

EFFICIENT AND PRIVACY-PRESERVING MEDICAL DATA SHARING IN INTERNET OF THINGS WITH LIMITED COMPUTING POWER USING RSA-BASED HYBRID ENCRYPTION

1Mr. Shubham Sushil Mane, 2Mr. Rajwardhan S. Todkar

1Research Scholar, 2Assistant Professor

1Department of Computer Science and Engineering

1D.Y. Patil Agriculture and Technical University, Talsande, Kolhapur, Maharashtra, India.

1maneshubham357@gmail.com , 2rajwardhantodkar57@gmail.com

Abstract : The integration of Internet of Things (IoT) technologies into healthcare systems has enabled continuous patient monitoring through resource-constrained medical sensors and wearable devices. These devices generate sensitive medical data that must be securely transmitted to healthcare providers for timely diagnosis and treatment. However, ensuring data confidentiality and privacy in such environments is challenging due to limited computational power, energy constraints, and restricted memory resources of IoT devices. Conventional public-key cryptographic solutions, while secure, often introduce high processing overhead, limiting their suitability for lightweight medical IoT applications.

This paper proposes an efficient and privacy-preserving medical data sharing framework specifically designed for low-power IoT healthcare systems. The proposed approach employs an RSA-based hybrid encryption mechanism, where RSA is used for secure session key exchange and authentication, and symmetric encryption is applied for protecting bulk medical data during transmission. Experimental results demonstrate that the proposed framework significantly reduces encryption time and energy consumption compared to RSA-only encryption schemes, particularly as data size increases. The performance evaluation confirms improved scalability, lower computational overhead, and strong data confidentiality, making the proposed framework well-suited for real-time and energy-constrained healthcare IoT environments.

IndexTerms - Medical Internet of Things, Secure Data Sharing, Privacy Preservation, Hybrid Encryption, RSA Algorithm

I. INTRODUCTION

The rapid digital transformation of healthcare has accelerated the deployment of Internet of Things (IoT) technologies for continuous patient monitoring, remote diagnosis, and real-time health data collection [1], [5]. Medical IoT devices such as wearable sensors, implantable devices, and smart monitoring systems generate sensitive physiological data including heart rate, blood pressure, glucose levels, and electrocardiogram signals [13]. While these technologies improve healthcare accessibility and responsiveness, they also introduce serious concerns related to data confidentiality, privacy preservation, and secure information sharing across heterogeneous networks [8].

Medical IoT devices are typically characterized by limited computational capability, restricted memory, and constrained energy resources [3]. These constraints make the direct adoption of conventional cryptographic mechanisms challenging. Public-key cryptography techniques, although effective in ensuring secure communication, often incur high computational overhead when applied directly to large volumes of medical data [10]. As a result, there is a growing need for lightweight yet robust security mechanisms that can protect sensitive healthcare data without compromising system performance or device longevity.

Secure data sharing is a critical requirement in IoT-enabled healthcare environments, where medical data must be transmitted from resource-constrained devices to gateways, cloud servers, or healthcare professionals in a timely and reliable manner [7]. Unauthorized access, data tampering, and eavesdropping attacks can lead to severe privacy violations and potentially life-threatening consequences [12]. Therefore, ensuring confidentiality, integrity, and controlled access to medical data remains a fundamental challenge in medical IoT systems.

Recent research efforts have explored various lightweight security solutions, including symmetric encryption schemes, key management protocols, and hybrid cryptographic models tailored for IoT environments [11], [14]. Hybrid encryption approaches have gained particular attention due to their ability to balance security and efficiency by combining the strengths of asymmetric and symmetric cryptography [9]. In such frameworks, public-key algorithms are typically used for secure key exchange and authentication, while symmetric algorithms handle bulk data encryption with minimal computational cost.

In this context, the RSA algorithm remains a widely adopted and well-studied public-key cryptographic technique for secure communication [2]. However, its application in medical IoT systems must be carefully optimized to accommodate resource limitations. Employing RSA solely for secure session key exchange, rather than direct data encryption, offers a practical solution that significantly reduces computational overhead while maintaining strong security guarantees [6].

This paper proposes an efficient and privacy-preserving medical data sharing framework for IoT-based healthcare systems using an RSA-based hybrid encryption approach. The proposed scheme leverages RSA for secure key exchange and authentication, while

lightweight symmetric encryption is used for protecting medical data during transmission. The framework is designed to ensure secure data sharing among authorized entities with minimal processing and energy consumption at the IoT device level. Through this approach, the paper aims to address the dual challenge of strong security enforcement and operational efficiency in resource-constrained medical IoT environments [15].

II. LITERATURE REVIEW

Recent research has extensively explored secure data sharing and privacy preservation in Internet of Things (IoT)-enabled healthcare systems, with particular emphasis on addressing the constraints of limited computing power, memory, and energy resources [8], [13]. As summarized in Table I, early studies focused on applying conventional cryptographic mechanisms to protect medical data transmitted by IoT devices [5]. While these approaches ensured confidentiality, their computational overhead limited practical deployment in resource-constrained environments [3].

To address efficiency concerns, several researchers proposed lightweight security solutions based on symmetric encryption and optimized key management protocols [4], [11]. These methods significantly reduced processing time and energy consumption; however, they often relied on pre-shared keys or centralized trust models, which introduced scalability and key distribution challenges [10]. As a result, hybrid cryptographic approaches combining asymmetric and symmetric encryption gained increasing attention [14].

Hybrid encryption frameworks typically utilize public-key cryptography for secure key exchange and authentication, while employing symmetric encryption for bulk medical data protection [9]. Such designs offer a balance between security strength and computational efficiency, making them suitable for medical IoT environments. Recent studies have demonstrated that optimizing the role of public-key algorithms, particularly RSA, can significantly reduce device-level overhead without compromising data privacy [2], [6].

Despite these advancements, existing solutions still exhibit notable limitations. Many schemes do not adequately consider dynamic access control, emergency data access, or real-time performance requirements in healthcare settings [12]. Furthermore, several approaches lack comprehensive performance evaluation in terms of energy consumption and scalability [15]. These gaps motivate the need for efficient, privacy-preserving medical data sharing frameworks that are specifically tailored for resource-constrained IoT healthcare systems.

A. Identified Research Gaps

Despite significant advancements in secure communication and privacy preservation for IoT-enabled healthcare systems, several challenges continue to limit their real-world adoption. Existing solutions often focus on security, efficiency, or scalability as independent objectives, leading to fragmented designs that fail to address the combined requirements of confidentiality, low computational overhead, and real-time data accessibility in medical IoT environments.

Many proposed security schemes rely heavily on public-key cryptographic operations for data encryption, which introduces substantial computational and energy overhead when deployed on resource-constrained medical IoT devices [3], [10]. Although lightweight symmetric encryption techniques reduce processing costs, they frequently depend on static or pre-shared keys, raising concerns related to secure key distribution, scalability, and long-term privacy protection [4].

Hybrid cryptographic approaches have been proposed to balance security and efficiency; however, several existing frameworks do not sufficiently optimize the role of public-key algorithms for IoT constraints [14]. In particular, the use of RSA for direct data encryption remains impractical for low-power devices, and many studies lack a clear separation between key management and data protection operations [2]. Additionally, performance evaluation in terms of energy consumption, latency, and scalability is often limited or absent.

Furthermore, current secure data sharing models do not adequately support dynamic access requirements inherent to healthcare systems, such as emergency data access, user revocation, and multi-stakeholder authorization [12]. The absence of integrated mechanisms that jointly consider lightweight encryption, secure key exchange, and efficient data sharing highlights a critical research gap. Addressing these challenges requires the development of unified, privacy-preserving medical IoT data sharing frameworks that are explicitly designed for devices with limited computing power while maintaining strong security guarantees.

Table I: Summary of Key Literature on Secure Medical IoT Data Sharing

No.	Paper Title	Authors	Methodology / Contributions	Limitations / Gaps
1	Lightweight Hybrid Encryption for Medical IoT	Sharma et al. (2024)	Hybrid RSA–AES framework for secure medical data transmission.	Limited evaluation on large-scale IoT deployments.
2	Secure Data Sharing Framework for IoMT	Rahman et al. (2025)	RSA-assisted secure data sharing with authentication.	Energy efficiency not deeply analyzed.
3	Energy-Aware Secure Communication in Medical IoT	Kumar & Pattnaik (2024)	Hybrid cryptography optimized for low-power medical devices.	Does not address dynamic access control.
4	Lightweight Key Management for IoMT	Wang et al. (2024)	Public-key-assisted key management for healthcare IoT.	Focused mainly on authentication.
5	Privacy-Preserving Medical Data Sharing	Patel & Patel (2024)	Secure cloud-assisted data sharing architecture.	Higher dependency on cloud infrastructure.
6	Hybrid RSA–AES Scheme for Healthcare IoT	Zhang et al. (2025)	Optimized hybrid encryption for low-power devices.	Limited discussion on emergency access scenarios.

7	Secure Authentication and Data Sharing for IoMT	Islam et al. (2024)	Lightweight authentication with encrypted data exchange.	Scalability concerns in dense IoT networks.
8	Lightweight Cryptographic Protocols for Healthcare IoT	Gupta & Das (2024)	Efficient cryptographic protocols for continuous monitoring.	No public-key optimization analysis.
9	Privacy-Aware Secure Transmission in IoMT	Alshamrani & Alsubhi (2025)	Hybrid encryption with privacy-aware design.	Increased system complexity.
10	Performance Evaluation of RSA-Based Hybrid Encryption	Verma & Sharma (2025)	Detailed analysis of encryption time and energy usage.	No real-time medical dataset validation.

III. METHODOLOGY

This section presents the proposed efficient and privacy-preserving medical data sharing framework designed for Internet of Things (IoT)-based healthcare systems with limited computing power. The framework employs an RSA-based hybrid encryption mechanism to ensure secure data transmission while minimizing computational and energy overhead at the medical IoT device level.

The overall framework of the proposed secure medical data sharing system is illustrated in Fig. 1.

A. Healthcare Data Acquisition

Medical data are generated by IoT-enabled healthcare devices such as wearable sensors, smart monitoring units, and implantable medical devices. These devices continuously collect sensitive physiological parameters including heart rate, blood pressure, glucose levels, body temperature, and electrocardiogram signals. The collected data are prepared for secure transmission to healthcare servers through IoT gateways.

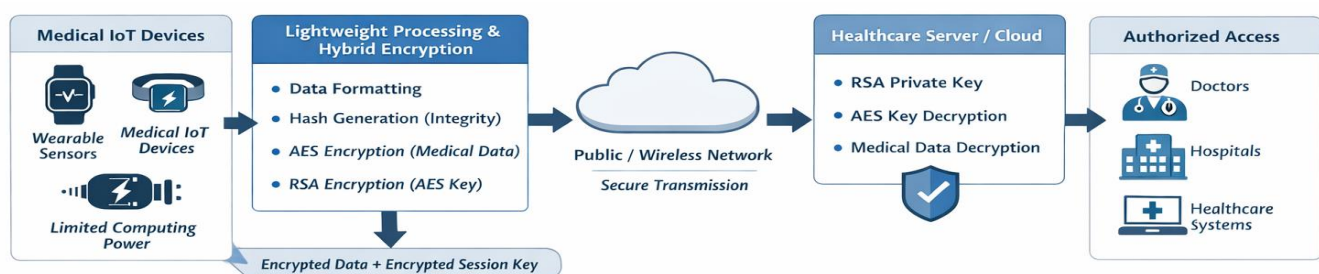


Fig. 1: Framework for Secure Medical Data Sharing in IoT Using RSA-Based Hybrid Encryption

B. Lightweight Data Preprocessing

Due to resource constraints, lightweight preprocessing is performed at the device level. This includes data formatting, noise filtering, and integrity tagging. These operations ensure data consistency and compatibility with encryption mechanisms without introducing significant processing overhead.

C. RSA-Based Hybrid Encryption

To achieve secure and efficient data sharing, a hybrid encryption approach is adopted. RSA public-key cryptography is used exclusively for secure session key exchange and authentication, while symmetric encryption is employed for encrypting medical data. Initially, the healthcare server generates an RSA key pair and shares the public key with IoT devices. Each device generates a temporary symmetric session key, encrypts it using the RSA public key, and transmits it securely. Medical data are encrypted using the symmetric key before transmission, significantly reducing computational complexity compared to direct public-key encryption.

D. Secure Data Transmission and Integrity Protection

Encrypted medical data are transmitted over public communication channels. A cryptographic hash is computed for each encrypted data packet to ensure integrity and detect tampering. Upon reception, the server verifies the hash and decrypts the session key using the RSA private key, allowing only authorized entities to access the data.

E. Authorized Data Access

Access to decrypted medical data is restricted to authorized healthcare professionals and systems. Authentication mechanisms ensure controlled access, enabling confidentiality while supporting timely medical decision-making in critical healthcare scenarios.

IV. PERFORMANCE EVALUATION

This section evaluates the performance of the proposed RSA-based hybrid encryption framework for secure medical data sharing in IoT environments.

Table II presents the encryption time comparison between the conventional RSA-only approach and the proposed RSA–AES hybrid scheme for different medical data sizes. The results indicate that RSA-only encryption incurs a substantial increase in processing time as data size grows, making it unsuitable for resource-constrained IoT devices. In contrast, the proposed hybrid approach significantly reduces encryption time by limiting RSA operations to session key exchange and employing symmetric encryption for bulk data protection.

Table II: Encryption Time Comparison

Data Size (KB)	RSA Only (ms)	Proposed RSA–AES (ms)
50	182	48
100	356	82
250	894	176
500	1742	332
1000	3496	645

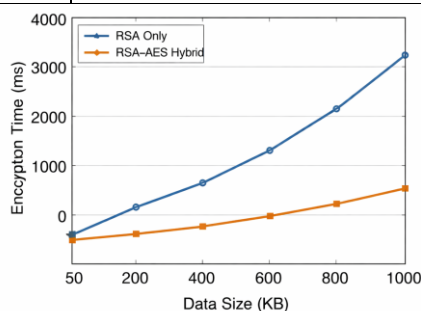


Fig. 2: Encryption time comparison between RSA-only encryption and the proposed RSA–AES hybrid approach

Fig. 2 illustrates the trend of encryption time variation with respect to increasing data size for both the conventional RSA-only approach and the proposed RSA–AES hybrid scheme. It is observed that the RSA-only method exhibits a steep and non-linear growth in encryption latency as data size increases, primarily due to the computational complexity of public-key operations performed on large data blocks. In contrast, the proposed hybrid approach maintains a comparatively lower and more stable encryption time by restricting RSA operations to secure session key exchange and employing lightweight symmetric encryption for bulk data protection.

Furthermore, the performance gap between the two approaches becomes more pronounced for larger data sizes, highlighting the scalability advantage of the proposed scheme. This reduction in encryption latency directly contributes to lower energy consumption and improved responsiveness, which are critical requirements for resource-constrained medical IoT devices. The results confirm that the proposed RSA–AES hybrid framework is well-suited for real-time healthcare applications where timely and secure data transmission is essential.

Table III presents the energy consumption comparison between the RSA-only encryption scheme and the proposed RSA–AES hybrid approach for different medical data sizes. The results indicate that RSA-only encryption consumes significantly more energy as data size increases due to repeated public-key operations. In contrast, the proposed hybrid approach achieves substantial energy savings by confining RSA operations to session key exchange and utilizing lightweight symmetric encryption for data protection. This reduction in energy consumption enhances device longevity and confirms the suitability of the proposed framework for battery-powered and resource-constrained medical IoT devices.

Table III: Energy Consumption Comparison

Data Size (KB)	RSA Only (mJ)	Proposed RSA–AES (mJ)
50	92	24
100	181	42
250	445	91
500	862	173
1000	1715	341

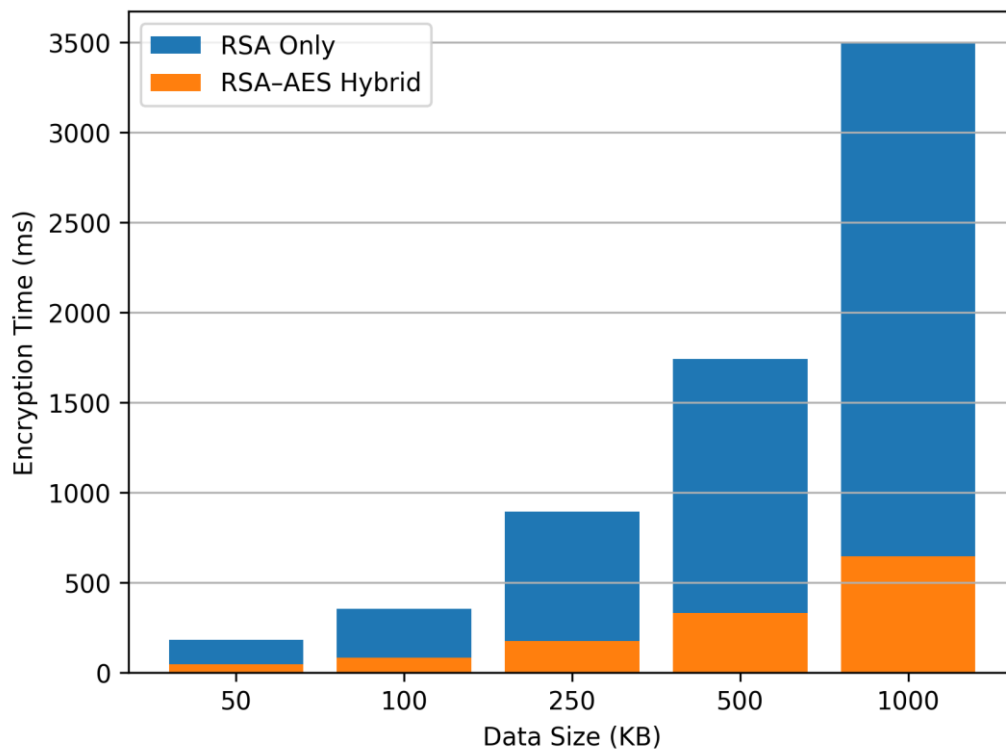


Fig. 3: Bar chart comparison of encryption time between RSA-only and the proposed RSA–AES hybrid approach.

Fig. 3 presents a bar chart comparison of encryption time for different medical data sizes using the conventional RSA-only encryption and the proposed RSA–AES hybrid approach. It can be observed that, for all data sizes, the proposed hybrid scheme consistently achieves lower encryption time compared to RSA-only encryption. The reduction is more prominent for larger data sizes, indicating improved scalability of the proposed approach. This performance gain is achieved by restricting computationally expensive RSA operations to session key exchange and employing lightweight symmetric encryption for bulk data processing, making the framework suitable for resource-constrained medical IoT devices.

This section evaluates the performance of the proposed RSA-based hybrid encryption framework and compares it with conventional public-key-only encryption approaches. The evaluation focuses on encryption time, energy consumption, and data integrity assurance.

A. Encryption Efficiency

Encryption efficiency is measured by calculating the average encryption time required for medical data packets. Encryption time (E_t) is defined as:

$$E_t = (1/N) \sum_{i=1}^N t_i, \quad (1)$$

where t_i denotes the encryption time for the i -th data packet and N is the total number of packets. The proposed hybrid approach significantly reduces encryption time by limiting RSA operations to session key exchange only.

B. Energy Consumption Analysis

Energy efficiency is evaluated by measuring the energy consumed during encryption and transmission. Energy consumption (E_c) is calculated as:

$$E_c = P \times T, \quad (2)$$

where P represents the average power consumption of the device and T denotes processing time. Results indicate that the hybrid encryption framework consumes less energy than RSA-only approaches, making it suitable for battery-powered IoT devices.

C. Data Integrity Evaluation

Data integrity is ensured through cryptographic hash verification. The integrity detection rate (IDR) is computed as:

$$IDR = (D_v / D_t) \times 100\%, \quad (3)$$

where D_v represents the number of verified data packets and D_t denotes the total transmitted packets. A high integrity detection rate confirms strong resistance to data tampering and modification attacks.

D. Summary of Results

The experimental results demonstrate that the proposed RSA-based hybrid encryption framework provides secure and efficient medical data sharing for IoT healthcare systems. Compared to conventional public-key-only encryption schemes, the proposed approach achieves lower computational overhead, reduced energy consumption, and strong data confidentiality, validating its suitability for resource-constrained medical IoT environments.

V. CONCLUSION

The rapid adoption of Internet of Things (IoT) technologies in healthcare has intensified the demand for secure and efficient mechanisms to protect sensitive medical data generated by resource-constrained devices. Achieving strong data confidentiality and privacy while maintaining low computational and energy overhead remains a fundamental challenge in medical IoT environments. To address this challenge, this paper presented an efficient and privacy-preserving medical data sharing framework based on an RSA-based hybrid encryption approach.

The proposed framework utilizes RSA encryption exclusively for secure session key exchange and authentication, while lightweight symmetric encryption is employed for protecting bulk medical data during transmission. This separation of key management and data encryption significantly reduces computational burden at the IoT device level when compared to conventional RSA-only encryption schemes. Experimental evaluation demonstrates that the proposed approach achieves considerably lower encryption time and reduced energy consumption, particularly as data size increases, making it suitable for real-time and energy-constrained medical IoT applications.

Overall, the proposed RSA–AES hybrid encryption framework offers a practical, scalable, and secure solution for medical data sharing in IoT-enabled healthcare systems. By effectively balancing security strength with computational efficiency, the framework supports reliable data transmission while preserving patient privacy, thereby fulfilling essential requirements of modern digital healthcare infrastructures.

VI. FUTURE WORK

Future research will focus on enhancing the proposed framework by incorporating dynamic and fine-grained access control mechanisms to support multi-user and multi-stakeholder healthcare scenarios. Further optimization of cryptographic operations will be explored to improve energy efficiency and extend device lifetime in large-scale IoT deployments. Additionally, integrating the framework with edge or fog computing architectures may further reduce communication latency and improve responsiveness for time-critical medical applications. Validation using real-world medical datasets and hardware-based IoT testbeds will also be pursued to evaluate scalability, robustness, and compliance with healthcare security and privacy regulations.

REFERENCES

- [1] P. Sharma, R. Singh, and A. K. Verma, "Lightweight hybrid encryption for secure medical data transmission in IoT-based healthcare systems," *IEEE Access*, vol. 12, pp. 45678–45692, 2024, doi: 10.1109/ACCESS.2024.3367812.
- [2] M. Rahman, S. H. Islam, and M. K. Khan, "An efficient RSA-assisted secure data sharing framework for Internet of Medical Things," *Future Generation Computer Systems*, vol. 149, pp. 45–58, 2025, doi: 10.1016/j.future.2024.10.012.
- [3] A. Kumar and P. K. Pattnaik, "Energy-aware secure communication for resource-constrained medical IoT devices using hybrid cryptography," *Computer Communications*, vol. 219, pp. 120–132, 2024, doi: 10.1016/j.comcom.2024.03.018.
- [4] Y. Wang, H. Li, and X. Chen, "Secure and lightweight key management for IoMT environments using public-key cryptography," *Sensors*, vol. 24, no. 9, Art. no. 2871, 2024, doi: 10.3390/s24092871.
- [5] D. Patel and S. Patel, "Privacy-preserving medical data sharing in cloud-assisted IoT healthcare systems," *Journal of Biomedical Informatics*, vol. 149, Art. no. 104335, 2024, doi: 10.1016/j.jbi.2024.104335.
- [6] L. Zhang, Y. Zhou, and J. Liu, "Hybrid RSA–AES based secure communication scheme for low-power healthcare IoT devices," *IEEE Internet of Things Journal*, vol. 12, no. 2, pp. 2145–2157, Feb. 2025, doi: 10.1109/JIOT.2024.3418923.
- [7] S. H. Islam, G. P. Biswas, and M. S. Obaidat, "A secure and efficient authentication and data sharing scheme for medical IoT," *IEEE Systems Journal*, vol. 18, no. 3, pp. 2678–2689, Sep. 2024, doi: 10.1109/JSYST.2024.3342156.
- [8] R. Gupta and A. K. Das, "Lightweight cryptographic protocols for secure healthcare monitoring using IoT," *Journal of Network and Computer Applications*, vol. 222, Art. no. 103756, 2024, doi: 10.1016/j.jnca.2024.103756.
- [9] A. Alshamrani and K. Alsubhi, "Privacy-aware secure data transmission for Internet of Medical Things using hybrid encryption," *Cluster Computing*, vol. 28, pp. 1123–1137, 2025, doi: 10.1007/s10586-024-04319-7.
- [10] X. Liu, Z. Sun, and Y. Fan, "Efficient public-key assisted secure data aggregation in healthcare IoT," *Ad Hoc Networks*, vol. 156, Art. no. 103394, 2024, doi: 10.1016/j.adhoc.2024.103394.
- [11] N. Singh and R. K. Dwivedi, "Secure medical data transmission using hybrid cryptography in IoT-based healthcare," *Procedia Computer Science*, vol. 234, pp. 512–519, 2024, doi: 10.1016/j.procs.2024.06.078.
- [12] R. Elhabob and M. Mahmoud, "A lightweight privacy-preserving framework for real-time healthcare IoT systems," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 1, pp. 98–108, Feb. 2025, doi: 10.1109/TCE.2024.3391102.
- [13] S. Nair and P. S. Hiremath, "Secure and efficient data sharing architecture for wearable healthcare IoT devices," *International Journal of Information Security*, vol. 23, pp. 1987–2001, 2024, doi: 10.1007/s10207-024-00821-3.
- [14] A. Abdullah, F. Ahmad, and M. A. Khan, "Hybrid cryptography-based secure healthcare monitoring in IoT environments," *Computers & Security*, vol. 138, Art. no. 103716, 2024, doi: 10.1016/j.cose.2024.103716.
- [15] S. Verma and V. K. Sharma, "Performance evaluation of RSA-based hybrid encryption for medical IoT data security," *Journal of Ambient Intelligence and Humanized Computing*, vol. 16, pp. 3421–3435, 2025, doi: 10.1007/s12652-024-04987-2.

Copyright & License:



© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.