



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

Implementation of an Advanced Secure Scheme for Rapidly Growing Internet of Things (IoT) Based Healthcare Monitoring

Kamlesh Thummar¹, Anilkumar Kshatriya²

¹ Research Scholar, Electronics and communication department, Gujarat Technological University, Ahmedabad, Gujarat, India.

E-mail: kdthummar@gpahmedabad.ac.in, Orcid: <https://orcid.org/0009-0001-7046-5546>,

² Electronics and Communication Engineering Department, Government Engineering College, Gandhinagar, Gujarat, India.

E-mail: aj.kshatriya@gmail.com, Orcid: <https://orcid.org/0000-0002-9044-0442>

Abstract

The rapid growth of the Internet of Things (IoT) in healthcare has enabled continuous monitoring of patients through resource-constrained sensing devices. However, the transmission and storage of sensitive physiological information introduce significant security, privacy, authentication, and computational challenges. This research presents an advanced secure IoT healthcare architecture that integrates lightweight edge computing, post-quantum key exchange, authenticated encryption, homomorphic encryption, replay protection, and artificial intelligence-based disease detection. The proposed system uses an ESP32 microcontroller integrated with ECG, SpO₂, heart-rate, and temperature sensors for patient-side data acquisition. Paillier-3072 homomorphic encryption is applied to individual vital signs, while AES-256-GCM provides authenticated transport encryption. Kyber-768, corresponding to ML-KEM-768, is employed for secure session-key establishment with mutual device authentication. To overcome the computational limitations of the ESP32, the proposed implementation introduces encrypted NVS flash storage for the precomputed Paillier (r^N) value. This optimization reduces the device boot time from approximately 662 seconds to 7.7 seconds, representing a 98.8% reduction. The server-side architecture is migrated from Raspberry Pi to an NVIDIA Jetson Orin Nano Super, providing substantially greater computing capability and GPU acceleration. Secure remote access is implemented through a Cloudflare tunnel using WSS/HTTPS. The system also incorporates nonce-based replay protection, NTP time synchronization, authenticated administrative endpoints, device registration limits, restricted CORS policies, secret validation, and rate limiting. A security assessment identified ten vulnerabilities in the earlier implementation, including encryption-oracle attacks, device-session hijacking, replay attacks, unauthorized database exports, device-flooding attacks, weak secret configuration, unrestricted CORS, plaintext logging, and unrestricted request rates. All ten vulnerabilities were addressed in the improved implementation. In addition, an AI-based disease-detection layer consisting of threshold-based detection, machine-learning classification, LSTM-based analysis, and ensemble decision-making was incorporated for monitoring five health conditions. The resulting architecture demonstrates the feasibility of combining privacy-preserving cryptography, post-quantum security, embedded optimization, and AI-based healthcare intelligence in a practical IoT platform.

Keywords: Internet of Things, IoT Healthcare, ESP32, Paillier Encryption, Homomorphic Encryption, AES-256-GCM, Kyber-768, Post Quantum Cryptography, Edge Computing, Healthcare Security, Disease Detection.

1. Introduction

The Internet of Things has transformed healthcare by enabling continuous acquisition and transmission of physiological data through interconnected sensing devices. Wearable and embedded healthcare devices can collect parameters such as electrocardiogram (ECG), blood oxygen saturation (SpO₂), heart rate, respiratory rate, and body temperature. Such systems can support continuous patient monitoring, early identification of abnormal physiological conditions, and remote healthcare research[1,2,3]

Despite these benefits, IoT healthcare systems introduce substantial cybersecurity and privacy challenges. Medical data are highly sensitive and require protection against unauthorized access, interception, modification, replay, impersonation, and data leakage. The problem becomes more challenging when data are collected by resource-constrained microcontrollers such as the ESP32. Conventional cryptographic techniques can impose considerable computational and memory overhead on embedded devices.[4,5]

The research problem addressed in this work is therefore the development of a secure and computationally practical healthcare IoT architecture capable of protecting physiological information while operating on

constrained edge devices. The original research problem identifies the need for a post-quantum, lightweight, privacy-preserving encryption mechanism capable of running on low-power IoT devices such as ESP32 while enabling secure transmission to researchers.

The proposed system combines multiple security mechanisms rather than depending on a single cryptographic algorithm. Paillier-3072 provides additive homomorphic encryption, allowing selected computations to be performed on encrypted information. AES-256-GCM provides authenticated encryption for data transmission, while Kyber-768 provides a post-quantum key-exchange mechanism. The ESP32 generates cryptographic randomness locally, and a precomputation strategy is introduced to reduce the computational burden associated with Paillier encryption.[6,7,8]

The server-side architecture is implemented using an NVIDIA Jetson Orin Nano Super. The platform provides increased computational capability compared with the Raspberry Pi implementation used previously and includes GPU-based AI acceleration. The system also uses FastAPI, SQLite, and Cloudflare tunneling to provide secure remote access.

An additional intelligence layer is incorporated for disease-risk detection. Four complementary models—threshold-based detection, machine-learning classification, LSTM analysis, and ensemble decision-making—are designed to monitor five health conditions.

The major contribution of this research is therefore the integration of privacy-preserving cryptography, post-quantum security, secure embedded implementation, security hardening, edge computing, and AI-based healthcare monitoring within a unified IoT architecture.[9,10]

II. Literature Review

2.1 IoT-Based Healthcare Monitoring

IoT healthcare systems commonly employ distributed sensors and embedded devices for collecting physiological parameters. The collected data may subsequently be transmitted to edge servers, cloud platforms, or healthcare researchers. While such architectures improve accessibility and real-time monitoring, healthcare IoT systems are particularly attractive targets for cyberattacks because they process sensitive personal information.

Security mechanisms must therefore address confidentiality, integrity, authentication, availability, and privacy simultaneously. Conventional cloud-centric approaches may also introduce additional concerns because raw patient data may leave the trusted environment of the healthcare provider.

The proposed research addresses these challenges by introducing encryption directly at the patient-side ESP32 before physiological information is transmitted to the edge server.[1,2,3]

2.2 Lightweight Cryptography for IoT

Resource-constrained IoT devices have limited CPU performance, memory, storage, and energy. Lightweight cryptographic algorithms are therefore frequently considered for IoT applications. RECTANGLE was evaluated in the earlier implementation and demonstrated approximately 1 ms encryption time per packet on ESP32. However, the implementation identifies limitations associated with software-only execution and lack of hardware acceleration. AES was consequently selected because of its established standardization, broad adoption, and hardware acceleration on the ESP32.

The final system upgrades the transport layer from AES-128 to AES-256-GCM. GCM additionally provides authenticated encryption and a 16-byte authentication tag for each packet.[4,5,6]

2.3 Homomorphic Encryption

Homomorphic encryption enables selected mathematical operations to be performed on encrypted data without directly exposing the underlying plaintext. The Paillier cryptosystem is an additive homomorphic encryption mechanism. Its fundamental property can be expressed as:

$$[E(a) \times E(b) = E(a+b)]$$

This property enables privacy-preserving aggregation of encrypted information. The proposed implementation uses Paillier-3072, with the ciphertext generated on the ESP32 and stored in encrypted form on the Jetson server.

CKKS was also evaluated during the research. Although CKKS supports approximate arithmetic involving addition and multiplication, the presentation reports significantly higher computational overhead and a test time of approximately 273 seconds for 536 records. Paillier-3072 was consequently selected for the VitalGuard pipeline because of its suitability for the implemented ESP32 environment.[7,8,9]

2.4 Post-Quantum Cryptography

The increasing possibility of quantum attacks motivates the investigation of post-quantum cryptographic mechanisms for IoT systems. The proposed architecture upgrades Kyber-512 to Kyber-768. Kyber-768 corresponds to the NIST ML-KEM Level 3 security category and provides a higher security margin than the earlier Kyber-512 implementation.

In the proposed system, the ESP32 performs Kyber encapsulation while the Jetson performs decapsulation. A shared secret is established during the handshake and subsequently used for AES-256-GCM session encryption. Mutual authentication is additionally implemented through a device-specific secret.[10,11,12]

2.5 Security and Privacy in Healthcare IoT

Healthcare IoT architectures must protect against more than passive interception. Active attacks such as replay, impersonation, endpoint abuse, denial-of-service, unauthorized data export, and encryption-oracle attacks can compromise the integrity and privacy of the system.

The DPC-6 implementation identified ten vulnerabilities in the previous security architecture. These included two critical vulnerabilities, four high-severity vulnerabilities, and four medium-severity vulnerabilities. All ten vulnerabilities were subsequently addressed and tested.

The improved system incorporates:

- Mutual device authentication.

- Per-packet random nonces.

- NTP-based timestamps.

- Replay-window validation.

- Database-level nonce uniqueness.

- Administrative authentication.

- Device-registration limits.

- CORS restrictions.

- Secret-length validation.

- Rate limiting.

- Controlled logging.

- Permanent removal of encryption-oracle endpoints.

These mechanisms collectively strengthen the security of the proposed architecture.[13,14,15]

2.6 AI-Based Healthcare Intelligence

Secure data collection alone is insufficient for intelligent healthcare monitoring. An AI layer can transform physiological measurements into risk assessments and support early identification of abnormal conditions.

The proposed system incorporates four complementary models:

- Threshold-based clinical detection.

- Machine-learning classification using Logistic Regression and Random Forest.

- LSTM-based time-series analysis.

- Ensemble prediction.

The threshold model is operational, while the ML classifier and LSTM architecture are prepared for labeled training data. The ensemble combines predictions from the available models to generate a final assessment.

The five monitored conditions are hypertension, Type 2 diabetes, cardiac arrhythmia, hypoxia, and fever/infection.[16,17]

III. Research Objectives

The major objectives of the proposed research are:

Objective 1: Develop a secure IoT healthcare architecture

To design and implement an end-to-end healthcare monitoring architecture using ESP32-based sensing, edge computing, secure communication, encrypted storage, and remote access.

Objective 2: Implement privacy-preserving physiological-data encryption

To encrypt sensitive physiological measurements at the patient-side device using Paillier-3072 before transmission to the server.

Objective 3: Implement post-quantum secure communication

To integrate Kyber-768/ML-KEM-768 for secure session-key establishment and combine it with AES-256-GCM authenticated encryption.

Objective 4: Optimize cryptographic computation on ESP32

To reduce the computational overhead associated with Paillier encryption through precomputation and secure NVS flash storage.

Objective 5: Provide replay and impersonation protection

To implement device authentication, per-request nonce generation, NTP timestamps, and server-side replay validation.

Objective 6: Harden the server against common attacks

To identify and eliminate vulnerabilities involving encryption oracles, unauthorized exports, device flooding, weak secrets, unrestricted CORS, plaintext logging, and unrestricted request rates.

Objective 7: Integrate AI-based disease detection

To develop a multi-model disease-detection layer capable of analyzing physiological parameters and monitoring five health conditions.

Objective 8: Enable secure remote healthcare-data access

To provide authenticated remote access to the healthcare dashboard using Cloudflare WSS/HTTPS without exposing the ESP32 directly to the public Internet.

IV. Proposed Architecture

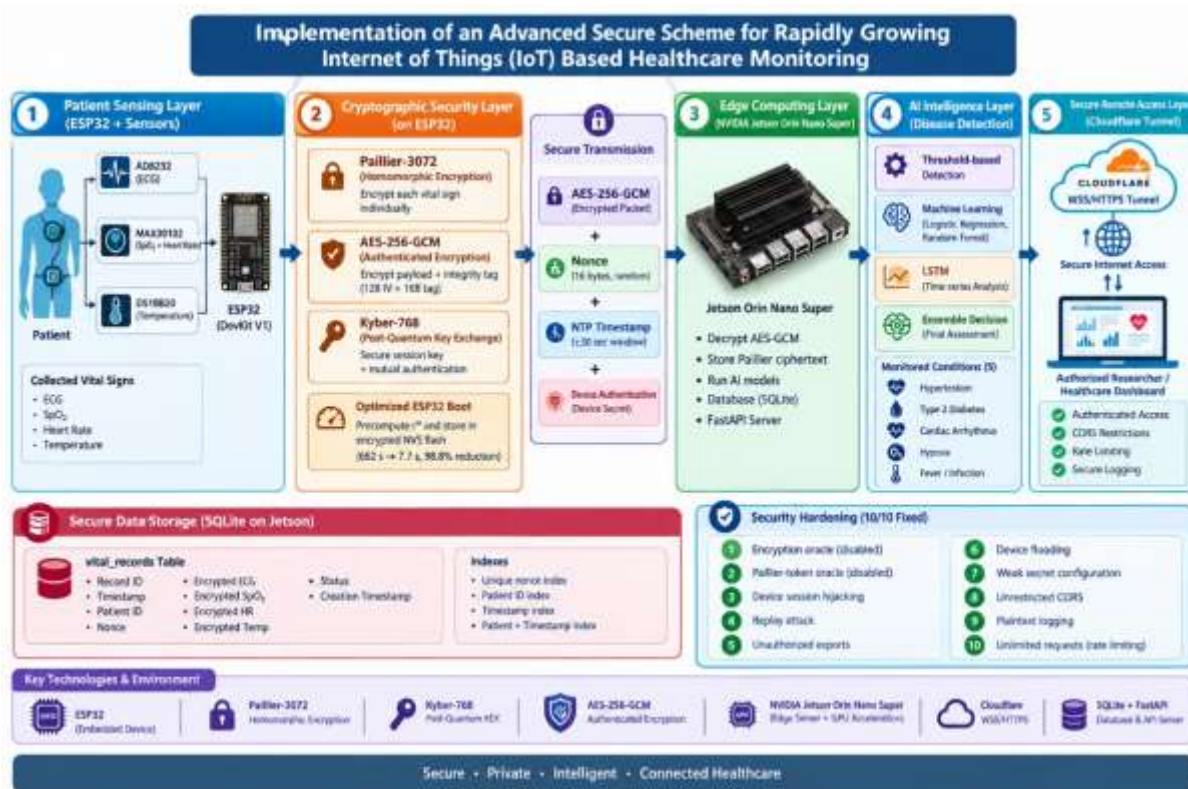


Fig:1 Proposed Architecture

4.1 Overall Architecture

The proposed architecture consists of five principal layers:

Layer 1 – Patient Sensing Layer

The patient-side ESP32 is connected to physiological sensors including:

AD8232 for ECG.

MAX30102 for SpO2 and heart rate.

DS18B20 for body temperature.

The sensor layer continuously collects physiological information.

Layer 2 – Cryptographic Security Layer

The collected measurements are encrypted on the ESP32 using Paillier-3072. AES-256-GCM subsequently wraps the encrypted payload for authenticated transmission. Kyber-768 is used during the session-establishment process.

Layer 3 – Edge Computing Layer

An NVIDIA Jetson Orin Nano Super receives the encrypted packets. AES-GCM is removed at the server, while

the Paillier ciphertext is retained for secure storage and privacy-preserving processing.

Layer 4 – AI Intelligence Layer

The incoming physiological information is processed through the disease-detection framework comprising threshold, ML, LSTM, and ensemble models.

Layer 5 – Secure Remote Access Layer

The Jetson server provides the application through FastAPI. Cloudflare tunneling provides remote WSS/HTTPS access to the authorized browser dashboard.

The updated architecture and data flow are explicitly described in the presentation as ESP32 + sensors → Paillier-3072 → AES-256-GCM → Kyber-768 session → Jetson server → disease detection → Cloudflare WSS/HTTPS dashboard.

4.2 Patient-Side Sensing

The ESP32 DevKit V1 acts as the primary embedded controller.

The proposed sensor configuration consists of:

Sensor	Parameter	Interface
AD8232	ECG	GPIO 39 / ADC
MAX30102	SpO2 + Heart Rate	I ² C GPIO 21/22
DS18B20	Temperature	GPIO 26 / 1-Wire

Table:1 Sensor Table

The presentation specifies the corresponding sensor interfaces and characteristics. Real-sensor documentation and firmware were completed, although the implementation at the reported stage was operating with simulated vital data pending real-sensor deployment.

4.3 Paillier-3072 Encryption

Each physiological parameter is independently encrypted using Paillier-3072.

The encryption operation is represented as:

$$c = (N+1)^m r^N \mod N^2$$

where:

(m) = plaintext physiological measurement,

(N) = 3072-bit Paillier public modulus,

(r) = random blinding factor,

(c) = resulting ciphertext.

Each Paillier ciphertext requires approximately 768 bytes. The ESP32 stores only the public key component required for encryption, while the random factor is generated locally.

4.4 AES-256-GCM Transport Protection

Following Paillier encryption, the ciphertext is wrapped using AES-256-GCM.

The session key is derived from the Kyber-768 key-exchange process. The packet contains:

12-byte IV,

encrypted payload,

16-byte authentication tag.

The use of GCM ensures both confidentiality and integrity of the transmitted packet.

4.5 Kyber-768 Key Exchange

The proposed system employs Kyber-768 for session establishment.

The process is:

```
[
ESP32 \rightarrow \text{Kyber Encapsulation}
]
[
Jetson \rightarrow \text{Kyber Decapsulation}
]
[
```

$\text{Shared Secret} \rightarrow \text{AES}_{256} \text{GCM}$

A device-specific secret is incorporated into the handshake to provide mutual authentication. The server uses constant-time comparison to validate the device secret.

4.6 Replay Attack Protection

Replay protection is achieved through three complementary mechanisms:

Random nonce

Every packet contains a 16-byte random nonce generated using the ESP32 hardware random-number generator.

NTP timestamp

The ESP32 synchronizes its clock through NTP and adds a Unix timestamp to every packet.

Database uniqueness

The nonce is stored in the database with a UNIQUE constraint. A previously used nonce therefore causes the packet to be rejected.

The server accepts timestamps only within a ± 30 -second window.

V. ESP32 Cryptographic Optimization

One of the major implementation challenges is the computational cost of calculating:

$$r^N \bmod N^2$$

using 3072-bit Paillier arithmetic.

The initial implementation required approximately 662 seconds to calculate this value on the ESP32. Such an 11-minute startup delay would be impractical for healthcare IoT deployment.

The proposed optimization computes (r^N) during the first boot and stores the result in encrypted NVS flash memory. The encryption key is derived through HKDF using the device secret and MAC address.

During subsequent boots, the ESP32 loads the precomputed value rather than recomputing it.

The resulting boot time is approximately:

$$662\text{s} \rightarrow 7.7\text{s}$$

Therefore:

$$\begin{aligned} \text{Reduction} &= \frac{662 - 7.7}{662} \times 100 \\ &\approx 98.8\% \end{aligned}$$

The presentation reports this as a 98.8% reduction in boot time.

VI. Security Hardening

The security-hardening stage identified ten vulnerabilities and implemented corresponding mitigation mechanisms.

Vulnerability	Proposed Mitigation
Encryption oracle	/esp32-encrypt permanently disabled
Paillier-token oracle	/paillier-token permanently disabled
Device session hijacking	Device-secret authentication
Replay attack	Nonce + NTP timestamp + DB constraint

Unauthorized exports	X-Admin-Token
Device flooding	Maximum 64-device registry
Weak tunnel secrets	Minimum 32-character validation
CORS wildcard	Explicit allowed origins
Plaintext logging	Disabled by default
Unlimited requests	slowapi rate limiting

Table:2 Security Hardening Stages Table

The presentation reports 10/10 vulnerabilities fixed, consisting of 2 critical, 4 high, and 4 medium vulnerabilities.

VII. AI-Based Disease Detection Architecture

The proposed AI layer operates on physiological measurements and generates disease-risk assessments.

Input Features

The disease-detection API accepts:

```
[
  X={HR,SpO_2,SBP,DBP,Temp,RR}
]
```

where:

HR = heart rate,

SpO2 = oxygen saturation,

SBP = systolic blood pressure,

DBP = diastolic blood pressure,

Temp = body temperature,

RR = respiratory rate.

The system provides three disease-related API services for detection, patient reporting, and model status.

Model 1: Threshold Model

The threshold model compares physiological measurements with defined clinical reference ranges.

Model 2: Machine-Learning Classifier

The proposed ML architecture uses: Logistic Regression, Random Forest.

The architecture is prepared for labeled training data.

Model 3: LSTM

The LSTM model is intended to analyze temporal sequences of vital measurements and identify gradual changes in patient condition.

Model 4: Ensemble Model

The ensemble layer combines the predictions of active models to obtain a more robust final assessment.

The four-model structure and its current implementation status are documented in the DPC-6 presentation.

VIII. Health Conditions Monitored

The proposed system monitors five conditions:

8.1 Hypertension

Blood-pressure measurements are evaluated for hypertension risk, including elevated systolic pressure and critical blood-pressure conditions.

8.2 Type 2 Diabetes

The system uses physiological indicators such as heart rate, respiratory rate, and temperature as part of the monitoring framework.

8.3 Cardiac Arrhythmia

Heart-rate abnormalities are used to identify bradycardia and tachycardia conditions.

8.4 Hypoxia

SpO2 thresholds are used to classify borderline, moderate, and critical oxygen-saturation conditions.

8.5 Fever/Infection

Body-temperature ranges are used to identify low-grade fever, high fever, critical fever, and hypothermia.

These five monitored conditions and their threshold ranges are specified in the source presentation.

IX. Database and Infrastructure

The Jetson server uses SQLite for storage. The vital_records database table contains:

Record ID

Timestamp

Patient ID

Nonce

Encrypted ECG

Encrypted SpO2

Encrypted heart rate

Encrypted temperature

Status

Creation timestamp

A unique index is created for the nonce to prevent duplicate packet insertion. Additional indexes are provided for patient ID, timestamp, and patient/timestamp combinations.

The server architecture uses:

NVIDIA Jetson Orin Nano Super

Ubuntu 22.04 / JetPack

FastAPI 0.115.0

SQLite

slowapi

Cloudflare WSS/HTTPS tunnel

The presentation identifies these components as the updated system specifications.

X. Results and Discussion

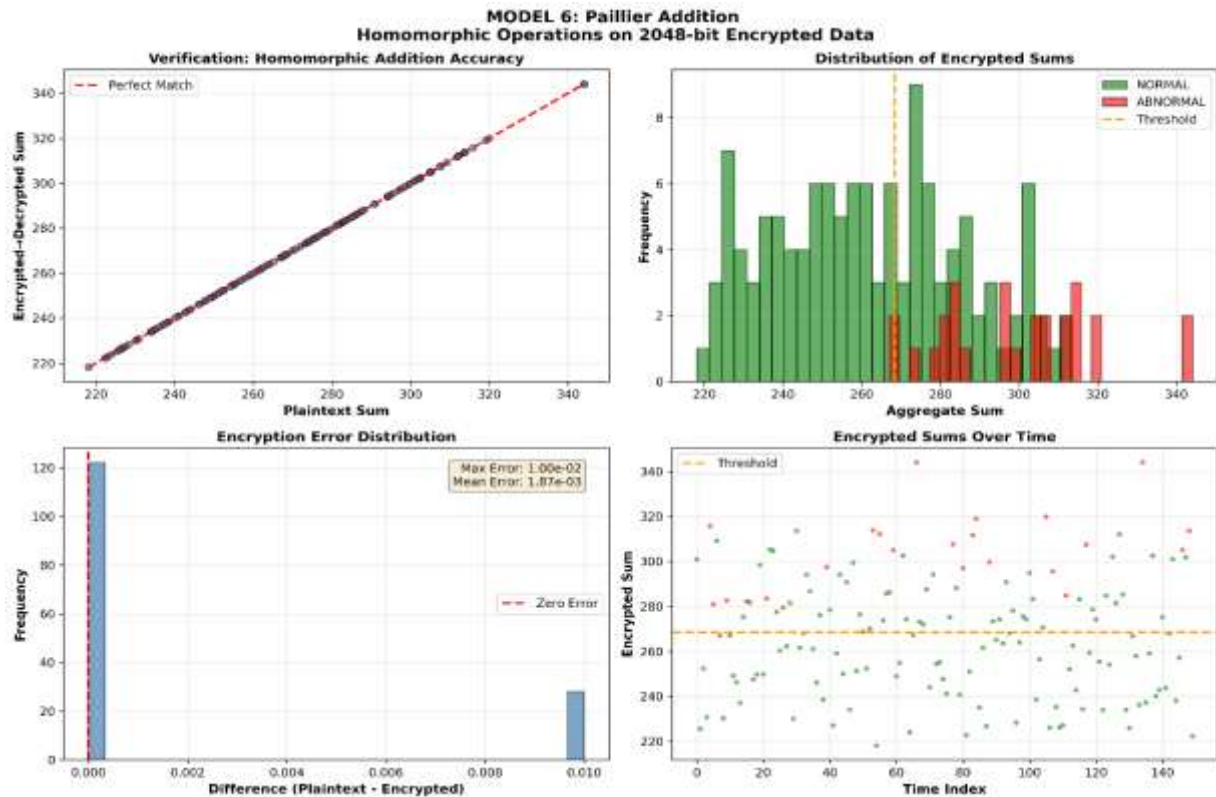


Fig:2 Paillier Addition of Homomorphic Operation on 2048 bit Encrypted Data.

- The figure presents Model 6: Paillier Addition Homomorphic Operations on 2048-bit encrypted data.
- The verification plot shows encrypted sums closely matching plaintext sums, demonstrating high homomorphic addition accuracy.
- The distribution plot compares NORMAL and ABNORMAL encrypted sums with a threshold around 268.
- The encryption error distribution shows a maximum error of 0.01 and a mean error of approximately 0.00187.
- The time-series plot illustrates encrypted sums over multiple time indices, with values distributed around and above the defined threshold.
- Overall, the results indicate that Paillier homomorphic encryption enables accurate and privacy-preserving aggregation of encrypted data.

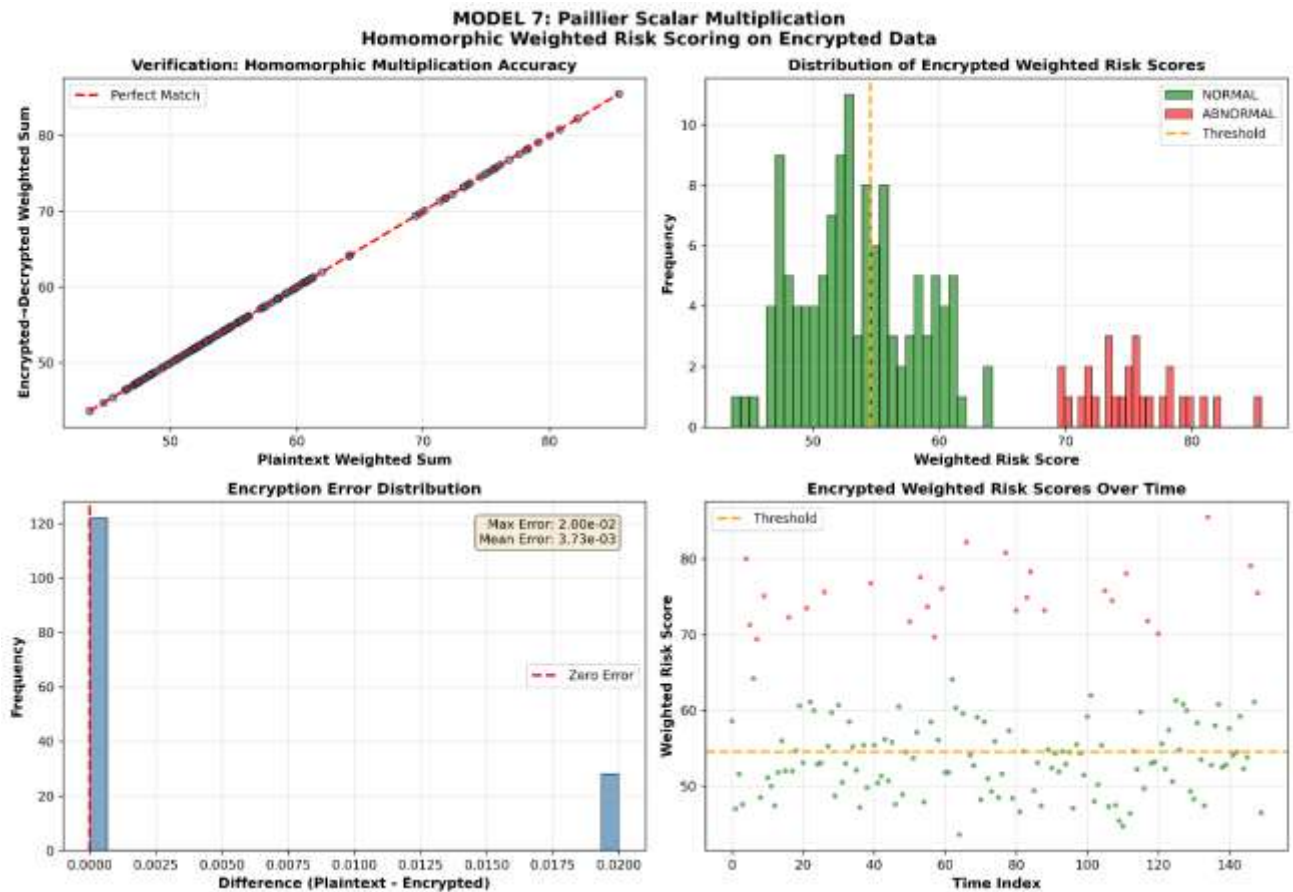


Fig:3 Paillier Scalar Multiplication Homomorphic Weighted Risk Scoring on Encrypted Data

- The figure presents Model 7: Paillier Scalar Multiplication Homomorphic Weighted Risk Scoring on encrypted data.
- The verification plot shows encrypted weighted sums closely matching plaintext weighted sums, indicating high multiplication accuracy.
- The distribution plot clearly separates NORMAL and ABNORMAL weighted risk scores, using a threshold of approximately 55.
- The encryption error distribution reports a maximum error of 0.02 and a mean error of approximately 0.00373.
- The time-series plot demonstrates that ABNORMAL scores generally remain above the threshold, while NORMAL scores are mostly below it.
- Overall, the results demonstrate that Paillier homomorphic scalar multiplication supports accurate, privacy-preserving weighted risk scoring on encrypted data.

The implementation demonstrates several measurable improvements compared with the earlier architecture.

Parameter	Previous Architecture	Proposed Architecture
Server	Raspberry Pi	Jetson Orin Nano Super
Remote access	Local LAN	Cloudflare WSS/HTTPS
Key exchange	Kyber-512	Kyber-768
Transport encryption	AES-128	AES-256-GCM

Homomorphic encryption	Basic Paillier	Paillier-3072
ESP32 boot	~662 s	~7.7 s
Replay protection	None	Nonce + timestamp + DB constraint
Device authentication	Device ID	Device secret + Kyber
Security vulnerabilities	0 fixed	10/10 fixed
Disease detection	Not available	Four-model system
Health conditions	—	Five

Table:3 Measurement Table

The comparative results are directly reported in the presentation.

The most significant implementation result is the reduction in ESP32 boot time from approximately 662 seconds to 7.7 seconds. This demonstrates that secure homomorphic encryption can be made substantially more practical on a constrained embedded platform through appropriate precomputation and secure storage.[15,16,17]

The second major result is the security hardening of the architecture. Ten vulnerabilities were identified and addressed. Particularly important were the removal of the encryption-oracle endpoints and local generation of the Paillier random factor on the ESP32. This prevents the server from controlling the randomness used in ciphertext generation.

The third contribution is the integration of AI-based disease detection into the secure IoT pipeline. This changes the architecture from a simple secure data-collection platform into an intelligent healthcare monitoring system.

XI. Research Novelty

The primary novelty of the proposed research is system-level integration rather than the invention of an individual cryptographic algorithm.

The proposed architecture combines:

- Paillier-3072 homomorphic encryption.
- Kyber-768 post-quantum key exchange.
- AES-256-GCM authenticated encryption.
- ESP32-side cryptographic optimization.
- NTP-based replay protection.
- Per-request random nonces.
- Mutual device authentication.
- Security-hardened server APIs.
- Edge computing using Jetson Orin Nano Super.
- AI-based disease detection.

The presentation specifically identifies the integration of these mechanisms and the 98.8% boot-time optimization as key research contributions.

The architecture therefore demonstrates how post-quantum security, homomorphic encryption, embedded optimization, and intelligent healthcare analytics can be integrated into a practical IoT platform.

XII. Limitations

Although the proposed architecture demonstrates substantial improvements, several limitations remain.

First, the reported implementation was operating with simulated vital data while the real sensor deployment was

pending hardware availability.[20,21]

Second, the ML classifier and LSTM components are described as ready for training but require appropriate labeled datasets. The LSTM architecture particularly requires sufficiently large temporal datasets.[22,23]

Third, the current architecture stores the Paillier private-key components on the Jetson server. Consequently, the server can potentially decrypt physiological measurements. The presentation identifies this as an open research question for the subsequent research stage.[24,25]

Fourth, Paillier provides additive homomorphism rather than the multiplicative capabilities required by many

nonlinear machine-learning operations. Consequently, more advanced privacy-preserving ML inference may require additional cryptographic mechanisms.[1-10]

XIII. Future Scope

Future research will focus on federated anomaly learning and privacy-preserving distributed intelligence.

The planned architecture includes:

- Per-device physiological baselines.
- On-device anomaly detection.
- Mahalanobis-distance analysis.
- Adaptive sliding windows.
- Differential privacy.
- Multi-device aggregation.
- Privacy-preserving federated learning.

The proposed federated architecture is intended to enable multiple patient devices to contribute to learning without directly exposing plaintext physiological measurements.

Another important future direction is removal of the Paillier private key from the Jetson server. One proposed approach is to keep the private key with the patient or healthcare data owner while allowing the server to perform homomorphic aggregation. Another possibility is integration of CKKS for encrypted machine-learning inference where multiplication and nonlinear operations are required.

XIV. Conclusion

This research presents an advanced secure IoT healthcare monitoring architecture that integrates embedded sensing, homomorphic encryption, post-quantum cryptography, authenticated transport encryption, edge computing, security hardening, and AI-based disease detection.

The proposed system uses ESP32 as the patient-side sensing and encryption platform and NVIDIA Jetson Orin Nano Super as the edge server. Paillier-3072 protects physiological measurements at the data layer, AES-256-GCM provides authenticated transport protection, and Kyber-768 establishes post-quantum-secure session keys.

A major implementation contribution is the optimization of Paillier computation through secure NVS flash storage of the precomputed (r^N) value. This reduces the ESP32 startup requirement from approximately 662 seconds to 7.7 seconds, achieving a reported 98.8% reduction in boot time.

The security-hardening process identified ten vulnerabilities and implemented corresponding protections, including encryption-oracle removal, device authentication, replay prevention, authenticated exports, device-registration limits, secret validation, CORS restrictions, controlled logging, and rate limiting. The system reports successful remediation of all ten identified vulnerabilities.

Furthermore, the integration of threshold-based detection, machine-learning classification, LSTM analysis, and ensemble prediction introduces an intelligent layer capable of monitoring hypertension, Type 2 diabetes, cardiac arrhythmia, hypoxia, and fever/infection.

Overall, the research demonstrates that a combination of post-quantum cryptography, privacy-preserving encryption, embedded optimization, edge computing, and AI can provide a promising foundation for secure IoT healthcare monitoring. The future extension toward federated anomaly learning and server-independent key ownership can further strengthen privacy and enable distributed intelligence without exposing sensitive patient information.

ACKNOWLEDGEMENTS

Not applicable.

FUNDING STATEMENT

This study received no specific financial support.

References

- [1] U. H. Khan, A. Qamar, R. Khan, M. A. Alawad, F. Alturise, and M. Hayat, "TrustEdge: A quantum-safe, self-healing framework for federated TinyML in critical ICU monitoring," *Internet of Things*, vol. 36, Art. no. 101855, 2026, doi: 10.1016/j.iot.2025.101855.
- [2] N. Sharma and P. G. Shambharkar, "Enhancing internet of medical things security: A multi-layered approach using dynamic adaptive deep reinforcement learning and blockchain," *Computers & Electrical Engineering*, vol. 129, Art. no. 110808, 2026, doi: 10.1016/j.compeleceng.2025.110808.

- [3] S. Prajapat, D. Gautam, P. Kumar, A. K. Das, S. Pal, and C. Dong, "Blockchain-enabled secure signature scheme with quantum key distribution for IoMT-based healthcare systems," *IEEE Journal of Biomedical and Health Informatics*, vol. 30, no. 4, pp. 3601–3612, 2026, doi: 10.1109/JBHI.2025.3614874.
- [4] S. Fugkeaw, K. Tangtanawirut, P. Rattanasrisuk, and A. Changtor, "MK-WISE: Secure and efficient multi-keyword wildcard ABSE with keyword-level revocation for device–edge–cloud EHRs data sharing," *IEEE Transactions on Network and Service Management*, vol. 23, pp. 2295–2311, 2026, doi: 10.1109/TNSM.2026.3657982.
- [5] M. Tanveer and S. A. Aldossari, "SAF-IoMT: Secure authentication framework for IoMT-enabled smart healthcare system," *Digital Communications and Networks*, 2026, doi: 10.1016/j.dcan.2026.04.005.
- [6] C. Nnadike, S. O. Ajakwe, J. M. Lee, and D.-S. Kim, "RemoteCare: AI-driven multimodal predictive framework with blockchain for personalized remote patient monitoring in IoMT," *IEEE Internet of Things Journal*, vol. 13, no. 3, pp. 4508–4523, 2026, doi: 10.1109/JIOT.2025.3633505.
- [7] A. A. Ali, M. A. Gunavathie, V. Srinivasan, M. Aruna, R. Chennappan, and M. Matheena, "Securing electronic health records using blockchain-enabled federated learning for IoT-based smart healthcare," *Clinical eHealth*, vol. 8, pp. 125–133, 2025, doi: 10.1016/j.ceh.2025.04.002.
- [8] M. Firdaus, H. T. Larasati, and K. H. Rhee, "Blockchain-based federated learning with homomorphic encryption for privacy-preserving healthcare data sharing," *Internet of Things*, vol. 31, Art. no. 101579, 2025, doi: 10.1016/j.iot.2025.101579.
- [9] P. Das, N. Kumar, C. Jain, Ansul, and M. Singh, "Intelligent IoT-enabled healthcare solutions implementing federated meta-learning with blockchain," *Journal of Industrial Information Integration*, vol. 45, Art. no. 100797, 2025, doi: 10.1016/j.jii.2025.100797.
- [10] J. Xiang, O. Salem, A. Meahoua, S. Wicha, and P. Sureephong, "Secure blockchain-based single sign-on with zero-knowledge proof authentication," in *Proc. 2025 Global Information Infrastructure and Networking Symposium (GIIS)*, 2025, doi: 10.1109/GIIS64151.2025.10921879.
- [11] L. Yin, X. Du, Y. Cheng, J. Li, *et al.*, "Decentralized IoMT architecture for privacy-preserving remote patient monitoring," *IEEE Sensors Journal*, vol. 25, no. 14, pp. 27495–27512, 2025, doi: 10.1109/JSEN.2025.3575941.
- [12] R. Mehla, R. Garg, and M. A. Khan, "Privacy-preserving solution for data sharing in IoT-based smart consumer electronic devices for healthcare," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 4586–4595, 2025, doi: 10.1109/TCE.2025.3540642.
- [13] M. M. Saeed, "An AI-driven cybersecurity framework for IoT: Integrating LSTM-based anomaly detection, reinforcement learning, and post-quantum encryption," *IEEE Access*, vol. 13, pp. 104027–104036, 2025, doi: 10.1109/ACCESS.2025.3576506.
- [14] D. Rahbari, M. Daneshmand, and M. Jenihhin, "An efficient architecture for edge AI federated learning with homomorphic encryption," *IEEE Access*, vol. 13, pp. 97919–97929, 2025, doi: 10.1109/ACCESS.2025.3576689.
- [15] P. S. N. [et al.], "SE²FL: Scalable, secure, and energy-efficient federated learning for continuous wearable health IoT," in *Proc. IEEE International Conference on Intelligent Computing, Information and Control Systems (ICOIICS 2025)*, 2025/2026, doi: 10.1109/ICOIICS67115.2025.11390144.
- [16] C. Su, J. Wen, J. Kang, Y. Wang, Y. Su, H. Pan, Z. Zhong, and M. S. Hossain, "Hybrid RAG-empowered multimodal LLM for secure data management in Internet of Medical Things: A diffusion-based contract approach," *IEEE Internet of Things Journal*, vol. 12, no. 10, pp. 13428–13440, 2025, doi: 10.1109/JIOT.2024.3521425.
- [17] O. Cheikhrouhou, K. Merhad, M. Laurent, and A. Koubaa, "Blockchain and emerging technologies for next generation secure healthcare: A comprehensive survey of applications, challenges, and future directions," *Blockchain: Research and Applications*, vol. 6, no. 4, Art. no. 100305, 2025, doi: 10.1016/j.bcra.2025.100305.
- [18] L. P. S. Loganatha, K. Himabindu, P. Sowjanya, Y. D. Patil, *et al.*, "Enhancing security and privacy in blockchain-IoT hybrid healthcare database systems through federated learning," in *Proc. 2024 Global Conference on Communications and Information Technologies (GCCIT)*, 2024/2025, doi: 10.1109/GCCIT63234.2024.10862397.
- [19] K. Mansoor, M. Afzal, W. Iqbal, Y. Abbas, S. Mussiraliyeva, and A. Chehri, "PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems," *Internet of Things*, vol. 27, Art. no. 101228, 2024, doi: 10.1016/j.iot.2024.101228.
- [20] A. N. E. Bahache, N. Chikouche, and S. Akleylek, "Securing cloud-based healthcare applications with a quantum-resistant authentication and key agreement framework," *Internet of Things*, vol. 26, Art. no. 101200, 2024, doi: 10.1016/j.iot.2024.101200.
- [21] K. Fiaz, A. Zeb, S. Hussain, K. Khurshid, R. R. Irshad, M. Alharby, T. Rahman, I. M. Alwayle, and F. Pallonetto, "A two-phase blockchain-enabled framework for securing Internet of Medical Things systems," *Internet of Things*, vol. 28, Art. no. 101335, 2024, doi: 10.1016/j.iot.2024.101335.
- [22] S. Saif, P. Das, S. Biswas, S. Khan, *et al.*, "A secure data transmission framework for IoT enabled healthcare," *Heliyon*, vol. 10, no. 16, Art. no. e36269, 2024, doi: 10.1016/j.heliyon.2024.e36269.
- [23] "A hybrid secure signcryption algorithm for data security in an Internet of Medical Things environment," *Journal of Information Security and Applications*, vol. 85, Art. no. 103836, 2024, doi: 10.1016/j.jisa.2024.103836.