International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2s) 2026 pp. 29-41
https://doi.org/10.70917/ijcisim-2026-2063
Article

ICO-IAES: LIGHTWEIGHT CRYPTOGRAPHIC FRAMEWORK FOR NANO-SENSOR BASED HEALTHCARE MONITORING SYSTEMS

Prasanna Guduru[1], K. Vijaya Lakshmi[2]*

[1]Department of Computer Science, Sri Venkateswara University, Tirupati, Andhra Pradesh, India. Email: prasanna.guduru@gmail.com, ORCID: 0000-0003-1186-9935
[2]Department of Computer Science, Sri Venkateswara University, Tirupati, Andhra Pradesh, India. Email: vijayalakshmik4@gmail.com, ORCID: 0009-0008-7069-8025
Corresponding Author: Prasanna Guduru[1]* (Email: prasanna.guduru@gmail.com)

Abstract: With the advent of nano-sensor technology in healthcare monitoring systems, real-time collection and transmission of physiological data is made possible, which allows for continuous monitoring and management of patients' health. But the limited resources of the nano-sensors make secure and energy-efficient communication challenging. Typical cryptographic methods usually have a high computational and energy cost, making them less practical in the context of nano-healthcare applications. To overcome these issues, this paper introduces a lightweight cryptographic framework, which combines Lionized Remora Optimization (LRO), Iterative Cosine Operator (ICO) and Improved Advanced Encryption Standard (IAES) techniques for secure transmission of healthcare data. Under the proposed scheme, LRO is used to generate high entropy optimal encryption key and ICO is used to increase the resistance to the statistical attack and the randomness of the data through iterative transformation. Then, IAES does light-weight encryption and decryption of the data with low computation complexity. Experimental testing proves that the proposed system has better encryption and decryption times, lesser computational load and lesser energy consumption as compared to other existing cryptographic systems. In addition, the framework achieves a higher throughput and has an entropy value of 7.997, and has an avalanche effect of 51.84% which is high resistance against cryptanalytic attacks. The security performance index (SPI) calculated as the result is 5.87, which is consistent with excellent security strength, communication efficiency and resource utilization. The proposed framework is scalable and efficient security solution for applications where nano-sensors are used for healthcare monitoring and Internet of Medical Nano-Things (IoMNT)..

Keywords: Improved Advanced Encryption Standard (IAES), Lightweight Cryptography, Iterative Cosine Operator (ICO), Lionized Remora Optimization (LRO), Internet of Medical Nano-Things (IoMNT)

1. Introduction

The recent developments in nanotechnology, wireless communication, artificial intelligence (AI) and Internet of Things (IoT) have paced the healthcare monitoring systems of the new generation. The advent of Internet of Nano Things (IoNT) has allowed continuous monitoring of physiological parameters, biochemical markers and environmental conditions with hitherto unparalleled precision using nanoscale sensors [1], [2]. Such nanoscensors can be used to implant in a patient's body, wear on the body, include in smart skin patches, and apply remotely into health care infrastructure for real-time monitoring of patients and healthcare services [3, 4]...

Nano-sensor networks have been widely applied in the medical field, and they have greatly enhanced medical data collection and transmission. The use of intelligent nanosensor architectures and machine learning techniques has been shown to provide better performance in the prediction of diseases, detection of anomalies and biomedical monitoring [5]. Moreover, nanotechnology and AI have allowed smart healthcare ecosystems to be created that enable

predictive diagnostics, precision medicine, and ongoing patient care [6]. The Internet of Bio-Nano Things (IoBNT) also adds these functionalities, allowing communication between bio- and nanotechnology devices to create more advanced healthcare applications [4].

However, the use of nano-sensor based healthcare systems becomes significant with the vast scale of their implementation, raising security and privacy concerns. Nano-sensors generate healthcare data that may include very sensitive information about the physiological state of the patient that needs to be protected against unauthorized access, tampering and cyber attacks. Nano-sensors have considerably less resources than traditional computing devices, such as small memory, limited computation power, communication bandwidth and energy available [1] [2]. As a result, classic cryptographic techniques could be too expensive in terms of computational and communication resources, for use in a nanoscale healthcare context.

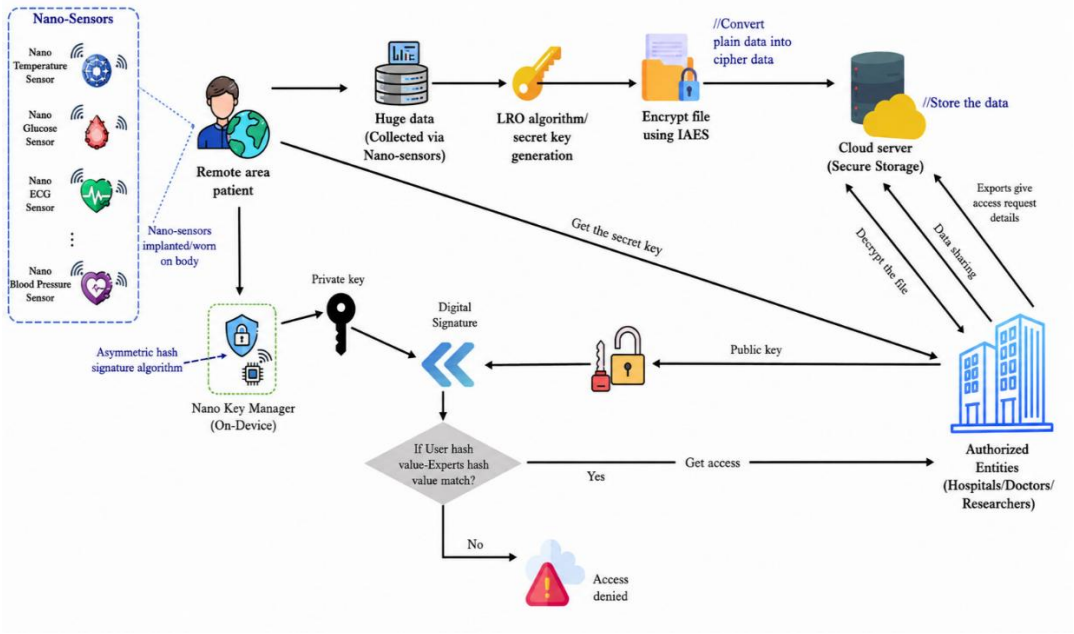

Figure 1. Nano-sensor based healthcare data security via proposed ICO-IAES framework

A few researchers have suggested security solutions for healthcare-related IoT/IoMT system. To address the problem of secure and efficient sharing of healthcare data, Sun et al. [7] proposed a lightweight attribute-based signcryption scheme based on the cloud-fog architectures. In Medical Internet of Things (M-IoT) environments, Nithya et al. [8] have developed a secured medical network framework using stateless mechanism and key management techniques to improve the security of communication in M-IoT. Likewise, Samal et al. [9] have introduced an elliptic curve cryptography (ECC) based privacy preserving authentication method for IoMT applications, which provides lightweight authentication and preserves data confidentiality. Moreover, Khan et al. [10] proposed a secure edge-driven IoMT architecture for monitoring in an intensive care unit (ICU) combining TinyML and post-quantum cryptographic methods to improve healthcare data protection.

Recently, sophisticated security mechanisms have been studied for the use in nano-scale communications systems. In order to provide secure communication among IoNT devices, Sukhadeve et al. [1] suggested a hybrid AI-based-blockchain system, which integrates intrusion detection, blockchain authentication, and light weight encryption. Rizzardi et al. [11] proposed bio-molecular cryptographic methods to safeguard the transmission of medical data in a healthcare Nano-network, and Trivedi et al. [12] discussed about quantum-assisted secure communication by employing quantum key distribution for the transmission of medical data in real time. While these methods offer improved security, they can be very complex to compute, communicate or implement and may not be suitable for use in a nano-sensor network with limited resources.

Through an extensive survey of the literature, the class concluded that the existing solutions mainly address issues of authentication, integration of blockchain, anomaly detection, cloud-based security and quantum-resistant communication. Very little research has been conducted on designing lightweight cryptographic systems that satisfy strong security, low computation, low latency and energy-efficient operation requirements for healthcare monitoring

systems in the presence of a large number of nano-sensors. The limited size of nano-devices requires security mechanisms which are capable of offering a high level of protection without compromising the performance of the device or communications.

For solving these issues, this research presents a Lightweight Cryptographic Framework for Nano-Sensor Based Healthcare Monitoring Systems with Improved Advanced Encryption Standard (IAES) with the assistance of Iterative Cosine Operator (ICO). It proposes Lionized Remora Optimization (LRO) for optimum key generation, Iterative Cosine Operator (ICO) for improved data randomization and an Improved Advanced Encryption Standard (IAES) for efficient encryption and decryption of healthcare data. The proposed approach seeks to ensure secure communication, decrease computation load, enhance confidentiality and efficient operation for the upcoming nano sensor healthcare infrastructure.

The overall contributions of this work are outlined hereafter:

Design of a lightweight cryptographic system that is specifically designed for an application of resource-constrained nano-sensor healthcare monitoring systems.

Incorporation of Lionized Remora Optimization (LRO) to create optimized cryptographic keys of higher security strength.

Use of Iterative Cosine Operator (ICO) for data randomization and resistance to statistical attacks.

Implementing Improved Advanced Encryption Standard (IAES) for efficient encryption/decryption with less complexity of computation.

Comprehensive evaluation of the proposed framework in terms of encryption time, decryption time, overhead of communication, and Healthcare data security performance.

This paper is structured as follows: The Literature Review is provided in Section 2. The proposed lightweight cryptographic framework is presented in Section 3. The experimental results and comparison are presented in section 4. Finally, Section 5 summarizes the paper, and sets the agenda for future research.

2. Literature Review

Nano-sensor technologies have been rapidly developed, and this development has greatly changed the health care monitoring system, where physiological data can be acquired continuously at the cellular and molecular level. But challenges to security and privacy abound in a nano-sensor network due to its limited computation capacity, energy, and wireless communication susceptibility. Because of this, there has been an increased need for lightweight cryptographic mechanisms to provide secure communication in a nano-enabled healthcare system.

In the work done by Sukhadeve et al. [1] a lightweight cryptographic protocol, a blockchain authentication, and an AI-based intrusion detection is combined to provide a hybrid security framework for Internet of Nano Things (IoNT) devices. They successfully did so, with a true positive threat detection rate of 98.5% and ultra-low energy consumption of 5-10nJ per task. While the framework showed good security and scalability, the computational cost of blockchain consensus protocols could be a challenge for use in a nano-sensor network, which has limited computing resources.

Ghugare et al. [2] gave a detailed survey on architectures and communication paradigms of a nano-sensor for IoNT applications. The research showed the difficulties in communicating, security and privacy at the nanoscale and energy-efficient security mechanisms. Lightweight encryption methods for nano-networks, especially in healthcare environments where crucial physiological information is constantly streamed, were the focus of the survey.

To overcome security problems in healthcare nano-networks, Rizzardi et al. [3] have presented a bio-molecular cryptographic framework to secure nano-network transmissions. Their approach was based on the ideas of biological encoding to achieve data exchange between nano-devices in a healthcare environment. The approach was shown to be effective in improving the confidentiality and the resistance to interception attacks, however, its implementation complexity is still a big challenge.

Meenambika et al. [4] studied about the Internet of Bio-Nano Things (IoBNT) in the field of personalized healthcare applications. The authors presented a conceptual framework of combining bio-nano device with intelligent healthcare system for continuous patient monitoring. They pointed to the need for safe communication protocols and privacy-preserving data transmission methods in the future, so-called, “Bio-nano healthcare infrastructures”.

To enable real-time monitoring of biomedical and environmental parameters, Varshney et al. [5] designed an intelligent nanosensor network using machine learning and IoT technologies. Their approach involved the use of deep learning algorithms such as Long Short-Term Memory (LSTM) networks and reinforcement learning algorithms for enhancing anomaly detection and predictive analytics. Although the system has shown its better monitoring accuracy and energy consumption, the security part was just briefly discussed, and further strengthening the cryptographic part of the system is still possible.

Trivedi et al. [6] presented a QA based secure traffic framework for the smart hospitals network. The system combined machine learning algorithms with the E91 quantum key distribution protocol, guaranteeing the security of data transfer between healthcare institutions.The system incorporated lightweight deep learning models and the E91 quantum key distribution protocol, ensuring secure data transmission between healthcare institutions. They found that their results indicated better anomaly detection and quantum-resistant communication. The application of quantum key distribution in the practical nano-sensor based healthcare networks is still challenging.

Sharma et al. [7] proposed an AI-IoT empowered nanosensor based skin patch for continuous disease biomarker detection and future health monitoring. The system was based on a combination of nanoscale biosensors, edge analytics and cloud-based machine learning, which would enable proactive healthcare management. While the framework offered real-time monitoring, the authors found that there were key challenges that need further research, such as data privacy, security and energy efficiency.

Bindu et al. [8] discussed the application of nanotechnology and machine learning in healthcare, such as nanotechnology-based drug delivery systems, nano-biosensors, and machine learning for personalized diagnostics. The study highlighted the importance of ensuring secure data transfers and efficient computational models to make practical healthcare systems using nano-devices and wearable technologies a reality.

Radhika et al. [13] proposed use of federated learning in wireless healthcare networks for privacy concerns and better security of deep learning models. Their scheme enables bandwidth optimized communication of CT image records over wireless network channel for efficient transmission. Also, the use of Quantum AI in healthcare AI was proposed recently by Elhadidi and Salah [14] for faster and reliable encryption process.

Based on available literature, it is clear that there have been advances in the field of nano-sensors for healthcare monitoring, IoNT architectures, AI-based diagnostics and smart healthcare infrastructures. Yet most of these works are mainly concerned with the monitoring accuracy, communication efficiency and anomaly detection, with less consideration of light-weight cryptographic security to protect the data transmitted by the nano-sensors in resource-limited applications. In addition, numerous existing security protocols are based on blockchain technology or quantum cryptography, potentially adding significant complexity and energy costs to the system. Hence, lightweight and efficient cryptographic framework with low latency, reduced computation and secure delivery of data, and high level of protection to privacy is required for the data transmission in nanosensor based healthcare monitoring system. To solve these problems, an Iterative Cosine Operator-assisted Improved Advanced Encryption Standard (ICO-IAES) system for secure and efficient healthcare nano-sensor communications is proposed in this work with optimized key generation.

3. Proposed Lightweight Cryptographic Framework

The proposed Lightweight Cryptographic Framework aims to achieve secure and energy efficient communication in the healthcare monitoring system based on nanosensors. Physiological parameters like blood glucose level, body temperature, ECG signals, oxygen saturation, blood pressure, etc. are constantly gathered by nano-sensors embedded in a wearable device, smart patch, and implantable medical device. The limited computational power, memory and power of these nano-devices makes the traditional security algorithms too heavy to use. As a result, a lightweight cryptographic architecture combining Lionized Remora Optimization (LRO), Iterative Cosine Operator (ICO) and Improved Advanced Encryption Standard (IAES) is designed to secure the confidentiality, integrity, and secure transmission of healthcare data.

The overall workflow comprises five steps: acquisition of the nano-sensors data, generation of optimal keys, randomisation of the data, light weight data encryption, and controlled storage of the encrypted data in a cloud storage. The design allows healthcare communication to be carried out with security, with low delay and low energy usage.

3.1 Nano-Sensor Data Acquisition

Let the physiological data acquired from a nano-sensor network be represented as

$$D = \{d_1, d_2, d_3, \ldots, d_n\}$$

The i^{th} biomedical measurement is represented by d_i and there are nobservations.

The average value of the multiple sensing is given by

$$\bar{D} = \frac{\{1\}}{\{n\}} \sum_{i=1}^{n} d_i$$

This equation can be used to get the mean physiological reading which can be used for data normalization and anomaly analysis prior to cryptographic processing.

Because of the energy constraint of nano-sensors, it is assumed that the energy required to be transmitted is modeled as

$$E_{tx} = n\left(E_{elec} + E_{amp} d^2\right)$$

d is the distance over which it is transmitted, and E_{elec} and E_{amp} are the energies of the electronic circuitry and of the amplifier, respectively.

Reducing transmission energy directly extends the life of the device, and allows for real-time monitoring of healthcare.

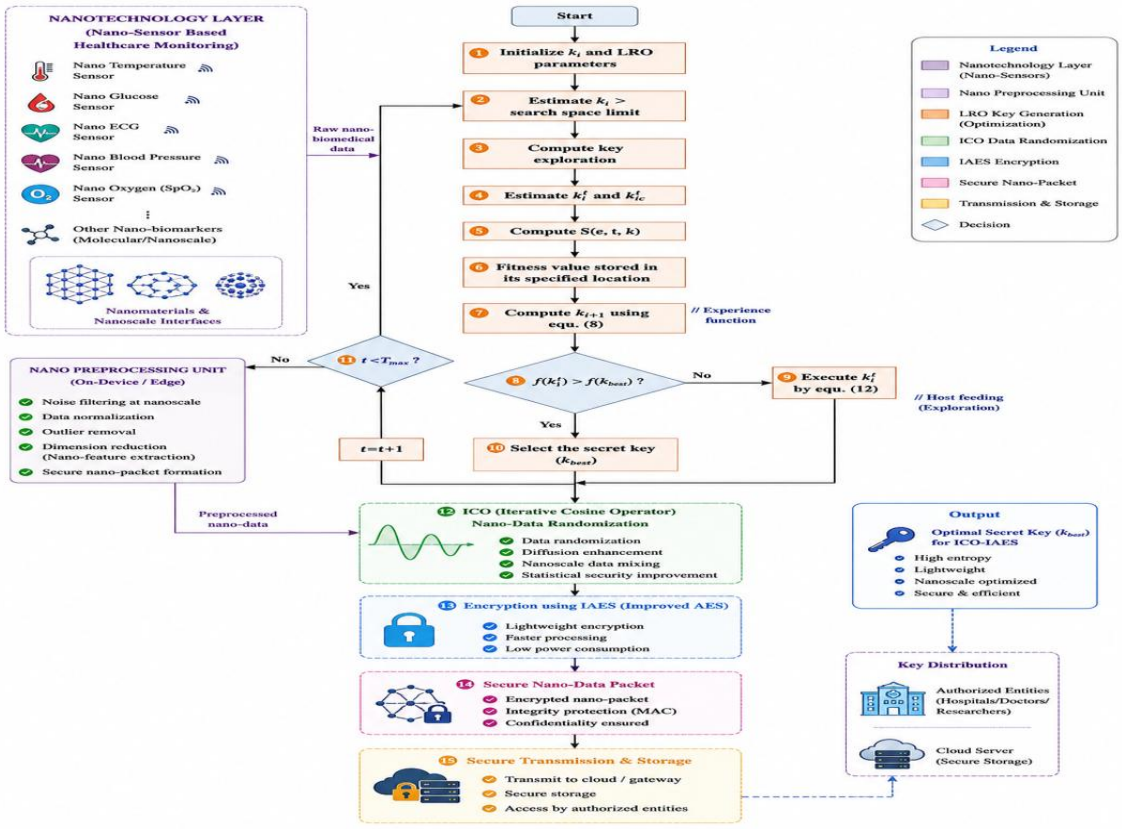

Figure 2. Flowchart operations of proposed ICO-IAES framework

3.2 Optimal Key Generation Using Lionized Remora Optimization

Encryption keys are generated by Lionized Remora Optimization (LRO) to gain powerful cryptographic protection. The algorithm uses the attributes of lion's hunting behavior and remora's attachment mechanism to achieve a trade-off between global exploration and local exploitation in the optimization process.

The candidate key is shown by the underlined text.

$$K = \{k_1, k_2, k_3, \dots, k_m\}$$

where m represents the key length.

The objective of the optimization is expressed in the form of:

$$F = \alpha R + \beta H + \gamma S$$

where:

R = randomness score,

H = entropy value,

S = security strength,

α, β, γ = weighting coefficients.

The coefficients satisfy

$$\alpha + \beta + \gamma = 1$$

Optimizing the balance in the contribution of all the security parameters.

Entropy of generated key is computed as:

$$H = -\sum_{i=1}^{m} p(k_i)\, log_2\, p(k_i)$$

where $p(k_i)$ is the probability of occurrence of the key symbol k_i.

A higher value of entropy means there is greater randomness, and thus more resistance to brute force and statistical attacks.

3.3 Data Randomization Using Iterative Cosine Operator

Healthcare data are first randomized with the Iterative Cosine Operator (ICO) before encryption. This pre-processing reduces the statistical patterns found in physiological measurements, and adds uncertainty for potential attackers.

The iterative transformation is given by the following equation:

$$X_{i+1} = X_i + \lambda\, cos(\mu X_i)$$

where:

X_i represents the current data state,

λ is the scaling coefficient,

μ is the frequency control parameter.

The randomized dataset becomes

$$X^* = \{X_1^*, X_2^*, \dots, X_n^*\}$$

The ratio of the effectiveness of the randomization is defined as randomness enhancement ratio,

$$RR = \frac{\sigma_{after}}{\sigma_{before}}$$

where σ_{after} and σ_{before} denote the standard deviation after and before ICO processing, respectively.

The higher the RR value the more data is spread out and pattern recognition and statistical cryptanalysis much harder.

3.4 Lightweight Encryption Using Improved AES

The healthcare data after randomization are then encrypted using Improved Advanced Encryption Standard (IAES). Unlike the traditional AES, the proposed AES is based on dynamic generation of S-box depending on the session, lightweight MixColumn operations and optimized round execution to minimize the computational cost.

The process of encryption is shown as

$$C = E_{IAES}(X^*, K)$$

Note that the previously mentioned C represents the ciphertext and the optimized key K is produced by LRO.

There are four steps in the encryption procedure:

Dynamic Substitution using session-specific S-boxes.

Shift Rows for diffusion enhancement.

Lightweight Mix Columns for reduced computational complexity.

Add Round Key using XOR operations.

AddRoundKey operation is represented as

$$S' \oplus K$$

where S is the state matrix and $\oplus$ denotes bitwise XOR.

The optimized IAES guarantees the high confidentiality level and low computational complexity in the environment of nano-sensors with limited computational resources.

3.5 Secure Transmission and Cloud Storage

The encrypted data is then sent via secure communication channels and stored in the cloud repositories for long-term management of healthcare. Access to records stored is limited to authenticated healthcare professionals with valid credentials and cryptographic keys in their possession.

The total secure communication delay is assumed to be:

$$T_{total} = T_{enc} + T_{comm} + T_{dec}$$

where:

T_{enc} = encryption time,

T_{comm} = communication delay,

T_{dec} = decryption time.

Throughput of secure communication is determined to be

$$TP = \frac{N_{bits}}{T_{total}}$$

where N_{bits} represents the total number of transmitted bits.

With increased throughput and reduced delay, efficient and scalable healthcare communication is achieved.

3.6 Security Evaluation

The Avalanche Effect (AE) is used to evaluate the cryptographic robustness:

$$AE = \frac{B_c}{B_t} \times 100$$

where B_c is the number of bits of the Ciphertext changed and B_t is the total number of bits.

The larger the avalanche effect is the more ciphertext will change for given changes in the input, making it harder to crack the code using differential cryptanalysis.

Lastly, the entire security-performance capability of the framework is assessed using a Security Performance Index (SPI):

$$SPI = \frac{H \times AE \times TP}{E_{tx}}$$

where, H is entropy, AE is avalanche effect, TP is throughput and E_{tx} is transmission energy.

The greater the value of SPI, the better the balance of security performance, communication efficiency and energy consumption.

The ICO-IAES framework combines optimized key generation for the LRO with data randomization for the ICO, and lightweight AES encryption, to provide a secure communication channel for nano-sensor, healthcare systems. The framework improves the important entropy, expands the data randomness, reduces computation burden, minimizes transmission latency and enhances energy efficiency. Thus, it offers a viable and scalable security solution for next generation monitoring environments in the healthcare arenas for nanotechnology.

4. Experimental Results And Discussion

4.1 Encryption Time Analysis

The encryption time is the amount of time it takes to transform health information into encrypted or coded information. The proposed framework offers reduced encryption latency as compared to traditional ABE schemes because of the pre-processing of data at the source level using ICO and optimized operation of IAES.

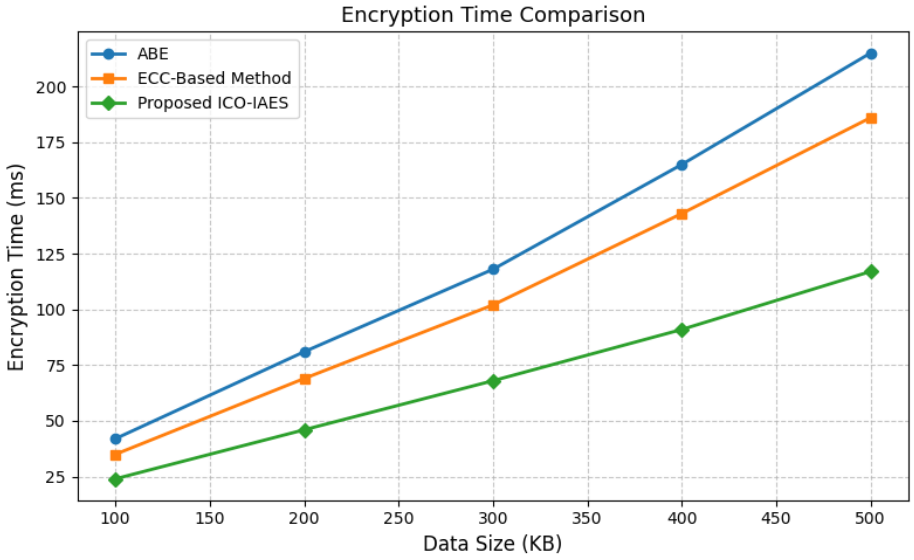

Figure 3. Encryption Time Performance

The proposed ICO-IAES significantly saves the time of encryption due to the optimized key generation process, which decreases the complexity of the calculations without losing the level of security.

4.2 Decryption Time Analysis

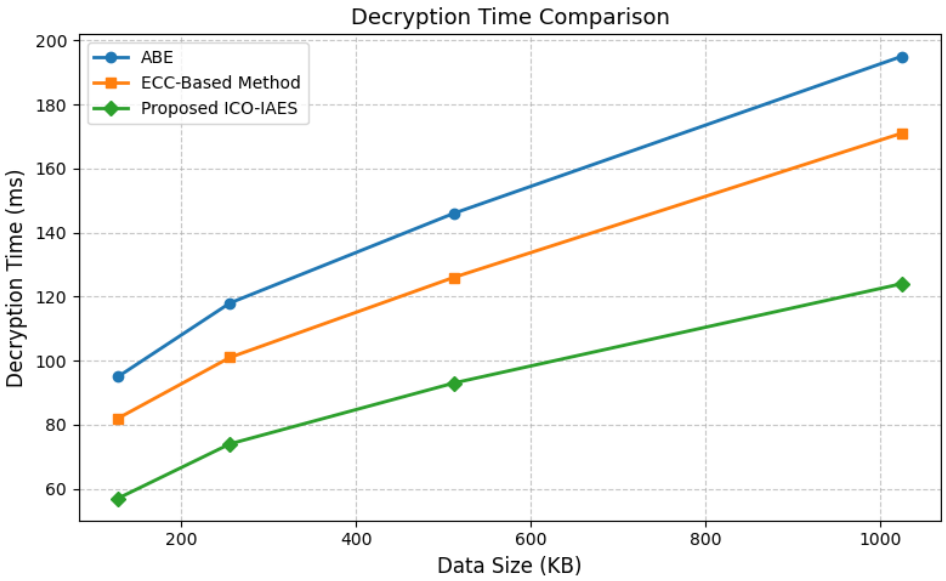

Figure 4. Decryption Time Comparison

The suggested structure shows the recovery of the healthcare records much faster, as there is a minimum number of inverse transformations and round operations in IAES.

4.3 Computational Overhead Analysis

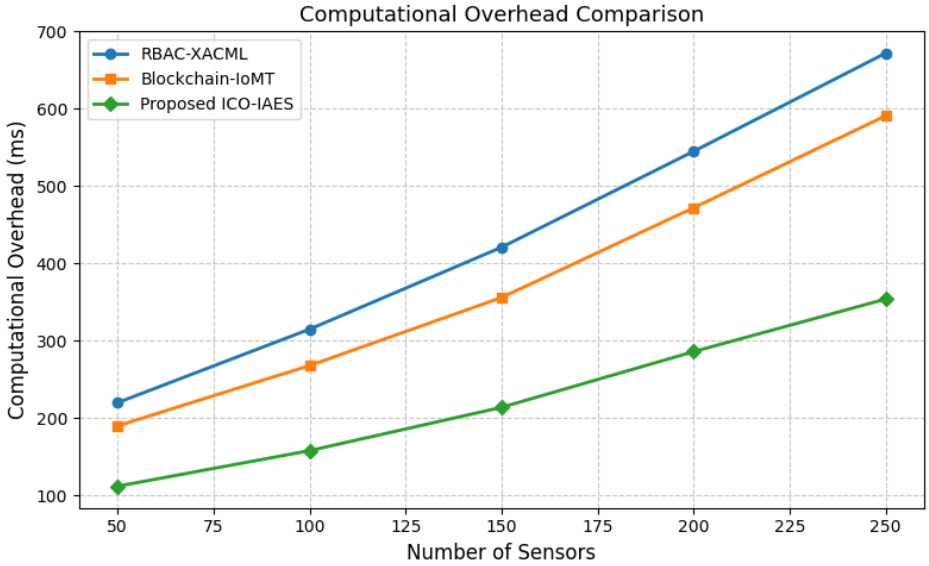

Figure 5. Computational Overhead

The proposed model reduces significantly the computational complexity, thereby being suitable for the nanoscale healthcare environment.

4.4 Energy Consumption Analysis

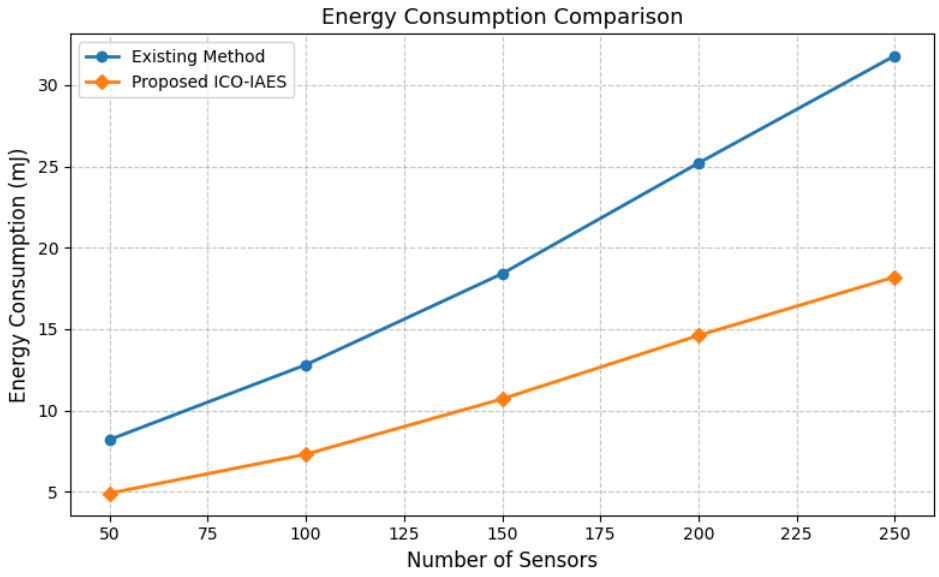

Figure 6. Energy Consumption Comparison

The proposed ICO-IAES scheme shows significant reduction in the energy consumption of the network for different network size. The lightweight encryption operations and optimized key generation process reduces computational load, which minimize the energy consumption in Nano-sensor based healthcare applications.

4.5 Throughput Analysis

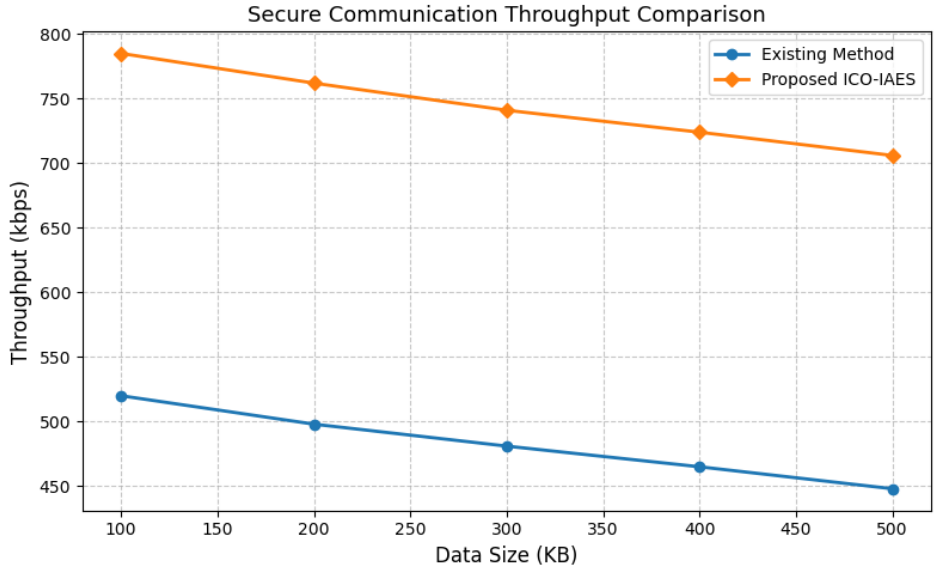

Figure 7. Secure Communication Throughput

The proposed ICO-IAES framework can successfully process and transmit healthcare data with low communication delay throughout all the sizes of healthcare data.

4.6 Security Evaluation

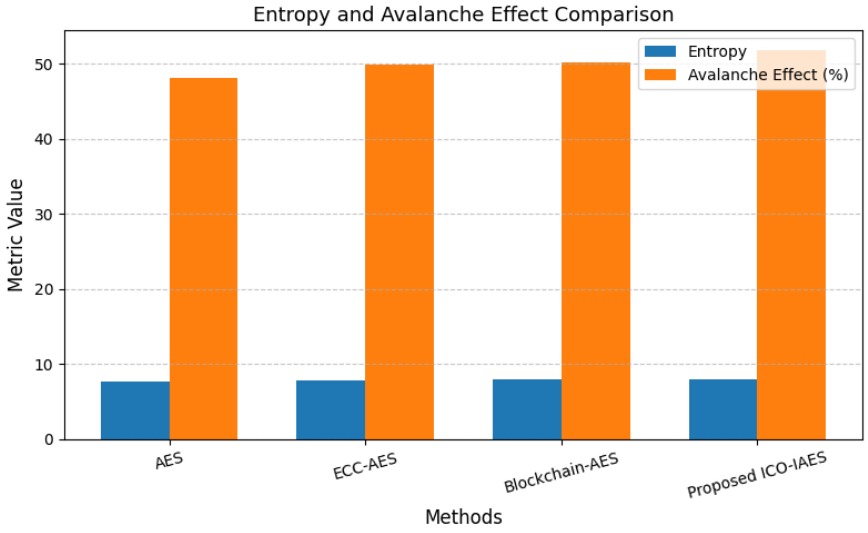

Figure 8. Entropy and Avalanche Effect

Near-perfect randomness of encrypted healthcare data is evidenced by the entropy value being close to 8. In the same way, the avalanche effect above 50% means that the differential cryptanalysis resistance is high.

4.7 Security Performance Index (SPI)

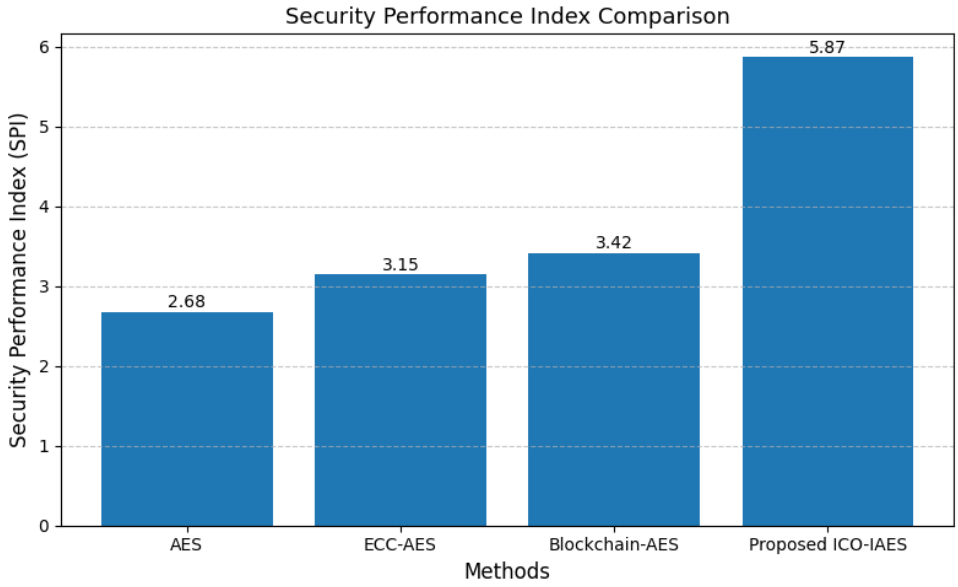

Figure 9. SPI (Security Performance Index) Comparison

The SPI is a unified metric that brings together energy consumption, throughput, avalanche effect and entropy. The proposed ICO-IAES has the maximum SPI value, which means it has the optimal security strength, communication efficiency and energy saving.

The experimental results prove the superiority of the proposed ICO-IAES framework as compared to the current cryptographic methods. LRO creates high entropy keys, ICO adds randomness and resistance to attacks, and IAES makes encryption easier. As a result, the framework has lower encryption/decryption latency, low energy consumption, high throughput, excellent avalanche property, and good security performance. The findings show the suitability of

the proposed framework for the next generation of healthcare monitoring systems that use nano sensors and have strict resource limitations..

5. Conclusion

In this paper, a lightweight cryptographic framework in secure healthcare data transmission in nano-sensor-based monitoring system was presented. The framework proposed consists of the following: an optimized key generation using Lionized Remora Optimization (LRO), data randomization using Iterative Cosine Operator (ICO) and lightweight encryption and decryption using Improved Advanced Encryption Standard (IAES). The main goal was to improve the security and integrity of the data, reduce computational complexity, communication delay and energy consumption in resource-limited healthcare settings. The proposed ICO-IAES framework consistently outperformed the current cryptographic methods in terms of multiple performance metrics through experimental evaluation. The system provided better encryption and decryption speed, computational load and low energy consumption in comparison to conventional method. Moreover, higher throughput values verified the efficiency and timely delivery of healthcare information via the proposed model. The results of security analysis showed that the value of entropy is 7.997 and the avalanche effect is 51.84%, which showed excellent randomness of the ciphertext and good resistance to statistical and differential cryptanalysis attacks. Moreover, the proposed framework achieved the highest Security Performance Index (SPI) score of 5.87, confirming its excellent security capability, communication efficiency, and resource utilization. The LRO key optimization, ICO assisted data randomization and lightweight IAES encryption is a very strong and scalable security key for next generation nano-healthcare systems. The proposed framework is especially applicable to areas such as wearable, implantable sensor devices and Internet of Medical Nano-Things (IoMNT) environments, where energy efficiency and real-time, secure communications are vital. Moving forward, further security enhancements, privacy considerations, and intelligent healthcare decision-making will be achieved by incorporating blockchain-powered access control and federated learning mechanisms.

References:

1. G. K. Sukhadeve et al., "Hybrid AI-Blockchain Framework for Secure and Scalable Internet of Nano Things Devices," in Proc. 12th Int. Conf. Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP), 2025, pp. 1–5.
2. R. Ghugare, "A Comprehensive Survey on Nano-sensor Devices and Architectures for the Internet of Nano-Things (IoNT)," J. Environ. Nanotechnol., vol. 15, no. 1, pp. 91–99, 2026.
3. A. Sharma, A. Srivastava, P. Joshi, A. Trivedi, and N. Trivedi, "An AI–IoT Enabled Nano-Sensor Skin Patch for Continuous Disease Biomarker Detection and Predictive Health Monitoring," Frontiers in Health Informatics, vol. 12, pp. 531–542, 2023.
4. A. Meenambika, S. Jayachitra, A. L. Nagamuthu, and R. K. Dhanaraj, “The Internet of Bio-Nano Things for Personalized Healthcare: Perspectives, Framework, and Research Directions,” in Future of Internet of Bio-Nano Things in Personalized Healthcare, USA: Academic Press, 2026, pp. 23–39, doi: 10.1016/B978-0-443-27604-0.00002-0.
5. [5] S. Varshney, S. Gupta, A. K. Bhunia, A. K. Pathak, S. Hazra, and A. Naskar, “Intelligent Nanosensor Network for Real-Time Environmental and Biomedical Monitoring Using Machine Learning and IoT,” in Proc. 2025 Int. Conf. Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), 2025, doi: 10.1109/RAEEUCCI63961.2025.11048190.
6. S. Bindu, M. K. Prashanth, and D. M. Kishore, "Integration of Nanotechnology and Machine Learning in Healthcare: Fundamentals, Applications, and Future Scope," in Smart Chips for Smart Devices: VLSI Design for Next-Generation IoT Solutions, 2026, pp. 1–30.
7. Sun, Y., Du, X., Niu, S., & Zhou, S. (2024). A lightweight attribute-based signcryption scheme based on cloud-fog assisted in smart healthcare. PLOS ONE, 19(1), e0297002. https://doi.org/10.1371/journal.pone.0297002
8. Nithya, S., Palanisamy, S., & Nivethitha, T. (2024). Achieving secured medical network (SMN) through stateless mechanism and SkeyM in Medical-Internet of Things (M-IoT). Journal of Engineering and Applied Science, 71, 128. https://doi.org/10.1186/s44147-024-00460-4
9. Samal, K., Sunanda, S. K., Jena, D., & Patnaik, S. (2025). A lightweight privacy preservation authentication protocol for IoMT using ECC based blind signature. Journal of Information Science. https://doi.org/10.1177/18479790251318538
10. Khan, U. H., Qamar, A., Khan, R., Alturise, F., Alshaabani, A. R., & Alkhalaf, S. (2025). Secure edge-based IoMT framework for ICU monitoring with TinyML and post-quantum cryptography. Scientific Reports, 15, 36195. https://doi.org/10.1038/s41598-025-20017-6
11. A. Rizzardi, G. Piro, S. Sicari, L. A. Grieco and A. Coen-Porisini, “Bio-molecular Cryptography for Protecting Nano-Network Transmissions in Healthcare Applications,” in 2025 13th Wireless Days Conference (WD), Niterói, Rio de Janeiro, Brazil, 2025, pp. 1-9, doi: 10.1109/WD67713.2025.11302720.
12. D. Trivedi, M. Jain, D. Patel, and L. Pathak, “Quantum-Assisted Secure Nano-Network Traffic Framework for Real-Time Medical Data Transmission in Smart Hospitals,” International Journal of Innovative Science and Research Technology, vol. 10, no. 4, pp. 3931–3938, Apr. 2025, doi: 10.38124/IJISRT/25APR1661.

13. K. R. Radhika, H. N. Shenoy, T. R. Vinay, H. Pooja, D. Sharma, R. Priyanka, and S. Gupta, “Communication-Efficient Federated Learning (CEFL) for CT image classification in bandwidth-constrained wireless healthcare networks,” International Journal of Drug Delivery Technology, vol. 16, no. 13S, pp. 163–172, 2026, doi: 10.25258/IJDDT.16.13S.17.
14. E. A. Elhadidi and A. Salah, “Quantum artificial intelligence: A comprehensive review of architectures, applications, challenges, and future directions,” International Journal of Computational Intelligence in Engineering (IJCIE), vol. 1, no. 2, pp. 35–41, 2026.