgamal et al. in 2013 (7) has introduced an efficient watermarking technique to secure the medical images over the cloud computing environment. The authors using two level of authentication in processed medical images through private secret key and embedding/extraction algorithms. In this paper, the scheme is implemented using a dynamic embedding/extraction process to exploit all the capacity of the original image in order to increase the visibility of the final watermarked medical image. A private shared key is also used to enhance the security needs. The authors discussed the experimental results which will secure medical images through its processing.

Rabi Prasad Padhy et al. in 2012 (8) have proposed a cloud based model for developing the healthcare systems. In this paper, the authors implemented cloud computing system in healthcare is not to compete with each other but serves to facilitate and improve the quality of patient care. They present a cloud based rural healthcare information system model to store medical records of their patients on cloud. This allowed a secured environment with easy management of data privacy and security and also the applications and documents are accessible from anywhere in the world, facilitating group collaboration on documents and projects with the use of cloud.

Chia-Chi Teng et al. in 2012 (2) developed a framework for medical imaging applications to securely communicate the medical image with cloud computing. This paper provides a framework which is cloud-based image storage and management service using a standard DICOM protocol. The design and implementation of this system demonstrated the feasibility of using the cloud computing infrastructure to provide an image repository and processing platform for some mobile devices. This implementation also improves the interoperability of previously standalone and proprietary mobile devices with existing clinical systems.

2.1 Cloud computing security Issues

When medical records are sent from one hospital to other through cloud computing environment, the following security issues (1) are raised.

Data security issues:

Since the medical record are placed in a public cloud, anyone from anywhere at any time can access those records. So at this level data loss and data modification may be affected due to its common storage.

Privacy Issues:

The cloud computing service provider must make sure that the patient personal records are well secured from other customer and user. As most of the servers are external so the cloud service provider should make sure who is accessing the data and who is maintaining the server. In this level privacy issues are the common problems.

Infected Application:

Any infected application may be uploaded by any malicious user onto the cloud, so this will affect the patient medical records.

Security issues:

In cloud computing security it has done on two levels, such as the provider level and user level. The provider makes

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

sure the originality of their uploaded contents and the user check if any data loss or stealing is concerned their retrieved content from the cloud.

III. BASE METHODOLOGY

With the use of new DICOM viewer (9) the .dcm file is read and it was split into Bmp image and tag. Both the portions are encrypted using transposed based AES encryption methodology.

In transposition based AES encryption methodology, it is the transposition technique rearranges the pixels in the original image according to some specific system and key. When DICOM Bmp image is given as input, the pixels in the image are rearranged. The method of transposition employed will be chosen randomly by combining the hash function. The transposed image is then encrypted using AES algorithm. In tag encryption method, the tag attributes are extracted and the whole attributes are converted into ASCII value, and then the values are rearranged and transposed by combining of the hash function. Finally, the transposed tag contents are encrypted using AES algorithm. The decryption is performed reversely on encryption.

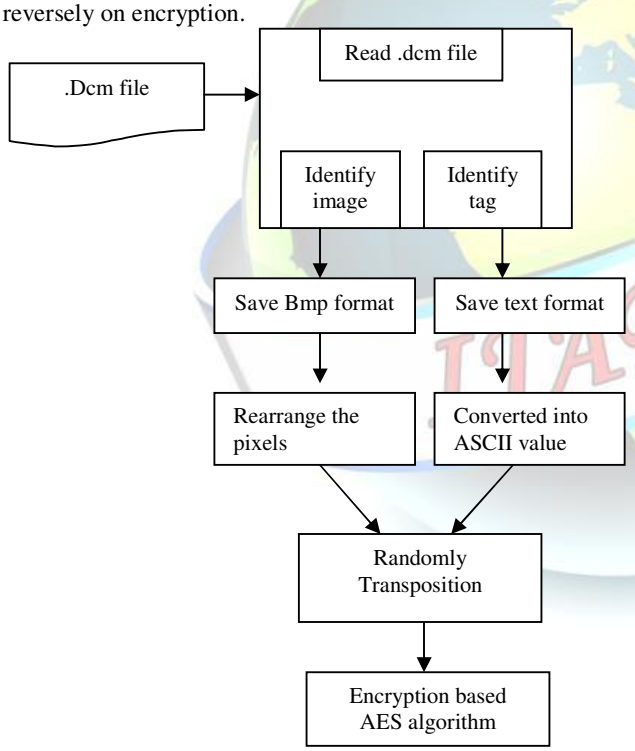

Figure 1. Proposed Architecture Design to encrypt the DICOM content

3.1 Cloud Configuration

DIOCM cloud storage configuration (10) is based on VM (Virtual machine) in Google cloud. The entire medical records instances are created by using the database add function. Then the content provider uploads the details about patient into the public cloud (10). The admin who saved the contents into cloud has the algorithm to encrypt the whole contents. After the encryption process is complete the contents are stored into cloud in secured way. When the user wants to access those contents they send a request to cloud admin, cloud admin provide a link to user. This link can be used to access the original DICOM contents in secured and authenticate way to the user.

IV. RESULTS & DISCUSSIONS

The following challenges are faced by existing methods,

- Absence of integrity and confidentiality.
- Excessive resources utilization due to redundancy of medical image storage at different locations.
- Difficulty in retrieval of patient's medical history in the Natural Disaster-affected areas.
- Lack of DICOM/IHE/HL7 Standards awareness and its importance among Doctors, Technicians, and PACS Administrator and Hospital staffs.

In order to overcome these pitfalls, a confidentiality system is proposed here. The proposed system will store the DICOM content in a Trustworthy Health Information public Cloud (10). Using transposition based AES cryptographic technique, the details are stored in secured way. Since the information are to be stored in the cloud data redundancy will be eliminated. Access to the resources will be done with suitable authentication.

The main features of the proposed work are;

- To provides integrity, confidentiality and authentication.
- To provide accessed based on authentication.
- To allows doctors to maintained advanced secret DICOM medical image.
- To provide a simple and intuitive interface to the commonly required functionality.
- To present a standard consistent model for common cryptography tasks.
- To improve security and efficiency in storage and retrieval of the DICOM content in public cloud.
- To ensure individual's privacy of DICOM medical images through cryptographic methods.
- To define trust boundaries between Cloud Providers (CP) and consumers to clearly establish and promulgate boundaries of responsibility for providing security.

V. CONCLUSIONS

In this paper, a new mechanism which is transposition based AES algorithm was proposed to ensure the security of DIOCM content in public cloud. These types of medical records sharing systems will improve the security of the contents to be shared across all healthcare institutions. Quick

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

and secured access is very essential to share the medical records. This proposed scheme, also provides the authentication for patient to access the DICOM in public cloud is. So it will improve the quality of the original content and also increases its safety.

REFERENCES

[1] F.A.Alvi., B.S.Choudary and N.Jaferry, "Review on cloud computing security issues & challenges", iaesjournal.com, vol.2, 2012.
[2] Chia-Chi Teng et al., "Mobile Ultrasound with DICOM and Cloud Connectivity", Proceedings of the IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI 2012) Hong Kong and Shenzhen, China, 2-7 Jan 2012, pp. 667-670.
[3] Cloud computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.com.
[4] C.N. Höfer and G. Karagiannis, "Cloud computing services: taxonomy and comparison", Internet Serv Appl (2011).
[5] DICOM security chapter 11, ACR-NEMA (National Electrical Manufacturers Association files, pp. 247-261.
[6] Digital Imaging and Communications in Medicine (DICOM) Part 15: Security Profiles, Published by "National Electrical Manufacturers Association" USA, in 2003.
[7] Fatma E.-Z. A. Elgamal et al., "A Trust Management Scheme for Sharing Secure Medical mages over Cloud Computing Environment", Journal of Advances in Computer Network, Vol. 1, No. 3, September 2013, pp. 201-207.
[8] Rabi Prasad Padhy et al., "Design and Implementation of a Cloud based Rural Healthcare Information System Model", UNIASCIT, Vol 2 (1), 2012, ISSN 2250-0987, pp. 149-157.
[9] P.Subhasri and Dr. A. Padmapriya, " Enhancing the Security Of Dicom Content Using Modified Vigenere Cipher", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.55, May 2015, pp. 1951-1956.
[10] P.Subhasri and Dr. A. Padmapriya, "Secured Sharing of DICOM Contents in a Public Cloud using Random Encryption Methodology", Communicated on Elsevier Computer Standards & Interfaces Special Issue on Cloud Computing Security and Privacy: Standards and Regulations , March 2016.