A Comparative Study of Secured Medical Images in Cloud Environment

D. Linett Sophia
Department of ECE
S.A Engineering College
Poonammalle, Chennai

S. Balambigai
Department of ECE
Kongu Engineering College
Perundurai, Erode

***Abstract*— In recent years, health care organizations produce more number of medical images for processing and storing of medical records. With the advancement in medical field, security and confidentiality is of great concern as medical images are more sensitive. Also as medical images requires lot of space to be stored, an emerging technology known as cloud environment is mostly used for this purpose. Sharing of medical images in cloud helps the physicians to diagnose the problem from remote areas. As data are used among the cloud, medical images have to be protected to avoid illegal access of attackers. There are various techniques to solve the problem of securing such images. This paper makes a comparative analysis of various algorithms for providing security to medical images in cloud environment**.

Keywords— medical images, cloud environment, security

I. Introduction

The cloud computing technology is used by many consumers because of its accessibility, high throughput, and less timing. Due to advancements in medical field, Health care organizations produce lots of medical images day by day. These images are used for clinical decisions and diagnosis. As medical images are huge, requires lot of memory space to be stored. The medical practitioner also is in demand of medical images to diagnose the patients from remote centers. Hence one of the emerging technique of cloud computing is involved in this area to access all medical images at any time from any place. Though it seems to be a very attractive technique, it has lot of limitations in it.

The main aspect of medical images in cloud environment is its security and privacy. People are much concerned about their data to be much secured and also to maintain privacy. As medical images are transmitted to cloud, they are to be processed for security purposes. Both during transmission and storing of data in cloud, it has to be secured well.

Cloud computing involves many businesses and clients to access from any computers at any place. So a perfect authentication is also required to prevent or secure data in cloud environment. Authentication of users can be opf any form like iris, biometric etc. This also increases high security of medical images in cloud. Various algorithms have been put forward for security issues and merging it with the cloud environment. Cloud computing is actually an internet which can be accessed based on demand and charged only for the time and resources used. Though e-health care system has lot of advantages, still it’s in very slow growth compared with other sectors. The only reason for it is storing of sensitive data online[7]. A proper security mechanism is mandatory to prevent from unauthorized third parties.

This paper presents a brief description of various algorithms and techniques implemented to improve cloud environment for e-health care applications. The paper is ended by providing a comparative analysis of all algorithms and techniques of security in medical images.

II. Cloud Environment For Medical Images

Medical images play a vital role in modern health care units. More number of medical images has to analyzed and saved resulting in sufficient amount of hardware and software requirements. This ended with increase in healthcare costs. To overcome this limitation a cloud based environment is accessed for storage purpose. A cloud is a nothing a but internet containing huge amount of resources where the user can access it on-demand. The use of medical images on the cloud can be stated for following reasons a)cloud is dynamic providing at minimum cost of resources b) As all medical images are centralized, they can be accessed at any time anywhere.

The cloud consumer can have any of the following cloud models i)private cloud ii)public cloud iii) Hybrid cloud. Private cloud is for single organization so that ensures security for accessing the data. Public cloud is shared in public through internet. This model is mostly suitable for non sensitive data. Hybrid cloud is the combination of both private and public cloud. These above cloud model provide services in three different aspects IAAS[Infrastructure as a service],PAAS[platform as a service],Software as a service[SAAS].

The cloud environment creates various issues concerning with access of medical images. The two important aspects are Security and privacy of medical images. These two concepts are a challenging issue which has to be overcome. From the point of view of cloud architecture, there are certain factors which it faces in processing of medical images.

1) Resource availability and API[8]: Ensuring availability of resources for data storage has to done in cloud. The application programming interface and web application has to meet all security issu*es* during medical image transfer.

2) *Confidentiality and Integrity[8]:* As medical images are sensitive, the data should be protected and kept secret. The cloud architecture should make sure of the confidentiality of medical images. Ensuring integrity of medical images is also to be faced by provider of cloud services

The general idea of how cloud architecture is implemented with e-health applications is depicted by the below figure 1.

With all these factors, the rest of the section in this paper provides various techniques and algorithms for security in medical images and their computation in cloud environment.

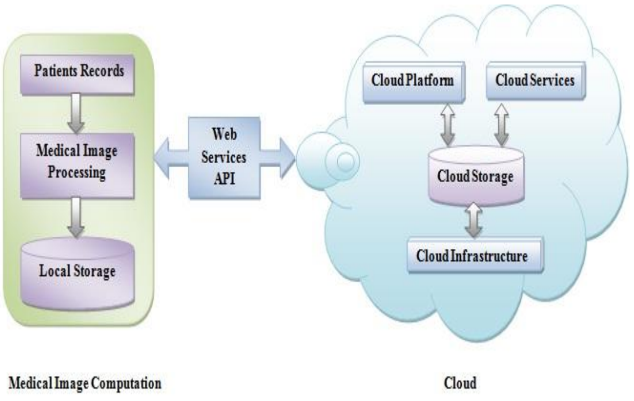


Fig.1. Idea of medical image computation in cloud

III. Current Techniques And Algorithms For Medical Image Processing

This section gives various existing techniques of providing secured medical images before transmission in cloud architecture and also the efficiency of cloud based medical image processing offered by the resource providers.

- Water marking scheme algorithm[1] ,uses a double secret key for preventing information in cloud. First the secret key is used for randomizing the medical information and then embeds these images into another secret key image.This algorithm uses DCT and DWT coefficients for embedding purpose. This scheme if good for JPEG compression images.

- In[2], states about the security aspects while migrating the medical information to cloud. This paper gives a confidentiality and integrity of cloud services by using a Melior system.A protocol for storage is implemented in this system.

- Content based water marking algorithm [3] presents a new method of encrypting medical records before it is transferred to cloud. This also involves Hadoop system and map reduction technique for a perfect solution. This paper separates the LSB of the image, provides signature, encrypt the data and finally construct a watermarked images. Security is given to medical images by watermarking and encryption mechanisms.

- Iris recognition technique[4] provides the authentication to the access of medical images. In this paper Iris recognition is used as a human biometrics for protecting the data in cloud. First the user iris is stored as a database in cloud and then matched with enrolled one This technique provides increased security aspects compared with other techniques.

- Homomorphic encryption Algorithm[5] is a useful tool to work with encrypted data. This algorithm provides improvement in CPU performance along with security of medical records.This paper involves NTRU scheme and GSW homomorphic encryption algorithm. The results of this algorithm are compared with other algorithm in terms of its system performance and its parameters.

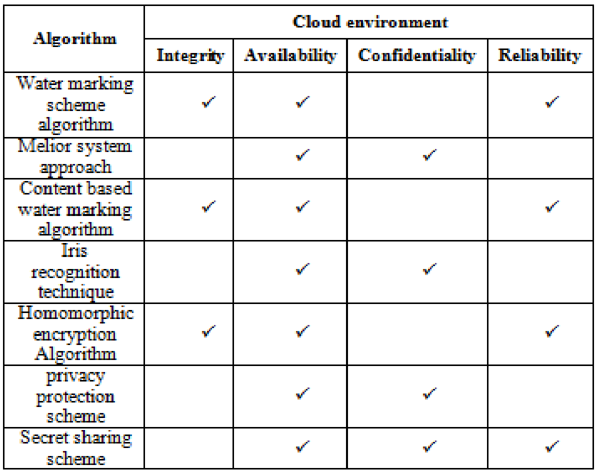
- As only security is taken as a major disadvantage in all the literatures, this paper[6] gives a platform for privacy protection. This is achieved by preventing the cloud provider usingoblivious transfer for knowing the usage of images by customer.

- Secret sharing scheme[7] presented in this paper gives security of medical images in cloud architecture. Here the medical images are split into many portions using this scheme and they are sent into different cloud. In this approach a multi cloud architecture is used for storing the images. This method increases the data confidentiality and availability resources in cloud.

IV. Comparison Between Algorithms

The comparison of different algorithms can be tabulated by explaining in terms of its security issues and its reliability in cloud architecture.

TABLE I. COMPARATIVE ANALYSIS W.R.T TO CLOUD ENVIRONMENT



Algorithm	Cloud environment			
	Integrity	Availability	Confidentiality	Reliability
Water marking scheme algorithm	✓	✓		✓
Melior system approach		✓	✓	
Content based water marking algorithm	✓	✓		✓
Iris recognition technique		✓	✓	
Homomorphic encryption Algorithm	✓	✓		✓
privacy protection scheme		✓	✓	
Secret sharing scheme		✓	✓	✓

The security of medical images and their speed in cloud environment of various literature reviews discussed above is tabulated as:

TABLE II . COMPARISON OF ALGORITHM IN TERMS OF ITS SECURITY AND SPEED

Literature	Speed	Security
Ref [1]	Medium	high
Ref [2]	High	high
Ref [3]	Medium	Low
Ref [4]	Low	Medium
Ref [5]	High	Medium
Ref [6]	Medium	High

Ref[7]	Medium	High

V. Limitations Of Algorithms Proposed

The joint watermarking algorithm and encryption algorithm[1] requires lot of processing power compared with standard algorithms. The reliability and security approach by this algorithm is less compared with others due to nature of data available. Security requirement for deployment of Melior covers only fraction of challenges faced by e-health care systems[2]. Content based algorithm[3] uses water marking algorithm which is not a robust one. The image features are secure against cipher text model only.

A better watermarking scheme is required for robustness. Iris recognition algorithm[4] uses iris recognition for security of medical images in cloud. This is tedious step of making matching technique with stored image and enrolled one for accessing the data. This can also be extended by applying hybrid biometrics mechanism to increase its performance. Homomorphic encryption algorithm [5] achieves greater speed. This scheme computes on encrypted data which does not require any decryption. Though encryption provides security, still this paper aims for only speed. Hence security aspects cannot be taken into consideration.

Concerning with Privacy of medical records stored in cloud, this paper [6] proposes two mechanism of preventing cloud provider to link the record for accessibility and provide Oblivious transfer mechanism to prevent cloud provider from knowing what data are accessed. This algorithm is provides much security over images in cloud but there is no idea of where the link do the cloud provider will make and wide approach in this area is required for implementing this algorithm. This paper [7] provides a cost efficient service and also provides security to medical images. The algorithm can be improved by using new storage systems in cloud and also security for shadow images.

VI. Conclusion

This paper thus presents a comparative study of all algorithms used till. With increasing demand of medical images in e-health care applications, secured transfer of medical images has to be taken into account seriously. Also a cost efficient service has to be implemented for secure transmission and storage of medical images in cloud. Each and every algorithm has certain amount of limitation in it. This has to overcome by new technologies meeting all needs by the user. Still research on various security mechanism can be implemented with best security standard and robustness.

References

[1] SiddhantBansal, Garima Mehta “Comparative analysis of Joint encryption and watermarking algorithms for security of biomedical images” 2017 IEEE.

[2] AntonisMichalas, NicolaePaladi, Christrian Gehrmann”Security aspects of e-health systems migration to the cloud” 2014 IEEE.

[3] ZhihuaXia,XinhuiWang,LiangaoZhang,ZhanQIo”A privacy preserving and copy deterrence Content-based Image Retrieval Scheme in Cloud Computing”2016 IEEE.

[4] Heba M sabari,NashaatElkhanmeesy,HeshamA.Hefny” Using Iris Recoognition to secure medical images on the cloud”2015 IEEE.

[5] AlhassanKhedr,Member IEEE and Glenn Gulak, Senior memberIEEE”SecureMEd: Secure Medical computation using GPU-Accelerated Homomorphic Encryption Scheme”2017 IEEE.

[6] Johann Vincent, WelPan ,”Privacy protection and security in ehealth Cloud platform for medical image sharing,2016 IEEE.

[7] Mbarek Marwan, Ali Kartit and Hassan Ouahmane”Secure cloud-based medical image storage using secret share scheme” 2016 IEEE.

[8] MbarekMarean, Ali Kartit, Hassan Ouahmane” Using Cloud solution for Medical image processing: Issues and Implementation efforts,2017 IEEE.

[9] MicheleLarobina ; LoredanaMurino;" Medical Image File Formats "JDigit Imaging. 2014 Apr; 27(2): 200– 206. Published online 2013 Decdoi: 10.1007/s10278-013-9657-9

[10] K. Toennies, Guide to medical image analysis. London:Springer,2012.. Chapter 2, Digital Image Acquisition,pages-21-82, DOI10.1007/978-14471-2751-2_2

[11] N. Nikolaidis and I. Pitas, “Digital image watermarking: an overview,” in Proc. Int. Conf. Multimedia Comput. and Syst., ICMCS99, vol. 1, pp.1-6, Florence, Italy, June 7–11, 1999

[12] J. Cox, Matt L. Miller, “ The first 50 years of electronic watermarking,” EURASIP Journal on Applied Signal Processing , Vol.2002, no.2, pp.126-132 , 2002

[13] Giakoumaki, S. Pavlopoulos, D. Koutsouris, “Secure watermarking on medical images,” Medical Biological Engineering & Computing, Vol. 44, pp.619-631, 2006.

[14] Wei Pan, GouenouCoatrieux, DalelBouslimi, and Nicolas Prigent.Secure public cloud platform for medical images sharing. Studies inhealth technology and informatics, 210:251–255, 2014.