Storage and Security Issues of Medical Images using Cloud Platform

Smita Khond, Bellamkonda Vijayakumar

Abstract: ***In this current era of technology people are interested more in online medical facilities for more faster and comfortable life. Because of huge demand, health care field is growing rapidly. The data in the form of x-rays, diagnosis reports, MRI images, videos is generated. Such form of data consumes large amount of storage space and processing power, therefore nowadays alternate solutions such as cloud storage are used to store such huge data. As the medical data in the form of images or videos is very important and confidential it is very crucial to concentrate on the issues like storage and security. The proposed work discuss about the image security techniques like watermarking using different types combined with data encryption techniques during transmission so as to ensure better security along with reduction in cost for storage with the use of cloud environment. In this study, we offer a deeper insight into the challenges hindering the adoption of this technology. Then we analyze and compare these findings of the cloud based medical image process implementation with security necessities.***

Index Term: Image security, Watermarking, Health care, transmission.

I. INTRODUCTION

In the supportive associations field, recuperating picture planning through cloud will show to be a standard blueprint. As a last resort masters are benefitted as it gives epic pictures through which end should be conceivable with exactness and better treatment can be given through chronicled data and current data which will be investigated. In like way, this new perspective licenses empowered exertion between helpful associations specialists planned at better places.

Removing the distinctive perfect states of passed on getting ready, moving towards cloud a risings faltered troubles.

In such way, security and affirmation are the standard obstructive fragments for the wide confirmation of healing picture getting ready over virtual stage. Starting at now, different executions are proposed pointing towards the advantages of this new perspective.

Common pictures hold tight in progress data structures, cloud or elective systems are of key criticalness. Affirmation and security must be protected for such pictures through encryption and underwriting structures. Mixed and watermarked pictures during this required to be reversible in like way the plain picture handled inside the encoding and watermarking structure will be absolutely redeemable. In this paper, we will if all else fails undertaking an absolutely redeemable mixed and watermarked picture process system for the insistence of helpful pictures in progress data structures. The methodology is used to endure observer to and secure the accommodating pictures. Our results showed up, obviously, to be terribly reasonable and strong for completely recoverable pictures.

In the power disclosures the symmetric encryption figuring is proposed in which the riddle key is passed on from the patient individual data what's more watermarking is created for underwriting.

II. CLOUD SYSTEM ARCHITECTURE

The proposed system consists of the cloud architecture as shown in the figure 1, that describe some problem and it consist of four parts

1) IaaS that is the Infrastructure as a service
2) The Proxy service
3) The Server meant for security
4) Entry

A. IaaS

The IaaS is answerable for data accumulating and search segments. In any case, ethically the cloud organization supplier should not be empowered access to the information changed or hold tight inside the cloud. In these conditions, it is definitely not a clear task to develop a cloud based help that has server viewpoint data amassing and looking frameworks.

This organization abundance could in like manner be used to guarantee the game plan of the organization, and conjointly to help the quality of the system in passing on data. This is as often as possible potential through weight bargain of the sales through the specific assistance suppliers. Without a doubt, this organization is fundamentally the same as the guideline cloud organization IaaS which is referenced, since it should got the chance to go about as an exchange for the most cloud organization. Everything considered, what makes it not exactly equivalent to the most cloud organization is that the risk of having only a bit of the information.

B. Proxy Service

As earlier referenced, even cloud organizations have openings in their solace. To figure around this disadvantage, one objectives is to utilize more than one cloud organization and create the system so that, if one among the cloud organizations become inaccessible, various structures can keep up the structure working.

One of the eventual outcomes of keeping up mediator organizations is the help costs are extended which can be lessened by fragmented replication of data even more well on the way to be required

C. Server meant for Security

Revised Manuscript Received on December 30, 2019.

Smita Khond, PhD Research Scholar, CSE Department, Pacific University Udaipur (PAHER), Rajasthan

Dr. Bellamkonda Vijayakumar, Educator and HOD CSE Department Vidya Jyothi Institute of Technology (VJIT) Hyderabad

The Server provided for security is important here the encryption and decryption can be done ,it helps to provide secret keys and other parameters required for encryption. It plays crucial role in authentication and taking decision whether to share the important arguments required for encryption-decryption process.It is only required when the user is connected with the cloud network.

D. Entry

Customarily, the cloud associations have each show and HTTPS interfaces, regardless to demand the authenticity and security of data, when it is moved between the section and thusly the cloud association has picked HTTPS appear. Thusly, the most basic movement of the zone part is to go about as an arbiter among DICOM and HTTPS. To do in that limit, the zone encapsulates the DICOM show messages inside HTTPS messages. During this framework the zone grants correspondence between the instrumentality inside the foundation and thusly the cloud

In this way the four components of the suggested architecture are helpful to securely store information in which is important for the healthcare industry.

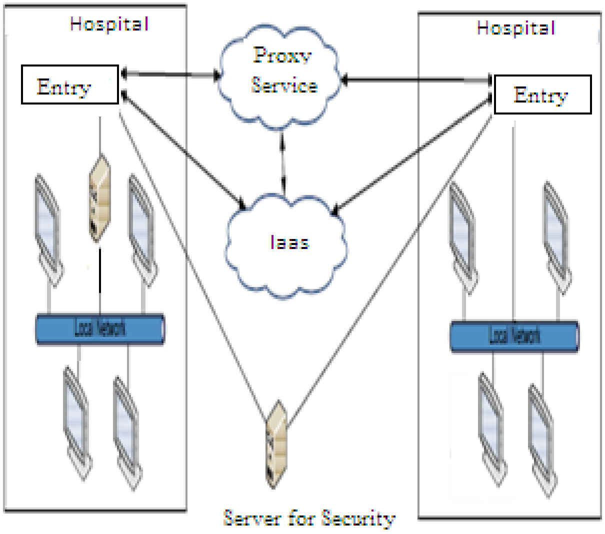


Figure 1 Proposed cloud Architecture

A. The Encryption process

1) Extract information from input and create an image graphics object by considering every pixel in a matrix.
2) Get the size of s as [r, c]
3) Get the Entropy of the input Image
4) Get the average of the input Image
5) Compute the shared secret from the image
6) Engage SecK for 7) to 17) using secret key value
7) Extract the red component as 'Red'
8) Extract the green component as 'Green'
9) Extract the blue component as 'Blue'
10) Let Red =Transpose of Red
11) Let Green =Transpose of Green
12) Let Blue =Transpose of Blue

13) Reshape Red into (Red, r, c)
14) Reshape g into (Green, r, and c)
15) Reshape b into (Blue, r, and c)
16) Concatenate the arrays Red, Green, Blue into the same dimension of 'Red' or 'Green' or 'Blue' of the original image.
17) Lastly the output will be converted into an image format to get the encrypted image.

The secret key is calculated as shown

$$Seck = [(r * c) + |(E * 10^3)|] \bmod p$$

Where r, c are number of rows and columns of the image and E is the entropy value of the image

B. The Decryption process

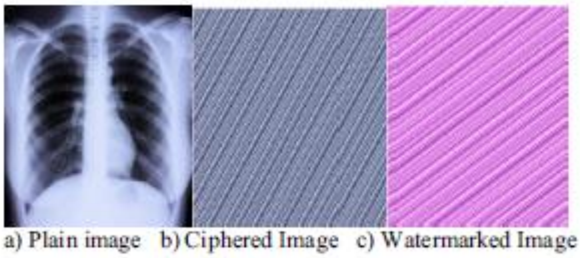
The Decryption process is reverse of encryption as it is symmetric algorithm and same secret key is used to decode the encoded data into normal image. The secret key is generated using some of the parameters from patient personal data like age, blood group etc.

C. The Watermarking process

Watermarking is a method by which we can ensure the authentication of the image. In this method the encrypted image which is divided into 3 components is watermarked and at receiving end the watermarked image is first separated from the watermark and then decrypted using decryption process. In the proposed work, reversible watermarking technique is used.

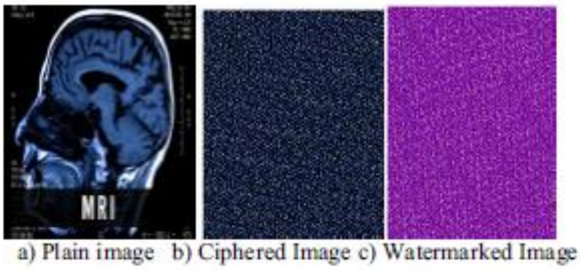
III. EXPERIMENTAL RESULTS

The Experiment were conducted for encryption and decryption using the mentioned technique and the secret key was used from the patient's data. This was implemented using MATLAB software for image processing. As shown in the figure 2 and figure 3 the results are obtained which can be further stored using the IaaS services offerd by cloud.



a) Plain image b) Ciphered Image c) Watermarked Image

Figure 2 X-ray Image of chest



a) Plain image b) Ciphered Image c) Watermarked Image

Figure 3 MRI scan of brain

Retrieval Number:B10041292S519/2019©BEIESP
DOI: 10.35940/ijitee.B1004.1292S519

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IV. CONCLUSION

This assessment found that eagerness for neighborhood server farms would increment operational costs, so to decrease operational worth supportive affiliations utilizes flowed figuring. The key sharing subject which we can utilize visual cryptography that can improve security and confirmation of remedial pictures and annals. This technique can even improve the helpful picture insurance. Moreover it spare the expense as information will be safely open in cloud reliant on pay as showed by utilize model. In future most by a wide margin of information will be open in virtual servers.

REFERENCES

1. Mbarek Marwan*, Ali Kartit and Hassan Ouahmane, “Using Cloud Solution for Medical Image Processing:
2. Issues and Implementation Efforts”, 2017 IEEE
3. Shruti Neralkar and Jayashree Katti, “An Efficient Technique of Parallel Share Generation and Reconstruction for Medical Images”, 2018 IEEE
4. LEI Li-hong ,BAI Feng-ming,HAN Xue-hui, “ New Image Encryption Algorithm Based on Logistic Map and Hyper-chaos”, 2013 International Conference on Computational and Information Sciences.
5. Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire,Jojo M. Eghan, Nii Narku Quaynor, “A Security Technique for Authentication and Security of Medical Images in Health Information Systems”, 2015 15th International Conference on Computational Science and Its Applications.
6. Mahadevan Gomathisankaran, Xiaohui Yuan, Patrick Kamongi, “Ensure Privacy and Security in the Process of Medical Image Analysis”, 2013 IEEE International Conference on Granular Computing (GrC).
7. Hiba Abdel-Nabi and AliAl-Haj, “Medical Imaging Security Using Partial Encryption and Histogram Shifting Watermarking”, 2017 8th International Conference on Information Technology (ICIT)
8. Stallings, W., Cryptography and Network Security—Principles and Practice. Englewood Cliffs, NJ: Prentice-Hall, 2016.
9. S.Manimurugan, Dr.K.Porkumaran,”,A New Fast and
10. Efficient Visual Cryptography Scheme for Medical Images
11. with Forgery Detection”, 978-1-4244-7926-9/2011 IEEE
12. Ali Al-Haj, Gheith Abandah, and Noor Hussein, “Crypto-based algorithms for secured medical image transmission”, IET Information Security, 9(6), pp. 365-373, Nov. 2015.
13. C. Cachin, I. Keidar, and A. Shraer, "Trusting the cloud," ACM SIGACT News, vol. 40, pp. 81-86, 2009.
14. Carlos Viana-Ferreira, Carlos Costa, "A cloud based architecture for medical imaging services",2013 IEEE ,15th International conference on e-Health and networking

AUTHORS PROFILE

Smita Khond is a research scholar under the guidance of Dr B.Vijayakumar from Pacific University (PAHER) Udaipur, Rajasthan. She is working as Associate Professor in Computer Science and Engineering (CSE) Department of Malla Reddy Engineering College for Women , Hyderabad

Dr B. Vijayakumar is Professor in Vidya Jyothi Institute of Technology (VJIT) ,Hyderabad and have more than 50 publications in the field of Image Processing and watermarking.