Assessing the Efficacy of Lightweight Encryption Methods for Protecting Medical Imaging Data in Internet of Medical Things (IOMT) Environment

Mekala Rohith
College of Engineering & Comp. Sci.
Syracuse University
Syracuse, New York, USA
rmekala@syr.edu

Mergoju Anoushka
College of Engineering & Comp. Sci.
Syracuse University
Syracuse, New York, USA
amergoju@syr.edu

Nachireddi Sreeram
College of Engineering & Comp. Sci.
Syracuse University
Syracuse, New York, USA
snachire@syr.edu

***Abstract*—In the rapidly evolving landscape of the Internet of Medical Things (IoMT), the protection of sensitive medical imaging data such as X-rays, MRIs, and CT scans poses a significant challenge. This project aims to assess the efficacy of lightweight encryption methods in securing this critical data, a task of paramount importance in the context of limited resources and stringent privacy concerns inherent to IoMT environments. Our research undertakes a comprehensive analysis of various lightweight encryption techniques, evaluating their suitability and effectiveness for IoMT applications by comparing their performance with traditional cryptographic techniques. We focus on key performance indicators including encryption and decryption speed, resource utilization (CPU and memory), and resilience to common attack vectors. Through a blend of theoretical research and practical experimentation, this study seeks to offer valuable insights into the challenges and opportunities associated with implementing encryption in IoMT. The outcome of our research aims to contribute to the development of more secure, efficient, and compliant encryption practices for protecting medical imaging data within IoMT frameworks.**

***Index Terms*—lightweight encryption, internet of medical things, cryptography techniques**

I. INTRODUCTION

In the era of digital healthcare transformation, the Internet of Medical Things (IoMT) stands at the forefront, revolutionizing the way medical data, particularly sensitive imaging like X-rays and MRIs, is managed and utilized. However, this technological advancement brings forth significant challenges in securing and protecting this critical data against various cyber threats. This report delves into the heart of this challenge, focusing on the assessment and application of cryptographic solutions suitable for IoMT contexts.

With IoMT devices often constrained by limited computational resources, traditional encryption methods may prove inadequate, potentially impeding the timely processing and transmission of crucial medical data. This scenario underscores the urgent need for lightweight cryptographic methods that are not only resource-efficient but also robust in security. Our research specifically explores various lightweight encryption techniques, evaluating their effectiveness and suitability for IoMT applications.

This research aims to contribute to the evolving field of IoMT by presenting a comprehensive analysis of these cryptographic solutions. Through this, we aspire to advance the development of secure, efficient, and compliant encryption practices that safeguard medical imaging data, thereby enhancing the reliability and trustworthiness of IoMT systems in healthcare.

II. PROBLEM DEFINITION

The integration of medical imaging technologies into the Internet of Medical Things (IoMT) has revolutionized healthcare, offering unprecedented opportunities for diagnosis and treatment. However, this advancement brings with it a critical challenge: ensuring the security and privacy of sensitive medical imaging data. As IoMT devices are often limited in their computational resources and power, traditional encryption methods may not be suitable, potentially causing delays in data processing and transmission, which is unacceptable in healthcare scenarios where timely access to data can be critical.

The problem, therefore, lies in finding and implementing lightweight encryption methods that not only provide robust security against various cyber threats but also operate efficiently within the resource constraints of IoMT devices. This study focuses on identifying, testing, and evaluating such encryption methods to determine their efficacy in protecting medical imaging data while maintaining compliance with legal and ethical standards, and ensuring minimal impact on the performance and usability of IoMT systems.

A. Significance

This project holds significant importance in the context of the burgeoning field of the Internet of Medical Things (IoMT). As medical imaging devices increasingly connect to the internet, the security of sensitive medical data becomes paramount. The significance of this research lies in its focus on lightweight encryption methods that are uniquely suited for IoMT environments. By addressing the specific challenges

of data security in the context of limited computational resources and strict privacy regulations, this study contributes to the safeguarding of critical healthcare data. The implications of this research extend beyond academic interest, offering practical solutions that can be implemented in real-world IoMT applications. This ensures that healthcare providers can leverage the benefits of IoMT without compromising on data security and patient privacy.

B. Novelty

The research presents novel methodologies in the field of lightweight encryption, including the incorporation of Block-Based Transformation, Combination Technique, and a Proposed Algorithm, in addition to well-established lightweight approaches such as ChaCha20, Salsa20, and RC4. This combination provides new perspectives on the efficacy of both innovative and conventional approaches in Internet of Medical Things (IoMT) settings.

1. Concentrated examination of medical imaging data: This study stands out due to its specific emphasis on medical imaging data in the context of the Internet of Medical Things (IoMT), effectively addressing the security requirements and the constrained processing capabilities of these systems.

2. Comprehensive Performance Evaluation: Our research provides a distinct assessment of both encryption/decryption speeds and entropy. However, it only compares entropy among lightweight approaches. This comprehensive review offers a balanced viewpoint on the effectiveness of these encryption techniques in the context of the Internet of Medical Things (IoMT). These innovative components contribute to the discipline by improving the comprehension of how lightweight encryption can be efficiently employed in the Internet of Medical Things (IoMT) sector, specifically for safeguarding confidential medical information.

III. LITERATURE SURVEY

A comprehensive literature survey has highlighted the growing interest in lightweight cryptographic solutions within the Internet of Things (IoT) and the Internet of Medical Things (IoMT) fields. Research such as [1] brings forth innovative block-based encryption methods tailored for IoMT, focusing on computational efficiency and image security. It goes beyond traditional encryption techniques by offering a solution that is not only highly secure but also optimized for computational efficiency. This is crucial in the context of IoMT where processing power and speed are often limited.

The paper [2] introduces a novel cryptographic approach for health monitoring in IoT, striking a balance between energy efficiency and data security, notably using AES-128 encryption and lightweight hashing. This approach is particularly relevant for continuous health monitoring systems where energy conservation and data integrity are paramount.

The exploration extends to [3] which advocates for adaptive, resource-efficient security protocols, emphasizing the integration of machine learning for diverse IoT devices. The integration of machine learning algorithms allows for a more responsive and intelligent security system, making it a significant contribution to the field of IoT security.

The complexities of IoT design and security are discussed in [4] emphasizing the need for lightweight cryptographic solutions adaptable to varied device capabilities. By providing a comprehensive overview of the challenges and potential solutions, this paper serves as a crucial guide for designers and developers in the IoT domain, emphasizing the need for versatile and robust security strategies.

In [5] the trade-offs between security and computational efficiency in IoT are evaluated. It provides an extensive evaluation of various cryptographic algorithms, highlighting their strengths and weaknesses in terms of security features and the computational resources they require. This paper is particularly valuable for those seeking to understand the balance needed between maintaining high-security standards and ensuring efficient performance in IoT devices.

This comprehensive review performed in [6] explores various encryption methods used in IoT, focusing on the intricate balance between computing requirements and security. It evaluates different encryption techniques, offering insights into their suitability for various IoT applications. The paper emphasizes the necessity of finding balanced cryptographic solutions that cater to the unique demands of IoT environments, contributing significantly to the ongoing discourse on IoT security.

Nevertheless, our research makes a substantial contribution to the current body of knowledge in this sector. Although the aforementioned studies highlight the significance of lightweight cryptographic solutions on the Internet of Things (IoT) and Internet of Medical Things (IoMT), our research stands out by offering a thorough comparative analysis of different algorithms and their appropriateness for safeguarding sensitive medical data in practical IoMT applications. Our research presents innovative approaches in the domain of lightweight encryption, which involve the integration of Block-Based Transformation, Combination Technique, and a Proposed Algorithm. This combination offers fresh insights on the effectiveness of both groundbreaking and traditional methods in Internet of Medical Things (IoMT) environments.

In addition, our study focuses exclusively on the encryption of medical imaging data, considering the distinct security needs and limited processing capabilities of these devices. Our research provides a comprehensive view of the usefulness of lightweight cryptography in the context of the Internet of Medical Things (IoMT), considering both encryption/decryption speeds and entropy. Together, these inventive elements enhance the understanding of how lightweight encryption might be effectively utilized in the IoMT industry, particularly for protecting sensitive medical data.

IV. METHODOLOGY AND IMPLEMENTATION

In this study, we extended our analysis to include top-performing algorithms from our base paper: Block-Based Transformation, Combination Technique, and the Proposed Algorithm. The ”Block-Based Transformation” algorithm

reorganizes image data into blocks to improve encryption. The ”Combination Technique” integrates many encryption algorithms to enhance security. The ”Proposed Algorithm” is an innovative method specifically designed to optimize the encryption of medical images in the Internet of Medical Things (IoMT), effectively managing resource allocation while ensuring high levels of security. These methods are being developed to enhance encryption mechanisms for medical pictures in Internet of Medical Things (IoMT) environments.

These models, alongside ChaCha20, Salsa20, RC4, Hybrid Encryption (AES+RSA), and 3DES, were evaluated using custom Python scripts for encryption and decryption of a medical image, emphasizing the importance of secure and efficient data processing. This comprehensive approach ensures a thorough comparison of both lightweight and standard cryptographic techniques, highlighting the effectiveness and efficiency of the novel algorithms from our base paper in real-world IoMT applications. The process for each algorithm follows a consistent pattern:

1. Encryption: The image file is first encrypted using the algorithm in question. During this phase, the script records the time taken to complete the encryption process, providing a measure of the algorithm's efficiency.

2. Decryption: Following encryption, the script then proceeds to decrypt the newly encrypted file, again measuring the time taken to complete this process.

3. Entropy Calculation: In addition to speed analysis, the project also delves into the security aspect of each algorithm by calculating the entropy of the encrypted data. Entropy, in this context, is a statistical measure of randomness, which is commonly associated with the unpredictability and thus the security of the encryption method. A higher entropy value generally indicates a more secure encryption.

4. Script Design and User Accessibility: A key consideration in the design of the Python scripts was user accessibility. The scripts are crafted to be straightforward and user-friendly, requiring minimal input from the user - only the path of the image file and, in some cases, the generation of a random key.

5. Comparative Analysis and Visualization: The culmination of the project is a detailed comparative analysis, visually represented through bar graphs. These graphs compare the performance metrics (encryption/decryption speeds and data entropy) of lightweight versus standard encryption methods.

V. RESULTS

A. Lightweight Cryptography Techniques

The tabulated results and visualizations are as follows:

The entropy measurements obtained from our study indicate that ChaCha20, Salsa20, and RC4, which are lightweight encryption approaches, exhibit a high entropy level of 7.99 bits per byte. This high entropy number signifies robust security for these encryption algorithms. The Block-Based Transformation and Combination Technique exhibit entropy values of 6.48 and 6.21 bits/byte, respectively, which are slightly lower than the Proposed Algorithm's high entropy of 7.98 bits/byte.

TABLE I
ENTROPY VALUES OF LIGHTWEIGHT TECHNIQUES

Technique	Entropy(bits/byte)
ChaCha20	7.99
Salsa20	7.99
RC4	7.99
Block- Based Transformation	6.48037
Combination Technique	6.2105
Proposed Algorithm	7.98

B. Graphical Representation of comparison between our proposed lightweight cryptography models

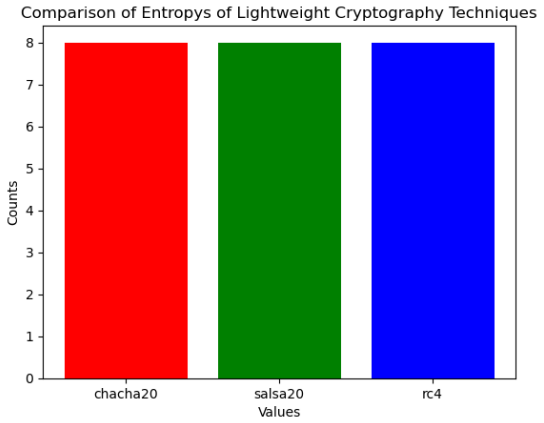

Fig. 1. Comparison of Entropy

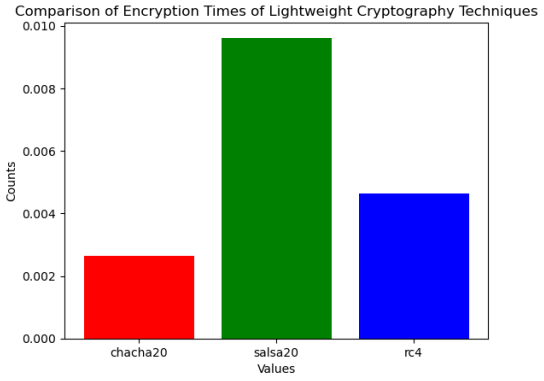

Fig. 2. Comparison of Encryption Times

From the above information and graphs, we can conclude that ChaCha20 is the best algorithm in terms of speed & entropy out of the three algorithms.

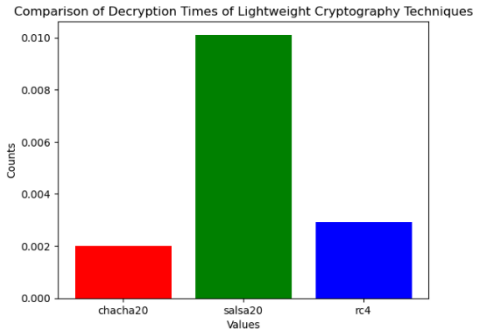

Fig. 3. Comparison of Decryption Times

C. Comparison between our proposed non - lightweight cryptography models

TABLE II
ENCRYPTION AND DECRYPTION OF NON-LIGHTWEIGHT TECHNIQUES

Technique	Encryption Time	Decryption Time
Hybrid Encryption (RSA+AES)	0.0152	0.0159
3DES	0.157	0.156

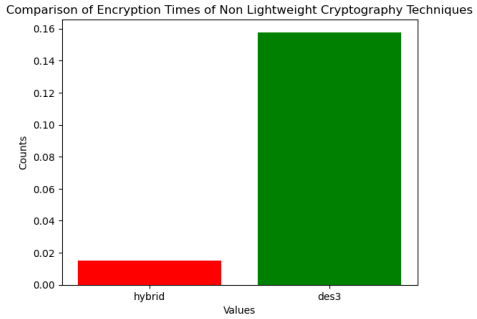

Fig. 4. Comparison of Encryption Times

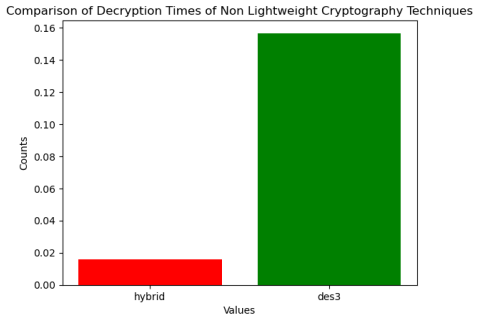

Fig. 5. Comparison of Decryption Times

From the above information and graphs, hybrid encryption is the best in terms of encryption and decryption time out of the two algorithms.

D. Comparison between our best performing models - ChaCha20 & Hybrid Encryption

After identifying ChaCha20 and Hybrid Encryption as the leading algorithms in their respective categories, we directly compared these two to determine the overall superior technique. The visualization for the same is as follows:

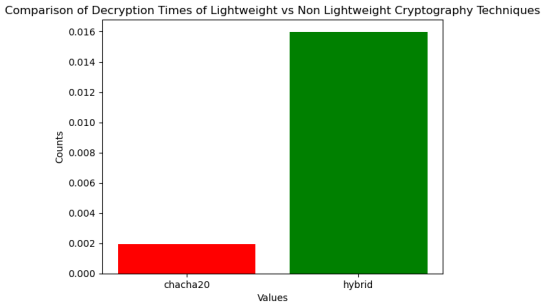

Fig. 6. Comparison of Decryption Times

E. Final Comparison of all techniques considered in our paper

TABLE III
ENCRYPTION AND DECRYPTION TIMES

Technique L - Lightweight NL – Non-Lightweight	Encryption Time	Decryption Time
ChaCha20 L	0.0033	0.0019
Salsa20 L	0.0096	0.10
RC4 L	0.0046	0.0029
Block- Based Transformation L	0.0002	0.0003
Combination Technique L	0.0006	0.0009
Proposed Algorithm L	0.0001	0.0003
Hybrid Encryption (RSA+AES) NL	0.0152	0.0159
3DES NL	0.157	0.156

Our study found that lightweight encryption techniques, particularly the suggested algorithm, exhibited improved performance in terms of encryption and decryption speeds when compared to non-lightweight methods. As an example, the suggested technique demonstrated exceptionally fast encryption and decryption speeds of 0.0001s and 0.0003s, respectively, surpassing the non-lightweight Hybrid Encryption (RSA+AES) which achieved encryption and decryption durations of 0.0152s and 0.0159s. This trend highlights the effectiveness of lightweight algorithms in the context of Internet of Medical Things (IoMT) environments.

VI. CHALLENGES FACED

During our inquiry into the use of lightweight encryption for medical images on the Internet of Medical Things (IoMT), we faced some notable obstacles, all of which we successfully resolved:

1. Algorithm Selection and Implementation: The process of choosing and applying the most appropriate algorithms, including the innovative ones derived from our research, was

intricate due to their distinctive designs. To address this obstacle, we performed a comprehensive evaluation of the merits and drawbacks of each method, taking into account variables such as security, computational efficacy, and suitability for the Internet of Medical Things (IoMT). The team exerted considerable effort to seamlessly include the algorithms, considering the complexities of each design.

2. Metrics for evaluating performance Adjustment: Precisely assessing the durations of encryption/decryption processes and the level of randomness was crucial. We accomplished this by carefully adjusting our Python programs. The calibration method entailed meticulous adjustment of the scripts to achieve accurate timing measurements, enabling us to collect dependable data on the performance of each algorithm. Obtaining precise outcomes was crucial to evaluate their effectiveness.

3. Striking a balance between the stringent security requirements of encrypting medical images and the computing efficiency of IoMT devices is a significant problem. We tackled this issue by performing thorough testing and fine-tuning of the algorithms. We optimized the parameters to strike a perfect equilibrium between security and efficiency, guaranteeing that the encryption procedure adhered to the rigorous standards of medical data protection while minimizing any substantial processing delays on IoMT devices.

4. Data Representation and Interpretation: The task of accurately describing and analyzing the performance data, particularly when comparing it with the models from our reference research, proved to be difficult. In response to this issue, we have devised explicit and thorough data visualization methods, which encompass intricate bar graphs. The visualizations provided a clear and perceptive comparison of encryption/decryption speeds and entropy levels, facilitating the derivation of significant inferences from the data.

In summary, we dedication to comprehensive examination, accurate adjustment, and inventive data visualization allowed us to successfully overcome these obstacles. Our study on lightweight encryption for medical images in the IoMT sector produced significant insights and contributions to the field.

VII. CONCLUSION

Our research article highlights that the models mentioned in the original research paper outperform other models. However, well-established lightweight algorithms like as ChaCha20, Salsa20, and RC4 also demonstrate impressive performance. These traditional lightweight algorithms provide a satisfactory trade-off between speed and security; however, they are significantly surpassed by the innovative techniques in terms of encryption and decryption efficiency. The comparison emphasizes the general advantages of lightweight encryption approaches in effectively handling medical images in IoMT contexts, showcasing its appropriateness for fast and confidential data processing.

VIII. CONTRIBUTIONS

1. Rohith Mekala: Implemented Non-Lightweight Techniques and worked on the Comparitive Analysis

2. Anoushka Mergoju: Implemented Lightweight Techniques and performed the Result Analysis

3. Sreeram Nachireddi: Implemented Lightweight Techniques and executed Visual Representations

Documentation work was divided equally among the members.

REFERENCES

[1] M. K. Hasan et al., "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," in IEEE Access, vol. 9, pp. 47731-47742, 2021, doi: 10.1109/ACCESS.2021.3061710.

[2] A. Chhaybi and S. Lazaar, "Definition of a lightweight cryptographic solution to secure health data on IOT and cloud," General Letters in Mathematics, vol. 10, no. 2, pp. 54–60, 2021, doi: 10.31559/glm2021.10.2.6.

[3] E. R. Naru, H. Saini and M. Sharma, "A recent review on lightweight cryptography in IoT," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 887-890, doi: 10.1109/I-SMAC.2017.8058307.

[4] Y.-S. Kim and G. Kim, "A Performance Analysis of Lightweight Cryptography Algorithm for Data Privacy in IoT Devices," 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2018, pp. 936-938, doi: 10.1109/ICTC.2018.8539592.

[5] M. N. Khan, A. Rao, and S. Camtepe, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4132-4156, March 15, 2021, doi: 10.1109/JIOT.2020.3026493.

[6] I. Batra, A.Kr. Luhach, and N. Pathak, "Research and analysis of lightweight cryptographic solutions for internet of things," in Proc. of the second international conference on information and communication technology for competitive strategies, ACM Other conferences, 2016, Available at: https://dl.acm.org/doi/10.1145/2905055.2905229 (Accessed: 05 November 2023).