International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 03 | Mar -2020 ISSN: 2582-3930

Secure medical data transmission for IOT using Honey Encryption algorithm

J. Sophia Jone[1], Pavanya.J.Kumar[2],Anchana.T.S[3]

[1]Assistant Professor/ECE,Bethlehem Institute of Engineering,Karungal)
[2]ECE,Bethlehem Institute of Engineering,Karungal
[3]ECE,Bethlehem Institute of Engineering,Karungal

Abstract -The major challenges in the internet linked world are to provide security. Now a day the number of hackers has increased to hack the secret and important information .So there is the need to tighten up the security and integrity for transmitting the data. The proposed encryption scheme is built using a combination of HE and Modified RSA algorithm .The initial step is done by encrypting the secret medical data and then the data is hidden back to cover image..

Key Words:*security, hackers, encryption,RSAalgorithm, HE algorithm*

1. INTRODUCTION

IoT creates an integrated communication environment of interconnected devices and platforms by engaging both virtual and physical world together With the advent of remote digital healthcare based IoT systems, the transmission of medical data becomes a daily routine Therefore, it is necessary to develop an efficient model to ensure the security and integrity of the patient's diagnostic data transmitted and received from IoT environment.[1] This goal is carried out using steganography techniques and system encryption algorithms together to hide digital information in an image.

With the development of computer-based communication in health services applications, the need for medical image security is urgent to protect the patient's sensitive data. Medical image analysis aims to solve medical problems using different imaging modalities and digital image analysis techniques. Images are easily manipulated using image processing tools, which have serious consequence. Hence, protecting the credibility and respectability of medical images is of a significant importance. There are two main types of image verification strategies: cryptography based techniques and fragile watermarking based techniques. A Message Authentication Code (MAC)[2] is computed in the cryptography based techniques, which utilizes a hash function to calculate the same code. Such MAC codes can decide whether an image tampering occurred without the ability to determine its region. The two main algorithms used for data encryption in this work are the Modified Rivest-Shamir-Adleman and the Honey Encryption (HE) algorithm[10]. The modified RSA is a private key algorithm, which is widely used in business and personal communication sectors.

HE has the advantage of eliminating brute force attack and side channel attack. The primary research in hiding data started with steganography which refers to the science and art of hiding information within an image. The benefit of steganography is that it can be utilized to transmit classified messages without the fact of the transmission being detected. The DWT has a tremendous spatial localization, frequency spread, and multiresolution characteristics, which are matching with the theory of forms in the human visual system.

II.METHODOLOGY

A.Modified RSA algorithm

RSA is a well-known public key cryptography algorithm and was one of the first great advances in public key cryptography. In asymmetric key cryptography also called Public Key cryptography, two different keys (which form a key pair) are used. One key is used for encryption & only the other corresponding key must be used for decryption. No other key can decrypt the message, not even the original (i.e. the first) key used for encryption[3]. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he /she can communicate with anyone else RSA is a well-known public-key cryptography algorithm. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography.

The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers know mathematical attack and the problem of trying all possible private keys know brute force attack Public-key cryptography is used where each user has a pair of keys, one called the public key and the other private key. Each user's public key is published while the private key is kept secret and thereby the need for the sender and the receiver to share secret information (key) is eliminated

B.Modified RSA cryptosystem using two key pairs:

In RSA algorithm if take large size key then its take more time in encryption and decryption operation and if we select small size key then security is compromised. Since RSA is block cipher so for each block of data we need to perform same operation and hence more time is required. In the proposed approach we generate two different keypair one of small size(public_key1,private_key1,n1) and one of very large size (public_key2,private_key2,n2) using same existing RSA key generation algorithm[5].

Encryption:

Step1. Encrypt data with public key of small size key(public_key1)

Step2. Encrypt n1 of small key pair with public key(public_key2) of large key pair.

Step3. Transmit results of step 2 n step3 to receiver.

Decryption:

Step1. First decrypt n1 with private_key2.

Step2. Now we have n1, so we can decrypt encrypt data with private_key1.

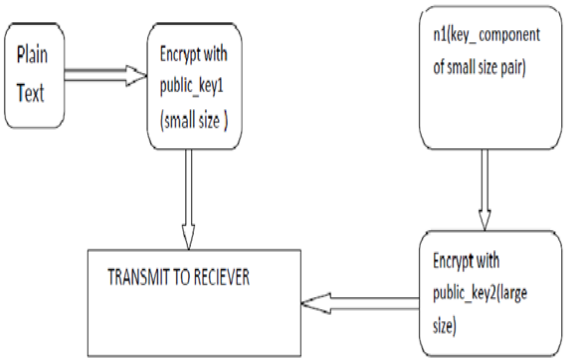

Fig 1. At sender's side

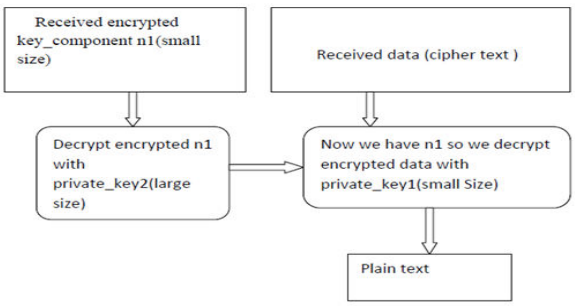

Fig 2. At receiver's side

C. HE ALGORITHM

The existing password-based encryption (PBE) methods that are used to protect private data are vulnerable to brute-force attacks. The reason is that, for a wrongly guessed key, the decryption process yields an invalid-looking plaintext message, confirming the invalidity of the key, while for the correct key it outputs a valid-looking plaintext message, confirming the correctness of the guessed key. Honey encryption helps to minimise this vulnerability. Most people in China (as in any other country) are annoyed by junk text messages. The Internet users can also be affected by identity theft when criminals are using someone's identity. This can occur because some sensitive private data was not well protected and was then maliciously used by other parties causing damage to finances and reputation of the data owner.

When purchasing a product online, we are asked to provide our mobile phone number for the delivery purpose. When buying a train ticket in China, we need to fill in the identification card number. The commercial parties gather such sensitive private data. Some store them in a plaintext format. Some employ PBE . However, the robustness of encryption depends on the key length. Although current encryption algorithms are considered secure, given enough time and computing power, they will be vulnerable to brute-force attacks. Also, the existing encryption mechanisms have vulnerability; that is, when decrypting with a wrongly guessed key, they yield an invalid-looking plaintext message,[6] while when decrypting with the right key, they output a valid-looking plaintext message, confirming that the ciphertext message is correctly decrypted.

. The honey term in the information security terminology describes a false resource. For example, honey pot is a false server that attracts attackers to probe and penetrate. Honey word is a false username and password in the database. Once used for login, an intrusion is detected. Honey encryption can also address the previously mentioned vulnerability. Even when a wrong key is used for decryption, the system can yield a valid-looking plaintext message; therefore, the attacker cannot tell whether the guessed key is correct or not.

The innovation of honey encryption[12] is the design of the DTE . According to the probabilities of a message in the message space, it maps the message to a seed range in a seed space, then it randomly selects a seed from the range and XORs it with the key to get the cipher text. For decryption, the cipher text is XORed with the key and the seed is obtained[7]. Then DTE uses the seed location to map it back to the original plaintext message. Even if the key is incorrect, thedecryption process outputs a message from the message space and thus confuse the attacker.

The contribution of this paper is threefold. First, we design and implement the honey encryption system and apply the concept to three applications including Chinese identification numbers, mobile numbers, and passwords. These applications are based on uniformly distributed message spaces and the symmetric encryption mechanism. We also extend honey encryption to applications with nonuniformly distributed message spaces and an asymmetric encryption mechanism (RSA). Second, we evaluate the performance of our honey encryption mechanism and propose an enhancement. Third, we discuss lessons learned from implementing and evaluating the honey encryption technique.

D.HE CONCEPT

Honey encryption protects a set of messages that have some common features (e.g., credit card numbers are such messages). A message set is called a message space. Before encrypting a message, we should determine the possible message space[11]. All messages in the space must be sorted in some order. Then the probability of each message that occurs in the space and the cumulative probability of each message are needed. A seed space should be available for the distribution-transforming encoder (DTE) to map each message to a seed range in the seed space (-bit binary string space). The DTE determines the seed range for each message according to the PDF and CDF of the message and makes sure that the PDF of the message is equal to the ratio of the corresponding seed range to the seed space. The -bit seed space must be big enough so that each message can be mapped to at least one seed. A message can be mapped to multiple seeds and the seed is randomly selected.

E.HE ALGORITHM

Inputs: secret plain text message.

Output: main_cipher message, key s

Begin

1. Divide plain msg into two parts (Medi_Data, Medi_image)

2. Generate new HE key s

3. EncData=HE-128(Medi_Data,s)

4. Generate new MRSA key(public=m) and (private=x)

5. EncImage= MRSA (Medi_image, m)

6. Build FullEnc Txt by inserting both EncData and EncImage in their indices

7. EncKey = HE-128(x , s)

8. Compress FullEncMsg by convert to hashs

9. Compress EncKey by convert to hashs

10. Define message empty main_cipher=“

11. main_cipher=Concatenate (FullEncMsg , EncKey)

12. Return main_cipher and s

III.RESULTS AND DISCUSSION

Compared to the state-of-the-art methods, the proposed model proved its ability to hide the confidential patient's data into a transmitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stegno-image [8].The main advantage of HE is that it avoid the brute force attack completely. The performance achieved using both HE and modified RSA is better than other method. Graph shows the analysis between modified RSA, standard RSA and AES algorithms. The better performance shown by modified RSA highlighted by blue line

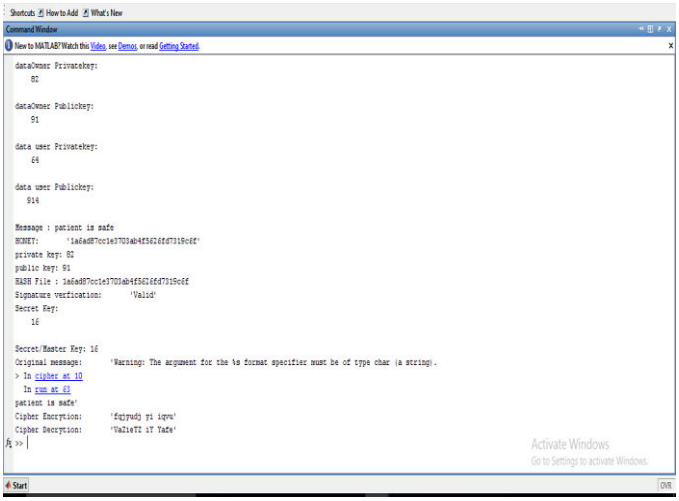

Fig.3 Honey Encryption message in receiver side output

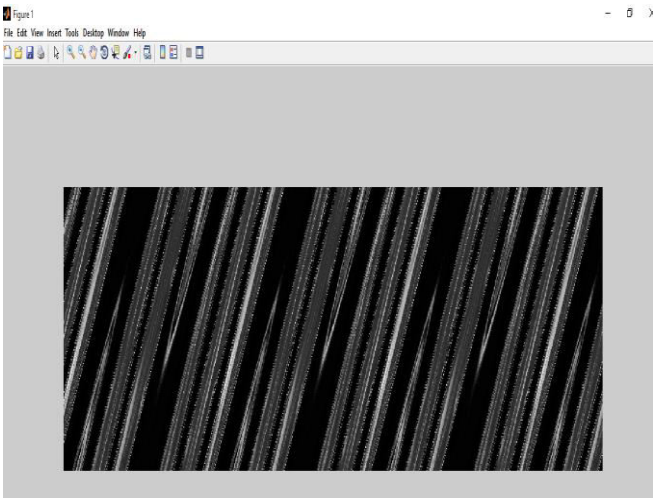

Fig.4 Encryption output –Input image is hidden by another data

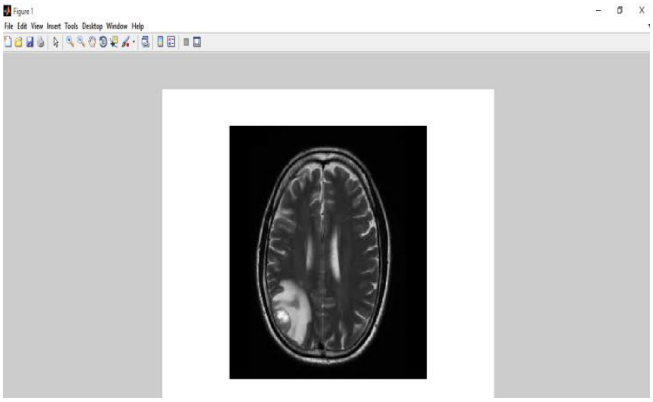

Fig.5 Decryption Output-Original Image send by Transmitter

IV.CONCLUSION

IoT creates an integrated communication environment of interconnected devices and platforms by engaging both virtual and physical world together. Now days the number of hackers were increased to hack the information which may be public or private so the security is the major issue. The main challenge is to avoid the brute force attack. Here the proposed two algorithm help to protect the data .In future we will try to cover the image using 2D DWT 1 level or 2D DWT 2 level.

V.ACKNOWLEDGEMENTS

First of all I would like to thank our Almighty God for giving me his blessings, strength and support to complete this work successfully. I am grateful to all of those with whom I have had the pleasure to work during this and other related projects.

VI.REFERENCES

1. A.Shehab,Abdulaziz Mohamed,Elhoseny,"Secure and robust fragile water marking scheme for medical images,"IEEE Access on soft computing techniques for image analysis in the medical industry

2. P.Kumar , H.J Lee, "Security issues in healthcare applications using wireless medical sensor networks :A survey," Sensor Basel

3. Siteshkumarsinha , Mayankshrivastava," A new way of design and implementation of hybrid encryption to confidential information from malicious attack in network," International Journal of computer applications

4. Shamim Ahmed Laskar , KattamanchiHemachandran," High capacity data hiding using LSB steganography and encryption,"International Journal of database management systems

5. Ahmed abdelaziz,Mohamed ,Elhosency,Ahmed," A machine learning model for improving health care services on cloud computing environment," Measurement.2018.01.022

6. AsmaaSabetAnwar,Kareemkamal A Ghany," Improve security of medical data, "International Journal of biomedical informatics and e-health

7. Anupamkumar, Bairagi,RahamatullahKhondoker," An efficient steganographic approach for protecting communication in the (IOT) critical infrastructure," Information security journal :A global perspective

8. M.I Khalil," Medical image steganographic : study of medical image quality degradation when embedding data in the frequency domain," International Journal of computer network and information security

9. Khan Muhammad , JamilAhmad,Haleem Farman ," A secure method for colour image steganography using grey level modification and multilevel encryption," KSII Transactions on internet and information systems

10. Mamta Jain, Anil kumar, Rishabhcharanchoudhary," Improved diagonal queue medical image steganography using chaos theory , LFSR and Rabin cryptosystem," Springer link(Brain informatics)

11. Seyyed Amin Seyyedi, Vasilisadau,NickIvanov," A Secure steganography method based on integer lifting wavelet transform," International Journal of network security

12. M.D.Anitha Devi , K.B.Shivakumar," A novel image steganography technique for secured online transaction using DWT and visual cryptography," IOP conference series : Materials science and Engineering

13. AsmaaHasan Mohsen, ShaimaaHameed Shaker," Image encryption using symmetric encryption algorithm based on random keys generator," International Journal of recent innovation in engineering and research

14. MirzaAbdurRazzaq,Riaz Ahmed Shaikh,Mirza Adnan Baig,Ashfaque Ahmed Memon," Digital image security : Fusion of encryption ,steganography and watermarking," International Journal of advanced computer science.