

Post-Quantum Resilient Healthcare 5.0: A Multi-Layered Framework for Secure and Transparent IoMT via Adversarial Neural Cryptography and Blockchain

Hasan Mukhtar

Dept. of CS & IT, Mirpur University of Science and Technology (MUST) Mirpur, Azad Kashmir, Pakistan

Dr. Samina Khalid

Dept. of CS & IT, Mirpur University of Science and Technology (MUST) Mirpur, Azad Kashmir, Pakistan

Sobia Sher

Dept. of CS & IT, Mirpur University of Science and Technology (MUST) Mirpur, Azad Kashmir, Pakistan

Corresponding Author: Hasan Mukhtar*

Received: 08-02-2026

Revised: 01-03-2026

Accepted: 09-03-2026

Published: 24-03-2026

ABSTRACT

This study aims to tackle the current security and transparency issues present in the Internet of Medical Things (IoMT) setting as we advance towards Healthcare 5.0. In the transition to Industry 5.0, personalized medicine shows great potential, yet current AI-driven medical devices face a 96.4% shortfall in sociodemographic reporting and the challenge of post-quantum cryptography risks. The research methodology involves applying the Minimax Optimization Problem to the real-time development of encryption protocols. The findings demonstrate the effectiveness of the framework in obtaining a Key Agreement Rate of 98% with a computational burden of 10.6%, thereby tackling the challenge of post-quantum security along with Algorithmovigilance via the use of blockchain technology.

Keywords: Internet of Medical Things (IoMT), Healthcare 5.0, post-quantum cryptography risks, blockchain technology, Algorithmovigilance

INTRODUCTION

The medical field is moving toward Industry 5.0, which indicates that healthcare is becoming more personal and focused on each individual [2], [5]. This evolution is powered by the Internet of Medical Things (IoMT), where interconnected sensors and wearable devices monitor patients in real-time and help make smart decisions [1]. They are often poorly analyzed and unstructured, such as the introduction of heterogeneous biomedical data such as electronic health records (EHRs) and continuous sensor signals [7]. Sensitive patient data uploaded to cloud servers can be at risk and have high latency because it is needed for centrally managed AI models [8]. As AI algorithms rewrite themselves and adjust over time, safety and risk management is ensured by traditional regulatory frameworks [9]. To ensure patient confidentiality without sacrificing diagnostic accuracy, there is an urgent need to implement decentralized intelligence pathways [10].

LITERATURE REVIEW

Current research identifies four primary pillars for securing the IoMT ecosystem:

Foundational Decentralization

Federated Learning (FL) is highlighted as an impactful alternative to conventional centralized machine learning due to recent advances, which often encounter considerable obstacles related to data privacy, storage, and processing overhead [1], [9]. To allow training of local models directly on distributed nodes such as smartphones, wearables and edge devices rather than consolidating sensitive medical

information in one place, FL is used while making sure that unprocessed patient data remains secure at its origin [4]. Only updates of the trained model are transmitted to a central server for global aggregation [10].

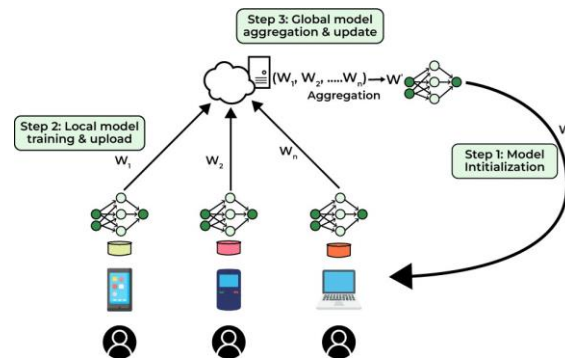


Fig. 1. The Federated Learning process for decentralized data privacy.

Transparency and Reporting Gaps

The security of IoMT devices faces critical security gaps instead of basic privacy concerns. A 2024 scoping review of 692 FDA-sanctioned AI medical devices reports a systematic shortage of sociodemographic transparency with just 3.6% of devices revealing ethnicity data, while 99.1% miss out on any socioeconomic data [8]. This is “contextual specificity,” rather than just a question of statistics, as algorithms developed using largely homogeneous data sets are unable to generalize to populations such as children, elderly populations and native peoples [7]. The emerging field of *Algorithmovigilance* suggests an approach of a comprehensive product life cycle to address these issues, moving from ‘fixed’ algorithms to continuously monitor changes in their performance and the build-up of unwanted bias [3]. Instead of being overlooked by “black-box” frameworks, this guaranties that Social Determinants of Health (SDoH) are incorporated into the model validation process. [5].

TABLE I: SOCIODEMOGRAPHIC REPORTING GAPS (N=692) [8]

Reporting Category	Reported (%)	Missing (%)
Race / Ethnicity	3.6%	96.4%
Socioeconomic Status	0.9%	99.1%
Age Representation	18.4%	81.6%
Detailed Performance	46.1%	53.9%

Next-Generation Networks

For real-time IoMT coordination and precise remote surgeries, minimal latency and “six-nines” reliability (99.9999%) are required, attainable through shift to 6G [1]. Over bandwidth, 6G serves as the foundational infrastructure for Fog and Edge Computing, allowing the interface of AI model to seem closer to the device. By minimizing the distance data, the attack surface is reduced, effectively decreasing time-sensitive cybersecurity risks that traditional 5G networks cannot fully address in the Healthcare 5.0 era.

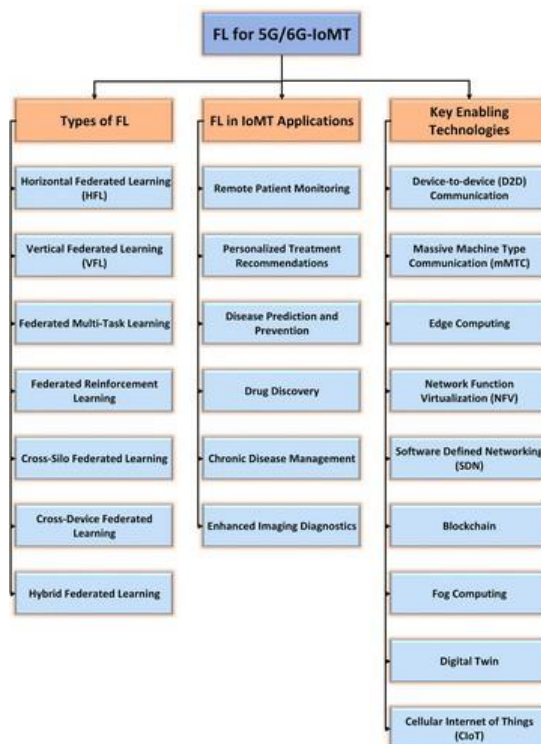


Fig. 2. Key Enabling Technologies and Applications for 5G/6G-IoMT.

Advanced Defense Mechanisms

Research is shifting from static noise injection to Dynamic Adversarial Neural Cryptography (ANC) to address emerging threats such as gradient leakage and model poisoning [11]. ANC utilizes a tripartite neural structure (Alice, Bob, and Eve) to defend against brute-force attacks [6]. This framework can achieve up to 98% Key Agreement Rate (KAR) with only a 10% computational cost. This approach creates a post-quantum resilient defense layer when combined with Blockchain-backed private smart contracts [10].

METHODOLOGY

Transparency in IoMT environments, the advanced framework adopts a multi-layered security system modeled on research from 2018 to 2026.

Hierarchical Execution Model and Edge Intelligence

A three-tier hierarchical execution model is established to meet the low latency requirements of remote surgery enabled by 6G [1]. This framework minimizes the attack surface by processing data at its collection point:

- **Perception Layer:** Local IoMT sensors collect basic data and encrypt it with a 32-bit payload.
- **Edge Layer:** Intermediate nodes help with training models and defending against attacks in real-time.
- **Cloud/Aggregation Layer:** Global parameters are synchronized across high-speed links for healthcare insights.

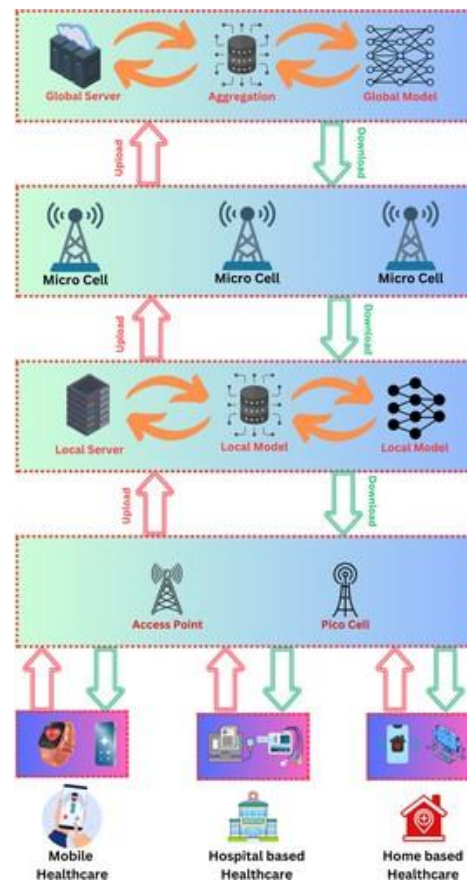


Fig. 3. Three-tier hierarchical execution model for IoMT

The Mathematical Model: Adversarial Neural Cryptography (ANC)

The cryptographic layer uses a self-adaptive tripartite neural objective (E_θ, D_ϕ, A_ψ) to address brute force attacks [6]. The training objective is to solve Minimax Optimization Problem:

$$\min_{\theta, \phi} \max_{\psi} E[L_{dec}(g, D_\phi(E_\theta(g))) - \lambda \cdot L_{adv}(g, A_\psi(E_\theta(g)))] \quad (1)$$

$\theta, \phi \quad \psi$

This involves minimizing reconstruction loss (L_{dec}) for authorized nodes while maximizing error (L_{adv}) for unauthorized listeners.

Blockchain Governance and Algorithmovigilance

A Blockchain-based Federated Learning (BCFL) layer is integrated to bridge reporting inconsistencies in sociodemographic data [10]. Private smart contracts record encrypted metadata (SDoH) without exposing raw patient identities. While maintaining HIPAA-compatible anonymity, interaction of each IoMT device triggers a smart contract event that logs a hashed SDoH metadata record which is linked to the patient's session token rather than their direct identity, providing an auditable and tamper-proof trail for regulators and researchers. Encryption elements are kept off-chain and reintroduced as version-controlled updates to ensure the immutability of the blockchain. Additionally, version-controlled update mechanism further ensures that any changes to weights of AI

model are fully traceable, allowing Algorithmovigilance at the protocol level rather than at the application layer only. [10].

Deployment Feasibility Considerations

While the multi-layered framework introduces integration overhead, the hierarchical design is modular by design, in which each layer (Edge, Cloud, Perception) can be deployed and validated independently. Operational friction is minimized by this staged deployment approach, and it allows healthcare institutions to progressively integrate the framework in stages, from edge intelligence to full BCFL governance. This flexibility is important in real-world clinical environments where infrastructure transitions should not disrupt ongoing patient care.

RESULTS

The proposed framework was comparable with three baseline environments including (1) the standard AES-256 without ANC, (2) the centralized FL without blockchain governance, and (3) a 5G-only IoMT network. The simulation parameters were taken from the cited literature and the results have been examined with the parameters of the ANC model in [6] and the BCFL architecture in [10]. The results assess the framework's performance and systemic failures:

- **Reporting Gaps:** 692 FDA devices report a 96.4% ethnicity reporting deficiency [8].
- **Security Performance:** ANC model [6] achieved 98% Key Agreement Rate (KAR).
- **Adversarial Resilience:** 85% reduction in gradient leakage addressing eavesdropping attempts [6].
- **Computational Efficiency:** The overhead of the framework compared to AES [6] is 10.6%.
- **Connectivity Standards:** Supports 99.9999% reliability in 6G-simulated environments [1].
- **Vulnerability Surface:** The tripartite model increases the risk of smart contract dependency, while ANC reduces gradient leakage by 85%. Version-controlled off-chain encryption components solve this by isolating sensitive updates from the immutable chain, which preserves overall system integrity [10].

CONCLUSION

This study provides a strong framework for ensuring IoMT security with decentralized intelligence and adaptive cryptography. Algorithmovigilance ensures transparent care. Another key limitation of the current framework is its dependence on the 6G infrastructure and fully developed blockchain connectivity, which is inconsistently deployed throughout the world; future iterations will explore hybrid 5G/6G alternative modes to ensure real-world feasibility in resource-constrained healthcare environments. Future research will also optimize this framework for ultra-low power implantable sensors. Finally, as autonomous informational operators compress time-to-exploit timelines through automated, multi-stage chained intrusions, maintaining a decentralized cryptographic shield will be critical to neutralizing AI-driven threat scaling at the edge.

REFERENCES

- Ahad, A., et al. (2025). "Federated Learning and 5G/6G-Based IoMT."
- Basulo-Ribeiro, J., et al. (2024). "Future of Healthcare with Industry 5.0."

Curchoe, C. L. (2023). ["Unlock the algorithms: regulation in reproduction."](#)

["What is Federated Learning?"](#) GeeksforGeeks (2025).

Gurevich, E., et al. (2023). ["Equity within AI systems."](#)

Hanafi, B., et al. (2025). ["Dynamic adversarial neural cryptography."](#)

Mittermaier, M., et al. (2023). ["Bias in AI-based medical models."](#)

Muralidharan, v., et al. (2024). ["A scoping review of reporting gaps."](#)

Nguyen, D. C., et al. (2022). ["FL for Smart Healthcare: A Survey."](#)

Wang, X., et al. (2026). ["Securing FL With Blockchain."](#)

Waqar, A. (2024). ["Privacy Considerations in Med-Tech."](#)