ADVANCED ENCRYPTION TECHNIQUE TO ENHANCE MEDICAL IMAGE SECURITY IN INTERNET OF MEDICAL THINGS

E. Kokul*¹, I. Mohammed Jaffir*², E.R. Ramesh*³

¹,²Dr. MGR Educational And Research Institute, Chennai-600095, Tamilnadu, India.
³Center Of Excellence In Digital Forensics, Chennai-600096, Tamilnadu, India.

ABSTRACT

In the past several years we've seen healthcare data breaches grow all over the world in both size and frequency impacting over 70 million people. Healthcare data breaches often expose highly sensitive information such as names, addresses, health insurance details, medical histories, And their scan reports. This paper particularly focuses on ensuring security to the medical image of the patients. Many ways are there to protect an image such as assigning a password to the folder, uploading it to a mail account or cloud but these techniques are not possible for a hospital to proceed with it. Hence we are going to encrypt the image. Again there are lots of ways to encrypt an image, but In this paper, we are going to see two types of encryption, one already exists method i.e secret sharing scheme and the other one is the proposed algorithm that we are going to use in this paper. The name of the algorithm is the Adaptive Neuro-Fuzzy Inference algorithm. Both algorithms have their own uniqueness, so we are going to compare the results of these two algorithm by using some validation parameters. It is very important to protect the e-health data because it contains sensitive information which may be potentially embarrassing. so this paper will definitely provide a solution to safeguard e-health data.

I. INTRODUCTION

In the authentication based on Advanced Encryption Technique schemes encrypting a single secret image, one way to detect tampering by an adversary is to divide the secret image into two disjoint areas: one for a message and the other for the detection advanced Encryption Technique schemes encrypting multiple images allow the authentication which can take the above two areas identical this authentication, equipped with the idea behind ANFIS method(adaptive neuro-fuzzy inference system), ensures that an adversary cannot tamper with the latter image without tampering with the former, which makes its security analysis simpler and more practical.

II. RELATED WORK

IOMT was very beneficial to hospitals and health groups. However, technology development is a concern about the organization’s security and privacy requirements with this innovation-IOMT’s concerns about normal security and privacy threats. The medical system involves risks in terms of confidentiality, integrity, and data and information availability. Security issues interrupt availability and relevance affect validity and confidentiality. In addition, medical data is used for fraud or identity theft and can discover medical recipes. Therefore, hackers can order drugs online. Hackers may also participate in threats and threats that also do not want to disclose a particular failure. The confidentiality, integrity, and availability of fitness trackers are also excellent. Another security output is access control and permission. Training for access control by the IOMT network is essential. It is important to determine if the user has been recognized and verified. This has the right to access the required resources. Access control requires communication between software entities to request and grant access. Nevertheless, effective access control of medical supplies on the Internet is a challenge. Identity management and authentication are other security and privacy challenges for IoMT. Identity management identifies unique objects and authenticates them to validate identity relationships between the parties. Authentication using the IoT is very important because, without it, confidentiality, integrity, and availability can be compromised. If an attacker can authenticate as a legitimate entity, the attacker has access to all data, jeopardizing confidentiality, integrity, and availability [1]. User identification and authentication with IoMT is an important topic. Password and user name pairs are the usual form of identification and authentication of people involved in an electronic system. Other methods include biometrics, shared keys, and digital certificates. High heterogeneity and large IoMT systems increase the security issues to the Internet today. Non-uniformity has a significant impact on network and protocol security services applied to IoMT [3].
Security solutions must support a variety of hardware specifications and provide IoT system approvals and certifications. Other security issues include communication and physical device restrictions. IoT devices are built into small-area, low-power processors, so the Internet Protocol should be applied to even the smallest devices. Limitations on IoMT devices limit the ability to process information at incredible speeds [19]. That is, it has limited memory, CPU, and power budget. A high degree of security is required to achieve the competing goals of minimal resource consumption and robust performance. Power and size constraints affect the integrity and confidentiality concerns of IoMT systems. Security analysis can be used to significantly reduce the issue of vulnerabilities on Internet of Medical Things applications. Security analysis includes collecting, correlating, and assessing data from a variety of sources that may help IoMT security vendors identify and eliminate the potential issue. In addition to monitoring the IoMT gateway, a multidimensional security analysis is required. By comparing multiple data, you can detect suspicious and malicious anomalies.

III. EXISTING SYSTEM

In encryption, secret sharing refers to the way secrets are distributed between groups of participants, with each participant assigning a secret share. Mysteries can only be rebuilt by combining parts. Individual stocks are useless on their own. The secret will only be opened if certain conditions are met. Everyone Multiple shares are given by n participants, and groups of shares above t (threshold) can open secrets, but groups of shares less than t cannot. The secure secret sharing scheme distributes shares so that anyone under t can share them. Shares don't have as much secret information as people with a share of 0. SS schemes that encrypt multiple secrets can easily be achieved with a collection of multiple SS schemes, each encrypting each secret. Therefore, in this task, we will consider an AET scheme that encrypts multiple secrets. This scheme allows each participant to receive a single visual share and, for each visual secret, reconstruct the secret in any qualified combination of participants. This scheme has been proposed to reduce the risk of infection at the stage of infection. However, it does not completely solve this problem.

IV. PROPOSED SYSTEM

The proposed system introduces a new scheme or algorithm called ADAPTIVE NEURO FUZZY INFERENCE SYSTEM (ANFIS). This is a combination of artificial neural networks and fuzzy logic systems. It is based on Takagi Kanno's fuzzy reasoning system. This technique was discovered in the early 1990s. Advanced encryption technology uses simple algorithms to encrypt visual information rather than the complex algorithms used in traditional encryption. To work around this issue, this paper presents an improved ANFIS scheme that helps avoid transmission risk issues. It has both neural networks and fuzzy logic principles, so it is possible to capture the benefits of both in a single model. The inference system conforms to a set of fuzzy IF-THEN rules that can be learned to approximate nonlinear functions. Therefore, Adaptive Neuro-Fuzzy Inference System (ANFIS) is considered a universal estimator. For more efficient and optimal use of ANFIS, you can use the best parameters obtained by the genetic algorithm. Used in intelligent situational awareness energy management systems. The advantages of ANFIS are fast convergence during training, high tolerance for uncertainty, and the high ability for interpolation, extrapolation, and generalization. Many image steganography techniques have been proposed in the past to hide confidential data so that the Stego image looks indistinguishable from the cover image.

V. METHODOLOGY

In this, we are going to take a medical image or any type of scan image. The format of the image should be in jpeg, png, and gif. First, we have to encrypt the image by using the algorithm which has been used in the existing method i.e., secret sharing scheme. We have to mention the key-value and also mention how many shares we want to split the image. By doing this the image will be broken into shares of what we mentioned. Then we have to decrypt the image by using the same algorithm that we have used in the existing method. by doing encryption the image quality might be reduced. To measure this the quality parameters have been used to check the quality of the image. Now we have to do the same step for the proposed method also. Here the encryption and decryption are done by using an algorithm. After finishing this we have to compare the results of the two images.
VI. RESULT ANALYSIS

Performance analysis for this project is done using two image quality factor metrics, PSNR and MSE. The PSNR calculates the peak signal-to-noise ratio between two images. This ratio is used as a quality criterion between the original image and the compressed image. The higher the PSNR value, the higher the quality of the compressed or reconstructed image. Compare image compression quality using root-mean-squared error (MSE) and peak signal-to-noise ratio (PSNR). MSE calculates the cumulative squared error between the compressed image and the original image, and PSNR represents the measured peak error. The lower the MSE value, the image will stay as original as it will be. The output is also displayed in chart format to show the comparison between the two schemas.

[Block diagram of the image compression process]

[Medical image]

[Shares of medical image]
Comparision of both algorithms result:

<table>
<thead>
<tr>
<th>ALGORITHM NAME</th>
<th>PSNR VALUE (PEAK TO SIGNAL NOISE RATIO)</th>
<th>MSE VALUE (MEAN SQUARE ERROR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECERT SHARING SCHEME</td>
<td>34.1563</td>
<td>24.9851</td>
</tr>
<tr>
<td>ADAPTIVE NEURO FUZZY INFERENCE SCHEME</td>
<td>70.1970</td>
<td>0.0149</td>
</tr>
</tbody>
</table>

Graphical representation of the results

VII. CONCLUSION

Advanced Encryption Technique is a technique that encrypts visual information's using the simple algorithm in place of complex ones that used in traditional cryptography. So, this paper presents an enhanced ANFIS scheme that helps in avoiding the transmission risk problem.

VIII. REFERENCE


