IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Iomt-Based Embedded Systems For Healthcare: Advancing Security From Cryptography To Dynamic Key-Based Steganography

[1]Aaron Baby Manoj, [2]Dr Sruthy S
[1]Student, [2]Professor
[1] Computer Science and Engineering (Cyber Security),
[1] St. Joseph's college of Engineering & Technology, Palai, India

Abstract: The Internet of Medical Things (IoMT) connects hospitals, clinicians, and patients through wearables, bedside instruments, and clinical apps linked to cloud and edge services. This connectivity reduces response times and allows for continuous care. However, it also puts highly sensitive data at risk of interception and tampering. Over the past few years, security designs for medical devices have evolved through several phases. Initially, there were heavy public-key systems that provided strong protection but put a strain on small devices. Next came hybrid methods that combined encryption with steganography to hide signals in plain sight. Recently, integrated approaches have emerged that link dynamic key generation with covert embedding to keep secrets fresh and hard to detect. This paper outlines that progression, explains why each step was necessary, and compares the technical trade-offs while focusing on embedded limitations. We conclude with a practical workflow that integrates session keys and medical image steganography. We also highlight research directions in post quantum readiness, AI-assisted monitoring, and energy-aware design.

Index Terms **-** Internet of Medical Things (IoMT), embedded healthcare, steganography, dynamic key generation, lightweight cryptography, privacy, secure telemetry

I. INTRODUCTION

Healthcare is quickly shifting to a data-driven model. Outside the hospital, smart patches and wearables keep track of heart rhythm, oxygen levels, and glucose trends. Inside, devices like infusion pumps, ventilators, and imaging suites constantly generate telemetry. Clinical portals and mobile apps collect, label, and process these measurements in the cloud. This expanded system, often called the Internet of Medical Things (IoMT), changes how clinicians interact with patients. It allows for remote monitoring, timely alerts, and tailored interventions. However, the same features that make IoMT effective also pose significant security challenges. Devices communicate over open radio frequencies, run on small batteries for weeks or months, and need to ensure immediate care. Meanwhile, the data they transmit—vital signs, images, prescriptions, and identifiers—must be safe and private. Traditional security measures from enterprise IT are not suitable for the IoMT environment. Public-key cryptography

provides strong confidentiality and integrity, but its computational and memory demands can be too much for low-power microcontrollers. On the other hand, using steganography to conceal information can divert attention from the existence of a message. However, relying solely on covert channels does not offer the solid cryptographic assurances needed. These challenges have led to research focused on combining methods: maintain cryptography but reduce its demands, incorporate covert embedding without harming clinical image quality, and change secrets more frequently to prevent cascading failures. This work summarizes that evolution along with its insights. We start with techniques that establish a strong confidentiality baseline, including post-quantum strategies to prepare for future threats. Next, we examine hybrids that encrypt first and hide second, describe lightweight key-exchange methods for low-power radios, and provide overviews that outline the healthcare security landscape. A notable integrated model—using fresh session keys with reversible steganographic embedding in medical images—gets special attention because it aligns with IoMT realities: devices are compact, connections can be unreliable, and data must blend with legit imate clinical traffic. Throughout the discussion, we emphasize practical decisions: what to measure (latency, energy, image quality), how to rotate keys, and where steganography makes sense.

A- Design goals for IoMT security • Strong confidentiality and integrity for data in motion and at rest. • Low overhead in CPU, RAM, and airtime to preserve battery life and responsiveness. • Graceful key management: secrets rotate often and never linger in plain text. • Regulatory awareness: methods align with privacy obli gations without disrupting workflow. • Clinical safety: security must not degrade diagnostic quality or device behavior

B. Threat model- We assume eavesdroppers on local wireless links, active network attackers who can replay and change messages, and occasional endpoint compromises, such as stolen gateways or misconfigured services. Insider misuse can happen, but it does not fall within the scope of our cryptographic methods. Our focus is on making captured traffic difficult to read and hard to fake

II. LITERATURE REVIEW

A. 2018: Lattice-Based Public Key Cryptosystem for IoT [1] Chaudhary et al. present a detailed study on how lattice based public key cryptosystems (LB-PKC) can secure the Internet of Things (IoT). This research is driven by the rapid rise of IoT across various industries like healthcare, transportation, and energy. This growth has led to an increase in cyber attacks targeting IoT systems. The paper highlights several significant attacks, including the Mirai botnet, Petya/NotPetya ransomware, and targeted denial-of-service incidents. This underscores the urgent need for stronger cryptographic solutions that can withstand both classical and quantum threats. Traditional cryptographic algorithms such as RSA and ECC are widely used, but they face scalability challenges in the IoT due to their high computational and communication costs. With the rise of quantum computing, Shor's algorithm poses a threat to the security of RSA and ECC. This makes them unsuitable for ensuring long-term data confidentiality in IoT and especially in IoMT systems. LB-PKC offers a promising alternative. It is based on tough problems like the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP), which remain difficult even for quantum computers. The authors provide a classification of lattice-based techniques, discussing NTRU, Learning With Errors (LWE), and Ring-LWE (RLWE) approaches. NTRU allows for efficient encryption and decryption but requires larger key sizes. LWE based systems use noise to hide linear equations, making them resilient against lattice attacks. RLWE further enhances efficiency by integrating the problem structure into polynomial rings, thus lowering computational demands. The paper categorizes RLWE applications into identity-based encryption, homomorphic encryption, and secure authentication key exchange. Each category includes examples. Identity based encryption enables secure messaging without needing pre-distributed certificates. Homomorphic encryption allows privacy-preserving computations on encrypted IoMT data. RLWE-based key exchange maintains session confidentiality even against quantum threats. These mechanisms are particularly relevant for healthcare IoT. For example, in a hospital setting, wearable sensors send patient vitals to a gateway. While symmetric encryption like AES can protect the data, key management at scale remains a challenge. LB-PKC offers a method for securely distributing and refreshing keys between gateways and cloud servers. By using LWE-based key exchange, the gateway can create session keys that stay secure, even with future quantum computers. This guarantees that sensitive patient data remains confidential for many years. However, LB-PKC does have some downsides. The paper notes that larger key sizes and ciphertext expansion increase bandwidth needs. Additionally, the heavy arithmetic calculations can drain device batteries more quickly. These issues make LB-PKC impractical for extremely constrained devices like fitness bands or implantable sensors. The authors propose hybrid deployment models. They recommend using lattice cryptography to secure high-capacity nodes like gateways and servers, while lightweight symmetric cryptography should be used for low-power connections like sensor-to-gateway links. This layered approach offers a balance between post-quantum security and resource efficiency. The paper also points out ongoing challenges, such as reducing memory use of lattice algorithms, improving key storage, and creating energy-efficient hardware accelerators. In conclusion, LB-PKC is not a one-size-fits-all solution but an important part of the IoMT security framework. It offers future-proof encryption where resources allow and complements lightweight techniques in more constrained environments

B.2019: Hybrid Cryptography and Image Steganography [2] Nunna and Marapareddy suggest a hybrid method that combines cryptography with image steganography for secure data transfer over the Internet. The paper starts by discussing the limitations of traditional encryption on its own. While cryptography provides confidentiality, the visible ciphertext can attract the attention of attackers. In contrast, steganography hides the existence of communication by embedding secret data within a cover medium, like an image. The authors aim to achieve both strong cryptographic protection and secret communication by combining these two techniques. The method encrypts plaintext using a straightforward XOR-based cipher. Unlike complex algorithms like RSA or AES, the XOR operation is lightweight and suitable for devices with limited resources. After encryption, the ciphertext is embedded into an image using a pseudo-random technique that a user selects with a key. The cover image’s pixels, displayed in RGB format, are altered at the least significant bit (LSB) level to store secret bits. For instance, if an 8-bit pixel value is 11001001 and the secret bit is 1, the pixel can change to 11001011. These small changes are undetectable to the human eye, ensuring the cover image looks unchanged. The authors categorize types of steganography into image, audio, and text-based, detailing why images make effective carriers. A 600x450 image contains 270,000 pixels, and with each pixel offering three color channels, there are over 800,000 bytes available for embedding. Even if only the least significant bit of each channel is altered, a considerable amount of data can be hidden. This large capacity makes image steganography ideal for concealing medical records, keys, or diagnostic reports. In the Internet of Medical Things (IoMT) setting, this method fits well with healthcare workflows. Medical images like X-rays, MRIs, and CT scans are frequently created and shared. By embedding patient identifiers, cryptographic keys, or additional medical notes into these images, secure and discreet communication within existing processes is possible. For example, a radiology department sending CT images to a cloud-based diagnostic system could embed session keys within the image. In this way, only the intended recipient, using the stego-key, can extract and decrypt the information, while others see nothing unusual. The strengths of this approach include two layers of security (encryption plus concealment), resistance to casual inspection, and effective use of current data carriers. However, there are limitations. Embedding may create statistical artifacts that advanced steganalysis tools can detect. Additionally, in medical contexts, diagnostic accuracy is crucial. Even slight image distortion can impact automated processing or a radiologist’s assessment. To address this, hospitals might need to keep both the original and stego-images, which would double storage requirements. The method is also less ideal for real-time telemetry, such as ECG or temperature monitoring, where images aren’t the natural medium. In those situations, authenticated encryption with low overhead is usually a better choice. Despite these challenges, the hybrid method shows promise for improving IoMT security. It demonstrates that cryptography and steganography can work together effectively. By hid ing encrypted data in a familiar medium, the system benefits from both confidentiality and stealth. The authors conclude that future research should focus on making embedding more efficient, reducing perceptual and statistical distortion, and widening the approach to include multimedia carriers beyond images. For healthcare applications, especially those involving image-based communication, this hybrid technique offers a solid route toward multi-layered security.

C.2020: Restoration-Enhanced Reversible Steganography (MediSR-Net) [3] Chen et al. introduce MediSR-Net, a deep learning-based reversible information steganography network designed for CT images in IoMT. Unlike traditional least significant bit (LSB) or adaptive embedding methods, which often compromise the statistical properties of medical images, MediSR-Net uses a degradation-restoration strategy to reduce distortion. It includes an analysis module that accurately predicts pixel values and an encoding module that embeds and extracts secret data. Importantly, MediSR-Net guarantees full reversibility, allowing for the perfect recovery of both the hidden payload and the original image, ensuring that diagnostic integrity remains intact. The authors compare MediSR-Net with ten leading steganographic methods, showing that it outperforms them in embedding capacity, perceptual quality, and error reduction. Quantitative metrics like Peak Signal-to-Noise Ratio (PSNR) and distortion analysis confirm its reliability. This is particularly important in healthcare, where medical images must remain trustworthy for radiologists and AI-based diagnostic tools. The reversible nature of MediSR-Net complies with strict healthcare regulations such as HIPAA and GDPR. Beyond its performance, MediSR-Net marks a shift in steganography from basic bit replacement methods to deep learning-driven adaptive models. Earlier techniques like LSB replacement were easy to detect due to statistical anomalies. While adaptive methods improved imperceptibility, they still left subtle traces. MediSR-Net uses information distillation and attention mechanisms to improve embedding precision. This progress reflects the growing trend of integrating AI into security, where models learn the best embedding strategies to maximize capacity while reducing perceptual and statistical distortion. For IoMT, MediSR-Net has several implications. First, it allows for the secure sharing of diagnostic images across hospitals without affecting clinical accuracy. Second, it sup ports covert communication by embedding additional patient data or cryptographic keys directly within medical images. Third, it strengthens copyright protection for medical images in collaborative research. However, challenges remain. Deep learning models need significant computational power, making them unsuitable for use on resource-limited wearables or edge devices. Instead, they work best on gateways or hospital servers with GPU support. Additionally, MediSR-Net is lim ited to imaging channels; continuous numerical telemetry, such as ECG or oxygen levels, still requires cryptographic methods. In summary, MediSR-Net represents the cutting edge of reversible steganography, providing a powerful tool for IoMT systems where medical images are the main medium for exchange. It enhances confidentiality without sacrificing diagnostic usability and suggests a future where AI-driven reversible embedding becomes common in healthcare cybersecurity.

D. 2021: Lightweight Authenticated Key Exchange (LAKEE) [4] Nabavirazavi and Iyengar propose LAKEE, a lightweight authenticated key exchange protocol designed for limited IoT environments. Traditional handshake protocols like TLS and DTLS come with high communication and processing costs, making them unsuitable for IoT. LAKEE solves this by using elliptic curve cryptography along with pre-shared secrets to create short-term session keys without needing certificate au thorities. The protocol runs over the Constrained Application Protocol (CoAP) and shows significantly lower energy use and fewer message exchanges than current options like QUIC, DTLS-PSK, and ECC-CoAP. In healthcare IoT, where devices like wearables often wake and sync, a lightweight key exchange is essential for extending battery life while maintaining confidentiality. LAKEE offers mutual authentication and forward secrecy while keeping the overhead low. Once the session is established, the derived keys can work with authenticated encryption modes to secure medical data during transmission. One downside is that LAKEE only improves the handshake phase; overall data security still relies on integrating encryption and integrity measures at the application layer. However, the simplicity and efficiency of LAKEE make it a solid choice for securing IoMT communication in settings where resource use directly affects device performance and patient safety. Unlike standard PKI-based handshakes, which require certificate checks and multiple communication rounds, LAKEE simplifies the protocol. This reduces both delays and energy use. This is particularly important in IoMT situations such as continuous glucose monitoring or remote patient tracking, where devices send frequent small data packets. The lowered handshake overhead leads to longer device lifespans and lower maintenance costs. The authors also highlight the formal security validation of LAKEE, confirming that it can resist common threats like replay and impersonation attacks. Overall, LAKEE strikes a practical balance between lightweight design and strong security measures. While it is not a complete solution on its own, it establishes a secure base on which full IoMT data protection systems can be built.

E. 2023: Steganography in IoT– A Comprehensive Survey [5] Driss et al. present a detailed survey of steganography techniques designed for IoT environments. The study looks at methods across spatial, frequency, and hybrid domains, along with new approaches like deep learning-based and quantum steganography. Each technique is assessed based on important factors like imperceptibility, robustness, embedding capacity, and computational efficiency. The survey points out that while traditional encryption is important, it can be costly in terms of computation and easily detected. This detection may create suspicion in sensitive IoT settings. In contrast, steganography hides both the content and its existence, making it especially useful in highly monitored areas like healthcare. The survey highlights specific challenges in IoT, such as limited CPU and memory, energy limitations, real-time needs, and the variety of devices. It also showcases practical applications, like concealing patient identifiers in physiological signals or embedding authentication keys in telemetry streams. The authors suggest blending steganography with other technologies. This includes using machine learning for adaptable embedding, blockchain for decentralized trust, and quantum methods for enhanced secure hiding. However, many methods are still theoretical and do not have real-world use in IoMT. The main point is that steganography should support encryption, rather than replace it. For healthcare uses, reversible methods should be prioritized for medical images, while authenticated encryption ought to secure ongoing sensor data. The paper wraps up by discussing future research paths, including AI-driven adaptive embedding, scalable systems, and resistance to IoT-specific steganalysis.

F. 2023: Healthcare IoT Threats and Challenges [6] Adil et al. provide a thorough review of security threats in Healthcare IoT (HC-IoT). They focus on vulnerabilities across device, network, and application layers. The study lists attacks such as eavesdropping, DDoS, impersonation, Sybil, wormhole, and jamming, along with weaknesses in cloud integration. Using a dataset of 243 papers published from 2015 to 2023, the authors create a taxonomy of security requirements that includes confidentiality, authentication, data integrity, availability, and non-repudiation. They highlight that wearable devices, often used in open and unstructured networks, are particularly vulnerable to intrusion due to wireless communication and weak authentication. In the context of the Internet of Medical Things (IoMT), this paper is important because it outlines clear priorities for layered defense. These priorities include securing device identity, using lightweight encryption with frequent rekeying, enforcing strict access control on gateways, and establishing secure APIs for cloud interactions. The review also emphasizes the need for audit trails and readiness for forensic investigations to aid incident response while protecting patient privacy. While the paper provides valuable descriptions, it does not suggest integrated architectures or implementation strategies. Instead, it acts as a guide, identifying ongoing research challenges such as achieving interoperability among different devices, reducing latency in secure communication, and ensuring compliance with healthcare regulations. Its contribution is valuable in defining the HC-IoT security landscape, making it an essential reference for researchers and practitioners.

G. 2024: IoMT Embedded Systems with Dynamic Key + Steganography [7] Nour-El Aine and Leghris propose an integrated method that combines dynamic session key generation with steganography for embedded IoMT systems. Unlike traditional methods that use fixed pre-shared keys, this approach creates new keys for each communication session. The encrypted data is hidden within medical images using steganographic techniques. This dual strategy offers both confidentiality through cryptography and covert communication through steganography. It significantly raises the difficulty for potential attackers. The benefit of dynamic keys is clear. They ensure forward secrecy, lower the risk of key compromise, and remove the need to store large key lists. Steganography offers stealth by embedding sensitive health data unobtrusively within existing medical imaging workflows. For IoMT devices, this method provides strong security while addressing resource constraints, enabling scalability without overloading limited processing power. The authors also stress the importance of complying with healthcare data protection regulations like HIPAA, showing that their approach is practically viable. However, there are operational challenges. Systems must store both original and stego images to maintain diagnostic integrity, and there needs to be standardization of embedding paths across devices for interoperability. Despite these challenges, this paper establishes a new standard by combining two complementary security strategies. It positions itself as a promising framework for secure, efficient, and privacy-preserving communication in IoMT environments.

H. Synthesis Across these works, three themes consistently emerge. First, strong mathematics like PQC and ECC are essential but must be tailored to hardware with limited resources. Second, steganography works well for image-based data, especially when reversibility is guaranteed, but it is less practical for continuous numeric telemetry. Third, frequent key refresh and simple handshake methods are important for minimizing the impact of a security breach. Together, these studies suggest a mixed IoMT security framework: using lattice-based or ECC key exchange for gateways, lightweight authenticated encryption for sensor streams, and reversible steganography for medical images. This layered approach offers both confidentiality and stealth while considering the performance limits of healthcare IoT devices.

II. INTEGRATED WORKFLOW FOR SECURE IOMT DATA HANDLING

The following explanation describes each stage of the workflow shown in Figure 1:

1) Data Collection Patient signals are captured by sensors and edge devices, such as ECG, temperature monitors, pulse oximeters, and imaging tools. Raw measurements are preprocessed at the edge. This includes noise reduction, baseline cor rection, and filtering. These steps help remove artifacts and reduce bandwidth while keeping clinically relevant features intact.

2) Session Key Generation A new session key is created for each communication session from a secure source of randomness, such as a cryptographic RNG or a physical-layer/LAKEE entropy source. These per-session keys reduce risk if a key is compromised. They also allow for forward secrecy across measurements.

3) Encryption + Steganography Sensor data is first secured with an authenticated en cryption scheme, such as AES-GCM or ChaCha20 Poly1305, to ensure confidentiality and integrity. When necessary, the ciphertext or selected clinical images are embedded using a reversible steganographic method. This method allows for data recoverability while main taining the visual quality of the carrier. This approach protects against passive eavesdropping and conceals sensitive information when required.

4) Transmission & Authentication Data is sent over a secure and authenticated channel to the server or clinician device. Device and gateway authentication, such as mutual TLS or strong device attestation, prevents impostors. Replay protection and sequence numbers stop injection and replay attacks. If steganography is used, the receiver extracts the payload before decryption.

5) Decryption & Clinical Use At the receiving end, the session key or a securely derived key is used to authenticate and decrypt the payload. The decrypted data goes into clinical diagnosis systems, EHR storage, or dashboards. Audit logs, access controls, and data retention policies ensure traceability and regulatory compliance

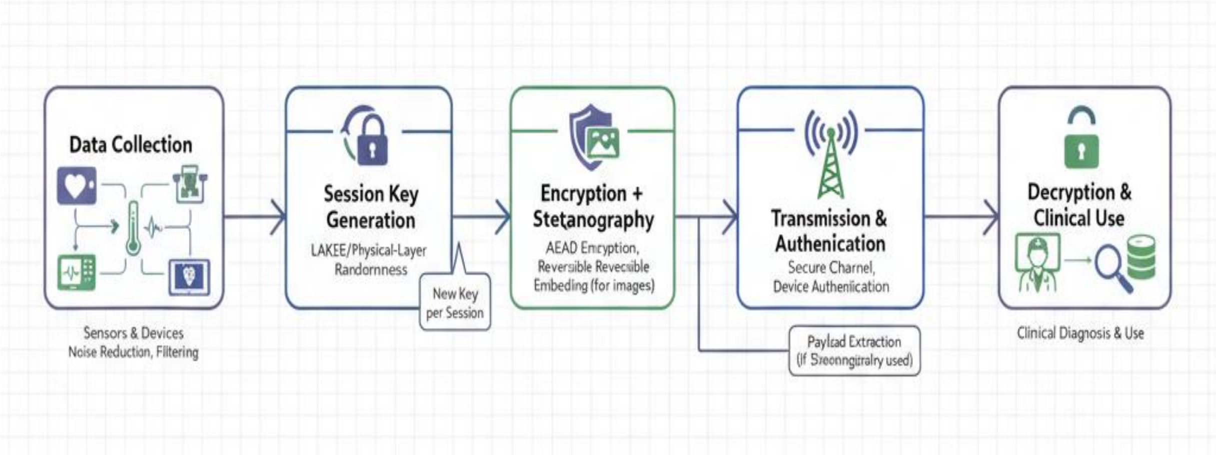
Data Collection
Sensors & Devices
Noise Reduction, Filtering
Session Key Generation
LAKEE/Physical-Layer Randomness
New Key per Session
Encryption + Stetanography
AEAD Encryption, Reversible Revecsible Embeding (for images)
Transmission & Authenication
Secure Charnel, Device Authenication
Paylzad Extraction (If Sreonngizaly used)
Decryption & Clinical Use
Clinical Diagnosis & Use

Fig. 1: Proposed workflow for secure IoMT communication: use strong encryption, change keys frequently, and embed data in a way that can be reversed when images are already being transmitted

III. STEP-WISE WORKFLOW ILLUSTRATION

To complement the integrated workflow (Figure 1), the following diagrams illustrate each stage individually in detail.

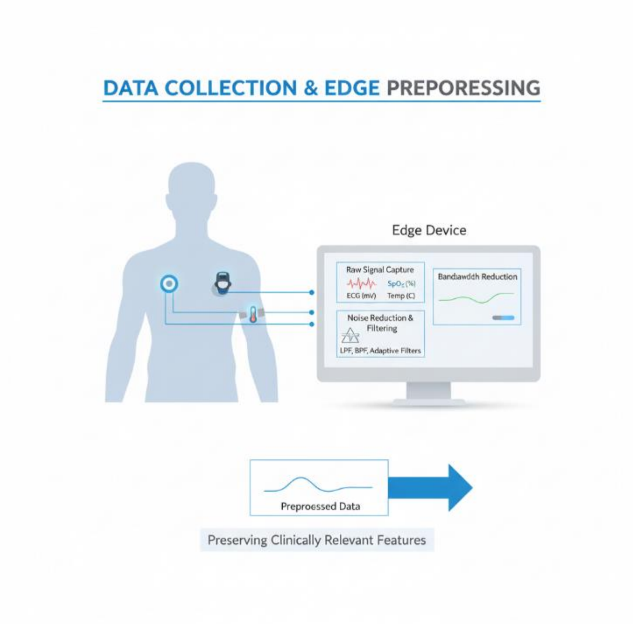
DATA COLLECTION & EDGE PREPORESSING
Edge Device
Raw Signal Capture
SpO₂ (%)
ECG (mV)
Temp (C)
Bandawdth Reduction
Noise Reduction & Filtering
LPF, BPF, Adaptive Filters
Preprocessed Data
Preserving Clinically Relevant Features

Fig. 2: Step 1: Data Collection & Edge Preprocessing

Patient physiological signals like ECG, blood pressure, tem perature, and SpO2 come from IoMT sensors and edge de vices. The raw data often has noise, baseline drift, and artifacts because of patient movement, environmental interference, or sensor instability. To ensure accuracy, the data goes through several preprocessing steps at the edge:

- Noise Reduction: Filters (low-pass, high-pass, or adap tive) remove unwanted frequency components.
- Baseline Correction: Drift in ECG or temperature read ings is stabilized using statistical normalization.
- Feature Extraction: Only medically relevant attributes are retained, reducing computational burden.
- Data Compression: Preprocessed signals are compressed to reduce bandwidth while preserving diagnostic features.

This step ensures that only high-quality and clinically mean ingful data proceeds for secure transmission

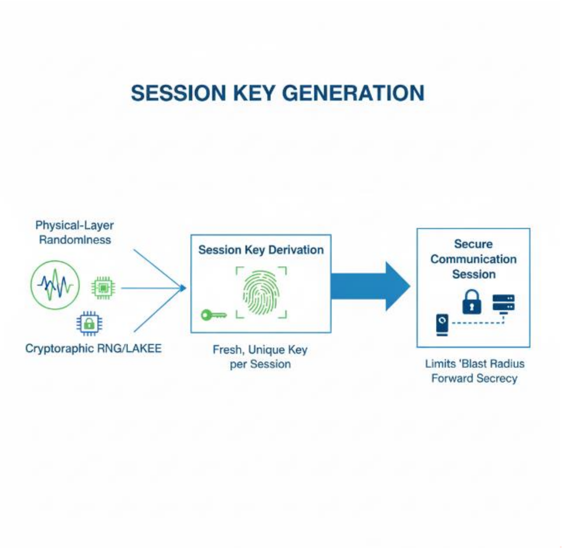
SESSION KEY GENERATION
Physical-Layer Randomness
Cryptographic RNG/LAKEE
Session Key Derivation
Fresh, Unique Key per Session
Secure Communication Session
Limits 'Blast Radius Forward Secrecy

Fig. 3: Step 2: Session Key Generation

For each communication session, a new cryptographic key is generated, ensuring forward secrecy. The process involves:

- Randomness Source: Either a cryptographic RNG or physical entropy (e.g., LAKEE).
- Key Derivation Function (KDF): Uses shared secret val ues, nonces, and timestamps.
- Session Uniqueness: Every session has a different key, isolating compromise impact.

The key derivation can be expressed as:

$$Ksession = KDF(S \parallel N \parallel T)$$

where S is the shared secret, N is a nonce, and T is a timestamp. This ensures that even if one session is exposed, previous and future sessions remain secure

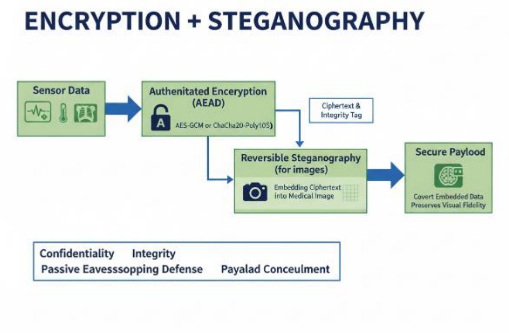
ENCRYPTION + STEGANOGRAPHY
Sensor Data
Authenitated Enceryption (AEAD)
A
AES-GCM or ChaCha20-Poly105)
Ciphertext & Integrity Tag
Reversible Steganography (for images)
Embedding Ciphertext into Medical Image
Secure Paylood
Covert Embedded Data Preserves Visual Fidelity
Confidentiality Integrity
Passive Eavesssopping Defense Payalad Conceulment

Fig. 4: Step 3: Encryption + Steganography

Sensitive patient data is secured in two layers:

1) Encryption: An Authenticated Encryption with As sociated Data (AEAD) scheme like AES-GCM or ChaCha20-Poly1305 encrypts the data. This ensures both confidentiality and integrity.

$$C = EncKsession\ (M \parallel AAD)$$

where M is the patient data and AAD provides metadata integrity.

2) Steganography: For image-based data (e.g., X-rays, MRI scans), ciphertext can be covertly embedded inside cover images:

$$I' = \mathrm{Embed}(I,C)$$

where I is the medical image and I′ is the stego-image containing hidden ciphertext.

This dual-layer approach prevents passive eavesdropping and disguises sensitive data during transmission.

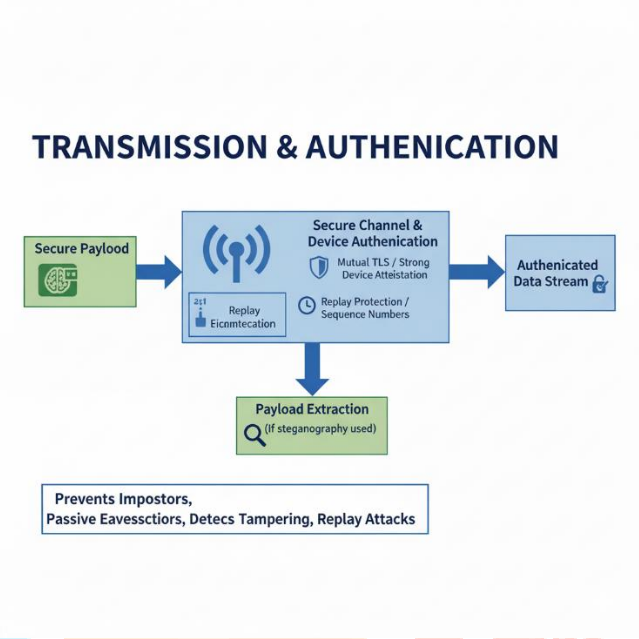
TRANSMISSION & AUTHENICATION
Secure Paylood
Secure Channel & Device Authenication
Mutual TLS / Strong Device Atteistation
2ɩ1
Replay Eicnmtecation
Replay Protection / Sequence Numbers
Authenicated Data Stream
Payload Extraction
(If steganography used)
Prevents Impostors,
Passive Eavessctiors, Detecs Tampering, Replay Attacks

Fig. 5: Step 4: Transmission & Authentication

Once protected, data is transmitted over a secure channel. The processes involved are:

- Channel Security: Mutual TLS or device attestation ensures the sender and receiver are legitimate.
- Replay Protection: Sequence numbers and nonces prevent adversaries from re-sending old packets.
- Steganography Extraction: If data is hidden inside an image, the ciphertext is extracted before decryption:

$$C = \mathrm{Extract}(I')$$

- Integrity Check: Ensures data is not altered during tranmission.

This step guarantees that data reaches its destination securely without exposure to tampering or impersonation.

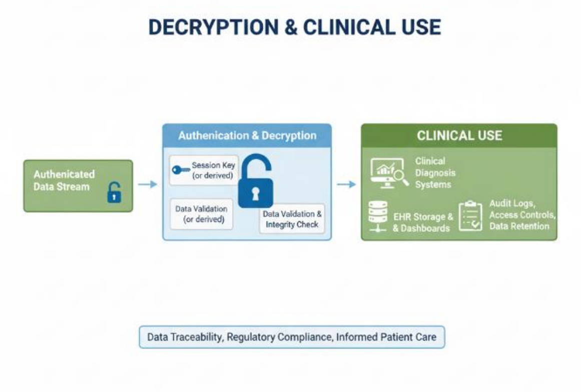
DECRYPTION & CLINICAL USE
Authenicated Data Stream
Authenication & Decryption
Session Key (or derived)
Data Validation (or derived)
Data Validation & Integrity Check
CLINICAL USE
Clinical Diagnosis Systems
EHR Storage & & Dashboards
Audit Logs, Access Controls, Data Retention
Data Traceability, Regulatory Compliance, Informed Patient Care

Fig. 6: Step 5: Decryption & Clinical Use

At the receiver's end, the following operations take place:

- Decryption: Using the session key, ciphertext is de crypted:

  M=DecKsession (C)

- Integrity Verification: AEAD ensures authenticity and prevents tampered data from being accepted.
- Clinical Integration: Decrypted signals/images are stored in EHR, processed in diagnostic dashboards, or forwarded to decision-support systems.
- Access Control: Only authorized medical staff can access the decrypted data.
- Audit Logging: Every access is recorded for compliance with HIPAA/GDPR and traceability.

This final step ensures data usability in healthcare while maintaining accountability and compliance. This workflow provides complete security for IoMT systems. It starts with collecting data that is filtered for noise and optimized for bandwidth. Then, it generates strong keys for each session. The system uses two layers of protection: encryption and steganography. It ensures secure and verified transmission, followed by decryption that integrates with clinical processes. This model protects confidentiality, integrity, authenticity, and compliance. By merging cryptography with hidden embedding and strict access control, the system protects patient privacy and supports dependable clinical decision-making in today's healthcare.

IV. COMPARATIVE ANALYSIS

Discussion of Relevance:

1) Vijayalakshmi et al. (2018)– Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions-This work uses lattice-based cryptography (NTRU, LWE, RLWE) to protect IoT gateways and imaging workstations from quantum threats. It provides strong confidentiality, but its high CPU and RAM needs make it impractical for resource-limited IoMT devices. Our base paper tackles this issue by presenting a lightweight dynamic key generation method paired with steganog raphy. This approach achieves similar confidentiality without the heavy resource demands. ⇒ Related to our base paper by highlighting the need for lightweight, resource-efficient alternatives for IoMT security.

2) Nunna & Marapareddy (2019)– Secure Data Trans fer Through Internet Using Cryptography and Image Steganography-This dual-layer approach combines AES encryption with image steganography to improve confidentiality. How ever, using AES adds high processing overhead and costs, which are not suitable for embedded healthcare devices. Our base paper addresses this issue by using dynamic key generation instead of AES. This keeps the benefits of dual-layer security while ensuring compati bility with low-power IoMT systems. ⇒ Related to our base paper as an early demonstration of crypto-stego integration, which we optimize for IoMT.

3) Zhang et al. (2020)– Restoration-Enhanced Re versible Information Steganography Network for CT Images in the Internet of Medical Things-MediSR-Net provides imperceptibility and full image reversibility for CT and radiology pipelines with deep learning. It works well for medical images, but it is restricted to imaging channels and needs substantial computational resources. Our base paper broadens steganography to cover telemetry and vital signals, while simplifying the process to fit IoMT limits. ⇒ Related to our base paper by showing the importance of steganography in medical data, but our work generalizes it to broader IoMT contexts.

4) Kumar et al. (2021)– LAKEE: A Lightweight Authenticated Key Exchange Protocol for Power Constrained Devices-LAKEE enables lightweight authenticated key exchange for wearables and low-power radios, ensuring fresh session keys at minimal handshake cost. However, hand shake processes and reliance on AEAD introduce delays. Our base paper advances this concept by enabling instant dynamic key generation per session, combined with steganography for covert transport. ⇒ Related to our base paper as both aim for lightweight key freshness, but our work integrates covert communication for enhanced privacy.

5) Shah et al. (2023)– Steganography in IoT: A Com prehensive Survey on Approaches, Challenges, and Future Directions-This survey analyzes IoT steganography techniques, of fering taxonomy and trade-off discussions. While useful for understanding IoT constraints, it lacks deployment or evaluation in healthcare.Our base paper builds on this survey bymoving from theoretical taxonomy to an implemented frame work using dynamic key generation with steganography in IoMT.⇒Related to our base paper by providing the conceptual groundwork that our study transforms into a practical solution.

6)) Rghiouietal.(2023)–Healthcare Internet of Things: Security Threats,Challenges, andFuture Research Directions-This paper categorizes security threats in healthcare IoT, proposing layered defenses but no integrated blueprint. Our base paper directly responds to these identified challenges by providing a deployable solution that prevents replay attacks via dynamic keys and ensures confidentiality through steganographic embedding.⇒Related to our basepaper by defining the threat landscape that our approach explicitl addresses.

7) Nour-El Aine &Leghris (2024)– IoMT Based Embedded Systems for Healthcare:A Confidentiality and Privacy Approach through Key Generation and Steganography-Our basepaper introduces dynamic session key generation with reversible steganographic embedding, over coming the key limitations of prior works: • Lattice cryptography→too heavy for IoMT.

- AES+steganography→high processing cost.
- Reversible steganography→limited to imaging only.
- Lightweight key exchange→residual handshake overhead.
- IoTsteganographysurveys→no practical deployment.
- Threat taxonomies→no actionable blueprint.

⇒Establishes a lightweight, scalable,and deployable confidentiality framework tailored specifically for embedded healthcare IoMT systems.

TABLEI:Comparison across technique,domain, security focus, and limitations.

Paper & Year	Technique	Application Domain	Security Focus	Limitations
2018 Vijay-Lakshmi	Lattice PQC	Gateways, imaging	Quantum resistance	Heavy CPU/RAM requirements
2019 Nunna	AES + Steganography	Image-based alerts	Confidentiality and covertness	Image distortion risk
2020 Zhang	Reversible Steganography	CT/MRI pipelines	Full reversibility	Limited to image-based data
2021 Kumar	LAKEE Key Exchange	Wearables, low-power systems	Lightweight session keys	Needs AEAD payload security
2023 Shah	Survey of IoT Stego	Cross-domain IoT	Design taxonom	No-deployment framework
2023 Rghioui	Threat Survey	End-to-end IoMT	Attack mapping	No unified framework
2024 Nour-El Aine	Dynamic Keys + Re-versible Stego	Imaging + telemetry	Replay resistance, covert transport	Operational complexity

Taken together, these studies illustrate the progression of IoT and IoMT security research from heavy post-quantum cryptography to crypto-stegohybrids, reversiblemedical image steganography, lightweight key exchange protocols, descriptive surveys, and threat taxonomies.Each provides valuable in sights but falls short of addressing the dual challenge of confidentiality and resource-efficiency in embedded health are systems. Our base paper synthesizes these directions by merging dynamic session key generation with steganographic embedding, thus achieving a balance between security strength, lightweight design, and practical deployability in IoMT environments

V. CONCLUSION

IoMT security has moved from mathematically powerful but device-heavy cryptography toward blended, device-aware designs. The field recognizes that (i) cryptography must fit the silicon, (ii) hiding encrypted traffic in legitimate media increases ambiguity for adversaries, and (iii) rotating secrets is inexpensive and effective risk control. The proposed work f low reflects those lessons: derive a new key often, encrypt decisively, embed reversibly when images are already in the loop, and keep the pipeline auditable and lightweight. Looking ahead, the community needs post-quantum options sized for microcontrollers, on-device anomaly detection that respects power budgets, and cross-layer frameworks that make secure defaults easy for clinicians and engineers alike

REFERENCES

[1] K. Vijayalakshmi et al., “Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions,” IEEE, 2018.

[2] K. C. Nunna and R. Marapareddy, “Secure Data Transfer Through Internet Using Cryptography and Image Steganography,” in Proc. IEEE SoutheastCon, 2019.

[3] L. Zhang et al., “Restoration-Enhanced Reversible Information Steganog raphy Network for CT Images in the Internet of Medical Things,” IEEE, 2020.

[4] R. Kumar et al., “LAKEE: A Lightweight Authenticated Key Exchange Protocol for Power-Constrained Devices,” IEEE, 2021.

[5] H. Shah et al., “Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions,” Elsevier, 2023.

[6] A. Rghioui et al., “Healthcare Internet of Things: Security Threats, Challenges, and Future Research Directions,” Elsevier, 2023.

[7] Y. Nour-El Aine and C. Leghris, “IoMT-Based Embedded Systems for Healthcare: A Confidentiality and Privacy Approach Through Key Generation,” IEEE, 2024