

Always On Trust for Remote Cardiac Monitoring: Quantum Safe Authentication with One Time PUFs and Edge Anomaly Screening

Shafiq Ahmed, *Student Member, IEEE*, Mohammad S. Obaidat, *Life Fellow, IEEE*,
Khalid Mahmood, *Senior Member, IEEE*, Mohammad Hossein Anisi, *Senior Member, IEEE*, Ayesha Iqbal,
Khawaja Qasim Maqbool, *Senior Member, IEEE*

Abstract—Remote cardiac monitoring is moving from occasional clinic visits to continuous observation at home. In a typical Intelligent Internet of Medical Things workflow a wearable ECG sensor sends readings through an edge gateway to a clinical platform for storage and review. That convenience also widens the attack surface. If a cloned device is admitted or telemetry is altered clinicians may rely on false signals and patient privacy may be exposed. A longer horizon problem is also emerging. Adversaries can store encrypted medical traffic today and target it later with stronger quantum tools. At the same time many lightweight schemes still rely on static Physical Unclonable Functions whose challenge response behavior may be learned from repeated observations. We address both concerns with a compact authentication fabric for real time cardiac monitoring. The design uses a reconfigurable One Time Physical Unclonable Function so each successful session refreshes response behavior and weakens modeling attacks. It also combines ML-KEM-768 for key establishment with ML-DSA-65 for device authentication. An Isolation Forest ensemble at the gateway then screens behavioral drift that may indicate misuse or compromise. Our prototype completes authentication in 14.7ms with about 4.6kB per session and reaches 94.5% precision with a 2.3% false positive rate.

Index Terms—Intelligent Internet of Medical Things (IIoMT), remote patient monitoring, device authentication, post-quantum cryptography, privacy by design, AI-assisted anomaly detection, audit and consent.

I. INTRODUCTION

In remote cardiac care the system should always answer a basic question. Which device produced this reading and under what authorized context? In a typical Intelligent Internet of Medical Things setup a wearable ECG sensor sends measurements to a nearby gateway such as a phone or home hub. The gateway then forwards the data to a clinical service for storage alerts and review. This model is convenient and may reduce pressure on hospitals. It also concentrates risk. If

an attacker impersonates a sensor tampers with telemetry or quietly extracts long term records clinicians may rely on false signals and patients may lose privacy.

Two attacker capabilities make this setting harder than many standard IoT deployments. One is the long horizon threat from quantum computing. An adversary can capture encrypted telemetry today and try to decrypt it later when stronger quantum resources become practical. The other is tied to PUF based authentication. PUFs are attractive because they bind identity to hardware. Yet a static PUF may leak enough challenge response observations over time to support modeling attacks. In that setting an attacker can train a predictor and later forge responses.

Recent work addresses parts of this problem but usually misses the practical limits of continuous cardiac monitoring. Bathalapalli et al. combine PUFs with blockchain style infrastructure to strengthen integrity and traceability. That can help accountability but ledger updates and consensus steps can add delay that is hard to justify in real time sensing loops [1]. Kalam et al. use PUFs with fuzzy logic for IoMT access control. The design still depends on conventional PUF behavior and may stay exposed to long term observation and modeling [2]. On the post quantum side Othman et al. propose a privacy aware aggregation framework. Its heavier cryptographic design appears better suited to multi region analytics than to a lightweight home monitoring setting [3]. Blind signature based authentication can reduce linkability in IoMT exchanges. Yet ECC based designs do not remove the quantum risk [4]. Yang et al. report efficient industrial IoT authentication using tokens and elliptic curve operations. Even so that model does not directly address healthcare requirements such as consent auditability and purpose bound access [5]. AI based detection is also gaining ground in IoMT and edge security. Even here anomaly screening is often treated as a separate add on instead of a safeguard tied directly to authentication and session setup [6] and [7].

Table I summarizes this picture and makes the gap clearer. Most existing schemes optimize one axis such as efficiency privacy or quantum resistance while leaving the remaining risks to operational assumptions.

A. Motivation and Contribution

This subsection explains the design pressure in continuous cardiac monitoring and states the main contributions of this

S. Ahmed and M. H. Anisi are with the School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, UK. M. S. Obaidat is with King Abdullah II School of Information Technology, University of Jordan, Amman, Jordan, Amity School of Engineering and Technology, Amity University, Noida, Uttar Pradesh, India. Khalid Mahmood is with Graduate School of Intelligent Data Science, National Yunlin University of Science and Technology, Douliu 64002, Taiwan. Khawaja Qasim Maqbool and Ayesha Iqbal are with the Department of Computer Science, Bahria University, Lahore Campus.
E-mail: s.ahmed@essex.ac.uk; msobaidat@gmail.com;
khalid@yuntech.edu.tw; m.anisi@essex.ac.uk; ayeshaiqbal0197@gmail.com;
qasim@bahria.edu.pk

TABLE I
COMPARISON OF RECENT IIoMT SECURITY AND AUTHENTICATION
SCHEMES

Work	Year	Main idea	PQC	PUF	AI	Key limitation
[1]	2024	PUF + ledger	No	Yes	No	High latency, no PQC
[3]	2025	PQC + ZK + edge AI	Yes	No	Yes	High comm. and energy
[4]	2025	Blind signature	No	No	No	No PQC, added complexity
[6]	2024	Edge IDS (DL)	N/A	No	Yes	IDS only, training cost
[7]	2024	DL anomaly det.	N/A	No	Yes	Model size and latency
[8]	2025	PQC + privacy survey	Yes	No	No	Mostly theoretical, no validation
[9]	2024	Anon. auth + KA	No	No	No	Classical only, no monitoring
[10]	2024	PUF + NLFSR	No	Yes	No	Static PUF, privacy gaps
[11]	2025	Lattice PQC for IoMT	Yes	No	No	High compute, no ML resilience

work. Continuous cardiac monitoring leaves very little room for security error. Wearables run on limited battery power. Gateways must respond quickly so clinical workflows do not stall. Care teams also need audit trails and consent aware access instead of a simple allow or deny result. Attackers meanwhile rarely rely on one tactic. They may mix stolen credentials with behavior imitation or store protocol traces for later cryptanalysis. Taken together these pressures point to a design that treats authentication post quantum migration and runtime monitoring as one security fabric rather than separate add ons.

The main contributions of this work are listed below.

- We introduce a reconfigurable OPUF mechanism that refreshes device response behavior after each successful session so earlier observations become less useful to a learning attacker.
- We design a hybrid handshake that uses ML-KEM-768 for key establishment and ML-DSA-65 for authentication while keeping a classical component for practical migration in near term deployments.
- We couple authentication with an Isolation Forest based detector at the gateway so suspicious access patterns and session behavior can be flagged early before wider leakage develops.
- We report end to end measurements and discuss privacy by design issues such as data minimization consent and audit so the solution stays credible for home monitoring rather than only for controlled lab settings.

The remainder of this article proceeds as follows. Section II defines the IIoMT entities, threat assumptions, and design goals. Section III presents the protocol while Sections IV and V analyze security and evaluate performance. Finally we conclude this article with future directions in Section VI.

II. SYSTEM MODEL AND ARCHITECTURE

Remote patient health monitoring in the IIoMT connects a wearable sensor, a home gateway, and a hospital service into a clinical pipeline. This section sets the reference architecture and the assumptions used throughout. We authenticate the device and establish fresh session keys for telemetry while anticipating quantum and learning enabled attackers.

A. Network Entities

The complete architecture, including all the network entities, is shown in Figure 1.

- 1) **Wearable ECG sensor (S):** The patient wears a battery powered electrocardiogram (ECG) sensor in the ESP32-S3 class. The sensor sends compact feature summaries to reduce radio cost and limit exposure, and it forwards them to the gateway over Bluetooth Low Energy (BLE). A reconfigurable OPUF in the secure element anchors identity to hardware. After each successful session, the OPUF refreshes its challenge-response behavior so observed pairs do not remain useful for long.
- 2) **Gateway (G)** A phone class gateway aggregates readings and mediates connectivity to the backend. It runs an Isolation Forest ensemble to spot unusual access behavior and can trigger step up authentication or shorten session lifetimes when risk rises. The edge gateway performs local temporal averaging and removes direct patient identifiers before sending these summaries to the backend.
- 3) **Hospital backend (B)** The backend registers devices verifies authentication evidence and enforces policy. It checks each request against consent state and clinical purpose and records decisions in tamper evident logs through hash chaining with signed checkpoints. Hardware Security Modules (HSMs) protect long term keys.

B. Security Preliminaries and Threat Assumptions

This subsection states the main cryptographic choices and the threat assumptions behind the design.

Cryptographic components. Session keys are derived through a hybrid key establishment that combines X25519 with ML-KEM-768. The shared secrets are then mixed with HKDF using SHA-256. ML-DSA-65 provides entity authentication. AES-256-GCM protects telemetry during transmission.

Threat model. We assume an active adversary who can intercept replay and modify traffic over BLE and the Internet. The same adversary may store ciphertext for later decryption attempts. We also consider a modeling attacker who learns from observed challenge response pairs and an insider who may use data beyond an approved purpose. The hospital backend is trusted. All communication links are treated as hostile by default.

III. PROPOSED AUTHENTICATION SCHEME

This section describes the proposed scheme as a simple, deployable workflow rather than a dense protocol listing. We structure it into three phases that mirror how hospitals provision devices in practice: (i) system initialization at the backend, (ii) one time registration of the sensor and gateway, and (iii) repeated session authentication with hybrid key establishment and continuous risk monitoring.

A. Phase 1: System Initialization (Backend Setup)

The hospital backend (B) acts as the identity and policy authority. It selects the cryptographic suite and prepares policy controls used in every session. Concretely, B enables a hybrid key establishment that combines X25519 and ML-KEM-768, uses ML-DSA-65 for signed credentials and server assertions,

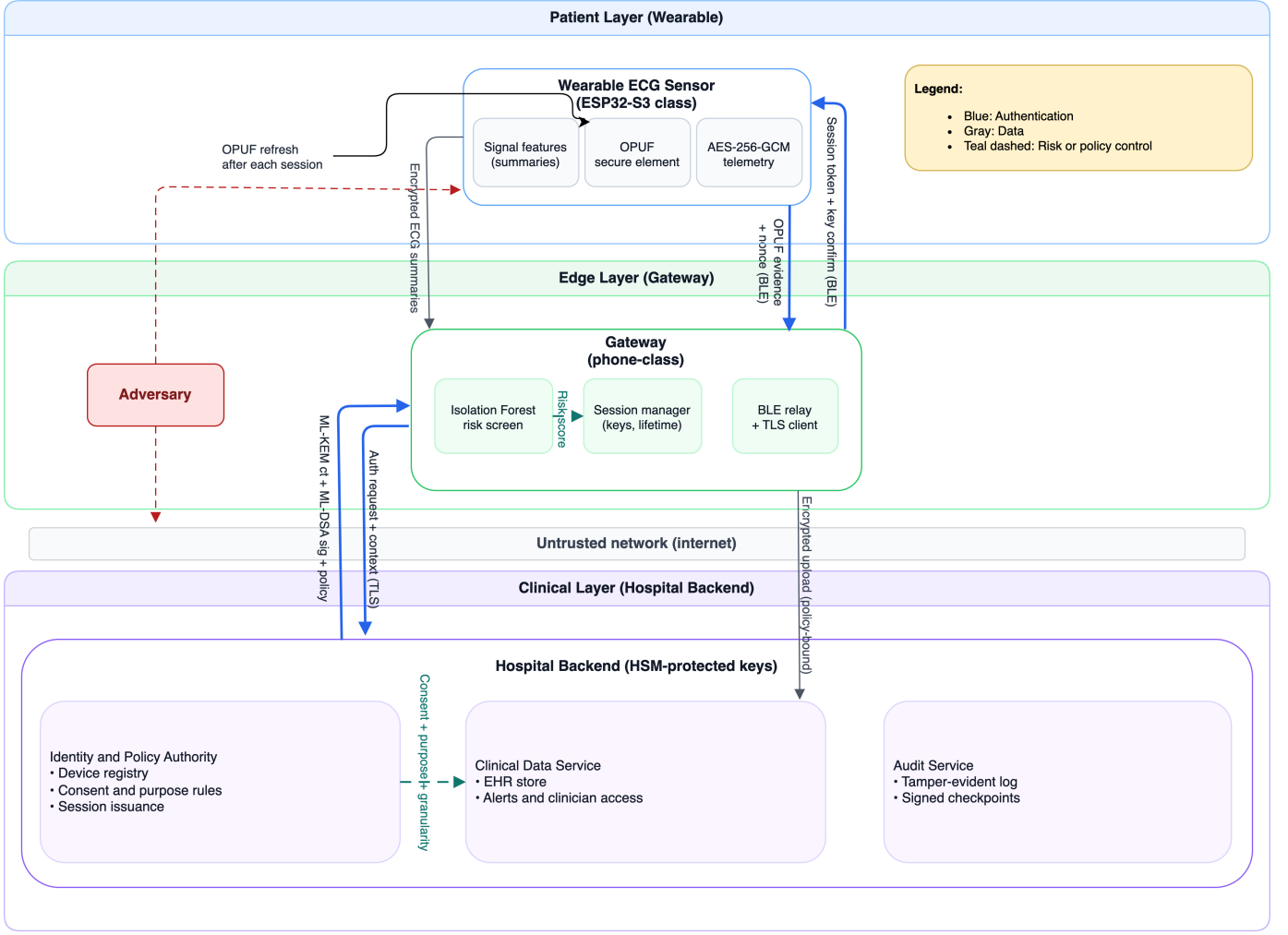


Fig. 1. System Architecture

and protects telemetry with AES-256-GCM. B also configures the audit service to record security relevant decisions (registration, session start, step up events, and session termination) in tamper evident logs.

In parallel, B configures policy templates that reflect common clinical needs. For example, treatment allows full fidelity streams, care coordination allows summaries and alerts, and research requires explicit opt-in and only releases de-identified features. These templates matter later because the system ties risk and consent to data granularity and session lifetime.

B. Phase 2: Registration (Controlled Enrollment)

Registration occurs once per device and runs in a controlled setting (for example, during patient onboarding).

Sensor enrollment. The wearable ECG sensor (S) activates its OPUF inside the secure element and derives a device bound fingerprint from its OPUF behavior and stable hardware identifiers. To ensure fingerprint stability against environmental noise (e.g., temperature variations), the secure element employs standard Helper Data Algorithms (HDA) during the OPUF enrollment and reconstruction phases. S then sends

an enrollment request to B over a protected provisioning channel. After validation (including manufacturer attestation where available), B issues a pseudonymous sensor identifier and a compact credential bound to that pseudonym. S stores the credential in the secure element and keeps the OPUF in an initial configured state.

Gateway and patient enrollment. The gateway (G) registers its device identity and obtains a credential that links it to the patient episode without exposing civil identity in routine protocol messages. During the same step, the patient records consent choices (for example, treatment and care coordination permitted, research denied). B stores consent state and policy bindings and treats them as first class inputs to later access decisions.

C. Phase 3: Authentication and Key Agreement (Routine Sessions)

When monitoring starts, S, G, and B establish an authenticated session in four practical steps.

Step 1: Sensor proves liveness to the gateway. S creates a fresh nonce and uses its current OPUF state to produce an

authentication response. S sends its pseudonymous identifier, nonce, and a keyed authenticator derived from its stored credential to G over BLE. This step proves that the message originates from the enrolled hardware rather than from a copied identifier.

Step 2. Backend verifies the sensor and receives the risk signal. G forwards the sensor evidence to B together with session context such as timing and recent session history. B checks the OPUF evidence against the enrolled sensor profile. In parallel G applies the Isolation Forest model to session metadata and sends the resulting risk level to B. When risk stays low B proceeds normally. When risk rises B can require step up confirmation at the gateway shorten session lifetime or downgrade data to summaries until confidence improves.

Step 3. Hybrid key establishment between gateway and backend. B and G establish fresh session keys using X25519 and ML-KEM-768 and then mix the outputs through HKDF with SHA-256. This hybrid design keeps the session protected even if one primitive weakens later. B signs the session parameters such as lifetime permitted data granularity and refresh interval with ML-DSA-65 so G can verify that the policy came from the hospital authority.

Step 4. Protected telemetry and ongoing control. S encrypts telemetry to G using AES-256-GCM under a session key derived from the authenticated context. G then forwards permitted data to B under the gateway backend session key. During the session G and B continue to watch behavioral signals. If anomalies appear such as unusual access bursts or repeated replays B can trigger re authentication or terminate the session and record the decision in the audit log.

OPUF refresh. After session completion S refreshes its OPUF state so the next authentication uses new response behavior. This refresh reduces the value of accumulated observations and directly lowers the feasibility of long term modeling attacks. The backend retains the previous OPUF state until the gateway confirms that session establishment is fully complete which helps prevent desynchronization if packets are dropped.

IV. SECURITY ANALYSIS

We evaluate security through an informal, scenario driven analysis, similar to how a deployment team would reason about likely failures. The goal is not to claim a formal proof, but to explain why the design resists the most relevant threats in home cardiac monitoring: impersonation, long term decryption risk, learning based modeling of device identity, and misuse that slips past simple accept or reject checks.

A. Security Evaluation

- 1) Mutual authentication and impersonation resistance: An attacker who tries to impersonate the wearable sensor must produce valid OPUF based evidence bound to the enrolled hardware. In our design, the backend validates this evidence against the sensor profile and session freshness, so replayed transcripts do not remain useful. The OPUF refresh step also matters here: after a successful session, the sensor changes its response

behavior, which reduces the value of previously observed challenge-response material and makes long term impersonation attempts harder to scale. An attacker who tries to impersonate the backend faces a different barrier. The gateway accepts session parameters only when the backend signs them with ML-DSA-65. Without that signing capability, an adversary cannot reliably push forged session limits, data granularity rules, or keying material that the gateway will accept.

- 2) Post quantum protection against harvest now decrypt later. A realistic attacker can capture encrypted telemetry and handshake transcripts and keep them for years. This is why the design uses hybrid key establishment. The gateway and backend derive the session key from both X25519 and ML-KEM-768 outputs and then mix them through HKDF with SHA-256. If future quantum machines weaken classical elliptic curve assumptions the ML-KEM part still protects the session key. This hybrid design also avoids an all or nothing migration and fits the way hospitals usually upgrade systems over time.
- 3) Resistance to learning based modeling of device identity. Static PUF schemes can leak enough observations to support modeling attacks. Our design tries to disrupt the attacker's learning loop. Because the sensor refreshes its OPUF state after every authenticated session the mapping the attacker wants to learn does not remain stable. This does not remove risk entirely but it raises the attack cost. The adversary must keep collecting fresh observations and retrain against a moving target while the backend rejects stale evidence.
- 4) Session integrity replay resistance and hijacking signals. We include fresh nonces and strict freshness checks to block replay. Even if an attacker captures encrypted telemetry AES-256-GCM still provides confidentiality and integrity under the negotiated session key. If a gateway token is stolen or a local session is compromised the anomaly detector adds another safety layer. Unusual timing burst patterns or repeated failures raise risk and can trigger step up actions or early termination before large scale leakage occurs.
- 5) Privacy controls unlinkability and auditability. Routine messages use pseudonymous identifiers so passive observers cannot easily map sessions to a real identity. The backend ties access to consent and clinical purpose and records decisions in tamper evident logs with signed checkpoints. Logging alone does not stop every misuse but it supports investigation accountability and operational oversight which healthcare settings usually require.

B. Security Feature Comparison with Recent Schemes

Table II summarizes how our scheme combines post quantum readiness, OPUF based modeling resistance, and gateway side monitoring, alongside consent and audit controls.

V. PERFORMANCE EVALUATION

This section evaluates whether the proposed protocol remains practical on commodity wearable hardware, despite

TABLE II
SECURITY FEATURE COMPARISON

Feature	[1]	[2]	[3]	[4]	Proposed
Post quantum ready	No	No	Yes	No	Yes
Modeling resistant device ID	Yes	Partial	No	No	Yes
Gateway side anomaly monitoring	No	No	Yes	No	Yes
Consent and purpose enforcement	No	No	Partial	Partial	Yes
Tamper evident audit trail	Yes	No	Yes	No	Yes
Low latency wearable focus	Partial	Partial	Partial	Partial	Yes

TABLE III
COMPUTATION COST COMPARISON

Scheme	Year	Latency	Notes
[1]	2024	3.66 s	Device authentication time on Raspberry Pi 4
[2]	2025	0.03024 s	Total execution time (authentication)
[3]	2025	12.5 ms/packet	Per packet security latency
[4]	2025	2.32 s	Total execution time (authentication)
Proposed	2026	14.7 ms/session	End to end session establishment

adding post quantum authentication, OPUF based device binding, and lightweight anomaly screening. We report prototype measurements on our three tier testbed and compare them with recently published IoMT schemes.

A. Experimental Setup and Measurement Approach

We implemented the protocol across a realistic home monitoring stack: (i) a wearable ECG node on an ESP32-S3 (dual core 240MHz, BLE), (ii) a gateway client on a Raspberry Pi 4 Model B (quad core Cortex-A72, 4 GB RAM), and (iii) a hospital backend on an AWS EC2 t3.medium instance, (iv) we used Bluetooth Low Energy (BLE) version 5.0, with the devices placed at a typical indoor monitoring distance of 3 meters in a standard home environment to account for realistic baseline interference. The wearable executes device authentication and session setup. The gateway mediates the handshake and enforces the local risk gate. The backend issues credentials and finalizes policy decisions.

For cryptography, the prototype uses X25519 for classical key agreement and ML-KEM-768 plus ML-DSA-65 for post quantum key establishment and signatures. We averaged end to end timing over 1000 session establishments. We measured wearable energy using a precision power monitor and isolated authentication energy from baseline sensing.

B. Computation Cost Comparison

Table III summarizes the latency figures of the selected baselines and our prototype. Note that Othman et al. report per packet security processing, whereas the remaining works and our prototype report an authentication session critical path [3]. We therefore treat the table as an indicative comparison.

The important point to consider is that our session setup remains well below typical clinical interaction latencies and does not interfere with continuous monitoring. The added cost

TABLE IV
COMMUNICATION COST COMPARISON

Scheme	Year	Overhead
[1]	2024	NR
[2]	2025	2688 bits
[3]	2025	4.46 to 8.92 kB/packet
[4]	2025	800 bits
Proposed	2026	4.6 kB/session

TABLE V
ENERGY AND BATTERY COMPARISON

Scheme	Year	Energy Consumption	Battery Note
[1]	2024	NR	Energy per authentication not reported
[2]	2025	NR	Energy per authentication not reported
[4]	2025	NR	Energy per authentication not reported
[3]	2025	0.40 mJ/packet	Battery life reported as 27.2 h (baseline)
Proposed	2026	59.6 mJ/session	Estimated wearable lifetime: 38 h

comes primarily from post quantum primitives, but we pay it once per session rather than per sample or per ECG feature packet.¹

C. Communication Cost Comparison

Table IV reports the session or packet overhead of the same four baselines. Classical schemes can be extremely compact, but they do not offer post quantum confidentiality against harvest now decrypt later collection. Othman et al. achieve post quantum security at the cost of larger per packet overhead due to encrypted payload expansion and proof material [3]. Our protocol keeps the authentication transcript bounded by a single session handshake.

In practice, the proposed transcript fits comfortably within BLE throughput limits and remains small relative to periodic clinical summaries uploaded over Wi-Fi or cellular links.

D. Energy Consumption and Battery Life

Table V summarizes the energy figures of our scheme because most IoMT authentication papers do not report energy directly, which limits strict cross paper comparison. We therefore report (i) our measured authentication energy per session and (ii) an end to end battery projection under a fixed re-authentication interval, consistent with wearable usage.

Although post quantum primitives increase computation energy, the proposed design keeps authentication infrequent and short. This preserves day scale operation for continuous monitoring while materially improving long term confidentiality.

E. AI Assisted Anomaly Screening Using CICIoMT2024

This subsection explains why gateway side anomaly screening is placed next to the cryptographic layer.

We added anomaly screening because cryptography alone cannot explain how a valid session should behave. In home

¹The ML-DSA-65 implementation requires approximately 120 KB of flash and 35 KB of RAM, leaving ample space on the standard ESP32-S3 (which typically features 8MB flash and 512KB SRAM) for physiological sensing tasks

monitoring attackers rarely reveal themselves through obviously malformed packets. More often they reuse stolen credentials script repeated session attempts or probe the backend through unusual access patterns. If every request becomes fully trusted once it passes a cryptographic check the system may still expose sensitive summaries or keep a long session alive under suspicious conditions. The gateway therefore serves as a small risk filter before the backend releases higher fidelity data or grants a longer session lifetime.

To build this filter we trained and validated an Isolation Forest model on the CICIoMT2024 dataset [12]. The dataset includes benign IoMT traffic and several attack families over Wi Fi MQTT and Bluetooth. We did not try to classify every attack type. Instead we treated the task as anomaly detection. The model learns what normal behavior looks like and flags sessions that deviate from it. That choice matches deployment reality because new attack variants appear often and labeled examples are usually limited.

The gateway forms a compact feature vector from session level metadata without inspecting clinical content. Features include inter arrival timing session duration retry rate message size statistics and a small set of behavior counts such as repeated authentication attempts and rapid reconnects. The vector is computed at session start and updated as the session evolves. The Isolation Forest returns an anomaly score which the gateway maps to a simple risk level of low medium or high. This coarse mapping is deliberate because operators need actions they can interpret quickly.

In evaluation the gateway side screen reached 94.5% precision with a 2.3% false positive rate while adding only 7.5 ms inference latency and about 2.4 mJ energy per authentication session. That latency appears low enough for a home hub to mediate concurrent sessions without becoming an obvious bottleneck. The practical benefit is a graded response rather than a blunt allow or deny outcome. Low risk sessions proceed normally. Medium risk sessions can trigger step up confirmation at the gateway or a shorter session lifetime. High risk sessions can be denied early and pushed to re enrollment or administrative review. This screen first and escalate second strategy reduces unnecessary cryptographic retries limits exposure during suspicious access patterns and strengthens resistance to credential misuse without turning the gateway into a heavy IDS appliance.

VI. CONCLUSION

Remote cardiac monitoring will not scale unless patients and clinicians can trust the identity of each device the freshness of each session key and the conditions under which data is released. We addressed that problem with three linked defenses. A reconfigurable OPUF binds each sensor to its silicon fingerprint and refreshes the authentication state in every session which makes modeling attacks harder. A hybrid post quantum handshake built from ML-KEM-768 and ML-DSA-65 helps protect recorded telemetry against future quantum adversaries. At the gateway an Isolation Forest ensemble supports graded responses such as step up checks or shorter session lifetimes instead of a simple accept or reject outcome.

Tests on commodity hardware showed 14.7 ms authentication latency about 4.6 kB session overhead and 59.6 mJ energy use which gave an estimated wearable lifetime of 38 hours. The anomaly screen reached 94.5% precision with a 2.3% false positive rate while adding only 7.5 ms inference cost. These results appear practical for home monitoring. Even so more work is still needed to reduce post quantum overhead on very low power devices tune risk thresholds for clinical workflows and extend the design to settings with multiple sensors.

REFERENCES

- [1] V. K. Bathalapalli, S. P. Mohanty, E. Kougianos, V. Iyer, and B. Rout, "Pufchain 3.0: Hardware-assisted distributed ledger for robust authentication in healthcare cyber-physical systems," *Sensors*, vol. 24, no. 3, p. 938, 2024.
- [2] S. Kalam and A. K. Keshri, "Advancing iomt security: A two-factor authentication model employing puf and fuzzy logic techniques," *Computers & Security*, vol. 148, p. 104138, 2025.
- [3] S. B. Othman and G. Kumar, "Quantum-resilient and adaptive multi-region data aggregation for iomt using zero-knowledge proofs and edge intelligence," *Scientific Reports*, vol. 15, no. 1, p. 37176, 2025.
- [4] K. Samal, S. K. Sunanda, D. Jena, and S. Patnaik, "A lightweight privacy preservation authentication protocol for iomt using ecc based blind signature," *International Journal of Engineering Business Management*, vol. 17, p. 18479790251318538, 2025.
- [5] Y.-S. Yang, S.-H. Lee, J.-M. Wang, C.-S. Yang, Y.-M. Huang, and T.-W. Hou, "Lightweight authentication mechanism for industrial iot environment combining elliptic curve cryptography and trusted token," *Sensors*, vol. 23, no. 10, p. 4970, 2023.
- [6] J. A. Alzubi, O. A. Alzubi, I. Qiqieh, and A. Singh, "A blended deep learning intrusion detection framework for consumable edge-centric iomt industry," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 2049–2057, 2024.
- [7] A. Khan, M. Rizwan, O. Bagdasar, A. Alabdulatif, S. Alamro, and A. Alnajim, "Deep learning-driven anomaly detection for iomt-based smart healthcare systems," *CMES-Computer Modeling in Engineering & Sciences*, vol. 141, no. 3, 2024.
- [8] K. Mansoor, M. Afzal, W. Iqbal, and Y. Abbas, "Securing the future: exploring post-quantum cryptography for authentication and user privacy in iot devices," *Cluster Computing*, vol. 28, no. 2, p. 93, 2025.
- [9] S. Hu, S. Jiang, Q. Miao, F. Yang, W. Zhou, and P. Duan, "Provably secure ecc-based anonymous authentication and key agreement for iot," *Applied Sciences*, vol. 14, no. 8, p. 3187, 2024.
- [10] P. Kumari and B. Mondal, "Lightweight encryption with data and device integrity using nlfsr and puf for the internet of medical things," *Internet of Things*, vol. 25, p. 101041, 2024.
- [11] Z. G. Al-Mekhlaf, M. A. Saare, J. M. H. Altmemi, M. A. Al-Shareeda, B. A. Mohammed, G. Alshammari, R. Alrashdi, Y. A. Alkhabra, and I. Alreshidi, "A quantum-resilient lattice-based security framework for internet of medical things in healthcare systems," *Journal of King Saud University Computer and Information Sciences*, vol. 37, no. 6, p. 126, 2025.
- [12] S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi, and A. A. Ghorbani, "Ciciomt2024: A benchmark dataset for multi-protocol security assessment in iomt," *Internet of Things*, vol. 28, p. 101351, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2542660524002920>