International Journal of Engineering Computational Research and Technology
Journal home page: www.ijecrt.org

ISSN (Online): 2456-9852 Volume 4, Issue 2, December 2019

Enhanced Hybrid System for Medical Images and Patient Information in Cloud Computing

Bhavna Sharma[a, *], Deeksha Verma[a], Avni Sharma[b]

[a]*PG Scholars, Department of Computer Science and Engineering, Himachal Pradesh Technical University, Daruhi, District Hamirpur- 177 001 (H.P.), India.*

[b]*Department of Computer Science and Engineering, Himachal Pradesh Technical University, Daruhi, District Hamirpur- 177 001 (H.P.), India.*

[*]Corresponding author.

E-mail address: sharma.bhavna341@gmail.com (Bhavna Sharma).

ABSTRACT

Cloud computing is the very popular in now a days. It provides computing services via internet on demand and pay per use. It provides various computing resources online like storage, server and various applications. User can have access and storage of the data remotely. It has some benefits like-accessibility, availability, on demand services, scalability, low cost, convenience etc. Also it have various issues regarding the security of data like-unauthorized access by unauthorized user, unwanted changes or the unavailability of the data etc. These security risks reduced by using encryption algorithm and other data hiding techniques. That will make the system stronger. Existing system had used hybrid techniques for providing security in medical field so that information of patients can be safely exchanged. Which will be further improved in the proposed system that uses new techniques (Transform domain embedding technique) to have more strong and efficient system.

Keywords:
Cloud Computing
Hybrid system
Medical Images
Patient Information
Data Security
Telemedicine

1. Introduction

Cloud Computing refers to accessing, manipulating, configuring the resources remotely. It means delivering hosted services to the customers over internet. Customers can buy the computing resources like virtual machines, storage as a utility and many more things instead of building their own computing infrastructures.

1.1. Providing Security in Medical Field:

The telemedicine provide the exchange of the information of patients and other medical images from one location to other location. While transfer of these kinds of information cause the risk of the data. There are many application areas like- tele-consulting, tele-radiography, tele-diagnosis, tele-surgery etc.

Therefore, securing medical information from unauthorised accessing becomes an important issue. Information remains confidential and protected from the external changes while transferring to other person, otherwise it can cause the big problem to patients.

For providing more security the efficient cryptography algorithm is used which is Modified Jamal Encryption Algorithm. This is a symmetric algorithm which used the same key for encryption as well as decryption of the data. It has 120 bit key. And it uses 8 rounds or has 64 bit block size.

For hiding the necessary information of patients we uses steganography algorithm .it is hide within the medical images. For more enhancements in the

processing of images TDET (transform domain embedding technique). By using this technique, the robustness can be improved of the algorithm.

2. Related work

A system that combined the cryptography and steganography technique called hybrid system. So, a hybrid system has been proposed by Jamal N. Bani et al. Which provide secrecy of the data while transferring through the internet. And the encryption key can be exchange very safely [1].

Data hiding through cover image can also be possible using the steganography algorithm. Which hide the important data from external environment.
And for cryptography, it uses a very popular algorithm which is MJEA. It is a symmetric encryption algorithm. It has 120 bit key size. These two algorithms are used to secure the transformation of the information between sender and receiver and after that whole process performance is checked. Various simulation metrics are used to evaluate this like- histogram analysis and visual testing is also there. These metrics proves the efficiency and the robustness of the system.

Another hybrid system is proposed by Jamal N. Bani Salameh. It also provide security in medical field[2]. He also proposed two steps method:

In first step, the encryptions of the medical images are done by using the MJEA encryption algorithm.

And in second, all the necessary medical information of the patients are hide or embedded within the cover image i.e. medical image. They uses different metrics to prove the efficiency of proposed system i.e. Mean Square Error, Histogram analysis And Peak Signal to Noise Ratio.

Another system presented by SVN Srivalli et al. This system provides high security to files that are in the textual form [3]. This system depends upon two phases. This makes the system stronger.

First, phase contain the storing process in this process the particular text file is selected and then it is divided into two parts. There are two encryption algorithms for two subparts one is AES and other is the Blowfish algorithm. Then those are combined into single text file and stored into the cloud by uploading that file. Then after that encryption key is hide by through steganography technique
Second ,phase define the process of retrieving the key then decrypting the text file subparts .hence by using this process text files are more secured on cloud.

One another security model given by Moshira Ebrahim et al. It also provide protection to the data by using various data security techniques [4].

It consists of 3 steps:

1. A secure hash algorithm used to hash the data.
2. Then that hash code encryption is done using public key cryptography algorithm.
3. In the final step that encrypted data hide in any type of image using the steganography algorithm.

3. Proposed Study

This proposed system will enhance the existing system by using transform domain embedding technique**.**

3.1 Transform domain embedding technique:

This is best suited for image processing. Image is processed in accordance with frequency content.
It perform the manipulation on the transform coefficient by the M operator, unitary transformation of images and then it inversing that transformation. Here, images have the orthogonal transformation which is further divided into two parts phase and the magnitude of the image. Both these parts contain the frequency of images and the restoring of image in spatial domain. The transform domain embedding techniques provide enhanced frequency content like subtle information of image and various edges etc. It will provide the best and roust system [5].

4. Tools

- System will be implemented through C language.
- For image processing MATLAB programming language version R2013a will be used.
- System histogram analyst test also used to check that whether system is robust or not.

5. Conclusion

After this analysis, we acknowledge that cloud computing brings both benefits and risks. It provide many facilities like-online storage, on demand resources, pay as per you use etc. and also it has various security issues.

The existing system uses hybrid system which Uses various cryptography algorithm for encryption of keys and steganography techniques for hiding the data and to make exchange of the information more secure .So that it does not arises any negative effect and also it reduce the risk of transferring the information over internet. The system will make use of transform domain embedding technique to provide better system to user.

References

[1] Jamal N. Bani Salameh et al "Secure Exchange Technique for Secret Information and Encryption Key Using Hybrid System" International Journal on Communications Antenna and Propagation · February 2019.

[2] Jamal N. Bani Salameh, "A New Approach for Securing Medical Images and Patient's Information by Using A hybrid System" IJCSNS, VOL.19 No.4, April 2019.

[3] S. V. N. Srivalli et al "Development of a Cloud-based Secure Text File Application using Hybrid Cryptography and Steganography" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019.

[4] Moshira A. Ebrahim et al "Hybrid Model for Cloud Data Security Using Steganography" December 2017.

[5] Sudhanshi Sharma1, Umesh Kumar, "Review of Transform Domain Techniques for Image Steganography", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.