IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Efficient Healthcare System Over Encrypted Data in Cloud

SHEHNA C S
Department of Computer Science
St. Joseph's college (Autonomous)
Irinjalakuda, Thrissur, Kerala
shehnacs95@gmail.com

AMBILY JACOB
Department of Computer Science
St. Joseph's college (Autonomous)
Irinjalakuda, Thrissur, Kerala
ambilyamy@gmail.com

***Abstract*— Security of data is one of the major issues in today's world. The medical data is kept on the healthcare cloud for the efficient storage and accessing. As the popularity of healthcare clouding increases security issues related to this also increases. The most serious issue is data medical data lose. In this paper the main focus has been given to provide security for the medical data stored in the healthcare cloud system. The system is consisting of medical image encryption and report watermarking. All medical images are stored by cloud and it generate OTP and it send by telegram and transfer the information of details in encrypted form. we use Golomb's Data compression algorithm is used for encryption.**

***Keywords*— OTP,Image Encryption,Golomb's Rice coding,**

## I. INTRODUCTION

Medical data in healthcare refers to the medical records such as lab reports, x-rays, MRI reports etc. these data is huge and complex due to these factors it is difficult to store in traditional software and hardware facility. Hence we use a healthcare cloud system to place those data. Healthcare cloud is a cloud computing facility which is used as the storage medium for different medical data. It provides the benefits of both software and hardware through the provision of services over the Internet. As the popularity of healthcare cloud increases the attacks on the system is also increases the main issue is related to security of those data stored in the system. The security issues are legal issues, policy issues, data and privacy protection etc. because of these problems cloud has less security mechanism.

The aim of this paper is to provide hundred percentage of security to the medical data. For security of data use image

encryption and text watermarking. This technique provides a high security of the medical details and it hard to access to the attacker.the main advantage of the system is secure than the filekeeping system.OTP(one time password) and key can be generate for decryption of images.telegram is provide the security of images and OTP only can be generate by the telegram.

Consider a cloud-based totally healthcare data system that hosts outsourced private health records (PHRs) from various healthcare providers. The PHRs are encrypted with a purpose to comply with privacy policies . In order to facilitate facts use and sharing, it's far fantastically applicable to have a searchable encryption (SE) scheme which lets in the cloud service provider to go looking over encrypted PHRs on behalf of the legal users ( lab assistant or doctors) without learning information approximately the underlying plaintext[2].

The existing system deals with only a precaution from unauthorized access and ofcourse no deals In the present system there is no any method to make secure the data after a hacking if a hacking is take place the whole data will lost from the security system. The healthcare data is a huge and complex amount of medical reports it needs a large amount of memory space to locate them our existing system also doen't provide any technique to manage this problem.

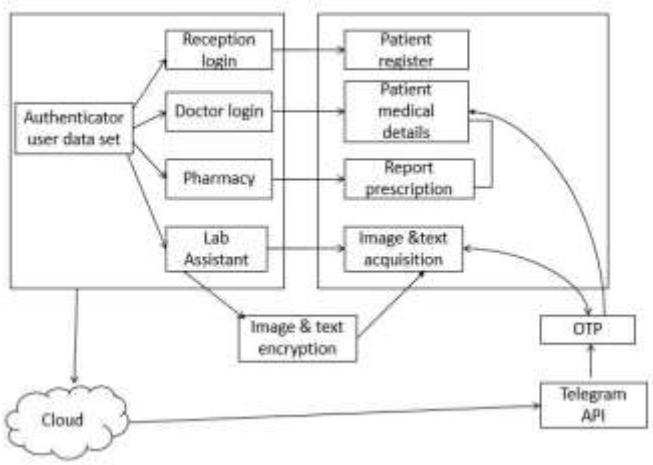
The system is mainly focused on providing protection for the Medical Data in healthcare cloud using Image Encryption with Text watermarking. All the medical details can be accessed using the private key and otp.it can be more secure to accessing unauthorized access. On the other hand the original medical data kept inside cloud with encrypted form. To confirm whether the user is legitimate or not using user profiling algorithm the legitimate user is entered only to the original data only after this verification. There is nothing to worry if any hacker gets access to the data file they get only the encrypted form of the original data and that data can be

available only private key and otp.otp and medical images can be send by telegram,images can be stored by cloud and it provide more secure than the existing system. we use a golomb's data compression algorithm to use th encryption.

## II. SYSTEM DESCRIPTION

The proposed system solves problems of existing system. The proposed system consists of Encryption, decryption technique can be used for healthcare system and some other data compression algorithms caused for image encrypted cloud computing. These project is These techniques in the proposed system provides 100% security for the medical data and there is no worry about a hacking if any happens the hacker gets a health record which looks like the encrypted form of the original one and it can be decrypted by only using key and one-time password. The proposed system implement for image encryption and text watermarking. And telegram application can be used for sending the OTP and the images of the report in the cloud is received to the telegram. For image encryption we use Golomb's data compression algorithm can be used. Hence the proposed system can make sure that the medical records are very secured.

Fig




Block diagram

## III. ANALYSIS OF IMAGE ENCRYPTION

### *A.RGB to YUV Conversion*

First of all, we convert the test images from RGB to YUV color space using (1)– (3) as follows:

Y=((66×R+129×G+25×B+128)/256)+16(1)
U=((−38×R−74×G+122×B+128)/256)+128(2)
V=((112×R−94×G−18×B+128)/256)+128.(3)

### *B. Optimized Golomb's–Rice Coding*

The next necessary step is to find an acceptable variable-length coding theme that's not solely in cryptography the variations (i.e., dX) however conjointly less erring. the target is to supply as fewer bits as attainable that may be sent to the transmitter for wireless transmission.
For this purpose, we tend to analyze the dX values of Y, U, and V elements. These changes (i.e., dY, dU, ANd dV) and their variety of incidence in a scrutiny image square measure [1]. analysis suggests that, in such case of distribution, the Golomb's code yields the optimum code length.

The Golomb's–Rice code could be a less complicated version of the Golomb's code, that is simpler to implement in hardware than the first version, however has similar compression efficiency. dX may be either positive or negative, and Golomb's–Rice code will work solely with positive integers, we tend to first map the field of positive dX to even integers and negative dX to odd integers victimization. we've conducted additional experiments to any customize the coding.

Our experiments show that the values of metallic element don't typically exceed the vary from 127 to −128 thanks to the absence of sharp changes between 2 consecutive pixels in scrutiny pictures, whereas the dU and dV values vary in a very narrower vary.
So, it may be assumed that the mapped positive integers (m−dX) can vary from zero to 255, which may be expressed in binary victimization 8bits [1].
Our planned optimized Golomb's–Rice cryptography is as follows.
1) initial we tend to initial I =2 eight = 256.
2) M could be a predefined number and an influence of two, M =2 k. m−dX is split by M as follows: letter of the alphabet = number m−dX M (8) r = m−dXmodM.
3) The quotient (q) is expressed in single in q 1 variety of bits. Then the rest (r) is concerned with the single code, and r is expressed in binary in k variety of bits. it's fascinating to limit the scale of the Golomb's–Rice code because it becomes terribly long for larger values. this can be done by employing a parameter named glimit. If q>= (glimit −log a pair of I −1), then the single code of glimit −log2I −1 is ready. This acts as AN escape code for the decoder and is followed by the binary illustration of m−dX in log2I bits.
4) the most length of Golomb's–Rice code (glimit) is chosen as thirty-two. The length of a Golomb's–Rice code may be calculated victimization
gr−len = letter of the alphabet 1 k,
nine that the foremost occurred worth of dU and dV is zero et al square measure terribly getting ready to zero [1].

## IV. SCOPE

Our proposed system is designed to provide security for the medical big data in the healthcare cloud using image encryption and text watermarking. This security system provides 100% security for the data before and after any attacks occur. This technique can be also used for different areas or field where a chance for hacking or unauthorized access. Here we chose Hospitality like this we can take any organization or institutuion and make secure with these techniques.

Telemedicine is one of the emerging fields for e-health research. In the telemedicine service, including medical data, images, and multimedia medical data are transmitted on the fly over insecure internet connections as they are required by the remote doctors. The healthcare cloud infrastructure would make it much easier to pull all different healthcare information together for a patient while the patient moves from one hospital to another; as a result, the patients' information can be managed and tracked easily. The healthcare cloud is a cloud computing infrastructure where all the healthcare service providers and stakeholders can communicate with each other through the cloud servers.

In this paper, a methodology is presented to secure patient's medical data in the healthcare cloud using the image encryption and text watermarking. So the medical data can be transferred one place to another place without unauthorized users. Unlike other methods, where the files are called when an attacker is detected as accessing the system, in our proposed methodology the files are retrieved from key and one-time password and it can be send via telegram it ensures better security. Additionally, it uses a double security technique by encrypting the original file he/she would need to figure out how to decode the original gallery. As a result, our methodology ensures that the users medical data are 100% secure and shortens the process. There is no need to worry if the user is an attacker, since by default it offers the data gallery directly to any user and keeps the original one hidden, which is only made available to a legitimate user after successful verification.

## V. CONCLUSION

We have already acquainted with distinctive strategies or strategies to make stable distinctive types of data. Here we focus on supplying safety for the information of patients in Hospitals. For this we use Encryption technique and one-time password method. It is extra stable than the file keeping device and defend unauthorized access. It can be used one of a kind fields for protecting their non-public details. Encrypted images are saved through to the cloud and OTP send thru telegram it provides extra secure than the existing system

This device may be greater in destiny with more advanced algorithms that provide extra protection to the medical details

## REFERENCES

[1] Tareq Hasan Khan, Student Member, IEEE, and Khan A. Wahid, Member, IEEE "Low Power and Low Complexity Compressor for Video Capsule Endoscopy"

[2] Hui Cui, Zhiguo Wan, Robert H. Deng, Guilin Wang, and Yingjiu Li "Efficient and Expressive Keyword Search Over Encrypted Data in Cloud"