An Efficient Multilayer approach for Securing E-Healthcare Data in Cloud using Crypto – Stego Technique

NAGAMANY ABIRAMI[1] , M.S. ANBARASI[2]
[1]Department of Computer Science and Engineering, Puducherry Technological University
Puducherry, INDIA
[2]Department of Information Technology, Puducherry Technological University
Puducherry, INDIA

Abstract: — Healthcare data has been moving to cloud platforms in recent years, which has increased accessibility and scalability but also raised security issues. Ensuring data integrity and safeguarding private health information from unwanted access are critical. This paper presents a comprehensive strategy to integrate effective Elliptic Curve Cryptography ECC-AES with steganography techniques to improve the security of healthcare data in the cloud. ECC-AES is especially well-suited for cloud situations with limited resources since it provides strong security with reduced key sizes. Confidentiality is guaranteed by encrypting healthcare data using ECC- AES before storage, reducing the possibility of data breaches. Steganography techniques are also integrated to improve security against skilled adversaries by adding an extra degree of obfuscation by concealing encrypted data inside innocuous files or images. Strict key management procedures, access control systems, and frequent security audits are important components of the proposed system that ensure adherence to Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) compliance requirements pertaining to healthcare data protection. Programs for employee awareness and training are also crucial for reducing the likelihood of human mistakes. Healthcare businesses can safely use cloud technology while protecting patient data integrity and privacy by putting in place multi-layered security safeguards. The proposed system provides the multilayer security on healthcare data in cloud environment than other existing systems.

Key-words—ECC, AES, Healthcare Data, Cloud Computing, Cryptography, Steganography, Encryption, Data Privacy

Received: March 14, 2024. Revised: August 17, 2024. Accepted: September 15, 2024. Published: October 14, 2024.

1. Introduction

The spectrum of completely integrated services and solutions that satisfy various socio-industrial demands has expanded due to the exponential rise of software and sophisticated hardware systems. Out of all the most recent emergent applications, data transmission and its allied forces in the exchange of knowledge have garnered widespread favour worldwide [1]. However, the rapid advancement of internet technology and its associated applications has given rise to a number of breakthroughs, including cloud computing and the Internet of Things (IoT). However, companies have traditionally faced difficulties in guaranteeing safe communication across diverse application contexts [2]. Many communication technologies that enable the Internet are used on a daily basis for a variety of purposes, including social networking sites, the medical services industry, e-commerce, Organizations of scientific community, the business sector, and many other industrial demands like monitoring and security systems [3].

Data transmission was transformed by the increased bandwidth and data rates of optical fiber communication and 4G/5G cellular technology. Data communication over the internet in the form of text, photos, audio, and video is now commonplace [4]. Governments, Agencies of law enforcement, and hospitals are exchanging multimedia data for telemedicine purposes. There was an increase in internet traffic throughout the lockdown in worldwide at the time of the COVID-19.Despite the fact that using the internet has many benefits, security and data privacy are still problems [5]. Hackers may now access a wide range of tools, data theft, modifications, and revisions are now feasible. As a result, maintaining data security has emerged as a difficult yet crucial problem for researchers. To solve data security challenges, a variety of information-protecting procedures have been proposed, including data concealing techniques and cryptography. Cryptography disintegrates and transforms the confidential information into a format that is unintelligible to an unapproved individual. Standard encryption methods or chaos-based encryption methods can be used for cryptography. Prior to embedding, the crucial data in these methods is encrypted using the secret key. However, the primary drawback of SETs—which renders them unreliable and unsecure for data encryption—is the volume of data with key lengths [6].

The chaos-based encryption techniques have helped to overcome the SETs' drawback. The original encryption keys used in the chaos encryption approach are susceptible to modifications. Therefore, more safe cryptographic techniques to guarantee data security are chaos-based encryption schemes. By using encryption to alter the original data's shape, cryptography can offer a high level of data security. However, cryptography by

itself is not impervious to security breaches because its encrypted form draws the attention of attackers and can thus be altered or compromised [7]. Encrypted shape could attract the curiosity of an eavesdropper; it is not a suitable way to ensure data security. As a result, data masking has been extensively employed by academics to conceal the presence of crucial data to stop drawing the attention of outsiders [8].

The IoT has advanced to the point that almost anything may be accessible at any time, from any location, and can perform almost any function. In order to enable cooperative computing scenarios, the IoT is typically made up of small components that are connected to one another. The cost of energy, connection of devices and processing power are some of the IoT's constraints. Medical devices ability to integrate IoT capabilities which improves service quality and efficiency, the healthcare industry has adopted IoT at a faster pace than others [9].

S-health, or smart health, is the situational enhancement of telehealth in intelligent cities, allowing for accurate and effective prevention of illness and accidents. Recently, the disease-centered approach by healthcare management has given way to the patient-centered approach globally. Because of how simple it is to handle and distribute health data, it has become ingrained in the medical industry. It allowing for continual monitoring of physiological conditions, long-term illness proposed, and therapy instruction [10].

Up until that point, s-health can reduce medical costs and raise the standard of service. Even though s-health is still in its early stages, a lot of problems still need to be resolved before it can be applied in practical situations. Individuals are becoming increasingly concerned about hacking attempts in the s-health industry and safeguarding the confidentiality and safety of highly sensitive individual healthcare information of the IoT users without sacrificing the data's usefulness remains a difficulty [11]. However, most access control systems only offer coarse-grained access limits or undermine data security. According to this logic, end-to-end data secrecy can be secured using sharing key mechanisms, but they are insufficient in these novel situations. This feature specifies the conditions that a subject needs to fulfill in order to fully decode a piece of data [12].

Examined the creation of a homomorphic encryption algorithm for the first time in that year. Numerous attempts by scholars to design homomorphic systems with different operations led to the development of this idea. Homomorphic encryption is a collection of encryption methods that can be used for a variety of computations on encrypted data. Some of the most common forms of homomorphic encryption include leveled fully homomorphic, partially homomorphic, slightly homomorphic, and absolutely homomorphic. It is possible to do an infinite number of tasks at once with Fully Homomorphic Encryption (FHE). IoT systems need to adhere to stronger security and dependability standards to safeguard people's privacy and confidentiality [13].

No matter its origin or geographic barriers, cloud computing offers real-time computing, data access, and cloud-based decision-making to a wide range of stakeholders. This is one of its primary characteristics. However, until a strong security mechanism is offered, information exchanged between nodes, between users, or throughout the cloud platform is extremely insecure. One of the main issues with cloud computing is how to securely communicate or preserve personal data, especially multimedia (audio, video, and image) [14]. Enabling computational effectiveness is also necessary, as cloud computing necessitates fast and dependable processing to fulfill real-time application requirements. This is in addition to ensuring secure communication [15]. In light of the rapidly increasing needs for computing power and related communication, it represents the guarantee of security, scalability, and manageability in the cloud computing environment. In cloud environments such as social networking, healthcare, etc., facilitating data security has become essential. The intricate architecture of cloud deployments faces serious risks from a loss of vision and control. A more sophisticated security strategy is also required since the elastic boundary of cloud usage causes the security perimeter to constantly shift [16].

2. Literature Survey

Pay-as-you-go model, the cloud makes use of technologies like cryptography and steganography for safeguarding user data transfer. The Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) techniques were the main topics of this work's review of numerous investigations [17]. The author’s primary concern is the hybrid approach combining AES and FHE. Unlike earlier methods, this hybrid strategy is safer, more redundant, and lets the user preserve data. They believe that if AES can encrypt data with 14 cycles using a 256-piece square, then, cloud computing may be able to benefit from this breakthrough as well. A FHE technique serves as the foundation for the second phase's encryption process. Two objectives are achieved by this method: multiplicative homomorphic and additional substance. Only the newly added substance calculations will be utilized by the user. The user is using the private key given that they possess the cipher text obtained through maiden scrambling. The secret key and the content of the Cipher will now be encrypted jointly using additional material homomorphic encryption. The user may safeguard privacy, confidentiality of data, and integrity of data from hackers by employing this method [18].

According to the authors of this paper, encryption makes it possible to send sensitive data across an unprotected channel without running the danger of it being lost or altered by unwanted parties [19]. ECC requires a very tiny key, it is utilized in this paper to encipher data on the cloud. Elliptic Curve uses the least amount of energy since its small key size minimizes computing power. In this work, ECC is used for key production, encryption, and decryption. The report suggests a two-tiered approach to cloud data protection. The data must first be divided into manageable portions

before being encrypted using randomized safe curves. A quantum computing system might may not be in position to compromise data security when the two stages are completed .

Value, Variety, Velocity, Veracity, and Volume—the five Vs.—all need to be taken into account in the healthcare industry since a variety of data, including patient names, birthdates, and vital sign numbers, are frequently collected and must be kept on file for several systems. Daily data collection would produce high velocity, which would cause the volume of data to expand quickly [20]. In a recent study that assessed the variety and volume of health information, developed a digital memory system supporting essential medical services. Its goal is to organize various biological records in an emergency situation and make them easily accessible to the necessary medical personnel [21].

On encrypted data, unrestricted computations such as additions and multiplications are obtainable by FHE producing results that, when decrypted, are exactly akin to the operations on plain data. As a result, cloud infrastructure can function lawfully using encrypted data without requiring any prior decoding [22]. Homomorphic technology began in 1978 with the introduction of asymmetric encryption, and it was who initially presented the concept of homomorphic encryption. RSA is a partial homomorphic method which solely considers operations that are multiplicative [23].

The deficiency in current research is the absence of a thorough security framework that is especially designed to meet the special needs of healthcare data in cloud systems. Although there is a wealth of literature on cryptography and general cloud security, there is a conspicuous lack of research that focuses explicitly on tackling the security concerns associated with processing and storing healthcare data in the cloud.

Previous research frequently fails to take into account the complex needs and legal limitations that the healthcare sector faces, which results in security solutions that might not be able to sufficiently safeguard patient data that is sensitive or guarantee adherence to laws like HIPAA and GDPR. Furthermore, even while encryption methods like RSA are frequently used to safeguard data, they are not the best choice as for as cloud environments where performance and efficiency are crucial due to their computational overhead and scalability problems [27].

Moreover, not much study has been done on combining steganography and sophisticated cryptographic methods such efficient ECC to offer multi-layered cloud security for medical data. Enhancing data confidentiality, integrity, and obfuscation through the combination of these strategies can reduce the likelihood of tampering, illegal access, and data breaches [28]. The creation of a thorough security architecture that takes into account the particularities of healthcare data, incorporates effective cryptography methods designed for cloud systems, and guarantees regulatory compliance is necessary to close this research gap. Future research can greatly advance cloud security for healthcare data and enable healthcare companies to use cloud technology safely and efficiently by bridging this gap [29].

3. Proposed System

The goal of the proposed system is to create a multilayer security framework that is especially made to safeguard medical data that is processed and stored in cloud environments. The core of this strategy is the combination of steganography and efficient ECC-AES aims to leverage cloud computing's scale and flexibility while addressing the particular security concerns associated with healthcare data. Compared to conventional encryption methods, efficient ECC-AES provides strong encryption with reduced key sizes, which makes it a good fit for cloud environments with limited resources. The framework guarantees data confidentiality and reduces the possibility of unwanted access or data breaches by encrypting healthcare data using ECC-AES. The framework uses steganography techniques in addition to encryption to even more obfuscate the existence of sensitive healthcare data.

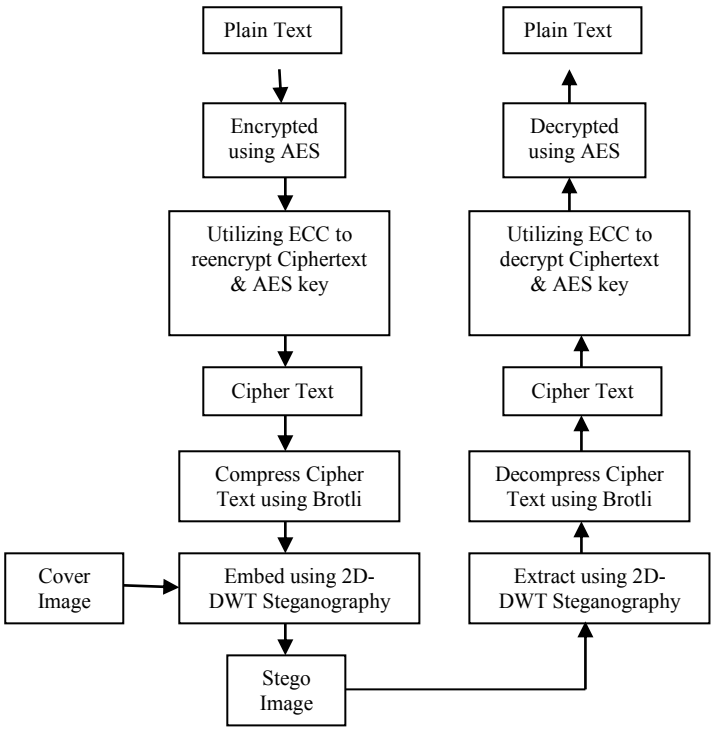

Fig.1. Framework for Multilayer Approach for Securing E-Healthcare Data

Strict key management procedures, strong access restrictions, and assurances of compliance to meet HIPAA and GDPR regulations are important parts of the proposed system shown in Figure 1. Maintaining the integrity and efficacy of the security measures also requires regular personnel training programs and security audits. The overall goal of the research is to close the gap in the literature by offering a complete security solution that is especially designed to meet the special needs of healthcare data in cloud environments. The framework aims to provide better protection against tampering, unauthorized access, and data breaches by combining steganography and efficient ECC. This will allow healthcare organizations to safely utilize cloud technologies for increased productivity and patient care.

Medical information poses the highest security risk in the experience of the medical business. Through the use of IOT devices hackers can use botnets to obtain patient information shown in Figure 2. For this reason, the safeguarding of IoMT devices security and medical data is essential. Modern communication techniques require the right information to be sent at the right moment to the right recipient. Patient records are safe and secured, this is significantly more necessary for individually identifiable medical information. A constantly evolving threat landscape, driven by sophisticated intrusion objectives, a growing number of security vulnerabilities and unskilled and unaware employees handling these private records often pose a threat to the sharing and safe storage of medical records. Healthcare records are typically protected/concealed using conventional cryptographic and steganographic methods, though these methods often suffer from failure of prompt executions.

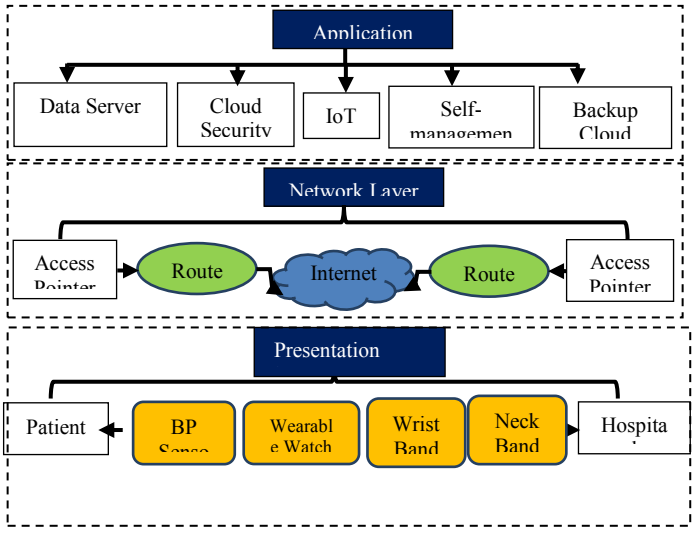

Fig. 2. Multi-layer Model

3.1 Steganoraphy

To make the secret image more secure from hackers and other attackers, it is incorporated within the cover image. An RGB image of a natural scene serves as the cover image. The YCbCr format is created from the RGB colour-secured image using the equations provided.

[Y Cb Cr]= [0 128 128] + [0.298 0.588 0.115 -0.170 -0.332 0.499 0.499 -0.420 -0.082]. [R G B]

The hidden image will be embedded in the luminance image plane (Y), leaving the other two image planes (Cb and Cr) unchanged. Grayscale medical imaging makes up the hidden image. Using the thresholding approach, this hidden grayscale image is transformed into a binary image. Depending on the threshold value, the thresholding process turns the pixels in the hidden images to either black or white. In this study, global thresholding is utilized to produce a binary image.

LSB approach is used to incorporate this binary secret image into the cover image. The preferred method for securing spatial domain images is LSB steganography.

a) Brotli Technique

Brotli is a good compression algorithm for handling data with numerous pattern and characters. These identical characters are summarized into same block. During the compression, this technique divides the text data into small blocks. Each block is then compressed separately and then encoding algorithm is applied which is Huffman coding, providing shorter codes to enhance the efficiency of the compression process.

The decompression process involves the Brotli decompression functions which includes Huffman decoding, Output buffering and sliding window. The Huffman decoding is used to restore the representation of symbols into their original values. The output buffering is used to store the decompressed data, and then the sliding window is used to track context during the decompression process.

b) Discrete Wavelet Transform (DWT)

Proposed approach used a DWT with a mother wavelet from HAAR. Applied 2D-DWT-2L on the image's row (blocks), which was designed as a sequential transformation process with the aid of low pass and high pass filters. It should be mentioned that level-2 coefficients were taken into consideration for embedding in the proposed 2D-DWT-2L idea. This was done primarily because

level-2 coefficients can offer a sizable local characteristic set for text-embedding sans adversely affecting the quality of the image.

Single-layer embedding can affect post-embedding image quality and result in increased visibility or perceptibility. Conversely, embedding at a higher level coefficient may yield better results, but at the expense of additional processing, which may not be appropriate given the needs of modern real-time applications. For this reason, we only used a 2-level DWT coefficient for embedding in this paper. The outcomes of this method are broken down in relation to the image's columns. Figures 3 a brief overview of this procedure.

The secret data T, which has already been processed as cipher data is inserted using LSB embedding to create stego image S. Even in the face of cloud attack scenarios like RS-Analysis or Steganalysis, our proposed solution aims to maintain optimal pixel adjustment to maintain maximum feasible imperceptibility, quality preserve, and continuous transmission.

Our proposed approach splits the original source image, also known as the cover-image, into several 8 × 8 blocks after processing it with HAAR-DWT. A secured database is required in homoeopathic or healthcare institutions to provide dependability and security. Healthcare networks might experience negative consequences like a denial of service due to security and privacy issues. A single component may be more severely impacted by some vulnerability than by other.

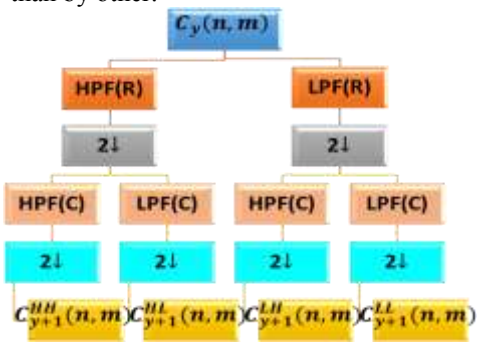

Fig. 3. 2D-DWT-2L Decomposition process

3.2 Algorithm – Hybrid Model

Data encryption using a multilayer security approach with ECC involves several steps to ensure robust protection against unauthorized access and data breaches. Here's an outline of the process:

Step 1: Key Generation

- Choose a suitable elliptic curve and base point G.
- AES: Generate AES symmetric encryption key Key_{AES}
- ECC: Generate ECC key pair (private key: Pr_{ECC} public key: Pu_{ECC}

Step 2: Encryption

AES Encryption

- Encrypt M using AES with key K_{AES}, resulting in cipher text $C_{AES.}$

ECC Encryption

- Compute Secret key $S=Pu_{ECC}*G$, where G is the generator point on the elliptic curve.
- Encrypt the Cipher text of C_{AES} and AES Key
- $C_{ECC}=C_{AES}*S_{AES}$

Step 3: Embed Encrypted Text into Cover Image using Steganography

Compression:

- The Cipher text data will be encoded using Brotli Algorithm. Then converted from UTF-8 to base64, transferring the data into hexadecimal format, finally the hexadecimal converted into Binary.
- The final output will be compressed text data in binary form.

Embedding:

- Compute 2D-wavelt transform of cover image. It produces four bands such as: LL, LH, HL and HH.
- Select LL sub-band for embedding procedure, this will be done using 2D-DWT technique.

Step 4: Extract the secret message from Stego Image using reverse process:

- Extraction procedure will be done using 2D-DWT, the bits will be extracted and grouped into binary form.
- The outcome will be converted into hexadecimal form and then decoded from base64 to obtain the compressed text data using Brotli.

Step 5: Decryption

ECC Decryption

- Compute Secret Key S = PrECC*G
- Compute C_{ECC}=C*S and AES Key

AES Decryption

- Compute Message=CECC*Key_{AES}

4. Performance Analysis

The proposed method used to look at an item is called ex-ante evaluation; it involves looking at the artefact before it is utilized and not evaluating it in a real-world environment. This proposed system approach assesses the artefact based on theoretical or speculative scenarios. The operations and strategies needed to successfully finish the processes of decryption and encryption were made available to us after installing these libraries data. Proposed model needed text data to be saved as an image file so that the AES and RSA algorithms could encrypt it.

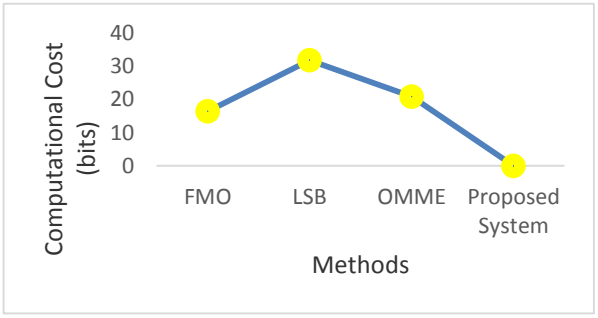

Fig. 5. Computational Cost between Existing and Proposed Method

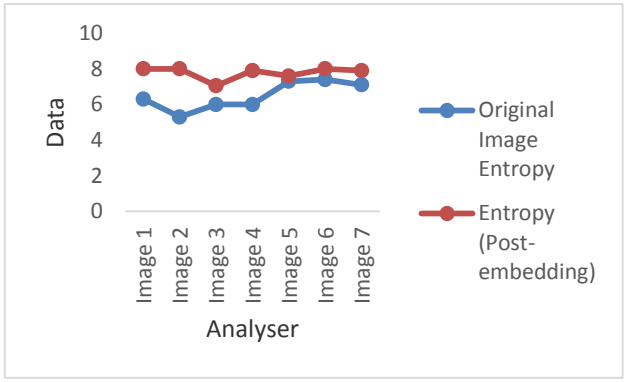

Fig.6. Image Entrophy Analysis

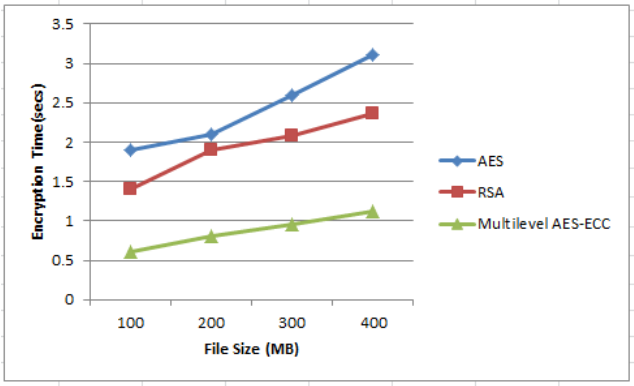

Fig.6. Encryption Time

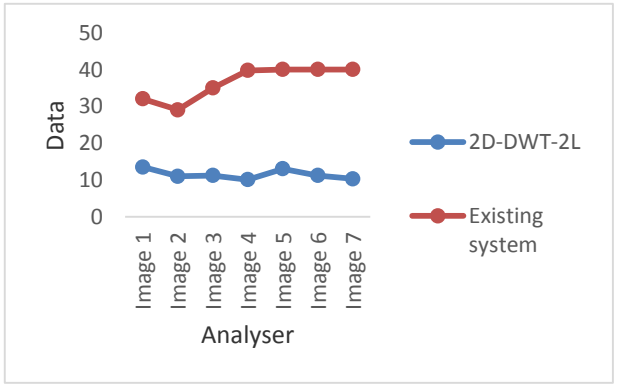

Fig. 7. Embedding Capacity Analysis

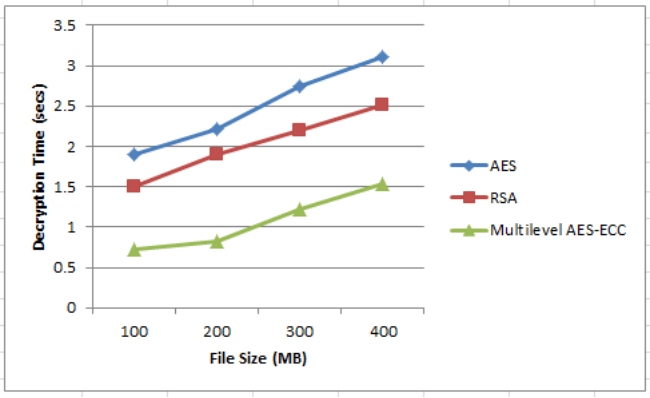

Fig. 7. Decryption Time

TABLE 1. COMPUTATIONAL COST EXISTING VS PROPOSED

Protocols	Computational Cost (bits)
FMO	16.410
LSB	31.8193
OMME	20.8795
Proposed System	11.97.33

4. Conclusion & Future Work

By integrating various symmetric encryption and steganography methods, the system offers several security levels that improve secrecy and Efficiency. Resource constrained cloud systems can benefit from ECC because of its effective encryption skills, which allow smaller key sizes to be generated sans sacrificing protection. Following the creation of shareable hidden keys and ephemeral keys, the encryption procedure yields a symmetric key that is derived from a hash function of cryptography. The E-Health data is subsequently encrypted using this symmetric key, guaranteeing privacy throughout storage. Steganography provides another degree of obscurity by

embedding the cipher text inside seemingly innocent documents or images, thereby rendering it harder for attackers to find or alter the information. The algorithm offers a thorough approach to safeguarding E-Health data in cloud environments, tackling the intricate security issues that arise with healthcare data governance.

In Future, checking the scalability of the proposed model using different kinds of biomedical images with other modalities. Introducing the various threats like image rotation, resizing, tampering, etc., and evaluating the performance analysis.

References

[1] Gadde, S., Amutharaj, J., & Usha, S., "A security model to protect the isolation of medical data in the cloud using hybrid cryptography", Journal of Information Security and Applications, Vol.73, March 2023.

[2] Padma Vijetha Dev, B., & Venkata Prasad, K., "An Adaptive Lightweight Hybrid Encryption Scheme for Securing the Healthcare Data in Cloud-Assisted Internet of Things", Wireless Personal Communications, Vol.130.Issue.4, pp:2959-2980, June 2023.

[3] Sneha Chaturya, A, "Enhancing Data Security through Innovations in AES-FBC Encryption and DWT Steganography". International Journal of Engineering Science and Advanced Technology, Vol.24.Issue.1, pp: 43-53, Oct.2017.

[4] Sasikumar, K., & Nagarajan, S., "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing", IEEE Access, pp:1-29, Jan.2024

[5] Awadh, W. A., Hashim, M. S., & Alasady, A. S., "Implementing the Triple-Data Encryption Standard for Secure and Efficient Healthcare Data Storage in Cloud Computing Environments", Informatic, Vol.48Issue.6, April 2024.

[6] Kumar, K. P., Prathap, B. R., Thiruthuvanathan, M. M., Murthy, H., & Pillai, V. J., "Secure approach to sharing digitized medical data in a cloud environment", Data Science and Management, Vol.7,Issue.2, pp:108-118,Dec2023.

[7] Abiodun, M. K., Imoize, A. L., Awotunde, J. B., Lee, C. C., Adeniyi, A. E., Chioma, U., & Li, C. T., "Analysis of a Double-stage Encryption Scheme Using Hybrid Cryptography to Enhance Data Security in Cloud Computing Systems", Journal of Library & Information Studies, Vol.21, Issue.2, pp:1-26, Dec.2023 .

[8] Awadh, W. A., Alasady, A. S., & Hashim, M. S., "A multilayer model to enhance data security in cloud computing". Indonesian Journal of Electrical Engineering and Computer Science, Vol.32, Issue.2, pp: 1105-1114, Nov.2023.

[9] Nahar, M., Kamal, A. H. M., & Hossain, G., "Protecting health data in the cloud through steganography: A table-driven, blind method using neural networks and bit-shuffling algorithm", Journal of Network and Computer Applications, Vol.217, July.2023.

[10] Ali, S., & Anwer, F., "Secure IoT framework for authentication and confidentiality using hybrid cryptographic schemes", International Journal of Information Technology, pp: 1-15,Feb.2024.

[11] Selvaraj, J., Lai, W. C., Kavin, B. P., & Seng, G. H., "Cryptographic encryption and optimization for internet of things based medical image security", Electronics, Vol.12, Issue.7, Mar.2023.

[12] Madhu, D., & Vasuhi, S., "Lightweight Encryption Assisted Man-in-The-Middle Attack-Resilient Steganography Model for Secure Satellite Imagery Services: LEMARS", Journal of Intelligent & Fuzzy Systems, pp: 1-23, May.2023.

[13] Nadhan, A. S., & Jacob, I. J., "Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications", Biomedical Signal Processing and Control, Vol.88, Feb.2024.

[14] El-Shafai, W., Khallaf, F., El-Rabaie, E. S. M., & El-Samie, F. E. A., "Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services" Journal of Ambient Intelligence and Humanized Computing, Vol.15, Issue.1, pp:1-28, July.2022.

[15] Goswami, C., Tamil Selvi, P., Sreenivas, V., Seetha, J., Kiran, A., Talasila, V., & Maithili, K., "Securing healthcare big data in industry 4.0: cryptography encryption with hybrid optimization algorithm for IoT applications", Optical and Quantum Electonics, Vol.56, Issue.3, Dec.2023.

[16] Goyal, A., Gupta, A., Chaurasia, K., & Bansal, A., "Assured Unlock: A Mobile App for Dual-Layer Encryption to Enhance Data Security", 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE, pp. 514-519, Jan.2024.

[17] Reddy, M. I., Reddy, M. P., Reddy, R. O., & Praveen, A., "Improved elliptical curve cryptography and chaotic mapping with fruitfly

optimization algorithm for secure data transmission", Wireless Networks, pp:1-14, Nov.2023

[18] Sai, B. M., & Bhatia, M., "A Survey on IoT Security Using Cryptographic Algorithms", In E3S Web of Conferences, Vol. 453, pp:1-8, Nov.2023.

[19] Lishomwa, K., & Zimba, "A Privacy-Preserving Scheme for Medical Diagnosis Records Based on Encrypted Image Steganography", Zambia ICT Journal, Vol.7, Issue.1, pp: 23-28, Mar.2023.

[20] Ali, N. A. M., Mohammed, S. G., Mohammed, F. G., & Ali, F. A. M. "Comprehensive on Exploring Advanced Ciphering for Enhanced Data Protection", Wasit Journal for Pure Sciences, Vol.2, Issue.4, pp:116-129, Dec.2023.

[21] Yan, F., Li, N., Iliyasu, A. M., Salama, A. S., & Hirota, K., "Insights into security and privacy issues in smart healthcare systems based on medical images", Journal of Information Security and Applications, Vol.78, pp:2214-2126, Oct.2023.

[22] Pothireddy, S., Peddisetty, N., Yellamma, P., Botta, G., & Gottipati, K. N. "Data Security in Cloud Environment by Using Hybrid Encryption Technique: A Comprehensive Study on Enhancing Confidentiality and Reliability", International Journal of Intelligent Engineering & Systems, Vol.17, Issue.2, pp: 159-170, Dec.2023.

[23] Odeh, A., & Taleb, A. A., "A Multi-Faceted Encryption Strategy for Securing Patient Information in Medical Imaging", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.14, Issue.4, pp:164-176, Dec.2023.

[24] Masdari, M., Band, S. S., Qasem, S. N., Sayed, B. T., & Pai, H. T., "ECG Signals-Based Security and Steganography Approaches in WBANs: A Comprehensive Survey and Taxonomy", Sustainable Computing: Informatics and Systems, Nov.2023.

[25] Sutradhar, S., Karforma, S., Bose, R., & Roy, S., "A dynamic step-wise tiny encryption algorithm with fruit fly optimization for quality of service improvement in healthcare. Healthcare Analytics", pp: 1-153, April.2023.

[26] Ahmad, I., Qudus, F., Qadir, M., Shah, S., Atif, M., Islam, M., & Jan, S., "Securing the Next Generation Cloud: A Survey of Emerging Technologies and their Impact on Cloud Security", The Sciencetech, Vol.4, Isuue.4, pp: 44-70, Dec.2023.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0
https://creativecommons.org/licenses/by/4.0/deed.en_US