IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Securing data in Iot using Steganography and Cryptography

Yashaswini A N[1], Dr Aswatha A R[2]

Dayananda Sagar College of Engineering, Student,Bangalore,India

Dayananda Sagar College of Engineering, Head of the department, Bangalore, India

***Abstract***— The Internet of Things (IoT) is a internetworking of physical elements (or "things") that are embedded with source code, sensing devices, and certain other approaches to allow devices as well as systems to connect and exchange information via the internet. Cryptography and Steganography techniques, on the other hand, can be used to protect this information. These methods are critical when it comes to user authentication and data security. In this article, the data from various medical sources and medical sensors is encrypted using a cryptography approach called dynamic sbox based rijndael cipher.Next a rom based LSB steganography technique that embeds encrypted data into a low-complexity image is used to add additional security. Various parameters are calculated based on the acquired results. Finally, the image's concealed information is extracted and decrypted.

***Keywords***— *Internetworking, Cryptography, Steganography, authentication, data security,*

## I. Introduction

Internet of things is a domain of computer gadgets that are linked with physical devices and software items which facilitate data exchange over a system without involving interaction between human and human or human and computer . To afford secure data transmission is the goal of IT infrastructure [1]. The assimilation of radio frequency identification (RFID) tags, sensors and actuators and technologies of communication is foundation of the Internet of Things. The Iot demonstrates the way how various technologies and the physical items are connected to the internet to allow them to collaborate and interact with one another in order to achieve common goals. The iot contains of teeny elements that are combined together to provide synergetic calculating scenarios. Energy constraint, connection, and computational capability are some of the limits in IoT [2].

Despite the fact that IoT gadgets have made living simpler, greater attention is required for their security. The creator's current goal is to enhance the capacity of these devices while paying little regard to their security. The data that is sent via an IoT network is vulnerable to attack. To preserve the user's privacy, the data in the network must be protected. If there is no security of data then the data rift takes place and the personnel information can be easily enraged from the system. Identification and authentication are some important notions of iot. These concepts are linked with each other which acts as functions of cryptography and seem to be important to ensure that whether data has been transmitted to correct person or not and also the source is trusted or not. If authentication is not provided a hacker can easily hack the system and steal the information.

When communication between two devices takes place there is transfer of data between those devices in which the data can be sensitive and also personnel. Consequently when such information is transferred from one device to another such type of data should be encrypted which alters the original data and aids in protection of data from invaders. Encryption is carried using cryptographic algorithms in which it is the procedure of converting plain text into unintelligible text. privacy, authenticity, non recognition are the primary objectives of cryptography. Dynamic sbox based rijndael cipher is the cryptographic method used in this proposed work. In contrast to the cryptographic mechanism the suggested work employs another way which is known as Steganography which adds additional security to the network. The goal of Steganalysis is not just to keep information hidden from others, but also to eliminate suspicion of having hidden information. The suggested work employs a technique known as rom-based Steganography.

## II. RELATED WORK

This article gives an overview of present studies on the IoT network's security of healthcare data.

Daniels et al. [3] introduced safety microvisor (SV) software, which used program virtualization and assembler layer program verification to provide memory separation and adjustable security. Banerjee et al. [4] proposed an energy-efficient datagram transport layer security (eeDTLS) variant of datagram transport layer security (DTLS) that has the same security level but requires less energy energy-efficient datagram transport layer security (eeDTLS) variant of datagram transport layer security (DTLS) that has the same security degree but requires less power.

Manogaran et al. [5] presented a mechanism based on medical sensor devices placed within the human body. These sensor devices capture abnormally high respiration rates, pulse rate, glucose level, blood pressure, and skin temperature and generate an alarm message with important health information that is delivered to a doctor via wireless network. These technologies used manages to protect enormous volume of industry's information.

The necessity to safeguard data that is transferred on second by second basis via the IoT network is urgent. The following are some of the ongoing data security studies.

Sun et al. [6] created Cloud Eyes, a cloud-based antivirus malware solution that provides reliable and efficient security services to IoT devices. Ukil et al. [2] presented methodologies and solutions for defending against cyber-attacks, as well as a technology for interfering embedded gadgets, which are both based on the concept of safety computing, which is a critical requirement of embedded security. Chervyakov et al. [7] proposed a information memory strategy that deals with a variety of objective preferences, workloads, and storage qualities in order to achieve the lowest chance of repition of data, data corruption, and encoding and decoding speed. This study found that if the repeated residue numbering scheme (RRNS) variables are correctly chosen, it not only increases the safety and dependability of the system, but it also increases the security with which encrypted data is processed. Raza et al. [8] proposed Lithe, a lightweight safety CoAP for the IoT that aided in the evolution of a new DTLS compression header approach that uses 6LoWPAN to reduce energy consumption. The DTLS header compression approach, on the other hand, does not affect security. The object security architecture (OSCAR) suggested by Vucini c et al. [9] provides security in the IoT. OSCAR is concerned with the security of the application payload, which is based on the concept of security of objects . The lightweight break-glass access control (LiBAC) system was invented by Yang et al. [10], and the proposed work uses two methods to encrypt medical files: There are two types of access: attribute-based access and break-glass access. In most cases, a medical professional can only access data by decrypting it if the attribute set matches the medical file's access policy. In an emergency, a break-glass access method is used to bypass the medical file's access control, allowing emergency medical care or rescue personnel to quickly access the data. The security and privacy of data exchanged across network of iot are extremely important to the medical and healthcare industries. Bairagi et al. [11] introduced three steganographic approaches for masking data in order to provide secure communication across the IoT network. By employing minimum noise in the least significant bit (LSB) and the sign of the content,content is buried in the lower image's layer. This method improved imperceptibility and ability when compared to the actual function.Huang et al. [12] suggested a steganography method that leverages the vector quantization (VQ) modification to integrate hidden content into an LSB carrier image. In level one, the pixels of a 4 *4 VQ-transformed picture block are divided into two groups: The two groups are the LSB group and the private data group. VQ indexes are stored in the LSB group at level two, whereas private data is maintained in the private group.

## III. PROPOSED METHODOLOGY

This paper proposes a cryptographic method called dynamic sbox based rijndael cipher to protect sensitive data obtained from various medical sources such as MRI images and also the data which came from ECG sensor .The image which is encrypted using dynamic sbox based rijndael cipher is hidden inside a carrier image using a Steganography technique called random ordered least significant byte Steganography and the obtained image is then sent to the iot cloud which is created through a developer dropbox account. Next the data is acquired from the cloud and the inverse Steganography is performed and the decryption is done and the original data is obtained as shown in Figure 1.

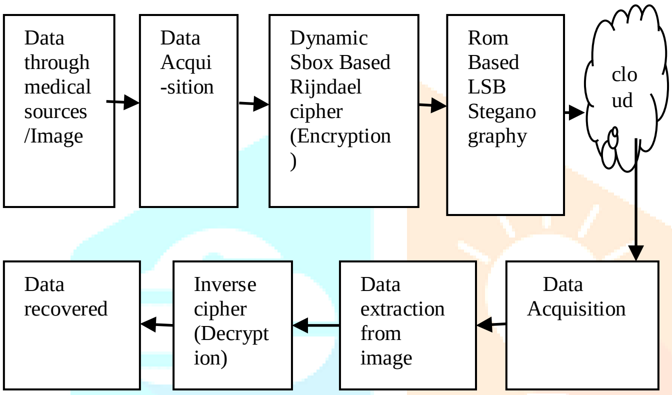
Data through medical sources /Image
Data Acqui -sition
Dynamic Sbox Based Rijndael cipher (Encryption )
Rom Based LSB Stegano graphy
clo ud
Data Acquisition
Data extraction from image
Inverse cipher (Decrypt ion)
Data recovered

Figure1:Block diagram of the proposed methodology

### a)Dynamic sbox based rijndael cipher

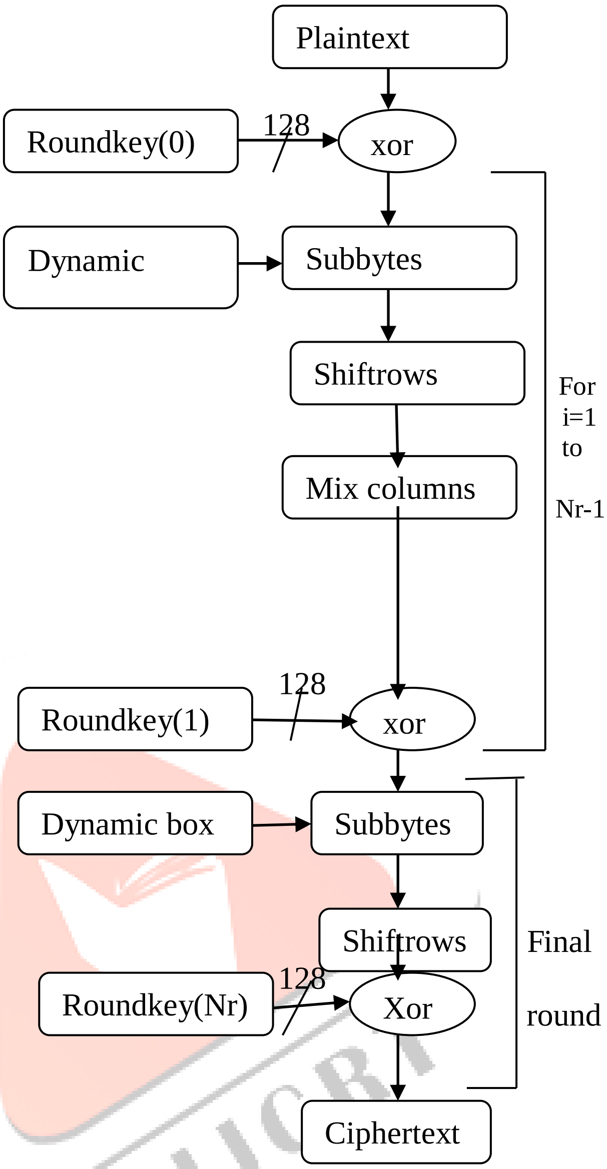

Figure 2:Flow diagram of dynamic sbox based rijndael cipher

The flow diagram of dynamic sbox based rijndael cipher is shown in Figure2. It is also known as advance encryption standard .

It's a block cipher that uses the following parameters:

- Size of block: 128 bits (also 192 or 256 bits)
- Length of key: 128, 192 or 256 bits
- Number of rounds: 10, 12, 14
- Key scheduling: 44, 52,or 60 sub keys with length=32 bits

Every round of this cipher is uniform and parallel composition except the last one

- Subbytes(substituting byte-by-byte using an S-box). A non-linear S-box is used to transform bytes.

$$S'_{(r,c)} \longleftarrow \text{S-box}(S_{(r,c)}) \quad (1)$$

$$S_{(r,,c)}=\text{binary}(\text{S-box}(r,c)) \quad (2)$$

Shiftrows are a type of shiftrow (it is a permutation which shift the last three rows in the state cyclically). Bytes are shifted left in a circular pattern.

- Mixcolumns (Substitution using Galois fields, GF)

b) Rom based LSB Steganography

After the data which came from different medical sources is encrypted using dynamic sbox based rijndael cipher this image/data is hidden using Rom based least significant byte Steganography in which the data is hidden in the carrier image randomly at random pixels which adds additional security so that intruder cannot even predict something is hidden and could not decrypt the original information.

## IV. RESULTS AND DISCUSSION

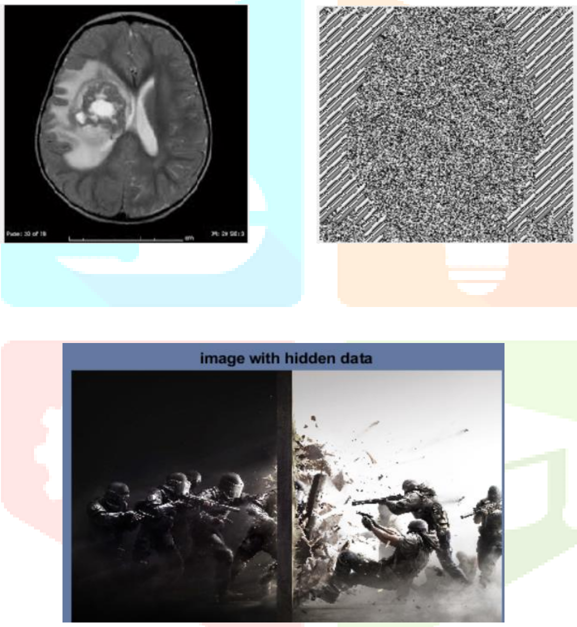

Figure3: input MRI image , encrypted image, Steganography image(image fused)

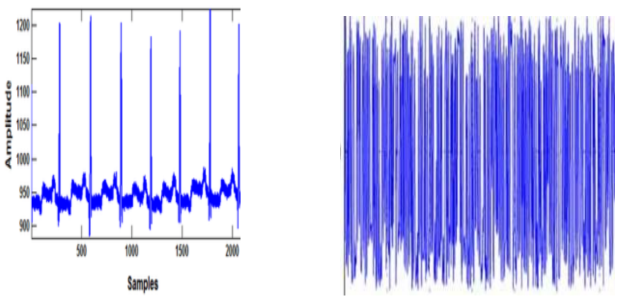

Figure4:Input ECG image, encrypted image,Steganography image(fused image)

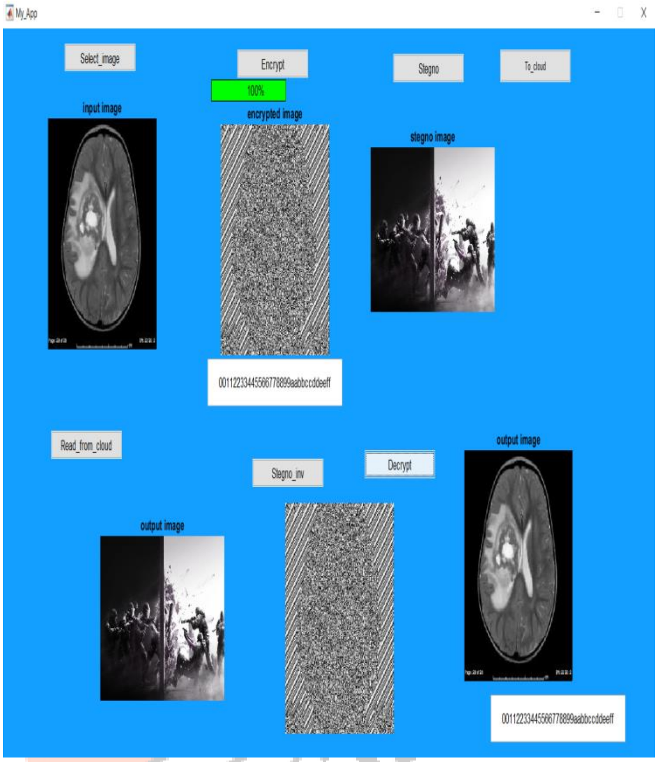

Figure5 : MRI data encrypted and decrypted

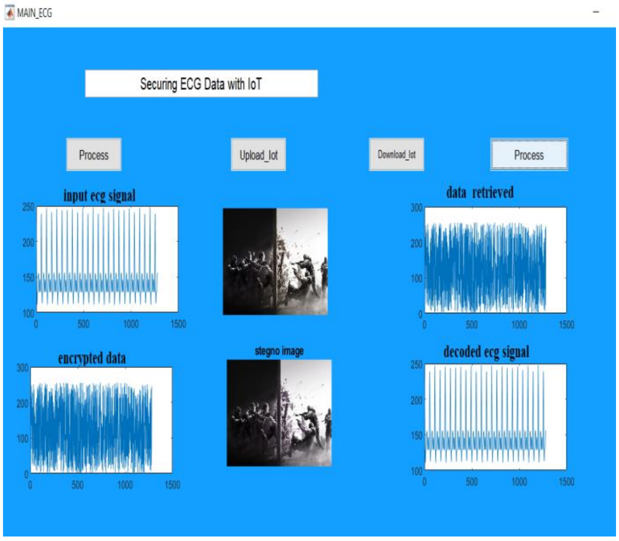

Figure 6: ECG data encrypted and decrypted

Parameter evaluation

1) PSNR:It calculates invisibility of the image.

$$\text{PSNR}=10\log_{10}\frac{255*255}{MSE} \qquad (3)$$

2) Embedding Efficiency: It is the number of bits stored in an image block which gives effectiveness of the system.

$$E_{n=}\frac{k+1}{k}n \qquad (4)$$

The overall number of secret bits in the embedding approach is n, where k is bit of the cover block and n is total number of hidden bits.

3) Mean square error:It is defined as the quantity of distortion of an image.

$$\text{MSE}=\frac{1}{N}\sum_{X,Y}^{n}(X-Y)^2 \qquad \mathbf{(5)}$$

4) Time complexity: It is the time it takes to encrypt and decrypt a message.

**5)** Carrier capacity*:* It is the system's capacity to conceal the hidden data.

$$\text{Carrier capacity}=\frac{\text{Total number of secret bits}}{\text{Number of bits in cover block}}$$

| Sl No. | Parameters | Values |
|---|---|---|
| 1 | PSNR | 72.314 |
| 2 | MSE | 0.1150 |
| 3 | Time complexity | 0.38807 |
| 4 | Carrier capacity | 22 |
| 5 | Embedding efficiency | 85 |

Table 1 : Various parameters calculated

In the proposed work two medical images one is MRI image and the other is the ECG signal which is obtained from the ECG sensor these both images are encrypted using dynamic sbox based rijndael cipher as shown in figure 3 and figure 4 and then the encrypted image is hidden inside a carrier image using Rom based LSB Steganography this encrypted data is sent to online iot cloud platform that is to the drop box account created .The data is retrieved from the cloud and inverse Steganography is performed and the data which is hidden is obtained by performing decryption as shown in figure 5 and figure 6.Various parameters MSE, PSNR , Time complexity ,Carrier capacity, embedding efficiency is calculated and are shown in Table 1

## V .CONCLUSION

The suggested technique gives a higher level of security to the information to which is transferred through a iot network. With the novel dynamic sbox based rijndael cipher cryptography the protocol provided better security. High embedding efficiency is obtained using Rom based least significant byte steganography through which the data is concealed in a deep layer of an image. Parameters are measured with factors such as embedding efficiency, time complexity, MSE, channel capacity, PSNR. Finally using matlab simulator the proposed work is implemented and 85 percent high embedding efficiency is obtained.

## REFERENCES

[1] R. H. Weber, "Internet of Things—New security and privacy challenges," Comput. Law Security Rev., vol. 26, no. 1, pp. 23–30, 2010.

[2] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for Internet of Things," in Proc. 2nd Nat. Conf. Emerg. Trends Appl. Compust. Sci. (NCETACS), Mar. 2011, pp. 1–6.

[3] W. Daniels et al., "SμV-the security microvisor: A virtualisation-based security middleware for the Internet of Things," in Proc. ACM 18th ACM/IFIP/USENIX Middleware Conf. Ind. Track, Dec. 2017, pp. 36–42.

[4] U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan, "eeDTLS: Energy-efficient datagram transport layer security for the Internet of Things," in Proc. GLOBECOM IEEE Glob. Commun. Conf., Dec. 2017, pp. 1–6.

[5] G. Manogaran, C. Thota, D. Lopez, and R. Sundarasekar, "Big data security intelligence for healthcare industry 4.0," in Cybersecurity for Industry 4.0. Cham, Switzerland: Springer, 2017, pp. 103–126.

[6] H. Sun, X. Wang, R. Buyya, and J. Su, "CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained Internet of Things (IoT) devices," Softw. Pract. Exp., vol. 47, no. 3, pp. 421–441, 2017.

[7] N. Chervyakov et al., "AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to

ensure security," Future Gener. Comput. Syst., vol. 92, pp. 1080–1092, Mar. 2019.

[8] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things," IEEE Sensors J., vol. 1, no. 10, pp. 3711–3720, Oct. 2013.

[9] M. Vucini ˇ c´ et al., "OSCAR: Object security architecture for the Internet of Things," Ad Hoc Netw., vol. 32, pp. 3–16, Sep. 2015.

[10] Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare Internet-of-Things," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3610–3617, Aug. 2017.

[11] A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," Inf. Security J. Glob. Perspective, vol. 25, nos. 4–6, pp. 197–212, 2016.

[12] C.-T. Huang, M.-Y. Tsai, L.-C. Lin, W.-J. Wang, and S.-J. Wang, "VQ-based data hiding in IoT networks using two-level encoding with adaptive pixel replacements," J. Supercomput., vol. 74, no. 9, pp. 4295–4314, 2018.