© 2020 IJSRST | Volume 5 | Issue 7 | Print ISSN : 2395-6011 | Online ISSN: 2395-602X

4th National Conference on Advances in Engineering and Applied Science
Organized by : Anjuman College of Engineering and Technology (ACET) Nagpur,
Maharashtra, India, In association with
International Journal of Scientific Research in Science and Technology

IoT Based Secure Medical Data Transmission Model

Sonali Madavi, Prof. Mohammad Nasirudding

Department of Electronics and Telecommunication, Anjuman College of Engineering and Technology, Nagpur, Maharashtra, India

ABSTRACT

The transmission of data through any channel of communication needs strong encryption techniques for the purpose of data security. Internet of things (IoT) creates an integrated communication environment of interconnected devices and platforms by engaging both virtual and physical world together. Due to the major advancement of the IoT in the healthcare sector, the security and the integrity of the medical data became big challenges for healthcare services applications. In this paper proposes a hybrid security model for securing the diagnostic text data in medical images. The propose model is develop through integrating 2D Discrete Wavelet Transform 2 Level (2D-DWT-2L) steganography technique with a proposed hybrid encryption scheme. The proposed hybrid encryption representation is built using a combination of Advanced Encryption Standard (AES), and Rivest, Shamir, and Adleman (RSA) algorithms. The recommend model starts by encrypting the secret data; then it hides the result in a cover image using 2D-DWT-2L. Both colour and gray-scale images are used as cover images to conceal different text sizes. The performance of the propose method was evaluated based on four statistical parameters; the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structural Similarity (SSIM) and Correlation. Compared to the state-of-the-art methods, the recommend model establish its ability to hide the confidential patient's data into a transmitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stego-image.

Keywords : IoT, security, privacy, DWT-2 level, AES, RSA, steganography, medical image.

I. INTRODUCTION

The rapid and constant development in information technology has forced computer networks to grow extremely in a very short time. This results in facilitating electronic data transfer and in large amounts. The awe-inspiring advancement in the electronic ways of data exchange and the widespread of image use have put a huge potential on both security and protection of top secret data from unauthorized permission. Accordingly, development of security systems is very dangerous to guarantee the security of data during transition through the internet.

Cryptography is considered as one of the largest part commonly utilized techniques to guarantee data security. In recent years, great development has been achieved in data encryption technology. several data encryption approaches are currently used especially for digital image security. Random encryption keys are formed in these techniques, whereas the genuine content becomes imperceptible.

Steganography is the science and art of hiding information within a carrier, where no one excluding the intended recipient, has the knowledge of the existence of hidden information. Steganography as a term is derived from the antique Greek words “steganos”, which means covered and “graphic” which means writing. In this operation, a secret message is hidden in another piece of normally looking information, which is known as the cover. This process aims to keep the secret information hidden without informative any kind of distrust to the viewer's.

Currently, there are lots of algorithms used to encrypt data in ways and styles. A hybrid encryption is a protocol using multiple codes of different types together. One of the common approaches is to generate a secret message to encrypt a random symmetric, and then encrypt this message into cipher message by using Hybrid Encryption (AES & RSA) Algorithm.

In this work, an integration of encryption algorithms on the basis of (AES and RSA) was used to develop the security of data transfer. It uses the AES algorithm for data transmission due to its high competence in the encryption block.

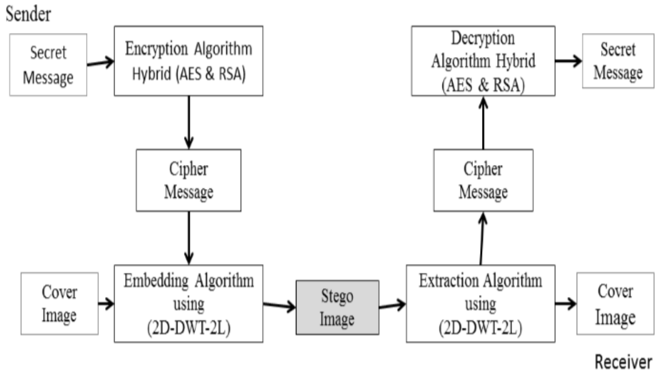
Sender
Secret Message
Encryption Algorithm Hybrid (AES & RSA)
Cipher Message
Cover Image
Embedding Algorithm using (2D-DWT-2L)
Stego Image
Extraction Algorithm using (2D-DWT-2L)
Cover Image
Cipher Message
Decryption Algorithm Hybrid (AES & RSA)
Secret Message
Receiver

Figure .1 Proposed Framework for hid information

II. LITERATURE SURVEY

A Survey on Internet of Things and Cloud Computing for Healthcare.L. M. Dang, Md. Jalil Piran, Dongil Han, Kyungbok Min and Hyeonjoon Moon.

The rapid development of the Internet of Things (IoT) technology in current years has supported connections of several smart things along with sensors and established faultless data exchange between them, so it leads to a stringy requirement for data analysis and data storage platform such as cloud computing and fog computing. Healthcare is one of the application domains in IoT that draws big interest from industry, the research association, and the public sector. The improvement of IoT and cloud computing is improving patient safety, staff satisfaction, and operational efficiency in the medical industry. This review is conducted to analyze the latest IoT components, applications, and market trends of IoT in healthcare, as well as study current development in IoT and cloud computing-based healthcare applications since 2015. We also consider how capable technologies such as cloud computing, ambient supported living, big data, and wearables are mortal applied in the healthcare industry and establish various IoT, e-health regulations and policies worldwide to determine how they support the sustainable development of IoT and cloud computing in the healthcare industry. Furthermore, an in-depth review of IoT privacy and security issues, including potential intimidation, attack types, and security setups from a healthcare viewpoint is conducted. Ultimately, this paper analyzes previous well-known security models to deal with security risks and provides trends, highlighted opportunities, and challenges for the IoT-based healthcare future development.

The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems.Ashraf

Darwish, Mohamed Elhoseny, Arun Kumar Sangaiah, Khan Muhammad, Aboul Ella Hassanien

The Cloud Computing (CC) and the Internet of Things (IoT) have emerged as new platform in the ICT revolution of the twenty first century. The adoption of the Cloud IoT concept in the healthcare field can bring several opportunities to medical IT, and experts believe that it can significantly improve healthcare services and contribute to its continuous and systematic improvement. This paper present a complete review of the current literature on integration of CC and IoT to solving various problems in healthcare applications such as smart hospitals, remote medical services and medicine control. Moreover, a brief introduction to cloud computing and internet of things with an application to health care is given. This paper presents a new concept of the integration of CC and IoT for healthcare applications, which is what we; call the Cloud IoT-Health concept. The term Cloud IoT-Health and some key mixing issues are presented in this paper to propose a practical vision to integrate current components of CC and the IoT in healthcare applications. Also, this paper aims to present the state of the art and gap analysis of different levels of integration mechanism, analyzing different existing proposals in Cloud IoT-Health systems. Ultimately, related researches of CC and IoT integration for healthcare systems have been reviewed. Challenges to be addressed and future directions of research are acknowledged, and an extensive bibliography is presented.

An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. Bairagi, A. K., Khondoker, R., & Islam, R.With the expression of the Internet of Things (IoT) and fog computing, the quantity of edge devices is increasing exponentially all over the world, providing better services to the end user with the help of existing and upcoming communication infrastructures. All of these devices are producing and communicating a huge amount of data and control information approximately this open IoT environment. A huge amount of this information contains private and important information for the user as well as for the organization. The number of attack vectors for malicious users is high due to the sincerity, circulated nature, and lack of control over the whole IoT environment. For building the IoT as an effective service platform, end users need to confidence the system. For this reason, security and privacy of information in the IoT is a great concern in critical infrastructures such as the smart home, smart city, smart healthcare, smart industry, etc. In this paper, we propose three information hiding techniques for protecting communication in significant IoT infrastructure with the help of steganography, where RGB images are used as carriers for the information. We hide the information in the deeper layer of the image channels with minimum distortion in the least amount significant bit (lsb) to be used as sign of data. We analyze our technique both mathematically and experimentally. Mathematically, we show that the challenger cannot predict the actual information by analysis. The proposed approach achieved better imperceptibility and capacity than the various existing techniques along with better conflict to steganalysis attacks such as histogram analysis and RS analysis, as proven experimentally.

“secure medical image steganography with RSA cryptography using decision tree.” Jain, M., Choudhary, R. C., & Kumar, A.
In this paper, a new technique about secure medical information transmission of patient inside medical cover image is presented by concealing data using decision tree concept. Decision tree shows a robust

mechanism by providing decisions for secret information concealing location in medical carrier image using secret information mapping concept. RSA encryption algorithm is mortal used for patient's unique information enciphering. The outcome of the RSA is structured into various similarly distributed blocks. In steganography, secret cipher blocks are assigned to carrier image for data inserting by mapping method using breadth first search. Receiver gets hidden secret medical information of patient using RSA decryption, so only authorized beneficiary can recognize the plain text. Performance is analyzed and measured using various parameters between medical stego and carrier images. Results are analyzed and compared with many of existing algorithms.

Hybrid security techniques for Internet of Things healthcare applications. Yehia, L., Khedr, A., &Darwish, A.The Internet of Things (IoT) describes the future where every day physical objects will be connected to the internet and be able to identify themselves to other devices. IoT is a new revolution of the Internet and it will effect in a huge number of applications such as smart living, smart home, healthcare systems, smart manufacturing, environment monitoring, and smart logistics. This paper provides integration, summarizes and surveys some of the security techniques specially hybrid techniques that can be applied with healthcare applications in IoT environment.

"secure medical image steganography with RSA cryptography using decision tree."Jain, M., Choudhary, R. C., & Kumar, A.In this article, a novel technique about secure medical information transmission of patient inside medical cover image is presented by concealing data using decision tree concept. Decision tree shows a robust mechanism by providing decisions for secret information concealing location in medical carrier image using secret information mapping concept. RSA encryption algorithm is being used for patient's unique information enciphering. The outcome of the RSA is structured into various equally distributed blocks. In steganography, secret cipher blocks are assigned to carrier image for data inserting by mapping mechanism using breadth first search. Receiver gets hidden secret medical information of patient using RSA decryption, so only authorized recipient can recognize the plain text. Performance is analyzed and measured using numerous parameters between medical stego and carrier images. Results are analyzed and compared with many of existing algorithms.

Hybrid security techniques for Internet of Things healthcare applications."Yehia, L., Khedr, A., &Darwish, A

The Internet of Things (IoT) describes the future where every day physical objects will be connected to the internet and be able to identify themselves to other devices. IoT is a new revolution of the Internet and It will effect in a large number of applications such as smart living, smart home, healthcare systems, smart manufacturing, environment monitoring, and smart logistics. This paper provides integration, summarizes and surveys some of the security techniques especially hybrid techniques that can be applied with healthcare applications in IoT environment.

III. OBJECTIVE

The aim of this Project is to improve and recommend a new hybrid technique for data security through combination between cryptography and steganography algorithms. This system is used to embed an encrypted secret message into a cover image to get high imperceptibility and robustness with minimal deterioration in the received stego image. The main objectives of this model is :

- ✓ Develop a security system for hiding text data in an image using hybrid (AES & RSA) and steganography 2D-DWT-2L techniques individually.
- ✓ Develop a hybrid security system which integrates both data encryption (AES and RSA) and steganography techniques 2D-DWT-2L to increase data imperceptibility, robustness and performance of stego image.

The Elements of Steganography:

Two pieces of data are required in steganography, which are the cover and the data to be hidden:

1. The Cover

The cover refers to the medium into which the information we will be embedded. The effectiveness of the steganography technique is dependent up on selecting the most suitable cover. The cover also work as a container for the given message. Steganography is based on hiding the data behind the cover to protect it from being known as secure, dislike encryption.

2. The Data

The data that are required to be hidden should be serilizable in order to be embedded bit by bit in the cover. The size of data shouldn't exceed the cover size in order to contain all the data. In case of images, both the cover and the data may have the same number of pixels; however the cover will have more color information for each pixel than the hidden data.

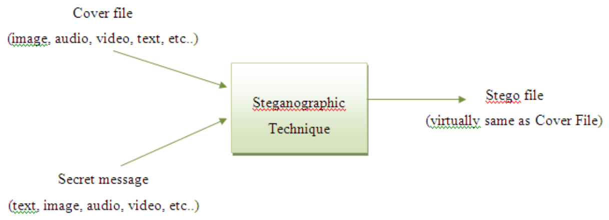
Cover file
(image, audio, video, text, etc..)
Steganographic Technique
Stego file
(virtually same as Cover File)
Secret message
(text, image, audio, video, etc..)

Figure shows the basic approach of steganography process.

IV. CONCLUSION

The main advantages of our system are providing more security, more flexibility, greater embedding capacity and more invisibility. There are two techniques are used in our system which are hybrid algorithm and steganography algorithm. This hybrid system is considered as an combination of AES and RSA algorithms. The hybrid encryption AES and RSA algorithm had higher performance when applied on color and grayscale images with different text sizes. This system is based on the four statistical parameters such as (PSNR, MSE, SSIM, and Correlation). The performance of the four approaches was further evaluate by comparing their results with those obtain from other approach on both color and grayscale images with different text sizes. Our approaches had higher PSNR values and lower MSE values than those obtained by the reference results. . However, the steganography (2D-DWT-2L) with hybrid (AES and RSA), shows the slowest performance when compare with other technique it was noticed that although text encryption increases the text security, it decreases the invisibility of the cover image. In conclusion, our approaches had higher performance in hiding secret data when compare with the reference approaches used in this study.

V. REFERENCES

[1]. Ashraf Darwish, MohamedElhoseny, Arun Kumar Sangaiah, Khan Muhammad, Aboul Ella Hassanien, "The Impact of the Hybrid Platform of Internet of Things and Cloud Computing on Healthcare Systems: Opportunities, Challenges, and Open Problems", Journal of Ambient

Intelligence and Humanized Computing, 2017 (https://doi.org/10.1007/s12652-017-0659-1)

[2]. Bairagi, A. K., Khondoker, R., & Islam, R. (2016). An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. Information Security Journal: A Global Perspective, 25(4-6), 197-212.

[3]. Anwar, A. S., Ghany, K. K. A., & Mahdy, H. E. (2015).Improving the security of images transmission. International Journal, 3(4).

[4]. Yehia, L., Khedr, A., &Darwish, A. (2015). Hybrid security techniques for Internet of Things healthcare applications. Advances in Internet of Things, 5(03), 21

[5]. Jain, M., Choudhary, R. C., & Kumar, A. (2016). Secure medical image steganography with RSA cryptography using decision tree. In Contemporary Computing and Informatics(IC3I), 2016 2nd International Conference on (pp. 291-295).IEEE.

[6]. Zaw, Z. M., &Phyo, S. W. (2015). Security Enhancement System Based on the Integration of Cryptography and Steganography. International Journal of Computer (IJC), 19(1), 26-39.

[7]. Mare, S. F., Vladutiu, M., &Prodan, L. (2011). Secret data communication system using Steganography, AES and RSA. In Design and Technology in Electronic Packaging (SIITME), 2011 IEEE 17th International Symposium for (pp.339-344). IEEE.

[8]. Sreekutty, M. S., &Baiju, P. S. (2017). Security enhancement in image steganography for medical integrity verification system. In Circuit, Power and Computing Technologies (ICCPCT), 2017 International Conference on (pp. 1-5). IEEE.

[9]. Abdel-Nabi, H., & Al-Haj, A. (2017). Efficient joint encryption and data hiding algorithm for medical images security. In Information and Communication Systems (ICICS), 2017 8th International Conference on (pp. 147-152).IEEE.

[10]. Yin, J. H. J., Fen, G. M., Mughal, F., &Iranmanesh, V.(2015). Internet of Things: Securing Data using Image Steganography. In Artificial Intelligence, Modelling and Simulation (AIMS), 2015 3rd International Conference on (pp. 310-314). IEEE.