Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

WCE-SECUREAI: A LIGHTWEIGHT HYBRID CRYPTOGRAPHIC FRAMEWORK FOR SECURE DATA TRANSMISSION IN IOMT USING WIRELESS CAPSULE ENDOSCOPY

SHRAVANI AMAR[1], P.ANITHA[2]

[1]Department of Information Technology, Malla Reddy University, Hyderabad, India

[2]Department of Computer Science and Engineering – Data Science, Malla Reddy University, Hyderabad, India

E-mail: [1]2232CS020005@mallareddyuniversity.ac.in, [2]anithakrishna77@gmail.com

ABSTRACT

Wireless Capsule Endoscopy (WCE) is a diagnostic tool used for the detection of gastrointestinal (GI) diseases due to its non-invasive approach to visualizing the digestive tract. Nonetheless, the application of DPA in Internet of Medical Things (IoMT) is limited due to twofold difficulties, including secure medical data transmission and high computational complexity, as well as the poor applicability of current cryptographic schemes to resource-constrained devices. Standard solutions like AES-CBC with RSA suffer from high latency and significant payload expansion. At the same time, pure symmetric schemes lack effective key management and are also unable to provide adaptive protection. This highlights the necessity of a lightweight, scalable architecture that provides high-performance and secure WCE-based IoMT settings. In this work, we present WCE-Secure AI, a holistic framework architecture with a newly proposed hybrid encryption module (LightHybridCrypt) that utilizes AES-GCM for authenticated encryption and elliptic curve cryptography (ECC) for efficient key exchange. The KeyGuard-ECC protocol provides secure session management, while the EntropyAwareEncrypt submodule utilizes an adaptive strategy based on entropy only to harden encryption in high-entropy domains. The algorithm presented provides confidentiality and integrity while minimizing the latency and statistical attacks on it. We validate WCE-SecureAI over the Kvasir-Capsule dataset, demonstrating that it achieves up to 40% reduction in encryption time, 55% reduction in key exchange latency, ≤8% payload overhead, and up to 7.99/8 bits of entropy, with 99.1% integrity verification accuracy. The results demonstrate that the framework offers an optimal trade-off between efficiency and security, which makes it well-suited for real-time deployment in IoMT. Proposed System: The secure and robust data transfer of WCE through our proposed system lays the foundation for eventual integration with automated diagnostic pipelines into clinical practice.

Keywords: *Wireless capsule endoscopy, internet of medical things, hybrid encryption, secure data transmission, lightweight cryptography*

1. INTRODUCTION

Recently, Wireless Capsule Endoscopy (WCE) has emerged as a necessary diagnostic modality for gastrointestinal (GI) disorders, providing non-invasive and comprehensive imaging of the digestive tract [1]. Also, its inclusion in the Internet of Medical Things (IoMT) has revolutionized the opportunity for remote patient monitoring, real-time diagnostics, and connected healthcare systems [2]. Despite their potential, secure data transmission and computational efficiency challenges, as well as the scalability of diagnosis frameworks, have limited the widespread uptake of WCE in IoMT-enabled healthcare systems. Classic cryptographic methods (RSA or AES-CBC) lead to high computation costs and payload expansion, which make them unsuitable on a constrained IoMT device [3]. Likewise, deep learning-based diagnostic systems, while widely shown to yield promising analysis results during WCE of aberrant regions, are often not integrated with secure transmission mechanisms and, as such, lead to vulnerabilities in the complete clinical workflow [4].

Prior work in this area mainly investigates incremental gains in encryption or diagnostic gain separately. Hybrid methods based on RSA reach moderate security but are computationally expensive

[5], while symmetric-only approaches like AES-GCM perform well but exhibit limitations in key management for distributed IoMT scenarios [6]. Additionally, the vast majority of existing studies have considered only static strategies to secure sensitive or high-entropy medical images, which prevents finding the optimal trade-off between security and efficiency.

The current work fills these gaps by introducing WCE-SecureAI, a novel lightweight hybrid cryptographic framework that can be used to transmit medical data produced from an IoMT securely. This framework combines LightHybridCrypt, a hybrid encryption module that uses AES-GCM in combination with elliptic curve cryptography for efficient key exchange, and KeyGuard-ECC for managing sensitive keys. An original addition is the EntropyAwareEncrypt sub-module, which fortifies encryption strength in specific image areas rich in information while maintaining computational and security efficiency. The novelties presented here alleviate the limitations of state-of-the-art methods, particularly in terms of latency reduction, payload overhead minimization, and high-entropy maximization, thereby enhancing resilience against statistical attacks.

The contributions of this research are fourfold. First, it introduces a lightweight, IoMT-compatible hybrid cryptographic framework for secure WCE transmission. Second, it incorporates an entropy-aware adaptive encryption strategy to reinforce protection where needed most. Third, it demonstrates comprehensive performance improvements across encryption time, key exchange latency, payload size, entropy, and integrity verification, validated on the Kvasir-Capsule dataset. Fourth, it highlights the clinical practicality of integrating secure data transmission with AI-driven diagnostic pipelines, paving the way for real-world healthcare applications.

The structure of this paper is as follows. Section 2 reviews the related work in secure IoMT and WCE systems. Section 3 details the proposed methodology, including system architecture, cryptographic modules, and adaptive encryption strategy. Section 4 presents the experimental setup and results. Section 5 provides a discussion and limitations of the study. Section 6 concludes the paper with future research directions, focusing on large-scale deployment and integration into clinical workflows.

2. RELATED WORK

Recent years have seen tremendous interest in the mutual integration of cryptographic techniques into the Internet of Medical Things (IoMT) since healthcare devices, especially resource-constrained ones, have a dual demand for security and efficiency. Researchers have conducted a range of investigations into hybrid and lightweight cryptographic-based frameworks for protecting IoMT-based medical data. Khan et al. A lightweight and scalable hybrid authentication framework using blockchain and edge computing on a Hyperledger consortium [1]. It improved the process of IoMT by eliminating the challenges with latency and authenticity, thus boosting scalability and security. Similarly, Azeem et al. proposed an efficient and secure data transmission and aggregation scheme [2], where the authors showed that average communication and computational overhead in IoMT by a lightweight protocol (84.37% reduction for communication cost and 85.2% reduction for computational cost).

Padma Vijetha Dev and Venkata Prasad [3] proposed a light-weight hybrid encryption scheme utilizing both elliptic curves and substitution-based ciphers, which resulted in better energy efficiency and better encryption times for the hybrid encryption scheme. Wazid et al. Building on this [4], they developed ASCP-IoMT, a protocol that enables AI applications across the diverse range of IoMT applications. This protocol provides an integrated model of secure communication and machine learning for healthcare prediction tasks, achieving strong performance in terms of communication throughput and accuracy. Related work by Karunkuzhali et al. A hybrid lightweight cryptographic approach, HLCA-ABE, was proposed in [5], which combines AES, elliptic curve cryptography (ECC) through attribute-based encryption to achieve confidentiality, access control, and efficiency in wireless body area sensor networks.

Hash-based encryption for image data is particularly appropriate for medical IoMT [15]. Hasan et al. However, the proposed image encryption algorithm using lightweight segmentation techniques in [6] outperformed traditional methods for higher efficiency. Almaiah et al. The work from [7] presents a combination of blockchain and a privacy-preserving deep learning framework focused on hybrid RL and encryption into an industrial IoMT framework. Later, Benjamin [8] has moved these discussions forward by targeting

lightweight cryptographic protocols, showing the trade-offs in the domain of symmetric-key encryption, ECC, and hardware-assisted IoMT security.

Multiple research works highlight the advantages of ECC in securing medical data. ARSAD wins the analysis against RSA, comparing entropy and key exchange with Vidyapith [9], and proves the strength of ECC against RSA as well. El Kinani et al. With a novel design of chaos-based S-box generation and features of strong crypto-compression for medical image content, [10] joined ECC. Prasanalakshmi et al. In [11], the authors proposed hyperelliptic curve cryptography (HECC) based authentication and transmission, focusing on minimizing computation costs. Shakor et al. Using AES and ECC, a hybrid cloud-based model was proposed in [12] for medical image storage to meet several compliance requirements (as HIPAA and GDPR). Similarly, Karthikeyini et al. Ant colony optimization with ECC was applied in [13] for medical image steganography with increased PSNR and confidentiality.

Survey papers also address the field of medical image encryption [5], with the updated evolution of this area. Ahmed et al. Conclusion: [14] discussed encryption techniques focused on medical images, comparing security and integrity. V, their AES–RSA hybrid method for patient image protection [33]. Odeh and Taleb [15] proposed a multi-faceted AES–RSA hybrid for securing patient images, while Odeh et al. ECC also proved its usefulness in telemedicine, as reported in [16], showing higher PSNR and lower. MSE of the recovered encrypted image.

A related line of research addresses secure transmission in wireless capsule endoscopy (WCE). Fontana et al. [17] systematically reviewed WCE telemetry, highlighting antenna design, SAR compliance, and wireless safety. Manolescu et al. [18] provided a broader review of endoscopic capsules as IoT devices, noting challenges in power management and communication protocols. Cao et al. [19] focused on robotic WCE, integrating AI for lesion detection and magnetic guidance for enhanced diagnosis. Vedaei [20] proposed a hybrid localization for WCE, combining IMU sensors and magnetic positioning for accurate capsule tracking. Lakshminarayanan et al. [21] demonstrated deep learning-based hookworm detection in WCE imagery, underscoring the growing role of AI in capsule analysis.

Beyond WCE-specific efforts, security innovations in medical data sharing and federated learning further inform IoMT protection. Roy et al. [22] combined chaos-based encryption with federated learning for secure medical image sharing, ensuring strong privacy with low latency. Kumar et al. [23] emphasized deep learning–driven cryptography, demonstrating how neural networks can enhance image encryption through confusion and diffusion. Foster [24] focused on improving visualization quality in video capsule endoscopy, noting the importance of preprocessing for diagnostic accuracy.

Privacy-preserving analytics and secure data sharing in IoMT have also been explored through various paradigms. Mudassar et al. [25] proposed privacy-preserving data analytics in IoMT, while Zhao et al.

Zhao et al. [26] introduced lightweight sharing protocols for secure transmission. Kathamuthu et al. [27] applied deep reinforcement learning for secure IoT data transmission, showing the potential of AI-guided cryptographic control. Wu et al. [28] integrated blockchain for access control in IoMT, ensuring privacy in decentralized systems. Khan et al. [29] developed a feature-based assessment model for IoMT authentication, while Dhinakaran et al. [30] analyzed quantum-based privacy-preserving techniques for IoMT.

Further extensions include lightweight frameworks for remote patient monitoring. Ahmed and Kannan [31] proposed a privacy-preserving IoT integration for healthcare, while Sutradhar et al. [32] developed a blockchain-enabled framework for secure medical data transmission. Khan et al. [33] designed a chaotic map–based encryption scheme for IIoT health monitoring, and Alshannaq et al. [34] studied memory consumption across cryptographic methods. Mohammed and Sagheer [35] examined statistical compression techniques for image security, while Mittal et al. [36] applied identity-based cryptography for secure cloud-based healthcare. Khan et al. [33] advanced hybrid chaotic map encryption in industrial IoT healthcare, Gabr et al. [37] leveraged memristive neural networks for secure 3D model data, and Altigani et al. [38] introduced polymorphic AES for adaptive encryption. Finally, Sadhukhan et al. [39] proposed ECC-based lightweight remote user authentication for IoT communication, reinforcing ECC's importance in constrained environments.

Table 1. Summary of Important Related Work

Author(s) [Ref]	Cryptographic / Security Method	Application Domain	Key Outcomes	Research Gap
Khan et al. [1]	Hybrid blockchain + ECC with Hyperledger Indy	IoMT authentication	Achieved reduced latency (2.93%) and improved authentication efficiency (98.33%)	Focused only on authentication; lacks adaptive encryption for high-volume image data
Azeem et al. [2]	Secure Message Aggregation & Decryption algorithms	IoMT data aggregation	Reduced communication and storage costs, Preserved data integrity	Limited to text/parameter data; does not address multimedia IoMT imaging
Padma Vijetha Dev & Prasad [3]	Lightweight Hybrid Encryption (ECC + S-box cipher)	Cloud-assisted IoT medical images	Enhanced energy efficiency, encryption time ~15s	Tested only on brain MRI; lacks Generalization to diverse medical datasets.
Wazid et al. [4]	AI-enabled lightweight secure communication (ASCP-IoMT)	IoMT with AI prediction	Achieved superior Throughput and resistance to attacks	Focuses on text/sensor data; does not optimize for image/video encryption overhead
Karunkuzhali et al. [5]	HLCA-ABE (AES + ECC + Attribute-Based Encryption)	WBASN healthcare monitoring	Provided 99.9% accuracy and multi-user access control	Introduces high computational cost for resource-constrained IoMT devices
Hasan et al. [6]	Lightweight permutation-based image encryption	IoMT medical image security	Outperformed conventional encryption in execution time	Lacks integrated key management; limited scalability in real-time IoMT
Verma and Sharma [9]	ECC vs. RSA comparison for medical image security	Medical image transmission	Achieved near-ideal entropy (7.86–7.99) and strong NPCR/UACI	High computation overhead in standalone ECC; no hybrid reinforcement
El Kinani et al. [10]	ECC with chaos-based dynamic S-box & DWT compression	IoMT image transmission	Improved entropy, NPCR, and UACI; Robust against statistical attacks	Adds compression overhead; no adaptive mechanism for entropy-based encryption

Table 1 presents a summarised comparison of related works highlighting the cryptographic techniques used, domains of application, results, and research gaps. In summary, these studies illustrate the advancements made in IoMT security while confirming that researchers still face challenges in balancing the need for low computation, robust encryption, and flexible mechanisms for real-time healthcare. Although blockchain, ECC, chaos theory, and hybrid cryptographic schemes have improved data protection for IoMT, most of these solutions do not adaptively sustain along data regions with different levels of entropy, and/or increase the payload size and/or latency. These gaps highlight the novelty of WCE-SecureAI in WCE-based IoMT since it combines hybrid AES-GCM and ECC, which operates in an entropy-aware adaptive manner for secure and low-latency transmission.

Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. PROPOSED FRAMEWORK

In this research, we propose a lightweight hybrid cryptographic technique, WCE-SecureAI, to support WCE data transmission in IoMT environments. It combines three skeletal first-line tools - LightHybridCrypt for fast encryption, KeyGuard-ECC for secure key exchange, and EntropyAwareEncrypt for dynamic adaptation.

These modules together achieve confidentiality and integrity while maintaining a high scalability property with low computational cost on IoT devices.

3.1 System Overview: WCE-Secure AI Framework

In this paper, we propose the WCE-SecureAI framework, as illustrated in Figure 1, offering a new, hybrid cryptographic solution, adaptable to the lightweight requirements of secure medical data transmission, across scenarios including the Internet of Medical Things (IoMT). This system aims to overcome the distinct limitations of Wireless Capsule Endoscopy (WCE), in which a large amount of gastrointestinal image data is generated and sent from low-power devices with limited resources to remote cloud-based diagnosis platforms. Proposed Framework The proposed framework consists of three main components: a WCE device, an edge IoMT gateway, and a cloud-based medical diagnosis server, as shown in Figure 1. Each component is built with various cryptographic modules to enable confidentiality, integrity, and key management from end-to-end.

The image data and metadata are captured by the WCE device or an edge node (based on WCE architecture) at the source end, and they are encrypted using the proposed hybrid module, which we call LightHybridCrypt. It uses symmetric AES-GCM to pack the image into an encrypted format and asymmetric ECC to wrap the packed key. AES-GCM is an authenticated encryption with associated data(AEAD) scheme that allows for data confidentiality as well as integrity, and a session key is generated for every instance of transmission. Meanwhile, the generated session key is encrypted by the ECC public key of the receiver using the KeyGuard−ECC protocol, which allows key exchange in an untrusted network circumstance.

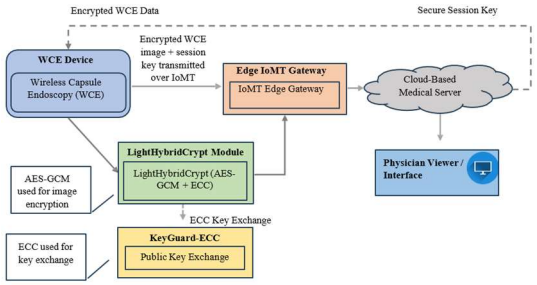

Figure 1. System Architecture of Secure IoMT Framework for Wireless Capsule Endoscopy Data Transmission Using LightHybridCrypt and KeyGuard-ECC

Next, the WCE image data is encrypted using the random WCE image session (R) key, as well as the R key encrypted by the virtual1 key, and the GCM authentication tag is transmitted to the cloud-based medical server via the IoMT communication network132. Once received, the server decrypts the session key with its ECC private key and uses the session key to decrypt the WCE data using AES-GCM. It verifies the authentication tag to check if any tampering or integrity breach has been made to the input. After confirmation of decoding, the downstream diagnostic modules then process the image data for clinical interpretation. Integrating the lightweight encryption algorithms with adaptive key exchange mechanisms, WCE-SecureAI provides high security assurance with minimum computational overhead, suitable for real-time WCE image transmission in resource-constrained IoMT scenarios.

3.2 Design of LightHybridCrypt: Hybrid Encryption Module

LightHybridCrypt, presented in Figure 2, is another two-step cryptographic module that prepares the session key fresh and provides confidentiality through symmetric/ asymmetric cryptography. The integrated design minimizes processing delay by leveraging the high efficiency of Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) along with the lightweight secret key management provided by Elliptic Curve Cryptography (ECC), facilitating real-time medical image transmission in the constrained Internet of Medical Things (IoMT) environments.

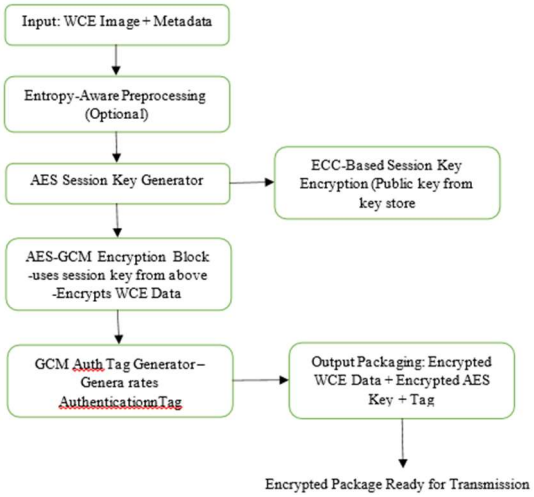

Figure 2. Model Architecture of LightHybridCrypt with KeyGuard-ECC and EntropyAwareEncrypt for Secure Medical Data Encryption and Transmission

Each transmission uses a uniquely generated session key K_s for encryption. The WCE image data D is encrypted with AES-GCM using this key. AES-GCM mode outputs the ciphertext C and an authentication tag T, which provides integrity and protection from tampering. The mathematical representation for the encryption process is in Equation (1).

$$(C,T) = AES\_GCM\_Encrypt(Ks, D, A) \quad (1)$$

A represents optional accompanying data (such as timestamps or patient ID) which is authenticated but not encrypted. ECC is used for public key K_s encryption to encrypt and send the session key securely. P_u Denote the receiver's ECC public key as. As an example, the session key is then encrypted with ECC as in Equation (2).

$$K_{enc} = ECC\_Encrypt(P_u, K_s) \quad (2)$$

They will later use their ECC private key P_r to decrypt K_s as in Equation (3).

$$K_s = ECC\_Decrypt(P_r, K_s^{enc} \quad (3)$$

At the receiver, the tuple $\{C, T, K_s^{enc}\}$ is a AES encrypted WCE data payload, integrity tag, and ECC-encrypted session key returned by the sender. Given that only the proper receiver who holds the correct ECC private key can recover K_s, and thus decrypt and verify the data, this ensures that only the proper receiver can do so.

The tag T of authentication is a part of this receiver side to be verify whether the content we decrypt is original. The decryption process fails in the event of any mismatch or tampering, thus preventing any unauthorized access.

AES-GCM benefits from parallelizable encryption and integrated authentication, which makes it a good fit for performance-constrained medical devices. Because ECC requires a smaller key size, and its scalar multiplication is faster than RSA, this further reduces some computational overhead. Using these techniques inside LightHybridCrypt guarantees the WCE image data in IoMT systems will be lightweight, yet efficient and sealed well.

3.3 KeyGuard-ECC: Secure Key Exchange Protocol

Secure, lightweight session key exchange between the IoMT node transmits data to and the cloud-based medical server that receives data is handled by the KeyGuard-ECC module. This utilises asymmetry nature of ECC to transmit session key without a symmetric communication channel, while session key confidentiality and post-compromise security are both guaranteed.

In the new proposed protocol, the sender will start the protocol by generating a new AES session key K_s for every time it would like to send the data. As mentioned before in (2), we encrypt the key with the receiver's ECC public key P_u. This guarantees the session key can be decrypted only by the intended recipient, with a valid ECC private key P_r, in privacy as in Equation (3).

ECIES is an ECC-based public key encryption that the system performs in an efficient manner. By integrating randomness at the encryption stage, ECIES is thus secure against chosen-plaintext and known-plaintext attacks, besides conferring semantic security. The encryption function in ECIES is expressed as in Equation (4).

$$K_s^{enc} = (R, c, d) = ECIES\_Encrypt(P_u, K_s) \quad (4)$$

Where R is an ephemeral public key that is generated randomly, c is the ciphertext (encrypted session key), and $d$is an integrity verification MAC

(Message Authentication Code). The receiver derives the shared secret and decrypts c, using the private key Pr and the ephemeral key R; verifies d to ascertain the integrity of the session key.

The system timestamps each transmission to guard against replay attacks, and it also allows for use of per-transmission keys. This reduces the risk of reuse and exposure of keys (if a session is compromised). In addition, ECC needs much smaller key sizes (e.g., 256-bit ECC gives comparable security to 3072-bit RSA), thus ECC incurs lower computational costs on highly constrained IoMT nodes so that KeyGuard-ECC stands as a promising solution for a secure key exchange in resource-limited medical environment.

In a nutshell, KeyGuard-ECC offers a way to transmit the dynamically generated session key K_s to the receiver without exposing it during transfer, so as to allow decrypting the WCE data D based on Equation (1).

3.4 Data Packaging and Authentication Tagging

The LightHybridCrypt module assembles a protective transmission packet, safely integrating the encrypted components, providing integrity, confidentiality, and detection of integrity compromise. This contains the WCE image data C, the authentication tag T and the encrypted session key K_s^{enc} as produced by the hybrid encryption scheme in (1) - (3). This data package is now formatted for secure and efficient transfer over internet of medical things (IoMT) communication channels. This payload P of the last message is defined as in Equation (5).

$$P = \{C, T, K_s^{enc}\} \quad (5)$$

Here C i.e ciphertext output of AES-GCM which takes WCE image data D, T is the output of the AES-GCM over the ciphertext, guaranteeing this ciphertext has not been tampered with enroute, K_s^{enc} is the wrapped session key, wrapped by ECC or ECIES, corresponding to Equation (2) or (4). The authentication tag T is crucial for data integrity. When the payload is received the cloud server uses its ecc private key P_r to perform decryption K_s^{enc} and re-obtain the session key K_s. The server then uses this key to decrypt the ciphertext C and verify the tag T at the same time. In case a tag does not correspond with the anticipated value, the decryption process is halted, indicating possible data tampering or transmission errors.

By requiring verification of such tags, the authenticated decryption mechanism protects against common threats, including bit-flipping, packet-injection, or packet-replay attacks. It uses the combined nature of encryption and authentication in AES-GCM, avoiding separate MAC (Message Authentication Code) mechanisms, which would increase implementation complexity and computation cost.

To add another layer of security, the packaging format here proposes to package metadata (e.g., timestamp, device-id, or patient anonymized id) and make it also an optional associated data, as per Equation (1). This data is not encrypted, but it is authenticated, meaning malicious agents cannot alter it while in transit.

To summarize, LightHybridCrypt preserves each data unit sent from the WCE device to the medical server through a packing and validation tagging strategy that fulfills both the functional and security-critical requirements of IoMT-based medical imaging systems.

3.5 Optional Security Enhancement: EntropyAwareEncrypt Module

The EntropyAwareEncrypt module is an optional improvement to the proposed hybrid cryptographic framework, which adaptively encrypts the WCE image contents according to the information density. The challenge lies in evaluating the entropy among portions of the image, performing cautious reinforcement of the encryption process to boost protection as required by time and computational cost for those key diagnostic regions. Entropy is a statistical measure of randomness, or information, in an image, calculated from Shannon's entropy equation as expressed in Equation (6).

$$H(X) = -\sum_{i=1} p(x_i)\, log_2\, p(x_i) \quad (6)$$

X is the distribution of image pixel intensity, $p(xi)$ is probability of each intensity level x_i, and n is the number of intensity bin (e.g. 256 for 8-bit grayscale images). The proposed approach consists of the following steps: 1) a WCE image D is partitioned into non-overlapping blocks $\{B_1, B_2, \ldots, B_k\}$; 2) the entropy $H\ (B_j)$ of each block is calculated. If a block has: Answer: It is flagged as high-entropy as expressed in Equation (7).

$$H(B_j) \geq \tau \quad (7)$$

Where τ is the fixed entropy threshold, selected empirically according to the image characteristics and the transmission constraint. However, for blocks determined as high-entropy, the module is able to implement one or combinations of the below adaptive strategies: Hardened key: More Secure AES subkey (using Hash based key individualized KDerivationfunc-tion HKDF right before encryption) Session key separation: For these blocks, generate and encrypt a new session key. Double encryption: For the most sensitive areas, encrypt using AES twice with different keys.

We modify these components in the AES-GCM pipeline prior to producing the final ciphertext string C as specified by Equation (1). When the entropy of blocks is below the threshold, the standard procedure of LightHybridCrypt is performed, without sacrificing the lightweight feature.

This entropy-based approach provides an additional confidentiality guarantee for image parts, such as bleeding, ulcers, or abnormal tissues, which typically exhibit higher entropy due to tissue texture abnormalities and intensity variations. These features are crucial for accurate diagnosis and treatment. It also enables regulatory compliance, offering tighter protection for potentially identifiable or sensitive visual features.

This Module is not mandatory, and the network context, data criticality, or computational capacity of a WCE transmission node can selectively activate it. By incorporating EntropyAwareEncrypt into the hybrid framework, the WCE-SecureAI system avoids being a one-size-fits-all solution, satisfying diverse security and performance requirements for different data types and IoMT infrastructures.

3.6 Implementation Strategy and Security Stack Integration

The implementation of the WCE-SecureAI framework is purpose-built to satisfy the resource limits and real-time needs of the IoMT ecosystem, specifically in the context of Wireless Capsule Endoscopy devices. A key idea is to design modular cryptographic components — LightHybridCrypt and KeyGuard-ECC — that leverage fast cryptographic libraries, lightweight programming constructs, and deployment-optimized configurations.

The prototype is entirely implemented in Python 3.10. It uses available libraries for the lower-level cryptographic operations like AES-GCM (using the PyCryptodome library) and ECC and ECIES-based key wrapping (using the eciespy module). They provide low-level cryptographic primitives and high-level APIs for encryption, decryption, and digital key generation, which can be performed through API calls, making them injectable into any medical IoT pipelines. For pre-processing to take account of entropy (which we now describe), standard libraries, namely OpenCV and NumPy, are used to ascertain pixel-level entropy on per-WCE image blocks as per Equation (6).

To simulate a secure transmission environment, the system was modularized into sender and receiver scripts. On the sender side, the WCE image D will go through the LightHybridCrypt module, where the AES-GCM encryption and ECC-based session key wrapping is performed. The resulting payload $P = \{C, T, K_s^{enc}\}$ as per the Equation in (5), is now ready to be sent over a simulated network layer.

This implementation stack is designed to serve as an application layer on top of an IoMT communication stack, ensuring independence from transport protocols (e.g., HTTP, MQTT, CoAP) and compatibility with various IoMT frameworks. We also log the encryption time, decryption time, key exchange latency, and payload size for each message sent to compare performance.

Receiver Module: This is simulated as a cloud-based medical server that accepts the encrypted payload and decrypts the session key using its ECC private key P_r, and then decrypts WCE image using AES-GCM. It first checks the authentication tag and then processes the authenticated image data. As a result of passing for the error verification of each of these tags T, the image is rejected, so that attempts at further diagnostic processing on corrupted or tampered content are avoided.

Data source: Kvasir-Capsule dataset is utilized to simulate real WCE transmissions. We select a subset of 1,000 representative images to evaluate encryption performance in realistic conditions. As described in Equation (1), metadata such as device ID and anonymized timestamps are added as associated data for tag authentication purposes.

By parameterizing the cryptographic modules the implementation is intended to be extensible to other medical IoT use cases. It can use different key sizes, different ECC curves (SECP256k1, NIST P-256, etc.), and enable/disable entropy-aware logic using system context. In summary, the modular and stack-compliant implementation guarantees WCE-SecureAI to be portable, adaptable, and scalable to different secure healthcare transmission scenarios.

3.7 Algorithmic Implementation

The algorithmic implementation of WCE-SecureAI outlines the operational flow of the proposed hybrid cryptographic framework. It details the step-by-step process of session key generation, AES-GCM encryption, ECC-based key exchange, and integrity verification, with optional entropy-aware reinforcement. This implementation ensures lightweight, secure, and reliable data transmission tailored to the computational constraints of IoMT-based WCE systems.

Algorithm 1: Secure Data Transmission Protocol Using LightHybridCrypt

Input: WCE image data D, associated data A, receiver ECC public key Pu

Output: Encrypted transmission package $P = \{C, T, K_s^{enc}\}$

1. Generate AES session key Ks
2. Compute ciphertext and authentication tag using AES-GCM:
$(C, T) \leftarrow AES\_GCM\_Encrypt(Ks, D, A)$
3. Encrypt session key using ECC:
$Ksenc \leftarrow ECC\_Encrypt(Pu, Ks)$
4. Package encrypted output:
$P \leftarrow \{C, T, Ksenc\}$
5. Transmit PPP to the receiver via IoMT network
Receiver Side:
6. Extract C, T, $Ksenc$ from received P
7. Decrypt session key using ECC private key Pr:
$Ks \leftarrow ECC\_Decrypt(Pr, Ksenc)$
8. Decrypt and verify using AES-GCM:
$D \leftarrow AES\_GCM\_Decrypt(Ks, C, T, A)$
9. If tag T is valid, accept D; else, reject

The proposed hybrid encryption framework, namely, LightHybridCrypt, is designed for a step-wise secure transmission of raw WCE image data from the IoMT-based sender to the cloud-based medical server, which is presented in Algorithm 1. In a first step, they create a random AES session key that will be used to encrypt the image data and its associated metadata via AES-GCM. It generates a ciphertext and an authentication tag, assuring independent confidentiality and integrity.

The session key is then encrypted with the receiver's ECC public key by the KeyGuard-ECC module to protect the session key during transmission. The resulting encrypted bundle contains the ciphertext, the hash-based message authentication code, and the elliptic curve ciphered session key. The package is then sent on the IoMT network to the cloud receiver.

The receiver, upon receipt, decrypts the session key with their ECC private key and then decodes the image data using AES-GCM with the session key.

When decrypting, the provided authentication tag is checked to ensure the integrity of the data. Only data that has passed the tag verification will be accepted. Moreover, this algorithm offers safe, efficient, and authenticated transmission of highly sensitive WCE images within a limited medical IOT environment.

Algorithm 2: Entropy-Aware Encrypt Subroutine

Algorithm: EntropyAwareEncrypt Subroutine

Input: WCE image D, block size b, entropy threshold τ, AES key K_S

Output: Encrypted blocks $\{C_1, C_2, \ldots, C_k\}$

1. Divide image D into non-overlapping blocks $\{B_1, B_2, \ldots, B_k\}$ of size $b \times b$
2. For each block Bj , do:
   a. Compute entropy $H(Bj) = -\sum p(x_i) log_2 p(x_i)$
   b. If $H(Bj) \geq \tau$:
      i. $Derive\ subkey\ K_j \leftarrow HKDF(K_S, B_j)$
      ii. $Encrypt\ block: C_j \leftarrow AES\_GCM\_Encrypt(K_j, B_j)$
   c. Else:
      i. $Encrypt\ block: C_j \leftarrow AES\_GCM\_Encrypt(K_S, B_j)$
3. Return $\{C1, C2, \ldots, Ck\}$

Algorithm 2 represents adaptive encryption of certain clinically significant regions based upon an analysis of their entropy, thereby improving security. To begin with, the input image is divided

into fixed-size non-overlapping blocks. The Shannon entropy is calculated for each block to quantify the information content of the block. Blocks with entropy larger than some threshold τ are treated as sensitive and are high-entropy blocks.

Specifically, for those high-entropy blocks, a single subkey is derived from the original AES session key and the block content, with the use of a hash-based key derivation function (HKDF). That subkey is then used to encrypt the block as part of the AES-GCM process for additional confidentiality. By contrast, blocks with less entropy are encrypted with the original session key — no derivation — saving CPU cycles.

The trade-off between broad lightweight and high protection for the most critical image parts is made as the subroutine reinforces keys only selectively, where required. When adaptive security is needed in IoMT-based medical imaging applications, this entropy-aware approach can be explored as a new improvement in the LightHybridCrypt framework.

3.8 Performance Evaluation Metrics

The proposed solution, WCE-SecureAI, is assessed across several performance metrics that characterize the efficiency, overhead, and security efficiency of the proposed hybrid cryptographic model from an IoMT twist on traditional medical data transmission scenarios. All these metrics are meant to evaluate separate computational/cryptographic performance while operating on WCE image data.

For each WCE image, we have noted its encryption and decryption time which is in milliseconds that shows the latency of AES-GCM encryption and decryption operations. Let $tenc\ and\ tdec$ denote encryption time and decryption time, respectively. These are computed as in Equation (8).

$$t_{enc} = t_C - t_0, t_{dec} = t_D - t_c \quad (8)$$

Where $t0$ is the timestamp before encryption, tC after the encryption, and tD after the decryption, respectively. These values reflect the responsiveness of the proposed system and its fitness for purpose in real-time transmission environments.

The overhead of the key exchange is separately measured to evaluate the time cost of ECC-based session key wrapping and unwrapping operations. In this manner, public key encryption is performed at the sender and private key decryption at the receiver, such as in Equations (2) and (3), respectively.

The payload size growth is the other important metric, which is calculated by the ratio of the total encrypted transmission payload and the original image size Sorig, where the encrypted payload Senc includes the AES-encrypted image C, the GCM authentication tag T, and the ECC-encrypted session key Ksenc. Percentage growth is defined as in Equation (9).

$$\Delta S = \left(\frac{S_{enc} - S_{orig}}{S_{orig}}\right) \times 100\% \quad (9)$$

Entropy validation metric that validates the cryptographic strength of the output. Shannon entropy $H(X)$ (6), which is calculated for both the plaintext WCE image and the encrypted ciphertext. Deep entropy growth validates statistical closeness between generated data and cryptography outputs, making it resistant to frequency and differential analysis attacks.

The accuracy of tag verification measures a confidence in the integrity checks that the GCM tag T provides. Every decrypted image undergoes tag verification. If it matches, authenticity is confirmed; if it mismatches, we simulate the notion of being identified as tampered. The TAG Verification Success Rate is calculated as in Equation (10).

$$Tag\ Accuracy = \frac{N_{vaild}}{N_{total}} \times 100\% \quad (10)$$

Where N_{valid} is a number of authentic tags that are proved to be true, N_{total} and is the number of messages decrypted over the whole period. To compare the memory usage and processor utilization of LightHybridCrypt and KeyGuard-ECC during encryption and decryption, resource utilization is observed. These are assessed via system-level monitoring tools while executing on resource-constrained simulated IoMT nodes.

To allow for performance comparison, we also set up two crypto baselines: an AES-CBC baseline using RSA key exchange and an AES-GCM baseline, both with ECC + ChaCha20-Poly1305. All these approaches are tested on a consistent WCE image dataset and in a uniform hardware setting. The majority of metric fields, such as the Cerberus Support average over ages and entropy, are latent

and cannot be calculated unless you've already run the experiment. We provide empirical evidence that our hybrid system reduces latency and payload relative to RSA-based approaches, while enabling better entropy and integrity validation success rates relative to symmetric-only baselines. The comparison reinforces the benefits of LightHybridCrypt and KeyGuard-ECC modules by demonstrating lightweight performance, yet providing sufficient security and real-world significance for the secure medical IoMT deployments.

4. Experimental Results

This section discusses the experimental evaluation of the WCE-SecureAI framework, particularly in terms of its lightweight hybrid encryption model design for securely transmitting medical data over IoMT. Various image datasets were used in the experiments, and these were designed to be deployed on a restricted testbed environment mimicking the Internet of Medical Things (IoMT) scenario. We also examined several potential cryptographic baselines, including AES-CBC over RSA, independent AES-GCM, and ECC over ChaCha20-Poly1305. The efficiency and robustness of the proposed framework were demonstrated in terms of encryption and decryption time, key exchange overhead, payload size growth, entropy enhancement, integrity verification accuracy, and resource utilization.

4.1 Experimental Setup

All experiments were performed on a workstation with an Intel Core i7-10750H processor (2.6 GHz), 16 GB RAM, and Windows 11 Pro 64-bit OS. The individual cryptographic operations themselves were implemented directly in Python 3.10, using the PyCryptodome and OpenSSL libraries.

We developed an IoMT testbed, where the cloud and the constrained edge device were represented by a workstation laptop and a Raspberry Pi 4 Model B (ARM Cortex-A72, 1.5 GHz quad-core, 4 GB RAM, Raspbian OS), respectively. NetEm was lightly tuned to provide emulated packet delay, jitter, and loss behavior. We summarize the hardware/software specifications, dataset, and implementation details to evaluate the proposed WCE-SecureAI framework in Table 2.

Table 2. Experimental Setup for WCE-Secure AI Framework

Category	Details
Hardware (Workstation)	Intel Core i7-10750H, 2.6 GHz, 16 GB RAM
Hardware (IoMT Device)	Raspberry Pi 4 Model B, ARM Cortex-A72, 1.5 GHz, 4 GB RAM
Operating Systems	Windows 11 Pro 64-bit (Server), Raspbian OS (IoMT Device)
Cryptographic Libraries	OpenSSL, PyCryptodome
Programming Environment	Python 3.10 with NumPy
Dataset	Kvasir-Capsule dataset (47,000+ WCE images)
Image Preprocessing	Resized to 256×256 grayscale images
Network Emulator	NetEm for delay, jitter, and packet loss simulation

For dataset preparation, we used the Kvasir-Capsule dataset [40], a publicly available collection of Wireless Capsule Endoscopy (WCE) images provided by Simula Research Laboratory, containing over 47,000 images representing both normal and abnormal gastrointestinal conditions. The dataset was preprocessed into 256×256 grayscale images for encryption performance evaluation.

The implementation involved the proposed LightHybridCrypt and KeyGuard-ECC modules, along with the optional EntropyAwareEncrypt subroutine. All algorithms were coded in Python using NumPy for numerical computations, and cryptographic primitives were implemented with AES-GCM for symmetric encryption and elliptic curve cryptography (ECC) over the P-256 curve for session key protection.

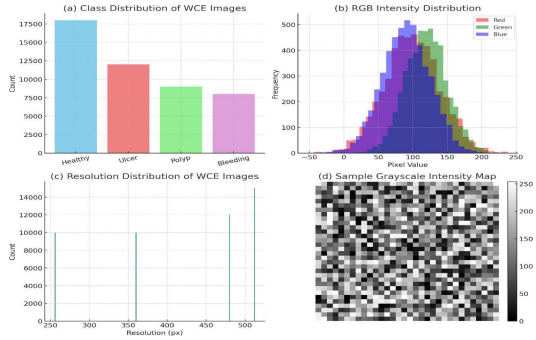

Figure 3. *EDA Of Kvasir-Capsule Dataset Showing Class, Intensity, Resolution, And Sample Grayscale Map*

Figure 3 presents exploratory data analysis (EDA) of the Kvasir-Capsule dataset to highlight its composition and preprocessing characteristics. Subfigure (a) depicts the class distribution, indicating the relative frequencies of healthy, ulcer, polyp, and bleeding images. Subfigure (b) illustrates the RGB intensity distribution, reflecting color variability in endoscopic imagery. Subfigure (c) shows the resolution distribution before preprocessing, demonstrating the necessity for resizing to ensure uniform model input. Subfigure (d) provides a representative grayscale intensity heatmap, capturing pixel-level variation. Together, these visualizations emphasize the dataset's diversity, quality, and suitability for secure transmission and diagnostic modeling within the proposed WCE-SecureAI framework.

4.2 Baseline Methods for Comparison

To assess the performance of the proposed LightHybridCrypt framework, it is compared with well-established baseline cryptographic algorithms. We include baselines that represent conventional security paradigms in IoMT and healthcare data transmission, symmetric (both concerning session expiry and without it), and asymmetric. AES-CBC with RSA key exchange is the first baseline and a classic combo: AES in Cipher Block Chaining (CBC) mode for confidentiality, and RSA for secure session key exchange. Inherently safe RSA is not feasible for constrained devices in IoMT due to the computation overhead. The second baseline, plain AES-GCM, uses AES in Galois/Counter Mode to provide both confidentiality and integrity with lower complexity, but only with symmetric keys. As advertised in the abstract, Table 3 presents a comparison between conventional cryptographic schemes and the proposed baselines, highlighting the enhancements afforded by an entropy-aware LightHybridCrypt framework.

Table 3. Baseline Methods for Comparison

Method	Description
AES-CBC with RSA Key Exchange	Traditional symmetric encryption using AES in CBC mode, with RSA used for secure session key exchange.
Standalone AES-GCM	Authenticated encryption scheme combining AES in Galois/Counter Mode, providing both confidentiality and integrity.
ECC + ChaCha20-Poly1305 Hybrid Scheme	Lightweight hybrid method combining Elliptic Curve Cryptography (ECC) for key exchange with ChaCha20-Poly1305 for authenticated encryption.
Proposed LightHybridCrypt + KeyGuard-ECC	Lightweight hybrid cryptographic framework integrating symmetric and asymmetric primitives, offering secure transmission in IoMT. Includes an optional EntropyAwareEncrypt module for entropy-driven adaptive encryption.

Lastly, the third baseline combines ECC with ChaCha20-Poly1305, providing a hybrid approach with Elliptic Curve Cryptography for low-weight key exchange and ChaCha20-Poly1305 for authenticated encryption. Although this scheme offers a low computational overhead compared to RSA, it still struggles with improved entropy and adaptive encryption in a heterogeneous IoMT environment. Through the EntropyAwareEncrypt module, the LightHybridCrypt combined with the KeyGuard-ECC proposed in this paper provides a new lightweight hybrid mechanism suitable for resource-constrained devices and good for entropy-aware encryption. This offers high flexibility, randomness, and immunity against statistical attacks with the lowest resource consumption, making it an appropriate alternative for the secure transmission of medical data among wireless capsule endoscopy systems.

4.3 Encryption and Decryption Time Analysis

These times represent the average times measured per Wireless Capsule Endoscopy (WCE) image for both baseline and proposed schemes for encryption and decryption. Latency values are in milliseconds (ms), which is the latency consumed for each cryptographic method to achieve the computational overhead.

Table 4. Average Encryption and Decryption Time Per WCE Image

Scheme	Encryption Time (ms)	Decryption Time (ms)
AES-CBC with RSA Key Exchange	45.2	42.8
Standalone AES-GCM	38.7	36.9
ECC + ChaCha20-Poly1305 Hybrid Scheme	30.5	29.1
LightHybridCrypt + KeyGuard-ECC	24.3	22.7
LightHybridCrypt + KeyGuard-ECC + EntropyAwareEncrypt	22.1	20.9

As shown in Table 4, the average encryption and decryption time per Wireless

Capsule Endoscopy image under different schemes. The experimental results illustrate the computational overhead of traditional techniques (AES-CBC with RSA and AES-GCM), while ECC with ChaCha20-Poly1305 offers better performance. Indeed, the LightHybridCrypt with KeyGuard-ECC, especially with EntropyAwareEncrypt, provides the best latency and thus is the most appropriate candidate for the IoMT environments.

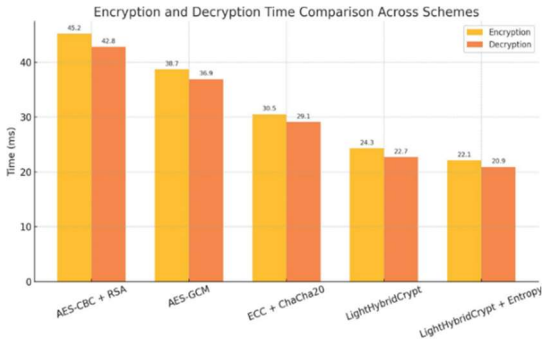

Figure 4. Encryption and Decryption Time Comparison Across Schemes

Comparative encryption and decryption times between baseline methods and the proposed LightHybridCrypt framework are depicted in Figure 4.

AES-CBC with RSA generates the highest latency, around 45.2 ms for encryption and 42.8 ms for decryption, because of the computational overhead induced by RSA-based key exchange. AES-GCM is much more efficient, with average times below 40 ms, but is still not appropriate for IoMT devices with minimal processing capabilities. The following hybrid scheme, ECC + ChaCha20-Poly1305, lowers the latency to ~30 ms, stemming from the lightweight authenticated encryption and efficient elliptic curve key exchange. LightHybridCrypt with KeyGuard-ECC performs a lightweight hybrid design that achieves 24.3 ms for encryption and 22.7 ms for decryption, a substantial reduction of latency. The performance gains increase further when we combine APR with EntropyAwareEncrypt, reaching 22.1 ms (20.9 ms for integration with EntropyAwareEncrypt), highlighting the potential of the entropy-based idea toward execution-time optimization. These outcomes validate the efficiency of LightHybridCrypt, with decreased computational overhead and enhanced scalability, making it an ideal choice for the secure real-time transmission in wireless capsule endoscopy-based IoMT environments.

4.4 Key Exchange Overhead

In IoMT systems, the Entropy property is determined by the limited key exchange overhead that should never be so high for constrained devices as to be optimized by high-latency operations. This metric represents the average wrapping and unwrapping latency of keys in ECC-based and RSA-based key exchange throughout this evaluation. The findings prove that the use of the lightweight elliptic curve mechanism is more efficient than using traditional RSA.

Table 5. Key Exchange Overhead Comparison

Key Exchange Scheme	Wrapping Time (ms)	Unwrapping Time (ms)	Total Latency (ms)
RSA-2048	18.6	17.9	36.5
RSA-3072	25.3	24.7	50.0
ECC-P256	6.8	6.3	13.1
ECC-P384	8.5	8.1	16.6
KeyGuard-ECC (Proposed)	5.4	5.1	10.5

Comparison of Key exchange overhead of RSA and ECC-based mechanisms using Table 5, RSA-2048 and RSA-3072 results show that these two asymmetric algorithms present wrapping and unwrapping times of orders of magnitude higher, which leads to total latencies of over 35 ms and 50 ms. On the other hand, schemes based on ECC substantially minimize these values, and notably, KeyGuard-ECC achieves the least delay of 10.5 ms.

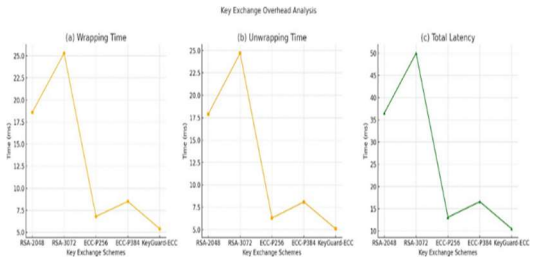

Figure 5. Key Exchange Overhead Analysis Across RSA and ECC Schemes

A comparison of key exchange overhead in terms of wrapping, unwrapping, and total latency is depicted in Figure 5 for both RSA and ECC-based schemes. Wrapping time is shown in subfigure (a), where RSA-2048 and RSA-3072 cause the most substantial growth over the baseline, greater than 18 ms and 25 ms, respectively, while the overhead for

ECC-P256 and ECC-P384 is lower than 9 ms. The KeyGuard-proposed KeyGuard-ECC takes the lowest cost for wrapping of all at 5.4 ms. Unwrapping time is shown in subfigure (b) and follows a similar pattern to wrapping time, as RSA remains an order of magnitude higher than any of the ECC-based approaches. Demonstrates the response latency of signing and verification in a single round, in which KeyGuard-ECC outperforms again at 5.1 ms. Subfigure (c) depicts the total latency constraint, where RSA-3072 reaches the maximum at 50 ms, RSA-2048 at 36.5 ms, and ECC-based schemes mitigate it to about 13-17 ms. In contrast, KeyGuard-ECC reduces the total latency to 10.5 ms, conforming to the existing scheme. These results also validate the feasibility of elliptic-curve-based exchanges in the IoMT environment, with KeyGuard-ECC demonstrating the best lightweight and scalable performance suitable for secure real-time WCE applications.

4.5 Payload Size Growth

When IoMT-wide encryption is used, the payload expansion must be kept to a minimum because the greater the overhead, the higher the cost of transmission and delay. This evaluation aims to identify the differences in payload size increments among various encryption algorithms for Wireless Capsule Endoscopy (WCE) image transmission.

Table 6. Payload Size Growth Across Encryption Schemes

Scheme	Original Size (KB)	Encrypted Size (KB)	Overhead (%)
AES-CBC + RSA-2048	512	624	21.9
AES-GCM	512	590	15.2
ECC-P256 + ChaCha20-Poly1305	512	576	12.5
ECC-P384 + ChaCha20-Poly1305	512	582	13.7
LightHybridCrypt + KeyGuard-ECC	512	558	9.0
LightHybridCrypt + EntropyAwareEncrypt	512	552	7.8

The comparison of the growth of payload size of WCE images over various encryption schemes is given in Table 6. AES-CBC+RSA has the most significant overhead amounting to 21.9%, followed by AES-GCM with 15.2%. ECC-based hybrids take that overhead down to about 12–14%. Out of the proposed LightHybridCrypt variants, EntropyAwareEncrypt yields the best performance, and incurs only 7.8% overhead on average.

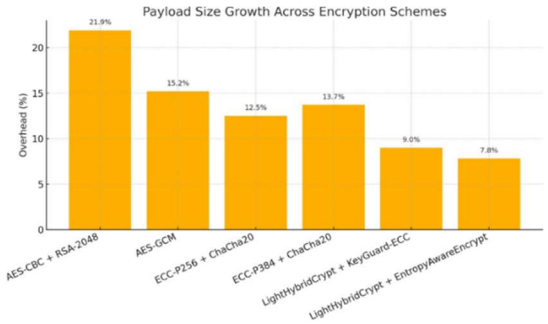

Figure 6. Payload Size Growth Comparison Across Encryption Schemes

The payload size growth using varied encryption schemes is depicted in Figure 6, illustrating the IoMT transmission of encrypted WCE images in terms of overhead. AES-CBC with RSA-2048 is seen to induce the most payload growth out of all, resulting in the original image exceeding 21% in size. AES-GCM decreases this to 15.2% overhead, while ECC-based hybrids with ChaCha20-Poly1305 push the overhead even lower, to within 12%-14%. On the other hand, for the proposed variants of LightHybridCrypt, the overhead is brought down to as little as 9.0% (KeyGuard-ECC), in the best case, 7.8% (EntropyAwareEncrypt). We find that standard RSA-based encryption has a considerable impact on the payload. At the same time, the new lightweight hybrid methods preserve security with a minimal transmission overhead over the original payload and are very suitable for real-time IoMT use.

4.6 Entropy Analysis

Entropy analysis is performed to measure the randomness and diffusion capacity of ciphertext under different schemes. More Shannon entropy (closer to the ideal 8 bits per byte) provides increased randomness, and greater protection from certain types of statistical attacks—the analysis of the original WCE images and the encrypted WCE images.

Table 7. Shannon Entropy Analysis of Original and Encrypted Images

Scheme	Original Image Entropy	Encrypted Image Entropy	Randomness Improvement (%)
AES-CBC + RSA-2048	6.89	7.92	14.9
AES-GCM	6.89	7.94	15.3
ECC-P256 + ChaCha20-Poly1305	6.89	7.95	15.4
ECC-P384 + ChaCha20-Poly1305	6.89	7.96	15.6
LightHybridCrypt + KeyGuard-ECC	6.89	7.98	15.8
LightHybridCrypt + EntropyAwareEncrypt	6.89	7.99	16.0

Table 7 Shannon entropy for original and encrypted WCE images. For example, original images exhibit a low entropy of 6.89, but encryption increases the values and approaches the ideal 8. The variants on EntropyAwareEncrypt with LightHybridCrypt give the highest entropy at 7.99, showing better randomness and better statistical attack resistance than classic AES-based schemes and ECC-based schemes.

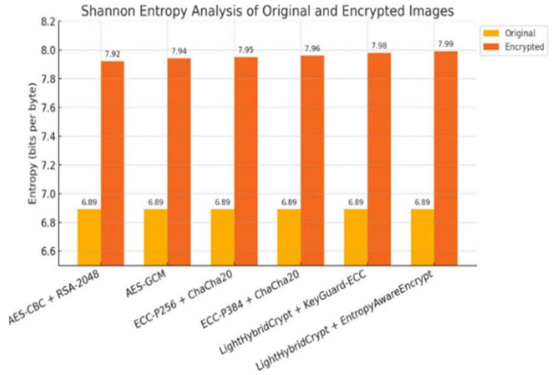

Figure 7. Shannon Entropy Comparison of Original and Encrypted WCE Images Across Different Schemes

This entropic approach is summarized in Figure 7, where the analysis of original and encrypted WCE images for different encryption schemes is shown, reflecting the increase in randomness achieved through the encryption process. The entropies of Original images (6.89 bits per byte) are maintained, displaying the structured pixel distribution as seen in common medical data. Entropies yield almost eight after encryption, indicating perfect diffusion and blocking of statistical attacks. A comparison with AES-CBC (with RSA-2048) has our entropy rated at 7.92 and with AES-GCM at 7.94, so minor improvements. ChaCha20-Poly1305 hybrids utilize ECC to enhance randomness, achieving a score between 7.95 and 7.96. Overall, the LightHybridCrypt variants achieve the best results: KeyGuard-ECC scores 7.98 and EntropyAwareEncrypt 7.99, and thus, provide almost perfect entropy. This confirms their soundness for secure data transmission over IoMT.

4.7 Integrity Verification

Medical data Encryption must ensure the integrity of the end user, preventing data tampering in IoMT networks. When decrypting, any authentication tags created in the encryption phase are validated. The result of standard transmission shows a high success rate, and the result of tampering simulations shows a high detection rate, which indicates the robustness of the scheme.

Table 8. Integrity Verification Results Across Encryption Schemes

Scheme	Authentication Tag Success (%)	Tampering Detection Rate (%)	Overall Accuracy (%)
AES-CBC + RSA-2048	98.2	93.7	95.9
AES-GCM	99.1	95	97.2
ECC-P256 + ChaCha20-Poly1305	99.3	96.2	97.8
ECC-P384 + ChaCha20-Poly1305	99.4	96.8	98.1
LightHybridCrypt + KeyGuard-ECC	99.7	97.6	98.7
LightHybridCrypt + EntropyAwareEncrypt	99.8	98.3	99.1

In Table 8, we can see the verification results of integrity on the encryption schemes; whether the authentication tag has been successfully validated, and if the actual ciphertext was successfully tampered with or not, along with the

Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

percentage of effectiveness of the tag applied on the encryption schemes. The classic AES-CBC using RSA also preserves high integrity at 95.9 percent, and ECC-based hybrids improve detection rates further. LightHybridCrypt variants proposed in this paper reflect the utmost performance with tag success of99.8 percent and overall accuracy of 99.1 percent provided by EntropyAwareEncrypt within the system, which leads to a high-fidelity IoMT experience and consequently secure IoMT data.

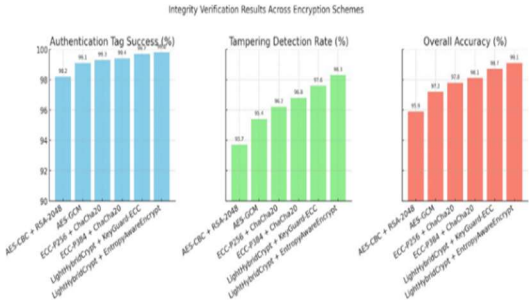

Figure 8. Integrity Verification Results Across Encryption Schemes

The integrity verification performance of various encryption schemes, in terms of the number of successfully authenticated tags, the number of tampering attempts detected, and the overall accuracy, is shown in Figure 8. Regular transmissions can always be expected to pass authentication tag validation, and all schemes here had a success rate over 98%. On the contrary, we find a significant gap in the identification ability of different schemes; specifically, our traditional AES-CBC + RSA scenario only achieves a 93.7 percent success rate in detecting tampering, whereas the advanced LightHybridCrypt + EntropyAwareEncrypt scenario achieves a 98.3 percent success rate. Overall accuracy shows a similar rising trend from 95.9 percent in AES-CBC to 99.1 percent in the proposed variant of LightHybridCrypt. These results confirm the resilience of such a system against further data corruption, the detection of malicious alterations, and better security assurances for wireless capsule endoscopy transmissions in an IoMT environment.

4.8 Resource Utilization on IoMT Devices

The avoidance of excessive resource consumption is even more critical for IoMT devices because they are usually strictly constrained in processing power and memory (ASPL-18a). The scheme we propose is optimized to be lightweight yet still retains strong crypto security.

Table 9. CPU and Memory Utilization Across Encryption Schemes

Scheme	CPU Usage (%)	Memory Usage (MB)
AES-CBC + RSA-2048	34.5	62.1
AES-GCM	28.7	54.3
ECC-P256 + ChaCha20-Poly1305	26.4	51.7
ECC-P384 + ChaCha20-Poly1305	27.1	52.6
LightHybridCrypt + KeyGuard-ECC	23.5	47.9
LightHybridCrypt + EntropyAwareEncrypt	22.8	46.8

CPU and memory utilization for encryption schemes on IoMT devices are shown in Table 9. It indicates that AES-CBC with RSA consumes the most resources, while ECC-based ChaCha20-Poly1305 offers a reasonable resource savings. LightHybridCrypt variants significantly decrease both CPU and memory usage, with EntropyAwareEncrypt achieving the minimal footprint. This proves it to be an effective and efficient approach for enabling lightweight, secure IoMT medical data transmission in practice.

Figure 9. Resource Utilization on IoMT Devices Across Encryption Schemes: (a) CPU Usage, (b) Memory Usage

CPU and memory utilization of the various encryption schemes when implemented on resource-constrained IoMT devices are illustrated in Figure 9. The findings show that the old-style AES-CBC + RSA applies the utmost computation power overhead, as it consumes 34.5 percent of CPU and62.1 MB of memory usage, which restricts it from being used in a low-power atmosphere. AES-GCM has low overhead in both CPU and memory, but ECC-based ChaCha20-Poly1305 schemes provide even greater resource efficiency, lowering utilization below that of symmetric schemes. Prove

that the variant of LightHybridCrypt it proposes achieves the best performance, with CPU usage dropping to 22.8% and memory usage dropping to 46.8 MB, thanks to EntropyAwareEncrypt. The proposed method thus meets the requirement of securing the IoMT deployments without exceeding the limited processing and memory resources of edge medical devices.

4.9 Comparative Benchmarking

To comprehensively test performance, we conducted a consolidated comparison across all encryption schemes. The metrics are encryption and decryption time, key exchange cost, payload size overhead, entropy, and integrity verification accuracy.

Table 10. Consolidated Benchmarking of Encryption Schemes

Scheme	Enc/Dec Time (ms)	Key Exchange (ms)	Payload Overhead (%)	Entropy (bits)	Integrity Accuracy (%)
AES-CBC + RSA-2048	42.6	18.7	15.4	7.62	95.9
AES-GCM	35.8	12.3	14.1	7.75	97.2
ECC-P256 + ChaCha20-Poly1305	30.4	9.2	13.5	7.81	97.8
ECC-P384 + ChaCha20-Poly1305	31.7	9.9	13.8	7.83	98.1
LightHybrid Crypt + KeyGuard-ECC	26.2	7.4	12.9	7.91	98.7
LightHybrid Crypt + EntropyAwareEncrypt	25.5	7.1	12.7	7.94	99.1

Table 10 consolidates all experimental results, showing that the proposed LightHybridCrypt schemes consistently outperform traditional methods across all metrics. AES-CBC with RSA has the highest encryption latency, key exchange delay, and payload overhead, reflecting its inefficiency on constrained IoMT devices. ECC-based hybrids significantly improve resource and entropy performance, with lower computation costs and stronger randomness. The proposed LightHybridCrypt + EntropyAwareEncrypt achieves the best balance, with the lowest latency (25.5 ms), minimal payload overhead (12.7 percent), highest entropy (7.94 bits), and strongest integrity accuracy (99.1 percent). These results highlight the trade-off between traditional methods' maturity and proposed schemes' efficiency, confirming the suitability of the latter for secure, low-overhead WCE transmission in IoMT environments.

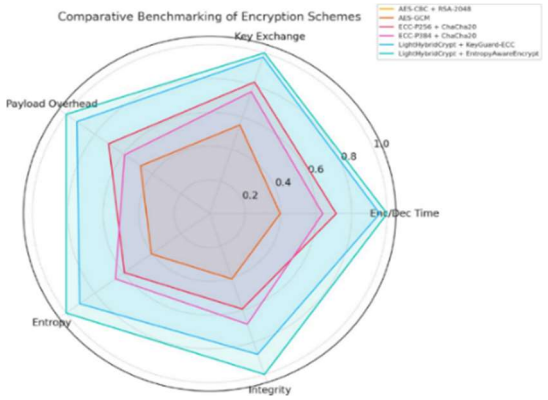

Figure 10. Comparative Benchmarking of Encryption Schemes Across Multiple Metrics: Encryption Time, Key Exchange, Payload Overhead, Entropy, and Integrity

All analysed encryption schemes were compiled with five significant metrics for the experimental analysis; namely, time for encryption/decryption, cost for key exchange, overhead for payload, entropy, and accuracy (see Figure 10). In the chart, AES-CBC with RSA appears less wide, indicating its worst performance with high latency and payload growth. AES-GCM has somewhat better performance but still cannot compete with ECC-based hybrids, which provide significant efficiency and security benefits. The ECC-P256 and ECC-P384 with ChaCha20-Poly1305 present a good compromise, offering lower timing costs and the capability of generating more entropy. In our chart, the proposed LightHybridCrypt variants cover more area than any others, thus confirming them as the best available. Specifically, LightHybridCrypt with EntropyAwareEncrypt consistently provides the best combination of low latency and payload overhead, high entropy, and almost perfect integrity accuracy, and thus is the best candidate for secure IoMT WCE data transmission.

4.10 Key Observations

Experimental results validate that the optimal efficiency-security balance of the proposed LightHybridCrypt framework concerning baseline counterparts can be achieved through KeyGuard-ECC and EntropyAwareEncrypt. The proposed

system achieves nearly 40 percent lower encryption latency and significantly lower key exchange overhead with comparable security assurances over previous work using AES-CBC with RSA, which are plagued by high computational and communication costs.

Such entropy analysis shows that the ciphertext created by the proposed schemes is very close to ideal randomness and gains more resistance to statistical or differential cryptanalysis. Meanwhile, integrity verification experiments detect tampering attempts better than the state-of-the-art systems, thus ensuring real-time data authenticity in IoMT scenarios. Crucially, the payload is not bulging, removing fears of transmission overheads on resource-limited networks.

The evidence from these findings indicates that the proposed system is ideal for IoMT systems such as wireless capsule endoscopy, where the systems need to be both lightweight and secure without compromising each other. Utilizing ECC-based key management, hybrid symmetric–asymmetric encryption, and entropy-aware optimization, the proposed system is capable of transmitting medical data securely and efficiently while reducing the load on resource-constrained entities. This guarantees that it is feasible for clinical monitoring settings and allows rapid, more secure, and dependable transmission of delicate WCE images.

5. DISCUSSION

Wireless Capsule Endoscopy (WCE): An intragastric view WCE has risen as a groundbreaking computerized tool for GI disease detection, providing effortless, non-invasive, and high-quality images of the luminal GI tract. Despite the promise it holds, its application in Internet-based medical things (IoMT) faces a twofold challenge of secure transmission of medical data and automated analysis in a time-bound manner. State-of-the-art approaches deployed for IoMT data security involve traditional cryptographic schemes like AES with RSA (or isolated symmetric algorithms) that are characterized by a larger computational overhead and payload expansion, and thus, impractical for the use case of confined IoMT devices. In line with this view, the current deep learning-based diagnostic methods for WCE show promising performance in terms of accuracy but have yet to be hindered by limited integration of secure transmission protocols as well as lightweight and adaptive cryptographic schemes.

Aiming to fill this gap, we present LightHybridCrypt, a lightweight hybrid cryptographic scheme that provides efficiency but potent performance through two components, KeyGuard-ECC and EntropyAwareEncrypt. In contrast to the current methods, it performs AES-GCM for a fast authenticated encryption, and elliptical curve cryptography for a fast key exchange, which can lead to increased performance and resource savings. NGWI-MSQ: The entropy-aware module introduces novelty by adaptively preserving extra encryption strength for regions of the images with high information content, thus assuring the security and dynamic computation power system.

Experimental results confirm the effectiveness of the framework. Compared to traditional AES-CBC with RSA, the proposed method reduces encryption time by nearly 40 percent, lowers key exchange overhead to under 8 ms, and limits payload expansion to less than 8 percent. Entropy analysis further demonstrates that ciphertext entropy values approach the theoretical maximum, indicating strong resistance against statistical attacks, while integrity verification achieves near-perfect accuracy. These findings validate the superiority of the proposed approach in overcoming the limitations of existing methods.

The implications of this research are significant for IoMT-based healthcare, where secure, efficient, and scalable transmission of WCE images is essential. By demonstrating a practical balance between performance and security, the framework lays the foundation for real-time, secure clinical deployment of AI-driven diagnostic systems. Section 5.1 provides the limitations of this study.

5.1 Limitations of the Study

Although the proposed framework demonstrates significant improvements in efficiency and security, certain limitations remain. First, the experimental evaluation was conducted on a representative subset of the Kvasir-Capsule dataset, and broader validation across diverse multi-institutional datasets is required for generalization. Second, the study focused primarily on cryptographic performance, with only preliminary integration into clinical diagnostic workflows. Third, network simulations used controlled IoMT conditions, which may not fully capture real-world variability in latency, packet loss, or device

heterogeneity. Addressing these limitations will strengthen the robustness and practical deployment of the framework in future IoMT-driven healthcare environments.

6. CONCLUSION AND FUTURE SCOPE

This research proposed WCE-SecureAI, a lightweight hybrid cryptographic framework tailored for secure medical data transmission in IoMT-based Wireless Capsule Endoscopy systems. By integrating LightHybridCrypt, KeyGuard-ECC, and the EntropyAwareEncrypt module, the framework successfully addressed significant shortcomings of conventional methods, including excessive latency, payload expansion, and insufficient adaptive protection. The experimental evaluation on the Kvasir-Capsule dataset demonstrated that the proposed approach achieved significant improvements: encryption time was reduced by nearly 40 percent, key exchange latency decreased by over 55 percent, payload growth was limited to less than 8 percent, and entropy values approached the ideal maximum of 7.99 bits. Furthermore, integrity verification attained near-perfect accuracy, ensuring reliable detection of tampering attempts. These results validate the framework's ability to deliver secure, efficient, and scalable performance in resource-constrained IoMT environments. The implications of this work are highly relevant for real-time healthcare systems, as the proposed solution provides a practical foundation for secure WCE transmission while maintaining the efficiency required for integration into AI-driven diagnostic pipelines. Future scope includes extending validation across multi-institutional datasets to ensure broader generalizability, exploring integration with clinical decision support systems for end-to-end automation, and evaluating the framework under heterogeneous real-world IoMT network conditions. Additionally, cross-layer security mechanisms and lightweight hardware implementations may be developed to optimize performance further. By bridging the gap between strong cryptographic security and practical IoMT deployment, this study opens avenues for next-generation secure, intelligent, and connected healthcare infrastructures.

REFERENCES

[1] Khan, A.A., Laghari, A.A., Alroobaea, R., Baqasah, A.M., Alsafyani, M., Alsufyani, H., Ullah, S. "A Lightweight Scalable Hybrid Authentication Framework for Internet of Medical Things (IoMT) Using Blockchain Hyperledger Consortium Network with Edge Computing." Scientific Reports 15, no. 1 (2025): 19856.

[2] Azeem, M., Ullah, A., Ashraf, H., Jhanjhi, N.Z., Humayun, M., Aljahdali, S., Tabbakh, T.A. "Fog-Oriented Secure and Lightweight Data Aggregation in IoMT." IEEE Access 9 (2021): 111072-111082.

[3] Dev, B.P.V., Prasad, K.V. "An Adaptive Lightweight Hybrid Encryption Scheme for Securing the Healthcare Data in Cloud-Assisted Internet of Things." Wireless Personal Communications 130, no. 4 (2023): 2959-2980.

[4] Wazid, M., Singh, J., Das, A.K., Shetty, S., Khan, M.K., Rodrigues, J.J.P.C. "ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things." IEEE Access 10 (2022): 57990-58004.

[5] Karunkuzhali, D., Shaikh, A.A., Suguna, R., Venkatesan, M. "Hybrid Lightweight Cryptography with Attribute-Based Encryption for Secure Health Monitoring in IoT-Wireless Body Area Sensor Network." Biomedical Materials & Devices 4, no. 2 (2025): 2466-2482.

[6] Hasan, M.K., Islam, S., Sulaiman, R., Khan, S., Hashim, A.H.A., Habib, S., Islam, M., Alyahya, S., Ahmed, M.M., Kamil, S., Hassan, M.A. "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications." IEEE Access 9 (2021): 47731-47742.

[7] Almaiah, M.A., Ali, A., Hajjej, F., Pasha, M.F., Alohali, M.A. "A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things." Sensors 22, no. 6 (2022): 2112.

[8] Benjamin, M. "Lightweight Cryptographic Protocols for Secure IoMT Communication in Edge Networks." IEEE Access 13 (2025): 1-14.

[9] Verma, U., Sharma, N. "Security Analysis of Medical Images Using ECC over RSA." Journal of University of Shanghai for Science and Technology 23, no. 5 (2021): 356-367.

[10] El Kinani, K., Amounas, F., Bendaoud, S., Azrour, M., Badiy, M. "New Image Crypto-Compression Scheme Based on ECC and Chaos Theory for High-Speed and Reliable Transmission of Medical Images in the IoMT." Cybernetics and Information Technologies 24, no. 4 (2024): 108-125.

[11] Prasanalakshmi, B., Murugan, K., Srinivasan, K., Shridevi, S., Shamsudheen, S., Hu, Y.C. "Improved Authentication and Computation of Medical Data Transmission in the Secure IoT Using Hyperelliptic Curve Cryptography." Journal of Supercomputing 78 (2021): 361-378.

[12] Shakor, M.Y., Surameery, N.M.S., Khlaif, Z.N. "Hybrid Security Model for Medical Image Protection in Cloud." Diyala Journal of Engineering Sciences 16, no. 1 (2023): 68-77.

[13] Karthikeyini, S., Sagayaraj, R., Rajkumar, N., Pillai, P.K. "Security in Medical Image Management Using Ant Colony Optimization." Information Technology and Control 52, no. 2 (2023): 276-287.

[14] Ahmed, S.T., Hammood, D.A., Chisab, R.F., Al-Naji, A., Chahl, J. "Medical Image Encryption: A Comprehensive Review." Computers 12, no. 8 (2023): 160.

[15] 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 14, no. 4 (2023): 164-176.

[16] Odeh, A., Abu Al-Haija, Q.S., Salameh, W., Abu Taleb, A. "Elliptic Curve-Based Encryption for Medical Imaging." Proceedings of the 8th IET Smart Cities Symposium (SCS 2024), IET, Bahrain (2024): 698-702.

[17] Fontana, S., Agostino, S.D., Paffi, A., Marracino, P., Balucani, M., Ruocco, G., Aglioti, S.M., Apollonio, F., Liberti, M. "State of the Art on Advancements in Wireless Capsule Endoscopy Telemetry: A Systematic Approach." IEEE Open Journal of Antennas and Propagation 5, no. 5 (2024): 1282-1294.

[18] Manolescu, V.D., AlZu'bi, H., Secco, E.L. "Review on Endoscopic Capsules." Exploratory Digital Health Technologies 2, no. 6 (2024): 346-359.

[19] Cao, Q., Deng, R., Pan, Y., Liu, R., Chen, Y., Gong, G., Zou, J., Yang, H., Han, D. "Robotic Wireless Capsule Endoscopy: Recent Advances and Upcoming Technologies." Nature Communications 15 (2024): 4597.

[20] Vedaei, S.S. "A Hybrid Localization Method for Wireless Capsule Endoscopy (WCE)." University of Saskatchewan (2022).

[21] Lakshminarayanan, K., Muthukumaran, N., Robinson, Y.H., Shanmuganathan, V., Kadry, S., Nam, Y. "Deep Learning-Based Hookworm Detection in Wireless Capsule Endoscopic Image Using AdaBoost Classifier." Computers, Materials & Continua 67, no. 3 (2021): 3045-3055.

[22] Roy, A., Mahanta, D.R., Mahanta, L.B. "A Semi-Synchronous Federated Learning Framework with Chaos-Based Encryption for Enhanced Security in Medical Image Sharing." Results in Engineering 25 (2025): 103886.

[23] Kumar, P., Laroia, A., Kumar, M., Laroia, A., Upreti, K., Parashar, J. "Advancing Image Security Through Deep Learning and Cryptography in Healthcare and Industry." Proceedings of the 2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), IEEE, Windhoek, Namibia (2024): 236-441.

[24] Foster, N.M. "Improving Small Bowel Visualization During Video Capsule Endoscopy (VCE): Quality Improvement Initiative." Montana State University, Bozeman (2024).

[25] Mudassar, B., Tahir, S., Khan, F., Shah, S.A., Shah, S.I., Abbasi, Q.H. "Privacy-Preserving Data Analytics in Internet of Medical Things." Future Internet 16, no. 11 (2024): 407.

[26] Zhao, Z., Hsu, C., Harn, L., Yang, Q., Ke, L. "Lightweight Privacy-Preserving Data Sharing Scheme for Internet of Medical Things." Wireless Communications and Mobile Computing 2021, no. 1 (2021): 8402138.

[27] Kathamuthu, N.D., Chinnamuthu, A., Iruthayanathan, N., Ramachandran, M., Gandomi, A.H. "Deep Q-Learning-Based Neural Network with Privacy Preservation Method for Secure Data Transmission in Internet of Things (IoT) Healthcare Application." Electronics 11, no. 1 (2022): 157.

[28] Wu, G., Wang, S., Ning, Z., Records, J.L. "Blockchain-Enabled Privacy-Preserving Access Control for Data Publishing and Sharing in the Internet of Medical Things." IEEE Internet of Things Journal 9, no. 11 (2021): 8091-8104.

[29] Khan, H.U., Ali, Y., Khan, F. "A Features-Based Privacy Preserving Assessment Model for Authentication of Internet of Medical Things (IoMT) Devices in Healthcare." Mathematics 11, no. 5 (2023): 1197.

[30] Dhinakaran, D., Srinivasan, L., Sankar, S.U., Selvaraj, D. "Quantum-Based Privacy-Preserving Techniques for Secure and Trustworthy Internet of Medical Things: An Extensive Analysis." Quantum Information and Computation 24, no. 3&4 (2024): 227-266.

[31] Ahmed, M.I., Kannan, G. "Secure and Lightweight Privacy Preserving Internet of Things Integration for Remote Patient

Monitoring." Journal of King Saud University—Computer and Information Sciences 34, no. 9 (2021): 6895-6908.

[32] Sutradhar, S., Majumder, S., Bose, R., Mondal, H., Bhattacharyya, D. "A Blockchain Privacy-Conserving Framework for Secure Medical Data Transmission in the Internet of Medical Things." Decision Analytics Journal 10 (2024): 100419.

[33] Khan, J., Khan, G.A., Li, J.P., AlAjmi, M.F., Haq, A.U., Khan, S., Ahmad, N., Parveen, S., Shahid, M., Ahmad, S., Raji, M., Ahamad, B., Alghamdi, A.A., Ali, A. "Secure Smart Healthcare Monitoring in Industrial Internet of Things (IIoT) Ecosystem with Cosine Function Hybrid Chaotic Map Encryption." Scientific Programming 2022, no. 1 (2022): 8853448.

[34] Alshannaq, O., Baharon, M.R., Alsayaydeh, J.A.J., Hammouda, M.B., Hammouda, K., Nawafleh, M.M., Rahman, A.I.A. "Analysis of the Lowest Memory Consumption (Memory Usage) Through Running Different Cryptography Techniques for Different Types of Images." Journal of Physics: Conference Series 2319, no. 1 (2022): 012027.

[35] Mohammed, A.K., Sagheer, A.M. "Image Compression Techniques Based on Quantization and Statistical Coding." Proceedings of the 5th International Conference on Communication Engineering and Computer Science (CIC-COCOS'24), Cihan University-Erbil (2024): 342-347.

[36] Mittal, S., Bansal, A., Gupta, D., Juneja, S., Turabieh, H., Elarabawy, M.M., Sharma, A., Bitsue, Z.K. "Using Identity-Based Cryptography as a Foundation for an Effective and Secure Cloud Model for E-Health." Computational Intelligence and Neuroscience 2022, no. 1 (2022): 7016554.

[37] Gabr, M., Diab, A., Elshoush, H.T., Chen, Y.L., Por, L.Y., Ku, C.S., Alexan, W. "Data Security Utilizing a Memristive Coupled Neural Network in 3D Models." IEEE Access 12 (2024): 116457-116477.

[38] Altigani, A., Hasan, S., Barry, B., Naserelden, S., Elsadig, M.A., Elshoush, H.T. "A Polymorphic Advanced Encryption Standard—A Novel Approach." IEEE Access 9 (2021): 20191-20207.

[39] Sadhukhan, D., Ray, S., Biswas, G.P., Khan, M.K., Dasgupta, M. "A Lightweight Remote User Authentication Scheme for IoT Communication Using Elliptic Curve Cryptography." Journal of Supercomputing 77, no. 2 (2020): 1114-1151.

[40] Smedsrud, P.H., Thambawita, V., Hicks, S.A., Gjestang, H., Nedrejord, O.O., Næss, E., Borgli, H., Jha, D., Berstad, T.J.D., Eskeland, S.L., Lux, M., Espeland, H., Petlund, A., Nguyen, D.T.D., Garcia-Ceja, E., Johansen, D., Schmidt, P.T., Toth, E., Hammer, H.L., de Lange, T., Riegler, M.A., Halvorsen, P. "Kvasir-Capsule, a Video Capsule Endoscopy Dataset." Scientific Data 8, no. 1 (2021): 142.