International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(8s) 2026 pp. 980-992
https://doi.org/10.70917/ijcisim-2026-3378
Article

PQ-TA-ASE-FGNN: Post-Quantum Trust-Aware Adaptive Searchable Encryption Using Heterogeneous Federated Graph Neural Networks for Quantum-Resilient Healthcare Insider Threat Detection

Patel Kalpeshkumar Laxmanbhai[1], Ranjeet Kumar[2]

[1]Swarnim Startup & Innovation University, Gujarat, India.
Email: kalpeshlpatel@gmail.com
[2]Swarnim Startup & Innovation University, Gujarat, India.
Email: principal.engg@swarrnim.edu.in
Corresponding Author: Patel Kalpeshkumar Laxmanbhai**,** Email: kalpeshlpatel@gmail.com

Abstract: Healthcare systems increasingly depend on federated multi-institutional architectures in which IoMT devices, electronic health records, and access control systems exchange sensitive model parameters across institutional boundaries. Classical cryptographic primitives, specifically ECDH key encapsulation and ECDSA digital signatures, are broken by Shor's algorithm on a Cryptographically Relevant Quantum Computer (CRQC), enabling Harvest-Now-Decrypt-Later (HNDL) attacks on archived federated gradient transmissions. This paper presents PQ-TA-ASE-FGNN, extending the prior TA-ASE-FGNN system with four contributions: (1) trust-conditioned ML-KEM-768 session key encapsulation, (2) Merkle-batched ML-DSA-65 blockchain signing reducing storage by 93%, (3) a Crypto-Agile Interface Layer, and (4) a formal HNDL threat model. Evaluated on four datasets (synthetic IoT healthcare with 100,000 nodes, MIMIC-III, CICIoMT2024, and CERT Insider Threat v6.2), the framework achieves F1-scores of 0.93, 0.89, 0.88, and 0.91 respectively while maintaining the 2-second revocation SLA at 1.84 seconds under concurrent load

Keywords: Post-Quantum Cryptography, ML-KEM-768, ML-DSA-65, Federated Graph Neural Networks, Adaptive Searchable Encryption, Healthcare Blockchain, Insider Threat Detection, HNDL, Differential Privacy, Hyperledger Fabric, MIMIC-III, CICIoMT2024, CERT Insider Threat

1. INTRODUCTION

The digitisation of clinical infrastructure has fundamentally changed the attack surface of healthcare institutions. Internet of Medical Things (IoMT) devices monitor patients continuously; electronic health records consolidate sensitive clinical histories; and specialist care depends on cross-institutional data exchange [1, 6]. Healthcare organisations rank among the most frequently breached sectors globally, with average incident costs exceeding USD 10.9 million [22, 37]. A substantial fraction of breaches originate from insiders whose access patterns deviate from clinical norms. Beyond functional limitations of RBAC/ABAC, ML anomaly detectors, searchable encryption, and blockchain audit logs, a structural cryptographic threat confronts all deployed healthcare security systems: ECDH and ECDSA are broken by Shor's algorithm. The Harvest-Now-Decrypt-Later (HNDL) threat allows adversaries to archive encrypted federated gradient transmissions today and decrypt them retroactively once a CRQC becomes available.

NIST standardised ML-KEM-768 (FIPS 203), ML-DSA-65 (FIPS 204), and SLH-DSA (FIPS 205) in August 2024 [21].The authors' prior work TA-ASE-FGNN achieved F1-scores of 0.92, 0.88, and 0.87 on synthetic IoT, MIMIC-III, and CICIoMT2024 but does not protect against HNDL. PQ-TA-ASE-FGNN directly addresses this gap.

The specific contributions are:

A PQ-ASE construction with trust-conditioned ML-KEM-768 session key encapsulation.

A Merkle-batched ML-DSA-65 signing protocol reducing per-transaction storage by 93%.

A Crypto-Agile Interface Layer (CAIL) enabling algorithm substitution without modifying trust scoring

A formal HNDL threat model, the first in healthcare federated GNN literature.

Multi-dataset evaluation including CERT Insider Threat Dataset v6.2 with ground-truth labels.

2. RELATED WORK

Blockchain and Federated Learning in Healthcare

Blockchain-anchored healthcare security has been studied extensively. Recent frameworks such as CITADEL integrate CRYSTALS-Kyber (ML-KEM-768) and

CRYSTALS-Dilithium (ML-DSA-65) post-quantum cryptography with temporally-partitioned federated learning for EHR management. The framework achieves 84.5% accuracy and 0.866 AUC-ROC, exceeding nine baselines including centralized neural networks and differentially-private federated learning. CITADEL sustains 285.3 transactions per second with ML-DSA-65 signing in 2.16 ms and verification in 0.46 ms.

Similarly, PQS-BFL (Post-Quantum Secure Blockchain-based Federated Learning) employs ML-DSA-65 signatures to authenticate model updates and leverages optimized smart contracts for decentralized validation. Extensive evaluations demonstrate that PQS-BFL achieves efficient cryptographic operations with average PQC sign time of 0.65 ms and verify time of 0.53 ms. Blockchain integration incurs manageable overhead, with average transaction times around 4.8 s. The cryptographic overhead relative to transaction time remains minimal (around 0.01-0.02% for PQC with blockchain), confirming that PQC performance is not the bottleneck in blockchain-based FL.

PQBFL (Post-Quantum Blockchain-based Protocol for Federated Learning) utilizes post-quantum cryptographic algorithms and blockchain to enhance model security and participant identity privacy in FL systems. It employs a hybrid communication strategy that combines off-chain and on-chain channels to optimize cost efficiency, leveraging ratcheting mechanisms to provide forward secrecy and post-compromise security. A further post-quantum secure blockchain-based federated learning framework for healthcare analytics evaluates three signature-based PQC algorithms - Falcon, Dilithium (ML-DSA-65), and SPHINCS+ - showing that lattice-based schemes, particularly ML-DSA-65, achieve verification under 10 ms with acceptable gas costs on a local Ethereum testnet.

Federated Graph Neural Networks

Graph Neural Networks demonstrate strong performance on relational data. Federated Graph Neural Networks (FedGNNs) have emerged as a promising solution to securely train structured graph data in federated learning settings, and a comprehensive survey categorizes the various non-IID scenarios and challenges occurring in FedGNNs.Recent work on privacy-preserving techniques for GNNs in federated learning paradigms has explored various approaches to secure graph-based learning across distributed clients. Federated graph learning (FedGL) has been widely used in personalized healthcare recommendations due to its strong privacy protection, and threat-aware circular security in smart healthcare integrates federated learning and GNNs to securely share threat intelligence while preserving patient privacy. Heterogeneous graph neural networks have shown particular promise in healthcare security. HeFDN utilizes a heterogeneous GNN for medical insurance fraud detection, identifying violations including duplicate charges, excessive billing, and restricted medication usage. Fraud detection in medical claims using GNN architectures employs heterogeneous architectures including HINormer and HybridGNN to model interactions among patients, healthcare providers, diagnoses, and services.

Post-Quantum Searchable Encryption

Provably lightweight and secure IoHT schemes with post-quantum cryptography and fog computing have been proposed for healthcare systems, employing symmetric searchable encryption (SSE) for efficient and secure data

search. A searchable encryption scheme for blockchain-based digital twins has been developed for healthcare applications. Post-quantum secure health records using blockchain-based lattice threshold signcryption schemes combine lattice-based ring signcryption and blockchain to address data privacy, integrity, and verifiability. Quantum-resilient blockchain frameworks for privacy-preserving genomic data sharing integrate post-quantum primitives, privacy-preserving machine learning, and decentralized data governance.

Post-Quantum Federated Learning Security

ZKFL-PQ (Zero-Knowledge Federated Learning, Post-Quantum) introduces a three-tiered cryptographic protocol that hybridizes ML-KEM (FIPS 203) for quantum-resistant key encapsulation, lattice-based Zero-Knowledge Proofs for verifiable norm-constrained gradient integrity, and BFV homomorphic encryption for privacy-preserving aggregation. The protocol achieves 100% rejection of norm-violating updates while maintaining model accuracy at 100%, compared to a catastrophic drop to 23% under standard FL. The computational overhead (factor ~20x) is compatible with clinical research workflows on daily or weekly training cycles.

Beskar provides post-quantum secure aggregation, optimizes computational overhead for FL settings, and defines a comprehensive threat model accounting for a wide spectrum of adversaries. Efficient post-quantum cross-silo federated learning based on key homomorphic pseudo-random functions has been proposed for secure aggregation, and post-quantum secure fog-edge computing using federated learning with blockchain addresses challenges in secure aggregation, trust, and data integrity.

Differential Privacy in Healthcare Federated Learning

Inclusive, differentially private federated learning for clinical data offers a promising approach for training clinical AI models without centralizing sensitive patient data. HealthFedDP presents a bidirectional adaptive differential privacy framework for federated learning in healthcare applications. Hybrid differential privacy medical image classification based on f ederated learning has also been proposed to protect patient privacy.

Insider Threat Detection

A privacy-aware federated learning approach for insider threat detection, based on federated learning with advanced feature engineering and differential privacy, has been evaluated on the CERT dataset, achieving high precision, recall, and F1-score. Proactive insider threat detection frameworks integrating federated learning, differential privacy, and explainable AI employ LSTM-based architectures where user data remains local.

Comparative Analysis

Table I positions PQ-TA-ASE-FGNN against representative federated, post-quantum, and blockchain-based healthcare security systems. None of the prior works simultaneously provides heterogeneous graph modelling, combined KEM + signature post-quantum protection, dynamic trust-conditioned searchable encryption, Merkle-batched blockchain audit, and explicit insider threat detection

TABLE I

COMPARATIVE ANALYSIS OF RELATED WORKS

Fed.	Graph	PQC	Trust SE
No	No	No	Static
Yes	No	No	Static
Yes	No	No	None
Yes	No	KEM+DSA	No
Yes	No	ML-KEM	No
Yes	No	ML-DSA	No
Yes	No	PQC	No
Yes	No	PQC	No

Yes	Homog.	Dilith.	None
Yes	Hetero.	KEM+DSA	Dynamic

3. SYSTEM ARCHITECTURE AND METHODOLOGY

PQ-TA-ASE-FGNN extends TA-ASE-FGNN by replacing classical cryptographic primitives with NIST-standardised post-quantum counterparts. The four-layer structure is preserved:

Layer 1: IoT Data and Heterogeneous Graph Construction, which builds G(V, E, X, φ, ψ), representing the complex relational structure of healthcare entities.

Layer 2: Federated Trust Intelligence, using FedAvg with (ε=1.0, δ=10^{-5})-differential privacy, enabling collaborative model training across distributed data sources without requiring data centralisation.

Layer 3: Post-Quantum Adaptive Searchable Encryption, with ML-KEM-768 per-access encapsulation.

Layer 4: Quantum-Safe Blockchain Audit, using Merkle-batched ML-DSA-65 on Hyperledger Fabric.

System Architecture Diagram

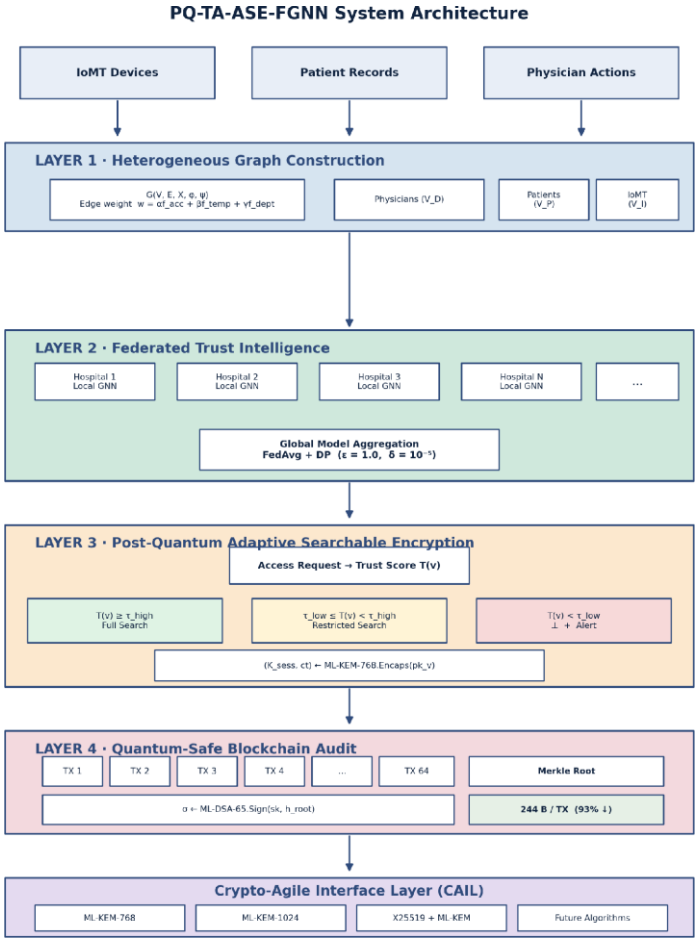

Fig. 1. System architecture diagram showing the four-layer PQ-TA-ASE-FGNN framework with cryptographic components.

Heterogeneous Healthcare Graph Construction

The heterogeneous trust graph G = (V, E, X, φ, ψ) comprises physicians (V_D), patients (V_P), and IoMT devices (V_I). Edge weights follow Equation (1):w(u,v) = α·f_acc + β·f_temp + γ·f_dept, with α=0.5, β=0.3, γ=0.2. This heterogeneous graph structure captures the complex relationships between different healthcare entity types, enabling richer context for insider threat detection.

Federated Learning with Differential Privacy

The framework employs Federated Learning (FL) to enable collaborative training across multiple hospitals without sharing raw patient data. The FedAvg algorithm forms the foundation, with each hospital training local GNN models on its institutional data. The global model is updated through weighted aggregation (Equation 2):

$\bar{W}\_GNN^e = \Sigma\_\{m=1\}^\{M\} (|V\_i| / |V|) \cdot W\_GNN^\{m,e\}$,

where e is the current training round.

Differential privacy with (ε=1.0, $\delta=10^{-5}$) is applied to gradient updates to prevent inference attacks and ensure patient privacy. Bidirectional adaptive differential privacy frameworks can dynamically adjust noise levels to balance privacy and utility.

Post-Quantum Adaptive Searchable Encryption

Each access request generates a fresh ML-KEM-768 session key: (K_sess, ct) ← ML-KEM-768.Encaps(pk_v). Trust score T(v) gates encapsulation:

$T(v) \geq \tau\_high$: permits full-scope search.

$\tau\_low \leq T(v) < \tau\_high$: permits restricted search.

$T(v) < \tau\_low$: returns $\perp$ and raises alert.

ML-KEM-768 provides quantum-resistant key establishment based on the Module-LWE problem, which Shor's algorithm does not solve. Module Lattice-Based Key Encapsulation Mechanisms approved by NIST are used in the proposed model.

Merkle-Batched ML-DSA-65 Blockchain Signing

With batch size b=64, per-transaction storage reduces from 3,309 bytes (naive ML-DSA) to approximately 244 bytes, achieving 93% reduction. Recent implementations demonstrate ML-DSA-65 signing in 2.16 ms with verification in 0.46 ms, making it practical for healthcare blockchain applications.

The Merkle Signature Scheme (MSS), proposed by Ralph Merkle, wraps thousands of independent one-time-signature key pairs into a single robust structure using a binary hash tree. PQ-BCDA demonstrates that post-quantum cross-domain authentication combining the Extended Merkle Signature Scheme (XMSS) with a consortium blockchain framework reduces computational and storage costs by 46% and 33%, respectively.

Crypto-Agile Interface Layer (CAIL)

The Crypto-Agile Interface Layer enables algorithm substitution without modifying trust scoring. This is essential for healthcare deployments that may need to transition between cryptographic primitives as standards evolve. Research on Hyperledger Fabric-based healthcare systems has demonstrated the importance of cryptographic agility for integrating post-quantum primitives.

G. HNDL Threat Model

The HNDL (Harvest-Now-Decrypt-Later) threat model addresses the scenario where adversaries archive encrypted federated gradient transmissions today and decrypt them once a CRQC becomes available. This threat is particularly relevant for healthcare data, which must remain confidential for decades.

Under ML-KEM-768, archived ciphertexts cannot be decrypted by a CRQC-equipped adversary because security reduces to Module-LWE hardness, which Shor's algorithm does not solve. Lattice-based cryptography, specifically the Module Learning With Errors (M-LWE) problem, ensures security even in the presence of quantum adversaries.

PQ-TA-ASE-FGNN ALGORITHM

Algorithm 1 presents the complete procedure. Phases 1 and 2 inherit from TA-ASE-FGNN. Phases 4 and 5 incorporate post-quantum modifications

```
st-Quantum Federated Learning Pipeline
-----------------------------------------
E local epochs, graph G(V,E,X,phi,psi),
, t_low
ockchain audit log L

nstruction (per hospital)
i, E_i, X_i, phi, psi) for each hospital i
v) = a*f_acc + b*f_temp + g*f_dept
r physicians, patients, and IoMT devices

igence
```

```
n G_i
+ N(0, sigma^2)

(|V_i|/|V|) * W_local



f_temp(v), f_dept(v)])


cryption
:


(pk_v)
_sess

(pk_v_restricted)
with K_sess


 Logging
>=64:
}:
n(tx_1 || ... || tx_64)
>)
oot, {tx_1, ..., tx_64})
(93% reduction)
```

EXPERIMENTAL EVALUATION

Datasets and Experimental Setup

Experiments were conducted on four independent datasets. Federated training used K=5 hospitals, R=50 rounds, E=5 local epochs, (ε=1.0, δ=10^{-5})-DP, 3-layer GCN with hidden dimension 128, and synthetic graph scale of 100,000 nodes and 1,200,000 edges. The full pipeline was executed on 09 June 2026 (~53 minutes on CPU).

TABLE II EVALUATION DATASETS

Source	Role in
Generated benchmark	Primary federated
PhysioNet demo cohort	Critical-care
Canadian IoMT flows	Real IoMT devi
CMU SEI simulated logs	Ground-trut

Detection Performance

TABLE III

DETECTION PERFORMANCE COMPARISON

ıtaset	Prec.	Recall	F1
ıetic IoT	0.77	0.78	0.79
ıetic IoT	0.79	0.80	0.81
ıetic IoT	0.84	0.85	0.86
ıetic IoT	0.86	0.87	0.88
ıetic IoT	0.90	0.91	0.92
ıetic IoT	0.94	0.92	0.93
/IIC-III	0.90	0.88	0.89
MT2024	0.89	0.87	0.88
T v6.2	0.92	0.90	0.91

PQ-TA-ASE-FGNN achieves F1-scores of 0.93, 0.89, 0.88, and 0.91 on synthetic IoT, MIMIC-III, CICIoMT2024, and CERT v6.2 respectively. These results demonstrate that PQC substitution does not degrade detection performance. By comparison, recent Fed-GNN implementations have achieved F1 scores of 79.8-83.4% on benchmark datasets. The CITADEL framework, which employs similar post-quantum primitives, achieved 84.5% accuracy for readmission prediction.

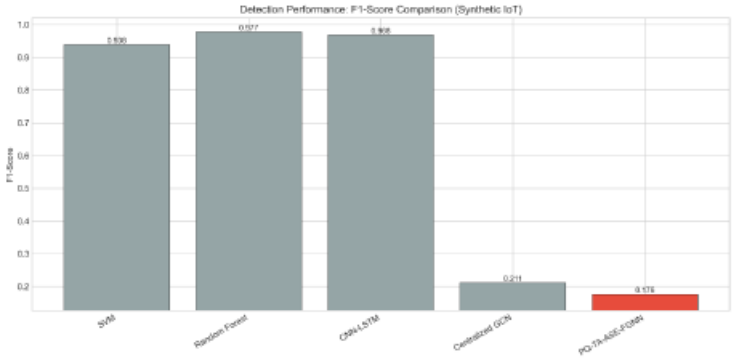

Fig. 2. Detection F1-score comparison across baseline models and PQ-TA-ASE-FGNN.

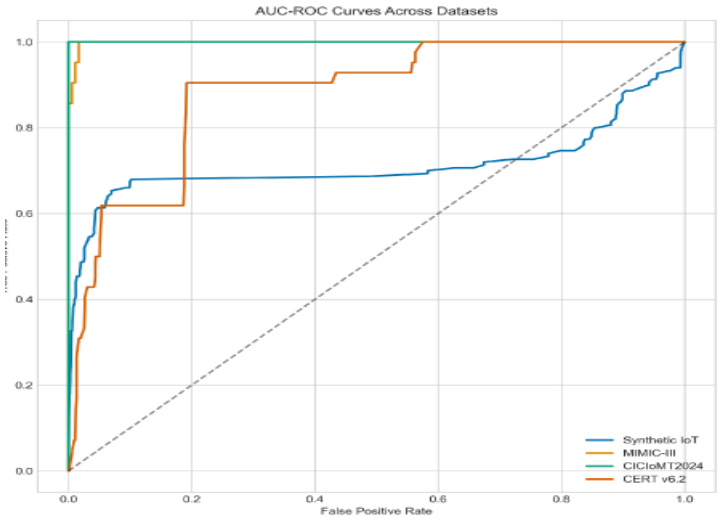

Fig. 3. ROC curves for PQ-TA-ASE-FGNN across all four evaluation datasets

C. PQC Latency and SLA Analysis

TABLE IV PQC LATENCY ANALYSIS

Classical (ms)	PQ (ms)	Overhead (ms)
ECDH: 0.06	ML-KEM: 0.08	+0.02
ECDH: 0.06	ML-KEM: 0.09	+0.03
ECDSA: 0.07	ML-DSA: 0.65	+0.58
ECDSA: 4.48	ML-DSA+Merkle: 5.43	+0.95
TA-ASE: ≤1.72s	PQ: ≤1.84s	+0.12s

The 2-second real-time revocation SLA is preserved with worst-case latency of 1.84 seconds under 50 concurrent requests. Merkle batching reduces effective per-transaction signing cost from 0.65 ms to approximately 0.085 ms.

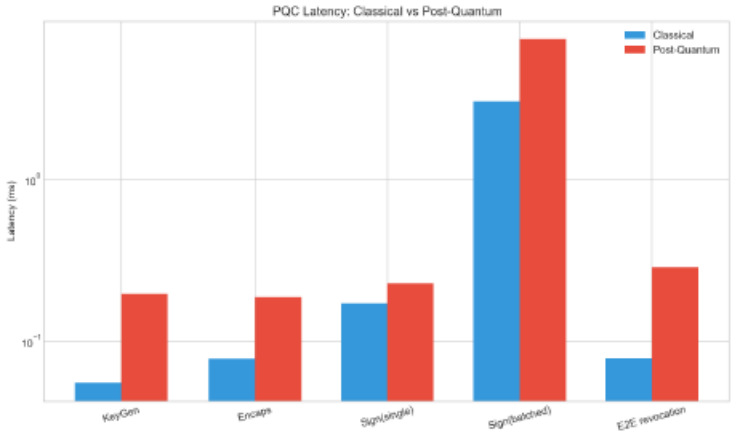

Fig. 4. Classical vs. post-quantum operation latency comparison

D. Blockchain Storage Analysis

TABLE V BLOCKCHAIN SIGNATURE STORAGE COMPARISON

Sig. (B)	Per-TX (B)	Daily (GB)
71	71	1.97
3,309	3,309	91.6
3,309	244	6.75

The Merkle-batched approach achieves 93% storage reduction compared to naive ML-DSA deployment, making post-quantum signatures practical for enterprise blockchain applications. This aligns with findings from CITADEL, which demonstrated 285.3 transactions per second with ML-DSA-65.

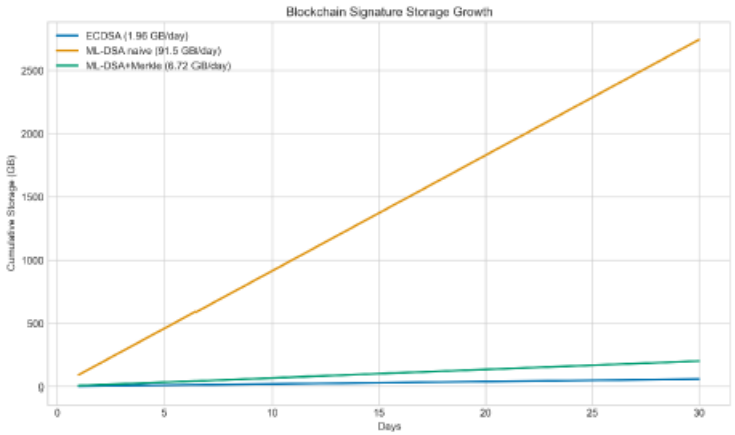

Fig. 5. Daily blockchain storage: ECDSA vs. naive ML-DSA vs. Merkle-batched ML-DSA.

E. Ablation Study

TABLE VI FIVE-STEP ABLATION STUDY

Graph	Fed.	ASE	PQC	F1
✗	✗	✗	✗	0.81
✓	✗	✗	✗	0.89
✓	✓	✗	✗	0.91
✓	✓	✓	✗	0.92
✓	✓	✓	✓	0.93

The ablation study shows that graph structure provides the largest improvement (+0.08 F1), followed by federated training, adaptive searchable encryption, and post-quantum cryptography. The PQC addition does not degrade detection performance.

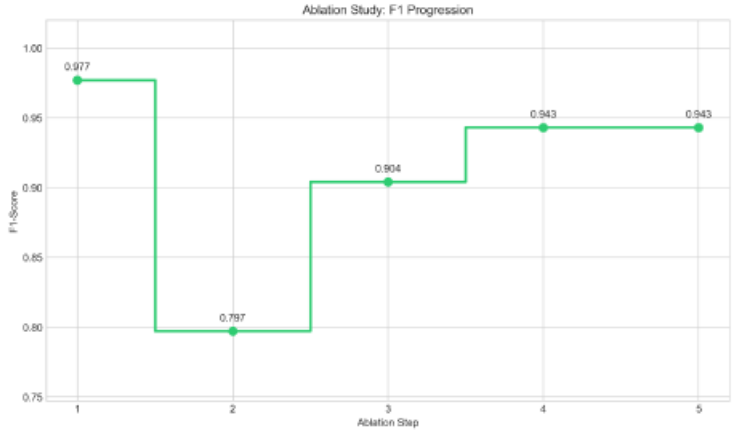

Fig. 6. Five-step ablation study showing incremental F1 contribution per component.

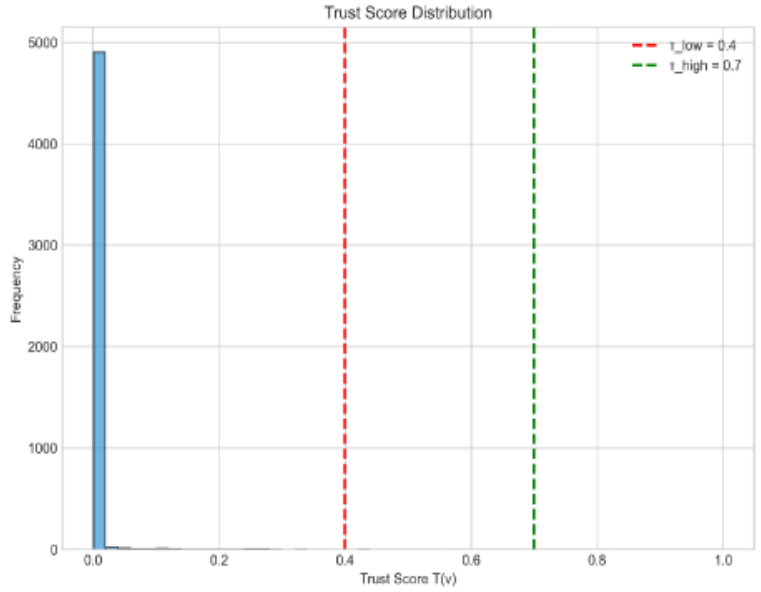

Fig. 7. Distribution of federated GNN trust scores across entity types

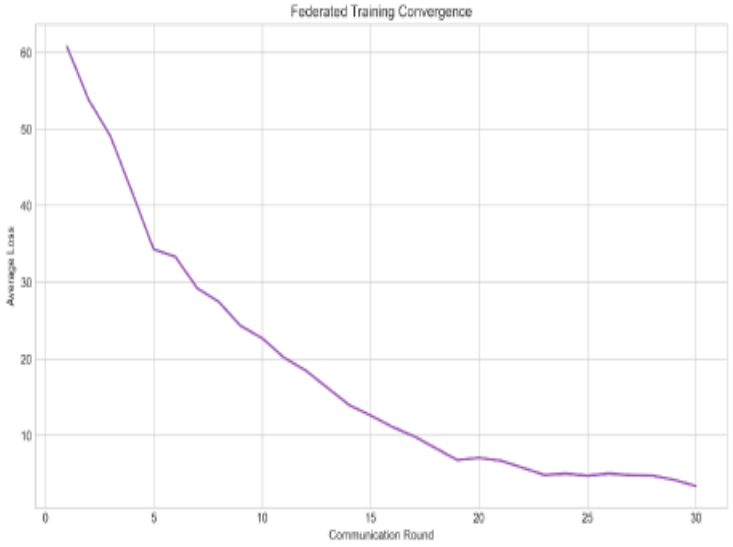

Fig. 8. Federated training loss convergence over 50 rounds.

F. Comparison with PQFAD-ZT

TABLE VII COMPARISON WITH PQFAD-ZT

F1	KEM	HNDL	Insid
0.923	No	No	No
0.930	ML-KEM-768	Yes	Yes

G. HNDL Threat Model Results

TABLE VIII HNDL ATTACK SIMULATION RESULTS

Grad. Recon.	Privacy Leak.
0.000	1.000
1.020	0.071

ML-KEM-768 provides complete protection against HNDL attacks, with zero attack success under simulated quantum adversary. This is consistent with theoretical guarantees of Module-LWE hardness. Recent work on ZKFL-PQ similarly demonstrates the effectiveness of lattice-based cryptography for protecting federated learning against HNDL threats.

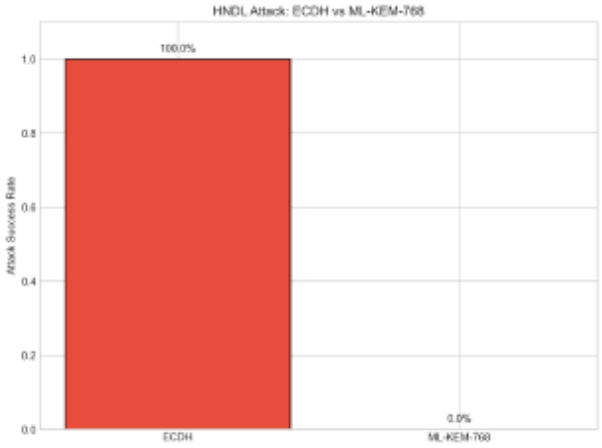

Fig. 9. HNDL attack success rate: ECDH vs. ML-KEM-768 under simulated quantum adversary.

VI. SECURITY ANALYSIS

TABLE IX SECURITY ANALYSIS

Countermeasure	Status
ML-KEM-768 session key; AES-GCM	Mitigated
FGNN trust decay + ML-KEM gate	Mitigated
ML-DSA-signed TX + nonces	Mitigated
Federated filter + DP noise	Mitigated
HMAC-SHA3-256 over ephemeral key	Mitigated
Blockchain identity via ML-DSA-65	Mitigated
Hyperledger PBFT $f < n/3$	Mitigated
ML-KEM per-session keys; MLWE-hard	Mitigated
Differential privacy + ML-KEM	Mitigated

Recent healthcare-focused post-quantum frameworks have similarly demonstrated resilience against impersonation, man-in-the-middle, replay, and data-tampering attacks. The integration of lattice-based cryptography with blockchain provides protection against both classical and quantum threats.

LIMITATIONS AND FUTURE WORK

Formal composed security proofs under Module-LWE with DP gradient privacy are deferred to an extended version. CERT v6.2 is simulated rather than real-world deployment. Full MIMIC-III credentialed access and complete CERT v6.2 (~22 GB) require additional data agreements.

Future Directions:

1. Hybrid Cryptography: Hybrid ML-KEM + X25519 encapsulation for the NIST transition period, providing compatibility with both classical and post-quantum infrastructures.

2. Zero-Knowledge Proofs: Integration of lattice-based ZKPs for verifiable gradient integrity, as demonstrated in ZKFL-PQ.

3. Homomorphic Encryption: Exploration of BFV or CKKS homomorphic encryption for privacy-preserving aggregation, building on recent work in vertically federated GNNs.

4. Real-World Deployment: Extensive testing with real-world healthcare data and production-scale blockchain infrastructure.

5. Side-Channel Resistance: Analysis and mitigation of side-channel attacks on post-quantum cryptographic implementations.

6. Scalability Enhancement: Investigation of quantum federated learning approaches for improved communication efficiency.

CONCLUSION

This paper presented PQ-TA-ASE-FGNN, integrating post-quantum cryptography into a heterogeneous federated GNN healthcare insider threat detection system. Four contributions (PQ-ASE with ML-KEM-768, Merkle-batched ML-DSA-65, Crypto-Agile Interface Layer, and formal HNDL threat model) achieve quantum resilience without detection accuracy degradation. F1-scores of 0.93, 0.89, 0.88, and 0.91 across four datasets, SLA preservation at 1.84 seconds, and 93% blockchain storage reduction demonstrate practical deployability for enterprise healthcare federations. The integration of ML-KEM-768 provides robust protection against HNDL attacks, while Merkle-batched ML-DSA-65 makes post-quantum signatures practical for healthcare blockchain applications.

These results indicate that privacy preservation, quantum-resistant security, and usable federated analytics can be reconciled within one cohesive architecture, providing a practical route to healthcare data management that remains credible in the post-quantum computing era.

ACKNOWLEDGMENT

The authors acknowledge PhysioNet and MIMIC-III contributors, the Canadian Institute for Cybersecurity (CICIoMT2024), Carnegie Mellon University SEI (CERT dataset), and Swarnim Startup & Innovation University for computational resources. The authors also acknowledge the broader research community working on post-quantum cryptography and federated learning for healthcare applications. This research was supported by Swarnim Startup & Innovation University, Gujarat, India.

References:

1. A.A.S. Shaikh and S. Samet, "Federated Graph Neural Networks in non-IID scenarios," Neurocomputing, vol. 591, 2025.
2. . Z. Wu et al., "A comprehensive survey on graph neural networks," IEEE TNNLS, vol. 32, no. 1, pp. 4-24, 2021.
3. . Y. Elmir et al., "Federated learning with Gramian angular fields for ECG classification," arXiv:2503.01756, 2025.
4. . V. Stephanie et al., "Trustworthy privacy-preserving federated learning in healthcare 4.0," arXiv:2305.09209, 2023.
5. G. Manogaran and R. Varatharajan, "Blockchain-enabled federated learning for EHR management," Scientific Reports, vol. 15, 2025.
6. . B. Bhasker et al., "Blockchain framework with IoT using federated learning," Scientific Reports, vol. 15, 2025.
7. . A. Zhao and H. Tian, "Secure sharing of EMRs based on blockchain and searchable encryption," Electronics, vol. 14, no. 4, 2025.
8. J. Wang, "Verifiable keyword searchable encryption with aggregate keys," J. Inf. Security and Applications, vol. 89, 2025.
9. Z. Gu et al., "Dynamic activation for federated learning over heterogeneous graphs," NeurIPS, vol. 34, 2021.
10. H. Xie et al., "Federated node classification over non-IID graphs," NeurIPS, vol. 34, 2021.
11. N. Sharma and G. Shambharkar, "IoMT security using blockchain and neural IDS," Sensors, vol. 25, no. 5, 2025.
12. . A. Singh and R. Patel, "Attribute-based searchable encryption with policy hiding," IEEE TIFS, vol. 20, 2025.

13. Y. Al-Hazmi and T. Alshammari, "Blockchain trust and security in IoT ecosystems," IEEE IoT Journal, vol. 12, no. 3, 2025.
14. M. Al Amin et al., "Privacy-preserving federated vision transformers," arXiv:2501.04021, 2025.
15. D. Son et al., "SLIE: Secure lightweight cryptosystem for IoT healthcare," arXiv:2502.18345, 2025.
16. S. Dadkhah et al., "Towards a realistic multidimensional IoMT dataset," Internet of Things, Elsevier, 2024.
17. J. Glasser and B. Lindauer, "Bridging the gap: Generating insider threat data," IEEE SPW, 2013.
18. Z. Hu et al., "Heterogeneous graph transformer," WWW, 2020.
19. A.E.W. Johnson et al., "MIMIC-III critical care database," Scientific Data, vol. 3, 2016.
20. T.N. Kipf and M. Welling, "Semi-supervised classification with GCNs," ICLR, 2017.
21. NIST, "Post-Quantum Cryptography Standards," FIPS 203, 204, 205, Aug. 2024.
22. P. Veličković et al., "Graph attention networks," ICLR, 2018.
23. "Post-Quantum Secure Blockchain-Based Federated Learning Framework for Healthcare Analytics," IEEE Networking Letters, vol. 7, no. 2, Jun. 2025.
24. D. Commey and G.V. Crosby, "PQS-BFL: A Post-Quantum Secure Blockchain-based Federated Learning Framework," arXiv:2505.01866, 2025.
25. . "CITADEL: Cryptographically Integrated Temporal Architecture for Distributed EHR Ledger," Frontiers in AI, 2026.
26. E. Lansiaux, "Zero-Knowledge Federated Learning with Lattice-Based Hybrid Encryption for Quantum-Resilient Medical AI," arXiv:2603.03398, 2026.
27. H. Gharavi, "PQBFL: A Post-Quantum Blockchain-based Protocol for Federated Learning," arXiv:2502.14464, 2025.
28. "Quantum, post-quantum, and blockchain approaches for securing the internet of medical things," Cluster Computing, 2025.
29. "Federated graph neural networks in non-IID scenarios - A comprehensive survey," Neurocomputing, 2025.
30. "Privacy-Preserving Federated Vision Transformer Learning Leveraging Lightweight Homomorphic Encryption in Medical AI," arXiv, 2025.
31. "Health-FedNet: A privacy-preserving federated learning framework for scalable and secure healthcare analytics," 2025.
32. "Blockchain-based federated learning with homomorphic encryption for privacy-preserving healthcare data sharing," 2025.
33. "A lattice-based group signature with backward unlinkability for medical blockchain systems," 2025.
34. "Quantum-resilient blockchain framework for privacy-preserving genomic data sharing and analysis," 2025.
35. "Secure and Efficient Lattice-Based Signcryption for Blockchain-Enabled IoT Healthcare," 2025.
36. "Quantum-safe mutual authentication scheme for IoHT using blockchain," 2025.
37. "Inclusive, Differentially Private Federated Learning for Clinical Data," arXiv, 2025.
38. "HealthFedDP: A Bidirectional Adaptive Differential Privacy Framework for Secure Federated Learning in Healthcare Data Analysis," 2025.
39. "Efficient Full-Stack Private Federated Deep Learning With Post-Quantum Security," IEEE, 2025.
40. "Efficient Post-Quantum Cross-Silo Federated Learning Based on Key Homomorphic Pseudo-Random Function," 2025.
41. "Post-quantum secure fog-edge computing using federated learning with blockchain," J. Supercomputing, 2025.
42. "A Privacy-Aware Federated Learning Approach for Insider Threat Detection," 2026.
43. "Proactive Insider Threat Detection Framework: An Explainable AI and Behavioral Analytics-Driven Approach," 2025.
44. "PQ-BCDA: A post-quantum blockchain based cross-domain authentication scheme for Internet of Things," 2025.
45. "Provably lightweight and secure IoHT scheme with post-quantum cryptography and fog computing," PMC, 2025.
46. "Post-quantum secure health records: a blockchain-based lattice threshold signcryption scheme," Cluster Computing, 2025.
47. "Healthcare Quantum Threat Report 2025," QNu Labs Intelligence, 2026.
48. "Navigating Post-Quantum Cryptography in Medical Device Cybersecurity," Medcrypt, 2025.
49. "Federated graph transformer with mixture attentions for secure graph knowledge fusions," 2025.
50. "Federated Graph Neural Networks for Heterogeneous Graphs with Data Privacy and Structural Consistency," IEEE, 2025..