Electronic Medical Reports Security in Cloud Storage Environment based on Visual Cryptography

Aparna Lanjekar
Pimpri Chinchwad College of Engineering Pune, India

Apurva K. Thakur
Pimpri Chinchwad College of Engineering Pune, India

Yaminee Koli
Pimpri Chinchwad College of Engineering Pune, India

Jayashree Katti
Pimpri Chinchwad College of Engineering Pune, India

ABSTRACT
Now a day's cloud computing is the changing way to store, compute and use the data and resources which are stored on the remote servers due its properties such as it provides on demand self-service, robustness, broad network access, measured resources and low cost. But data security is a major issue that prevents users from storing files on the cloud. Every day enormous amount of data is generated in multi-specialist hospitals. This article presents various techniques to protect electronic medical reports (EMR) stored on cloud. If doctors of various specialization want to go through the reports it will be easy for them if those are placed on the cloud. This will also help patient in not carrying the prescriptions or big size reports. This article addresses these issues by proposing Visual Cryptography Scheme (VCS) and multi secret sharing for securing the multiple EMR. In order to prevent issues like breaches and malware attacks on cloud, this innovative scheme helps in high level security to safeguard the files or reports that are stored on the cloud.

Keywords
Cloud Computing, Visual Cryptography, Multi Secret Sharing Scheme, Electronic Medical Reports (EMR).

1. INTRODUCTION
Medical image data is a central part of diagnostics in today's healthcare information systems. With the adoption of cloud computing approaches in the healthcare sector by most health institutions, medical image data are stored remotely in third party servers.

Privacy, safety and security needs to be guaranteed for such digital data by engaging encryption to ensure confidentiality and authentication methods to ensure authorship. Cloud is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer[3]. Cloud Computing provides us a means by which we can access the applications as utilities, over the internet. It allows us to create, configure, and customize the business applications online. Cloud computing, the environment that offers resources encapsulation on the Internet in the form of dynamic, scalable, and virtualized services, presents a variety of on demand services to the public such as the telemedicine services[3]. Over this environment, the user can enjoy a lot of benefits offered by this computing paradigm like transmission, storage, and further processing needs on the user data. In spite of the cloud computing advantages, it has a number of disadvantages such as the data security which considered a major problem that face the users of this technology since they outsource their data to distributed storage systems and not a local one. Therefore, when transferring user's data over the cloud environment, especially the medical data, this kind of data which contains crucial information about the patients, a high level of protection of the integrity and confidentiality of these data have to be guaranteed to overcome any attacking attempts that may face these transmitted data.

Visual cryptography is one of the techniques used to encrypt the images by dividing the original image into shares[2]. Visual cryptography (VC) is a secret-sharing scheme that uses the human visual system to perform the computations [7]. Visual Cryptography involves breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. The Visual cryptography provides the demonstration of encryption and decryption of images to the users. Due to the strong security and operation efficiency, the proposed secure cloud computing system should be extremely suitable for use in Health Information Exchange through cloud computing environment [6].

2. LITERATURE SURVEY

2.1 Cloud Based Medical Image Exchange-Security Challenges.
There are various mechanisms for medical image storing and sharing of medical images through cloud platform. The benefits of putting medical images in a cloud include:

a) **Data Portability:** With online patient health records, it is easier to access and share data between the patients and doctors and between the specialists.
b) **Increased and Flexible Storage Capacity:** With cloud-based EMR, doctors and other healthcare professionals do not have to administer/upgrade their own hardware. Additional data storage is available as needed.
c) **Data Migration:** The main benefit of cloud technology is that data need to be migrated only once. Then the data can be accessed and utilized with any PACS. It is necessary for an organization to work with a vendor

that can migrate data efficiently, since it is time and resource intensive criteria.

d) Patient-Centric Connected System: Consolidating and storing medical image information in single centralized repository in the cloud instead of multiple PACS in different sites means health care providers can quickly access and share images across various departments and organizations.

Confidentiality is the assurance that sensitive information is not disclosed. Received medical images have not been modified during the transmission [4]. The main threats in image storage and sharing in cloud are:-

- **Distributed Denial of Service attacks (DDoS):** This attack is a threat to the availability of cloud infrastructure and its resources.
- **Confidential Data Leakage:** Confidentiality of data cannot be maintained and protected easily because of lack of visibility, sharing of information and attacks of malicious insiders.
- **Access Control:** Cyber criminals are the main threat to security of contents in cloud.
- **Data ownership:** The embedding of the ownership seal in the images is achieved through means of watermarking and encryption techniques.
- **Zero tolerance:** Zero tolerant images are needed in which watermarking techniques should be performed carefully.

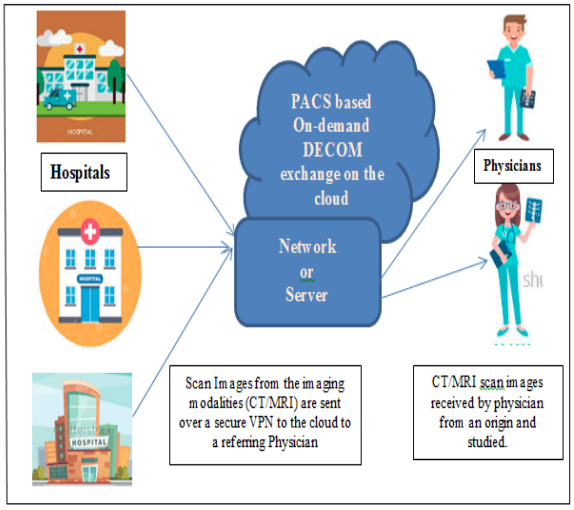

Fig. 1: Sharing medical image through cloud

2.2 Secure Medical Images Sharing over Cloud Computing environment.

While transferring user's data over the cloud environment, especially the data which contains crucial information, a high level of protection of integrity and confidentiality have to be guaranteed to overcome any attacking attempts that may face these transmitted data. Spatial watermarking technique provides the mean of trust management between data parties over the cloud computing environment. This method achieve the required goal through providing three levels of authentication, from data owner to the destinations, from the data owner to the cloud service provider and finally from the destination to data owner.

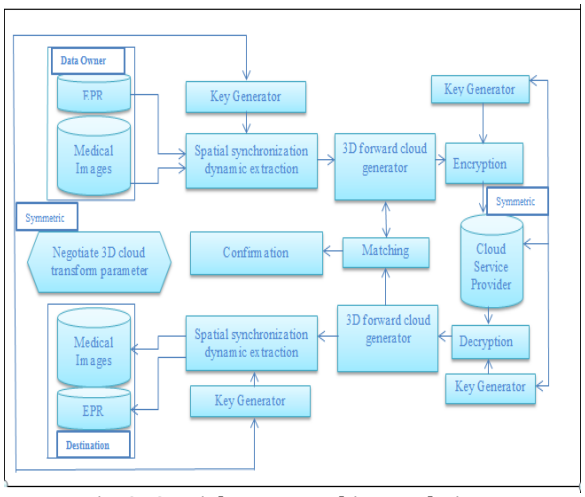

Fig. 2: Spatial Watermarking Technique

There are three main stages of this approach. The first stage dynamically embeds the EPR data into the original medical image. Then, the cloud model is applied to the medical image to extract the approximated version. Finally, the encryption process is done using a symmetric negotiated private key between the authorized parities of the data.

2.3 A Cryptographic Technique for Security of Medical Images in Health Information System.

A compromised health information system or unauthorized access to these data will violate the privacy of patients and wrong processing of a specific image for different patient will further affect the integrity of the medical institution. In addressing these issues of unauthorized access, effective security information system with a fully recoverable and reversible technique for authentication and security of medical images in heath information systems are provided [4].

The encryption process is symmetric and uses client's authentication system to grant access but uses patients' unique information in the encryption and watermarking of the medical images. With the proposed approach, disparate can easily access the medical images can communicate via the same services bus to access medical data such as x-ray image data etc. Any request made by an application residing in the same network infrastructure or external to it with regards to medical images will have services rendered to it via an abstraction level to that application. Data stored in the file servers, in databases and in the cloud, can only be accessed and decrypted successfully through transaction activities involving the security server and this prevent exposure of sensitive medical data when the file are being comprised or there have been backdoor access to storage servers in the cloud.

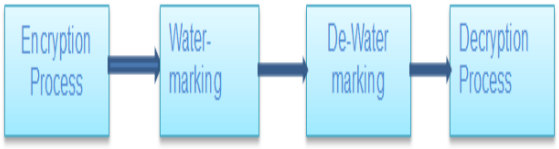

Fig. 3: Encryption Decryption Scheme using Watermarking

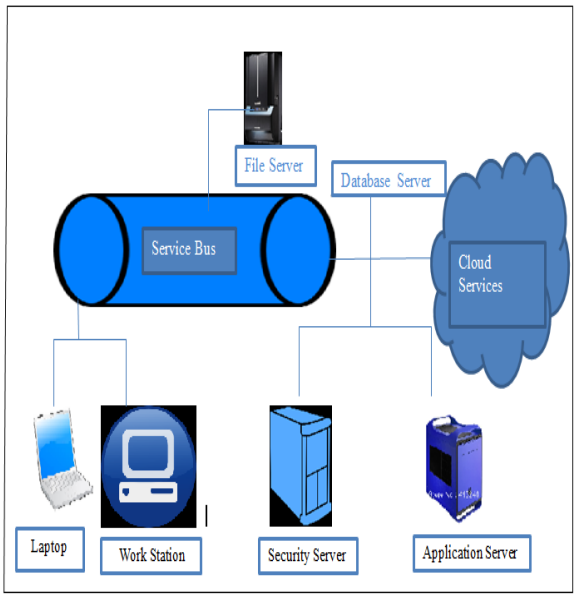

Fig. 4 Data Access through Cloud

- **Encryption Process**
  1. Import data from image & create an image graphics object by interpreting each element in matrix.
  2. Get the size of as [c,p].
  3. Get the Entropy and mean of the plain image.
  4. Compute the shared secret from the image.
  5. Engage Sk and extract the red(r), blue (b), green (g) component.
  6. Let r = Transpose of r, g = Transpose of g, b = Transpose of b.
  7. Reshape r into(r,c,p), b into(b,c,p), g into (g,c,p).
  8. Concatenate the arrays r,g,b into the same dimensions of 'r' or 'g' or 'b' of the original image
  9. Finally, encrypted image is generated.

The inverse of the algorithm will decrypt the encrypted image black into plain image.

$S_k = [(c \times p) + |(He \times 10^3| + |(x = 1/n * \sum_{i=1} x_i)|] \bmod p$

Where c,p = dimension of the image and H_e =Entropy value of the image and x is the arithmetic mean for all the pixels in the image. The technique engaged was very effective for all the images and there was no pixel expansion at the end of the all process. The total entropy and the mean of the plain images never changed for all the ciphered images and the plain images. The average total pixels values before encryption were the same as the average total pixel after encryption.

2.4 An Innovative Solution for Cloud Security through Quantitative Analysis of Various Visual Cryptography Schemes [1].

a) Visual cryptography scheme with sharing of one secret image.

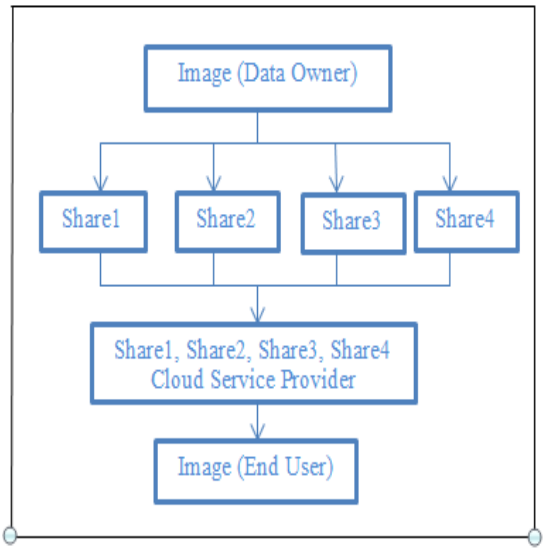

Fig. 5: Visual Cryptography with Sharing of One Image

b) Visual cryptography scheme with sharing of multiple secret images.

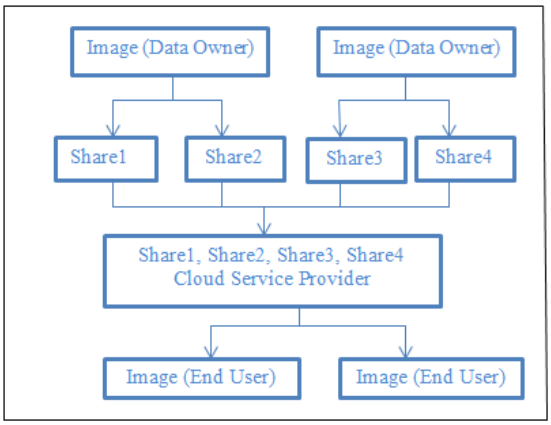

Fig. 6: Visual Cryptography with Sharing of Multiple Image

c) Extended Visual Cryptography Scheme (EVCS): It has meaningful transparencies [8]. The EVCS is a more secured scheme than traditional VCS as the shares cannot be easily guessed. But the disadvantage is bad visual quality of shares and the revealed secret images. Computation is also expensive. There is requirement of complementary images for revealing secret images.

d) Half toning Technique or Dithering Technique: This technique deals with the gray-scale image. There is Conversion of the gray-scale image into binary image.

e) Visual Cryptography scheme for Color images: This scheme uses CMYK color model. But there is pixel expansion.

3. PROPOSED SYSTEM

Medical image data is a central part of diagnostics in today's healthcare information systems. With the adoption of cloud computing approaches in the healthcare sector by most health institutions, medical image data are stored remotely in third party servers. Privacy, safety and security needs to be guaranteed for such digital data by engaging multi secret sharing to ensure confidentiality and authentication methods to ensure authorship.

3.1 Multi Secret Sharing

A secret sharing scheme starts with a secret and then derives from it certain shares (or shadows) which are distributed to users. The secret may be recovered only by certain predetermined groups which belong to the access structure. Secret sharing schemes have been independently introduced by Blakley and Shamir as a solution for safeguarding cryptographic keys [6]. A secret-sharing scheme is a method by which a dealer distributes shares to parties such that only authorized subsets of parties can reconstruct the secret.

Multi-secret sharing scheme is a generalization of secret sharing scheme and in the real-world application; multi-secret sharing schemes are very practical. A multi-secret sharing scheme is supposed to distribute many different secrets among the shareholders in one process [7]. The secret may be recovered only by certain predetermined groups which belong to the access structure. Hence original form of information arrived at destination side. The multi secret sharing is secure in most applications as it takes less space due to multiple secret can shared by only one share.

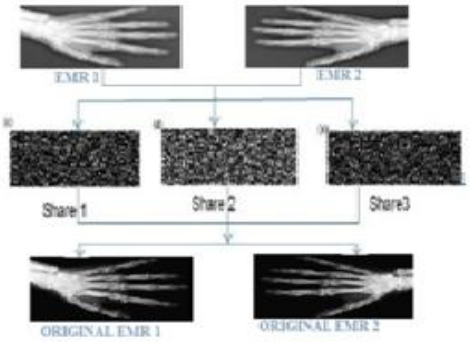

Fig. 7: Encryption and Decryption Process in Multi Secret Sharing

4. CONCLUSION

The proposed scheme improves the quality of patient care and also contributes to the management and moderation of health care costs. The visual cryptography technique is useful for encryption of EMR information to provide security while uploading on cloud. Cloud platform can form an ultimate platform that all healthcare organizations use and can serve as storage centre of medical records. Reliability and security are the main concerns about cloud computing. Using the proposed scheme, Doctors can appropriately access and securely share patients medical information electronically by improving the speed, quality, safety.

5. REFERENCES

[1] Cong Wang et al., "Ensuring data storage security in Cloud Computing", Quality of Service, 2009.

[2] Cheng TianFeiXin. "The identity authentication technology and application of gossip". Computer Security, 2005

[3] R. Kalaichelvi, Dr. L. Arockiam, "An Innovative Solution for Cloud Security through Quantitative Analysis of Various Visual Cryptography Schemes" International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 10, April 2014, ISSN: 2277-3754

[4] Cheng TianFeiXin. "The identity authentication technology and application of gossip". Computer Security, 2005

[5] Cao. N, C. Wang, M. Li, K. Ren, and W. Lou, (2011)"Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. Int. Conf. Comput. Commun. (INFOCOM), pp. 829–837.

[6] Aeloor, Deepak, and Amrita A. Manjrekar. "security Biometric Data with Visual Cryptography and Steganography." Security in Computing and Communications. Springer Berin Heidelberg,2013. 330-340

[7] M.H. Dehkordi, S. Mashhadi, "An efficient threshold verifiable multi-secret sharing", Computer Standards and Interfaces 30,2008,56

[8] ThottempudiKiran and K. Rajani Devi " A Review On Visual Cryptog-Raphy Schemes", Volume 3, No. 6, June 2012 ,Journal of Global Research in Computer Science, Review Article