A Survey On Security Issues And Solutions For Storage And Exchange Of Medical Images In Cloud

M.Anuja[1], C.Jeyamala[2]
[1]Thiagarajar College of engineering, India, anujjaa@gmail.com
[2]Thiagarajar College of Engineering, India, jeyamala.chandrasekaran@gmail.com

Abstract: Telemedicine helps health care professionals to evaluate, diagnose and treat patients from remote locations. Extending telemedicine over cloud offers numerous advantages such as data portability, increased and flexible storage capacity, data migration and patient-centric connected system. The patients need maintain their medical reports in the hands to consult the specialists. Telemedicine in cloud makes easier to communicate with the specialists across the world. Inspite of numerous advantages, security issues like confidentiality, integrity, availability, authentication, access control, privacy are of great concern. Many solutions have been proposed in the literature to address these issues. The performance and security of the techniques have been analyzed and is reported in detail.

Keywords : Cloud Computing, Telemedicine, Medical Imaging, Information Security, Confidentiality.

INTRODUCTION

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[1]. The five essential characteristics of cloud computing are on-demand self service, broad network access, resource pooling, rapid elasticity, measured services. The service models [1] are Software-as-a-service (SaaS): The consumer can use the applications running on the cloud infrastructure.
Platform-as-a-service (PaaS): The consumer can deploy the created applications onto the cloud infrastructure.
Infrastructure-as-a-service (IaaS): The consumer is provided with the fundamental computing resources where he can deploy and run arbitrary software.
The deployment models [1] are private, public, community, hybrid. Private cloud is used by a single organization consisting of many consumers. Public cloud is used by a general public. Community cloud is used by a specific community of users that have shared concerns. Hybrid cloud is a combination of two or more distinct cloud infrastructures.

Innovations in cloud computing and emerging technologies have created a great impact in healthcare sectors. Providing health services with the help of digital technology is known as e-health.Telemedicine is a rapidly developing application where medical information is transferred through the internet. It helps in remote delivery of healthcare to patient's home. The healthcare sectors deal with large amount of data including Patients Health Records, Electronic Health Records, medical images generated from Computed axial tomography, Magnetic Resonance Imaging , digital mammography.

The need for large storage and continuous availability of e-health data increased the necessity of cloud computing in healthcare sectors. [14] The Hospitals who wanted to use Cloud Computing for storing and exchanging the medical information must strongly adhere to the HIPAA (Health Insurance, Portability and Accountability Act).Medical Imaging plays a prominent role in telemedicine. Now-a-days, in hospitals enormous amount medical images are generated and they are required to be stored and exchanged among various specialists for the purpose of diagnosis. Cloud Computing is a better solution for handling medical images. The benefits [2] of storing medical images in cloud are

- Data Portability: With the help of cloud it is easy to access and share the medical images between patients and doctors and also between the various specialists.
- Storage: Cloud offers large storage space to the healthcare professionals, patients to store the medical data with minimal cost.
- Remote access: Physicians, doctors, patients, researchers can remotely access the healthcare data.
- Data Availability: The medical data stored in the cloud is made available for 24×7 to the patients, healthcare professionals by cloud service provider.

Cloud based Medical Image Exchange provides on demand medical imaging information remotely. The most commonly used digital format for medical images is DICOM (Digital Imaging and Communication in Medicine). DICOM is a standard for storing and transmitting medical images. The sender and receiver should be in capable of receiving the DICOM format so that only the transmission will be successful [3]. PACS (Picture Archiving and Communication System) is a medical imaging technology, provides storage and access to medical images from various organizations. The universal format of PACS is DICOM [4].
Even though there are many advantages in storing medical images in cloud, certain limitations are also there. The medical images are sensitive information and should be stored in a secure way.

CHALLENGES AND SECURITY ISSUES

Security is the main factor in storing the medical images in cloud. The main security components are Confidentiality, privacy, integrity, availability. When compared to medical data securing medical images is a tedious process. The medical images are the sensitive information of patients and high security should be provided. The following are the main security threats in storing and exchanging medical images in cloud:

Confidentiality
Confidentiality is the process of keeping the patient's personal health information stored in the cloud private unless the permission is provided by the patient to release. It should be maintained by the users (patients, healthcare professionals), cloud service provider. The users store the data in the encrypted form to maintain the confidentiality. While storing and retrieving the data key management issues should be solved.

Integrity
Integrity is the process of ensuring that the medical image captured or provided is the original representation of the information and has not been modified. Since many participants (patients, health professionals, specialists from various hospitals) are involved in the cloud based medical image exchange, any modification can occur due to the participants intentionally or unintentionally. Hence integrity is a big issue to medical images in cloud.

Access Control
The unauthorized usage of medical images in cloud can be prevented with the help of access control policies. Many organizations allow the users who have previously registered with their valid credentials only to access the resources. The access control policies defined varies for the patients and healthcare professionals. The access control policies outsourced in cloud should not be leaked out.

Availability
The medical image stored in the cloud should be always available to the authorized users. Suppose if the resources are not available to the specialists in other place, he cannot diagnose the report and give immediate solution for the patients. The unavailability may occur due to the poor internet connection and als0 theft of information by the unauthorized users.

Data Ownership
Most of the unauthorized users get access to the medical images due to the missing of the owner's identity in the encrypted medical images. If the embedding of the owner's seal or identity is done in the encrypted images through encryption or watermarking methods, it is difficult for the attackers to gain access.

Privacy
Privacy refers to the right of patients to determine when, how and to what extent their health information is shared with others. It involves maintaining confidentiality and sharing identifying data, only with healthcare providers and related professionals.

Authentication
The medical image stored in the cloud should be accessed only by the authorized patients and doctors. The credentials provided by the users must match with the stored credentials of the users in the authentication process. If the credential details are leaked out , there occurs a possibility for the unauthorized users to access the data.

STATE-OF-THE-ART SECURITY SOLUTIONS

The researchers are working to address the various security issues in storing and exchanging the medical images in the cloud. This section discusses in detail about the proposed security solutions.

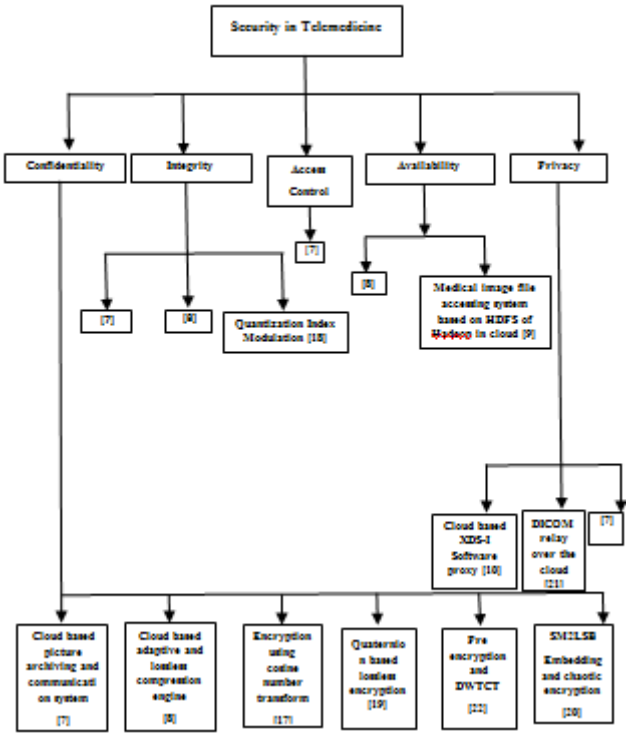

Fig 1: Taxonomy of security solutions

Confidentiality

Bastiao et al. [7] proposed an architecture for Cloud-based PACS (Picture Archiving and Communication System).Generally PACS has two components namely DICOM (Digital Imaging and Communication in Medicine) object repository and database system (RDBMS). In the proposed approach these two components are placed in the cloud using blobstore and database accessible through web services. This method supports multiple providers accessing the same information simultaneously. There are three main components: Gateway, MasterIndex, Cloud Slaves. The MasterIndex contains the confidential data. The cloud slaves perform blobstore and database. The Gateway provides interface between DICOM and cloud systems. The two DICOM services provided by Gateway are storage and query/retrieve. Storage process is done with the help of DICOM C-STORE command which stores the received medical images, waveforms.. The query/retrieve process

includes C-FIND (associated with queries), C-MOVE (associated with image retrieving). DICOM C-STORE is issued after the decryption of received object using the session key. They deployed the PACS modules in two cloud providers: Amazon S3 and Google Storage. This method mainly avoids unauthorized access by third party. Confidentiality of the medical images stored in the cloud can be enhanced with the help of MasterIndex.

Arcangelo et al.[8] proposed an engine for adaptive and lossless compression of 3D medical images. This allows embedding security watermarks within them to enhance the security of medical images in cloud. They also gave an architecture of a SaaS cloud system. The proposed model involves heterogeneous systems to interact in the cloud. The compression engine is based upon a predictive technique which includes image compression part and Least Significant bit (purpose of digital watermarking). The input to the engine is the 3D medical image and the output is the compression image with embedded secure watermarks. The compression engine consists of two prediction models: intra-slice and inter-slice prediction models. The images are divided into slices and in each slice watermark is embedded.. This system is deployed on Microsoft Azure platform. The system consists of three modules: virtual cloud, compression and digital watermark, storage and front-end interface. The virtual cloud module consists of two components discovery facility (to identify the location of the medical image) and communication facility (responsible for the transferring of medical images). The second module provides compression-as-a-service functionality. The storage module is based upon MySQL with CryptDB. CryptDB provides confidentiality against most attacks defined for SQL databases.

The medical images can be encrypted using the cosine number transform (CNT) proposed in [17]. This technique protects the image from rounding-off errors and the zero tolerance effect. This method can be applied only to the uncompressed images. The first step in the encryption scheme is to select a prime number over the field GF(p) where the cosine number transform is defined. The next step is to define CNT over the chosen field GF(p). The image blocks are selected in sequence. Two rounds are applied for encrypting the medical images. The dimensions of the transform, the overlapping of image columns and rows and the key space can be adjusted using the different algebraic structure proposed in the cosine number transform. Another technique used for encrypting the medical images is quaternion based encryption method proposed in [19]. It is proposed to encrypt both color and gray medical images. It is based on modified fiestel cipher. This technique enhances the confidentiality of the medical images stored in the cloud. The simulation results were shown for randomness tests, Avalanche effect. The computation speed is compared with the AES in ECB. It is difficult to identify the key value and the encryption is stronger. Experiments are conducted with a 512 × 512 px 8-bit gray-tone image decomposed from a 16-bit DICOM image. A new concept of medical image encryption scheme is adapted in [22]. The New Image Encryption System (NIES) consists of two parts namely a pre-encryption process and discrete-wavelet-transform-based-content transform. Permutation and substitution are used to change the image pixels and values in the pre-encryption process. It will yield a noise-like image. The noise-like image is transformed to visually meaningful encrypted image by discrete-wavelet-transform-based-content transform. It generates a visually meaningful images after encryption and protects the image from various noise attacks, data loss attacks. The decryption can be done with the secret key generated in the pre-encryption process and the parameter used in the transformation process. The experiments are conducted on the Amazon EC2 and tested.

Tao Xiang et al. [20] proposed an outsourcing chaotic selective image encryption technique with steganography. Here the important data is selected for encryption, embedded in a cover image. The stego image generated is then send to the cloud for outsourced encryption. After receiving the stego image the client can extract the secret data in the encrypted form and then decrypt the image. The SM2LSB embedding scheme is used for data reorganization and data embedding. The chaotic encryption technique is used which includes two steps: a multidimensional chaotic map to permutate the coordinates of pixels and one-dimensional chaotic-map to mask the pixel values. A 256×256 gray scale image is taken as the plain image and encryption technique is applied.

Work	Problem Characteristics	Model	Objective	Methodology
[7]	Storage of medical images in cloud	Amazon S3 and Google storage	Confidentiality	Cloud based PACS
[8]	Compressing the medical images, embedding security watermarks	Microsoft Azure platform	Confidentiality	Adaptive and lossless compression engine
[17]	Uncompressed medical images	Matlab	Confidentiality	Medical image encryption using cosine number transform
[19]	Secure storage of medical images	DICOM image	Confidentiality	Quaternian based encryption
[22]	Visually meaningful encrypted images	Amazon EC2	Confidentiality	NIES
[20]	Secure storage	Matlab	Confidentiality	Chaotic encryption,SM2LSB embedding

Table 1: Security solutions to obtain confidentiality

Integrity

The integrity is provided by the encryption algorithm AES (Advanced Encryption Standard) in the Cloud based PACS system [7]. The data is divided into chunks, encrypted with AES and send to blobstore. The patient name, {study, instance

UID}, encryption session key are securely transmitted and stored in MasterIndex. Data integrity is provided through SHA-1 cryptographic method in the adaptive and lossless compression engine [8]. The joint encryption/watermarking system proposed in [18] uses the combination of watermarking algorithm, the quantization index modulation. The encryption algorithm can be chosen as the stream cipher such as RC4 or block cipher (AES in cipher block chaining mode). This proposed technique ensures the image integrity. The watermark extraction and the decryption of the encrypted medical images are done independently. The AES in cipher block chaining mode makes the joint encryption/watermarking system compatible with the DICOM standard. Experiments were conducted on two different medical images:100 ultrasound images of 576 × 690 pixels of 8-bit depth and 200 PET images of 144 × 144 pixels of 16-bit depth This protects the system from unauthorized detection or extraction of messages, unauthorized embedding attack, unauthorized removal attack. The joint encryption/watermarking technique is slower than the encryption technique.

Work	Problem Characteristics	Model	Objective	Methodology
[7]	Storage of medical images in cloud	Amazon EC2 , Google storage	Integrity	Cloud based PACS
[8]	Compression of medical images and embedding security watermarks	Microsoft Azure	Integrity	Adaptive and lossless compression of medical images
[18]	Reliability of medical images	Matlab	Integrity	Quantizati- On index modulation

Table 2: Security solutions to obtain integrity

Access Control

The cloud based PACS [7] avoids unauthorized access by third party. The authorization to access the medical images stored in the cloud are provided by the access control policies defined in the proposed PACS system.

Work	Problem Characteristics	Model	Objective	Methodology
[7]	Secure storage of medical images in cloud	Amazon EC2 , google storage	Access control	Cloud based PACS

Table 3: Security solution to provide access control

Availability

Arcangelo et al.[8] proposed an engine for adaptive and lossless compression of 3D medical images. The compression engine consists of two prediction models: intra-slice and inter-slice prediction models. The images are divided into slices and in each slice watermark is embedded. The prediction errors can be reduced using prediction residual coding which uses Laplace transform. The main aim of the proposed system is to work in poor network condition. This system is deployed on Microsoft Azure platform. Chao-Tung et al.[9] made a study and developed a Medical Image File Accessing System (MIFAS) based on HDFS of Hadoop in cloud. The main aim of the proposed system is to solve the problems related to the storing and sharing of medical records and medical images between different hospitals. The system is implemented in OpenNebulla environment. Co-allocation mechanism allows parallel downloading from data nodes and solves the network problems. In this system the user uses MIFAS to access the medical images so that the co-allocation is enabled automatically. The system workflow involves five steps: 1. User inputs the username and password, 2. User inputs search terms to query patient information, 3. Users can view patient medical images, 4. User can configure in MIFAS. The experiments were conducted to compare the performance of MIFAS and PACS. The results show MIFAS reduces the single point failure, best suited for multiple user access. PACS is a high cost medical imaging system. The MIFAS can be further improved by enhancing the performance of file accessing.

Work	Problem Characteristics	Model	Objective	Methodology
[8]	Compression of medical images and embedding security watermarks	Microsoft Azure platform	Availability	Adaptive and lossless compression of medical images
[9]	Easy access to the medical images in cloud	OpenNebulla	Availability	MIFAS

Table 4: Security solutions for high availability

Privacy

Luis etal. [10] proposed a software proxy that enables the outsourcing of XDS architectural parts in cloud while preserving the interoperability, confidentiality and searchability of clinical information. They used a new searchable encryption scheme (SE), Posterior Playfair searchable encryption (PPSE). They described a solution that enables the outsourcing of standard XDS for imaging XDS-I. In XDS-I profile PACS, RIS, DICOM objects are considered in the XDS architecture. XDS-I compliant architecture is developed based on a proxy. It works as a privacy middleware system which converts plaintext flows into ciphered flows and vice-versa. The proxy contains the secret symmetric key which is used for encryption and decryption. 256-bit AES in cipher block chaining mode is used for encryption. The actors in this system are Image Document source, Image Document consumer, Document Repository and Document registry. They conducted experiments using the datasets from

radiology studies. The dataset composed of 130000 medical images generated from MRI, CT and CR. The system is deployed in Amazon's EC2 (Elastic Cloud Compute). The advantages of XDS-I are high availability, elastic resource allocation, efficient storage and a simple business model. XDS-I is suitable for heterogeneous datasets. Luis.A.Bastiao et al.[21] , interconnected the DICOM routers through a public cloud infrastructure. In this proposed technique ciphered data channel is introduced between the entities sharing the DICOM services. This ciphered data channel encounters the problems regarding data privacy and enhances the security. The DICOM services is implemented with two components: Storage and Query/Retrieval. The main advantage is that it provides remote search functionalities and secure exchange of medical images between various organizations. The proposed architecture includes DICOM bridge router and DICOM cloud router. This technique is implemented in the public cloud infrastructure. The tests are conducted on two different machines Intel Core 2 Duo 2.2GHz , 2GB RAM and AMD Athlon 1.6GHz 2GB RAM. Data privacy is only ensured in this technique and does not ensures other security parameters. The cloud based PACS [7] provides privacy and confidentiality through the MasterIndex. The MasterIndex contains the sensitive data of the patients.

Work	Problem Characteristics	Model	Objective	Methodology
[10]	Secure storage of medical images	Amazon EC2	Privacy	XDS-I software proxy
[7]	Secure storage and access to medical images	Amazon EC2, google storage	Privacy	Cloud based PACS
[21]	Secure transmission of the medical images	Public cloud	Privacy	DICOM relay over the cloud

CHALLENGES

Cloud Computing plays a major role in Medical Imaging. Security is the major drawback in cloud. Many security solutions have been proposed to address the issues in storing the medical images in cloud. No single solution addresses the key management issues while providing confidentiality, providing integrity with high computational speed. The time complexity will be more while using the encryption algorithm AES. The cloud based cryptanalysis is also not discussed in detail. Hence the scope for future works in storing and exchanging medical images in cloud is high.

REFERENCES

[1] Cary Landis and Dan Blacharski, "Cloud Computing Made Easy", version 3

[2] Shini S.G, Dr Tony Thomas, Chithranjan. K "Cloud Based Medical Image Exchange Security Challenges", Elsevier ,2012.

[3]DICOM, https://www.leadtools.com/sdk/medical/dicomspe

[4] PACS, searchhealthit.techtarget.com › PACS › Healthcare IT Glossary

[5] HIPAA, health.state.tn.us/hipaa/

[6] Louis Parsonson et.al, "A Cloud Computing Medical Image Analysis and Collaboration Platform", Cloud Computing and Services Science, Service Science: Research and Innovations in the Service Economy, Springer Science+Business Media New York 2012

[7] Luis A. Bastiao Silva, Carlos Costa, Jose Luis Oliveira, "A PACS archive architecture supported on cloud services", Springer, 2012.

[8] Arcangelo Castiglione et.al, "Cloud-based adaptive compression and secure management services for 3D healthcare data", Future Generation Computer Systems, Elsevier,2014

[9] Chao-Tung Yang et.al, "Accessing medical image file with co-allocation HDFS in cloud", Future Generation Computer Systems, Elseveir, 2014

[10] Luis S. Ribeiro et.al, "XDS-I Outsourcing Proxy: Ensuring Confidentiality While Preserving Interoperability", IEEE Journal of biomedical and health informatics, vol. 18, no. 4, July 2014

[11] Ji-Jiang Yang, Jian-Qiang Li, Yu Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment", Future Generation Computer Systems,2014

[12] Benjamin Fabian, Tatiana Ermakova, Philipp Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds", Information Systems, 2014.

[13] Telemedicine, http://www.americantelmed.org

[14] Medical Image Storage, http://www.cleardata.com

[15] Andrés Tello et.al, "RDF-ization of DICOM Medical Images towards Linked Health Data Cloud", Springer International Publishing Switzerland 2015

[16] A. Kanso , M. Ghebleh," An efficient and robust image encryption scheme for medical applications",Elsevier,2015

[17] J.B. Lima , F.Madeiro , F.J.R.Sales ," Encryption of medical images based on the cosine number transform", Elsevier, 2015

[18] Dalel Bouslim et.al, "A Joint Encryption/Watermarking System for

Verifying the Reliability of Medical Images", IEEE Transactions On Information Technology In Biomedicine, Vol. 16, No. 5, September 2012

[19] Mariusz Dzwonkowski et.al, "A New Quaternion-Based Encryption
Method for DICOM Images", IEEE Transactions On Image Processing, Vol. 24, No. 11, November 2015

[20] TaoXiang,Jia Hu, JianglinSun, " Outsourcing chaotic selective image encryption to the cloud with steganography", Elsevier, 2015

[21] Luís A. Bastião Silva," DICOM relay over the cloud", Springer, 2012

[22] LongBao, YicongZhou, "Image encryption:Generating visually meaningful encrypted images", Elsevier, 2015