History of Medicine, 2024, 10(1): 141-147

DOI: 10.17720/2409-5834.v10.1.2024.10

Optimizing IoT Healthcare Security with Advanced Hybrid Encryption and Data Embedding Techniques

Dr. L. K. Suresh Kumar[1*], Dr. D. Eshwar[2]

[1]Associate Professor, Department of Computer Science and Engineering, University College of Engineering, Osmania University, Hyderabad, Telangana
[2]Professor, Department of Computer Science and Engineering, KPRIT College of Engineering, Ghatkesar, Telangana
*Corresponding E-mail: suresh.l@uecou.edu

ABSTRACT

The term "Internet of Medical Things" (IoMT) describes a network of medical devices and apps that are connected and share healthcare data over the internet. Due to the swift progress of technology, IoMT applications have become essential in contemporary healthcare, enabling remote patient monitoring, instantaneous health data analysis, and enhanced medical services. Nevertheless, the transfer of confidential medical information via the internet gives rise to substantial security apprehensions. In order to deal with these difficulties, lightweight cryptography (LWC) approaches are utilized to ensure the security of medical data transmission in Internet of Medical Things (IoMT) applications. LWC prioritizes delivering strong security while minimizing computational and memory demands. The necessity for safe transmission of medical data in IoMT applications stems from the confidential and delicate nature of healthcare information. Hence, the objective of this study is to create a system that utilizes Lightweight Cryptography (LWC) approaches to provide efficient and secure transmission of medical data, while also optimizing resource utilization. Furthermore, the proposed system utilizes a hybrid security approach to ensure the protection of diagnostic text data in medical images. The suggested model is created by combining the Discrete Wavelet Transform (DWT)-based steganography approach with a hybrid LWC scheme. The hybrid encryption scheme is constructed by combining the Advanced Encryption Standard (AES) and Feistel algorithms. It facilitates effective, protected, and confidentiality-maintaining communication, promoting the development of inventive healthcare solutions in the age of digital revolution.

Keywords: Internet of Medical Things, Data privacy, secrete data transmission, Wavelet transform, lightweight cryptography.

1. INTRODUCTION

Over the past few years, the healthcare sector has experienced significant expansion and has played a significant role in generating money and creating jobs. In the past, the detection of diseases and abnormalities in the human body could only be achieved through physical examinations conducted in hospitals. The majority of the patients were required to remain in the hospital for the duration of their therapy. Consequently, there was a rise in healthcare expenses and a burden on healthcare facilities in rural and distant areas. The progress in technology has enabled the diagnosis of many ailments and health monitoring utilizing small devices such as smartwatches. Furthermore, technology has revolutionized a healthcare system that was focused on hospitals and shifted it towards a system that

prioritizes the needs and preferences of patients. For instance, various clinical assessments, such as monitoring blood pressure, blood glucose levels, pO2 levels, and others, can be conducted independently at home without the assistance of a healthcare expert. Moreover, improved telecommunication technologies facilitate the transmission of clinical data to healthcare centers located in remote places. The integration of communication services with emerging technologies such as machine learning, big data analysis, Internet of things (IoT), wireless sensing, mobile computing, and cloud computing has enhanced the availability of healthcare facilities.

The Internet of Things (IoT) establishes a cohesive communication ecosystem by connecting various devices and platforms, seamlessly merging the virtual and physical realms. The introduction of remote digital healthcare via IoT technologies has made the transfer of medical data a regular occurrence. Hence, it is imperative to create a highly effective model that guarantees the safety and consistency of the patient's diagnostic data as it is transferred and received inside the IoT environment. This objective is accomplished by employing steganography methodologies and system encryption algorithms in conjunction to conceal digital data within an image.

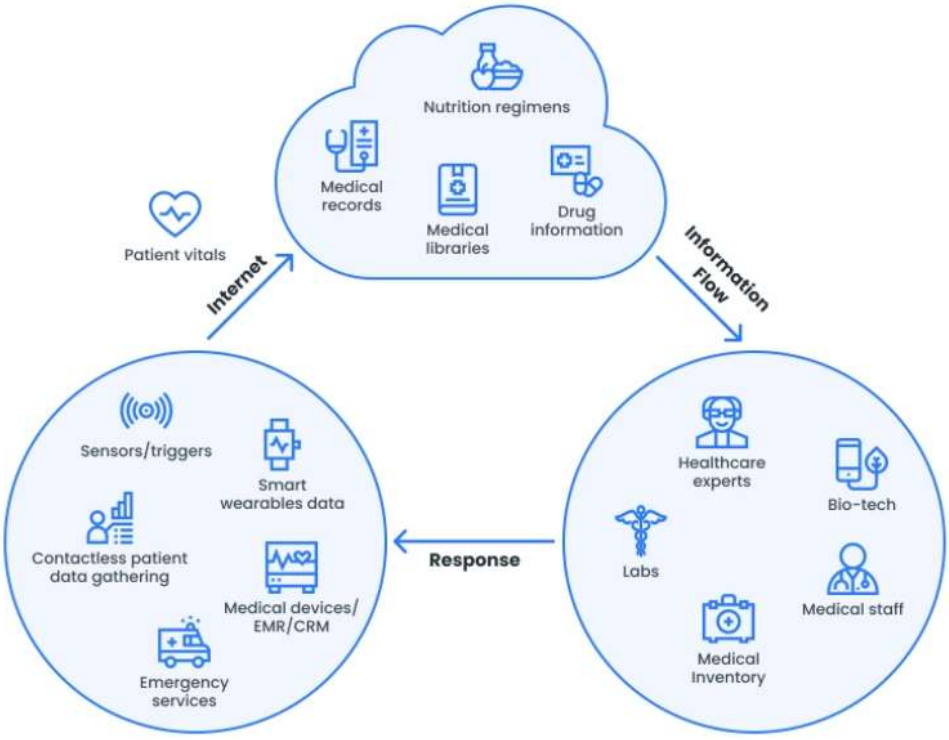

Figure 1: IoMT applications in real-time. (*Source:* https://www.elinext.com/industries/healthcare/trends/iomt-internet-of-medical-things/)

The Internet of Things (IoT) has not only increased human autonomy, but also expanded our capacity to engage with the external world in various ways. The Internet of Things (IoT), aided by advanced protocols and algorithms, has emerged as a significant driver of worldwide communication. It enables the connection of several items, including wireless sensors, home appliances, and electrical gadgets, to the Internet. The Internet of Things (IoT) is utilized in several industries such as agriculture, automotive, residential, and healthcare. The increasing popularity of the Internet of Things (IoT) can be attributed to its benefits of improved precision, reduced expenses, and enhanced predictive capabilities. In addition, the growing understanding of software and applications, along with advancements in mobile and computer technologies, the widespread availability of wireless technology, and the expanding digital economy have all contributed to the swift transformation of the Internet of Things (IoT).

The Internet of Things (IoT) gadgets, including sensors and actuators, have been incorporated with various physical equipment to oversee and share information over diverse communication protocols, such as Bluetooth, Zigbee, IEEE 802.11 (Wi-Fi), and others. In healthcare applications, sensors are utilized to gather physiological data from the patient's body. These sensors can be either embedded or worn on the human body and collect information such as temperature, pressure rate, electrocardiograph (ECG), electroencephalograph (EEG), and other relevant measurements. In addition, it is possible to capture environmental data such as temperature, humidity, date, and time. This data aids in generating significant and accurate conclusions regarding the patients' health problems. Data storage and accessibility are crucial components of the IoT system due to the acquisition and recording of substantial amounts of data from many sources, such as sensors, mobile phones, e-mail, software, and apps.

2. LITERATURE SURVEY

Humayun and colleagues [1] introduced a technique that ensures both security and energy efficiency in transmitting patient data from wearable IoT sensors (WIS) to a base station (BS). The healthcare sector extensively utilizes IoT devices to collect and transmit real-time data. Nevertheless, these sensors have limited computational power and storage, which increases the likelihood of security breaches and threats. Furthermore, as time, the energy level of IoT sensors diminishes, which might occasionally result in the loss of crucial patient data. Almulhim and Zaman (2) presented a secure group-based lightweight authentication strategy for IoT-based E-health applications. The suggested model ensures mutual authentication and energy efficiency, as well as efficient computing for healthcare IoT applications. The suggested model will utilize the concepts of elliptic curve cryptography (ECC) to provide the given features. In their study, Mallikarjuna et al. [3] introduced a novel approach that was evaluated using the NodeJs software and ApacheJmeter open source JMeter Cloud Test environment. The results demonstrated that the simulation-based approach, known as BEHR, is more efficient than the current conventional system in terms of response time and file storage and transmission of electronic health records (EHR).

In their study, the authors introduced an enhancement to the standard RSA method. This enhancement involves generating two public keys during the key creation process and utilizing both of these public keys simultaneously, in contrast to the ordinary RSA cryptographic algorithm which only uses one public key. In this case, the public key is transmitted twice, as opposed to the usual RSA technique where the public key is transmitted only once. This renders the attacker unaware of the encryption key being utilized, hence preventing them from deciphering the communication. Under certain circumstances, if a malevolent attacker manages to intercept the transmission of both public keys, they can exploit both keys to decrypt the encoded message. Abdulmalek et al. [5] suggested three methods of concealing information in color images for the purpose of safeguarding data in an IoT architecture. The first and third methods utilize three channels (red, green, and blue) to transmit information, but the second method employs only two channels (green and blue). The utilization of dynamic positioning strategies involves concealing information inside the lower layers of the picture channels, facilitated by a mutually shared secret key. Alkhabet et al. [6] suggested improving the security and privacy of patient information and E-health systems by utilizing distributed storage systems (DSSs) that employ public-key cryptography for storing patient data. Data storage and security requirements, including confidentiality, reliability, authentication, and dynamic integrity, are dispersed across individual nodes in the network simultaneously. The patient data is encrypted utilizing the redundant residue number system (RRNS) approach, which relies on a collection of moduli in the encryption process to produce residues.

In their study, Hussain et al. [7] proposed a security framework for real-time health monitoring systems. The framework aims to guarantee the confidentiality, integrity, and authenticity of data. To do this, the researchers utilized two widely used IoT protocols: constrained application protocol (CoAP) and

message query telemetry transports (MQTT). This security architecture is designed to protect sensor data from security vulnerabilities during continuous transmission across layers, utilizing hypertext transfer protocols (HTTPs) for this purpose. Consequently, it provides protection against the breach with a minimal risk ratio. This paper's methodology examines the security framework of IoT-based real-time health systems, specifically focusing on the protection provided by the CoAP and HTTPs tiers. CoAP operates in conjunction with HTTPs and is responsible for delivering comprehensive security solutions from one end to another. In their study, the authors in [8] examined the utilization of intelligent health methodologies and their progression over time, specifically focusing on the integration of IoT devices with cloud applications. E-Health refers to the ability to access, analyze, and assess health information from online databases in order to effectively address and resolve health concerns. The internet can protect consumers from harm and serve as a repository for health and e-health analysis, enabling them to make informed decisions regarding their health. Denis and Madhubala [9] proposed a novel method of combining data encryption with medical image diagnosis to protect the confidentiality of the data. The proposed model is created by integrating either 2D Discrete Wavelet Transform 1 Level (2D-DWT-1 L) or 2D Discrete Wavelet Transform 2 Level (2D-DWT-2 L) steganography with the proposed hybrid encryption technique. The hybrid encryption technique is constructed by strategically employing the Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) algorithms to safeguard diagnostic data that will be inserted into the RGB channels of a medical cover image.

3. PROPOSED METHODOLOGY

The Internet of Things (IoT) establishes a unified communication ecosystem by connecting various devices and platforms, bridging the gap between the virtual and physical realms. The introduction of remote digital healthcare via IoT technologies has made the transfer of medical data a regular occurrence. Hence, it is imperative to create a highly effective model to guarantee the safety and consistency of the patient's diagnostic data that is transferred and received within the IoT environment. This objective is accomplished by employing steganography methodologies and system encryption algorithms in conjunction to conceal digital data within an image. However, the rapid progress of the Internet of Things (IoT) in the healthcare industry has posed substantial hurdles in terms of ensuring the security and integrity of medical data for healthcare service applications. Figure 1 displays the suggested block diagram. This study presents a novel and efficient security model that combines different approaches to protect the diagnostic text data in medical images. The suggested model is created by combining the 2-D discrete wavelet transform steganography technology with a newly constructed hybrid encryption system. The hybrid encryption scheme is constructed by combining the Advanced Encryption Standard (AES) and Feistel encryption algorithms.

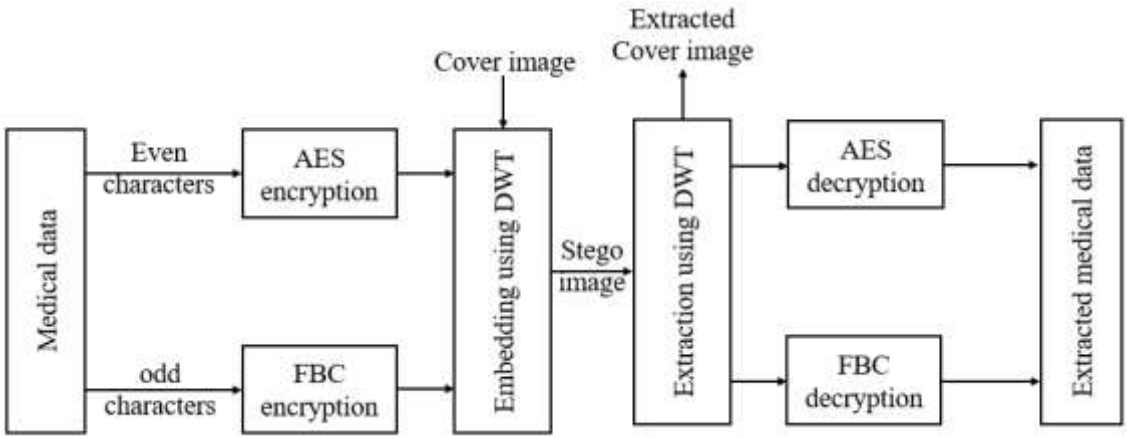

Figure 1: Proposed secure data transmission using AES-Feistel algorithm.

The project implements a secure, lightweight, model-based system for medical data transmission in IoT-based healthcare environments. It combines AES and RSA encryption algorithms for hybrid encryption of messages, enhancing security by splitting and separately encrypting message segments. Discrete Wavelet Transform (DWT) is used for embedding encrypted messages into images, ensuring data confidentiality and integrity. The project also introduces a Feistel encryption alternative to RSA, aiming to compare computational efficiency. Additionally, it provides functionality for encryption, decryption, message embedding, and extraction, along with performance metrics such as PSNR and MSE for image quality assessment, all encapsulated within a user-friendly graphical interface.

This project aims to develop a secure, lightweight model-based medical data transmission system for IoT-based healthcare environments. The system employs a combination of encryption algorithms (AES, RSA, and Feistel) and DWT-based data embedding techniques to ensure data confidentiality and integrity during transmission. Here is an overview of the key components and functionalities:

Key Components and Functionalities:

1. **AES (Advanced Encryption Standard):**
    - Used for symmetric encryption of the data.
    - Encrypts and decrypts the "even" portion of the split message.
2. **RSA (Rivest-Shamir-Adleman):**
    - Used for asymmetric encryption.
    - Encrypts and decrypts the "odd" portion of the split message.
3. **Feistel Network:**
    - An alternative to RSA for encrypting the "odd" portion of the message.
    - Provides a different encryption method to compare computational performance with RSA.
4. **DWT (Discrete Wavelet Transform):**
    - Used for embedding the encrypted message into an image.
    - Ensures that the hidden message is not easily detectable in the image.
5. **Graphical User Interface (GUI):**
    - Developed using Tkinter for user interaction.
    - Allows users to input a secret message, select encryption methods, and embed/extract messages from images.

4. RESULTS AND DISCUSSION

The invisibility and robustness of the suggested technique are examined in this section. To begin, the best adaptive scaling factor for watermarks with different sizes is determined by analyzing the scaling factor across NC, PSNR, and SSIM. In the trials, the adaptive optimum scaling factors of watermarks with different sizes are employed. Subjective eye observation and objective quantitative analysis are used to detect the suggested method's invisibility and resilience. Furthermore, a variety of assaults with varying characteristics are employed to test the resilience. Finally, the suggested method's invisibility and robustness are compared to previous studies.

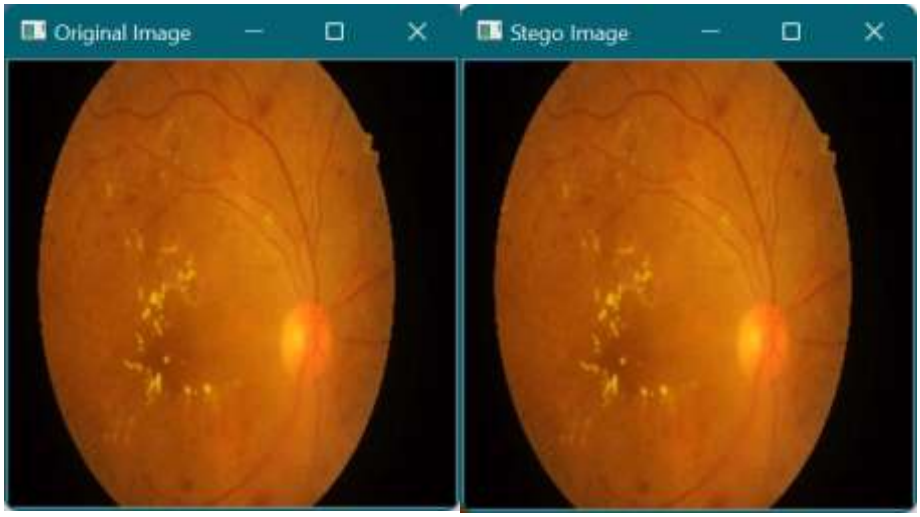

Figure 2: Original image and stego image (after embedding the secrete data).

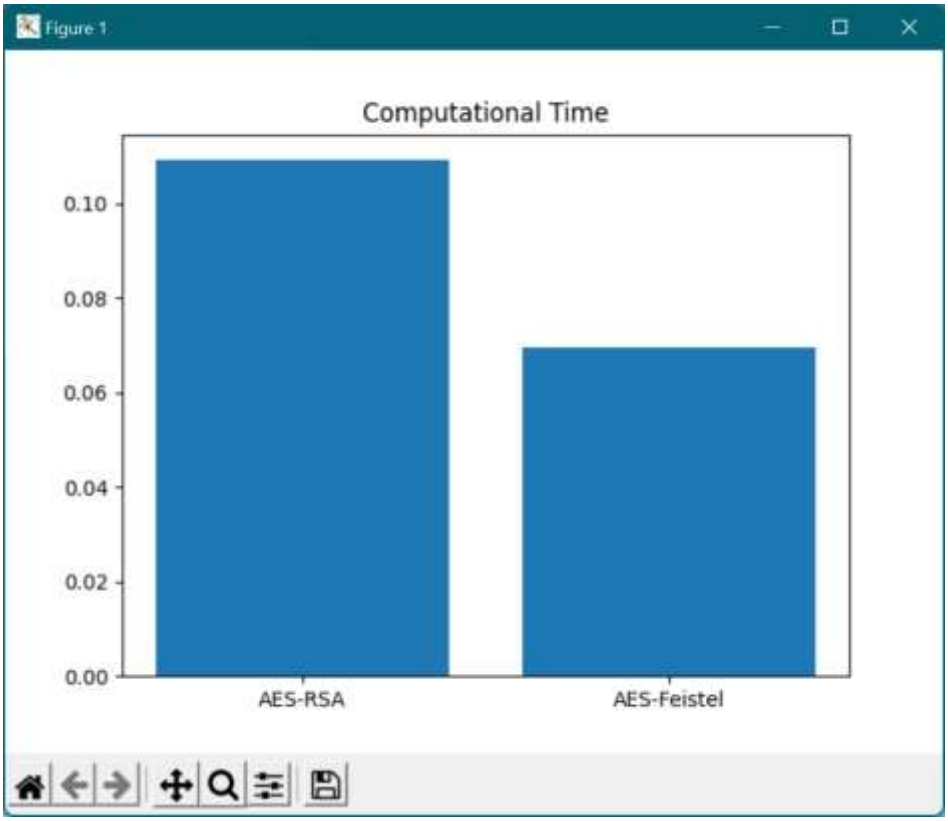

Figure 3: Performance comparison of computational time.

5. CONCLUSION

This project successfully implements a secure, lightweight model-based medical data transmission system designed for IoT-based healthcare environments. By integrating AES and Feistel encryption algorithms with Discrete Wavelet Transform (DWT) for data embedding, the system ensures robust confidentiality and integrity of sensitive medical data during transmission. The graphical user interface (GUI) facilitates user interaction, making the encryption, embedding, and extraction processes intuitive and accessible. Key findings from the project include enhanced security through the combination of AES for symmetric encryption and Feistel for alternative encryption, offering a double layer of protection that makes unauthorized data access extremely difficult. The use of DWT for data embedding

further ensures that the encrypted message is securely hidden within an image, enhancing data stealth. Additionally, the AES-Feistel hybrid encryption method demonstrated superior performance in terms of computation time compared to the AES-RSA method, reducing the computational load and making the system suitable for resource-constrained IoT devices in healthcare environments. The PSNR and MSE values indicate that the embedding process maintains the quality of the stego image, ensuring that the hidden message does not significantly distort the image.

REFERENCES

[1] Humayun, M., Jhanjhi, N. & Alamri, M. (2020). IoT-based Secure and Energy Efficient scheme for E-health applications. Indian J Sci Technol, 13(28), 2833-2848.

[2] Almulhim, M., & Zaman, N. (2020, February). Proposing secure and lightweight authentication scheme for IoT based E-health applications. In 2018 20th International Conference on advanced communication technology (ICACT) (pp. 481-487).

[3] Mallikarjuna, B., Kiranmayee, D., Saritha, V., & Krishna, P. V. (2021, June). Development of efficient e-health records using iot and blockchain technology. In ICC 2021-IEEE International Conference on Communications (pp. 1-7). IEEE.

[4] Ben Dhaou, Imed, Mousameh Ebrahimi, Meriam Ben Ammar, Ghada Bouattour, and Olfa Kanoun. 2021. "Edge Devices for Internet of Medical Things: Technologies, Techniques, and Implementation" Electronics 10, no. 17: 2104. https://doi.org/10.3390/electronics10172104

[5] Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuhaya, M. A. M., Bairagi, A. K., Khan, M. A., & Kee, S. H. (2022). IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review. Healthcare (Basel, Switzerland), 10(10), 1993.

[6] Alkhabet, M.M., Ismail, M. Security algorithms for distributed storage system for E-health application over wireless body area network. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-020-02733-1

[7] Hussain, A., Ali, T., Adeelaziz, F., Draz, U., Irfan, M., Yasin, S., ... & Alqhtani, S. (2021). Security framework for IoT based real-time health applications. Electronics, 10(6), 719.

[8] Dhatterwal, J.S., Kaswan, K.S., Baliyan, A., Jain, V. (2022). Integration of Cloud and IoT for Smart e-Healthcare. In: Mishra, S., González-Briones, A., Bhoi, A.K., Mallick, P.K., Corchado, J.M. (eds) Connected e-Health. Studies in Computational Intelligence, vol 1021. Springer, Cham. https://doi.org/10.1007/978-3-030-97929-4_1

[9] Denis, R., Madhubala, P. Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimed Tools Appl 80, 21165–21202 (2021). https://doi.org/10.1007/s11042-021-10723-4