Quantum Convolutional Neural Network for Secure Healthcare Data Management: An Extension of the IQ-HDM Framework

Subrahmanya Prasad P S
Dept. of Computer Science & Engg
NMAM Institute of Technology
Nitte (Deemed to be University)
subrahmanyaprasadps05@gmail.com

Dr. Pradeep Kanchan*
Dept. of Computer Science & Engg
NMAM Institute of Technology
Nitte (Deemed to be University)
pradeepkanchan@nitte.edu.in

Abstract*—Background: The IQ-HDM framework [1] combines Quantum One-Time Padding Encryption (QOTPE) with a Quantum Feed-Forward Neural Network (QFNN) for proactive malicious entity detection, achieving 89.02% accuracy across four benchmark healthcare datasets. Aim: This paper proposes replacing the QFNN prediction unit with a Quantum Convolutional Neural Network (QCNN) to improve feature extraction and classification accuracy while preserving the quantum security guarantees of the original framework. Methods: The QCNN applies hierarchical quantum convolutional and pooling layers (Conv→Pool→Conv→Pool) over 8 qubits with 36 trainable quantum parameters, implemented in PennyLane and trained end-to-end using the Adam optimiser over 100 epochs. Evaluation is conducted under two configurations: a two-dataset study (COVID-19 and Diabetes) and a four-dataset study (all four benchmarks including TCGA Brain Glioma Mutations and TCGA Grade). Comprehensive confusion matrix analysis quantifies TP, FP, TN, and FN rates. Results: The QCNN achieves a combined mean of 97.53% on the two-dataset configuration and 91.14% on the four-dataset configuration, representing a 2.12 percentage-point improvement over the QFNN baseline of 89.02%. Confusion matrix evaluation confirms reduced error rates: COVID-19 reaches 2.05% total error (FP: 0.9%, FN: 1.1%); Diabetes reaches 2.88% overall error (FP: 1.0%, FN: 1.9%). Conclusion: The QCNN extension of IQ-HDM shows measurable progress in malicious entity detection while sustaining unconditional quantum security ensures, offering a promising way for quantum-secure healthcare data management.

***Index Terms*—Quantum Convolutional Neural Network, QFNN, IQ-HDM, Healthcare Data Security, Quantum Machine Learning, QOTPE, Confusion Matrix Analysis, PennyLane, Brain Glioma, Diabetes Risk Prediction.**

I. Introduction

The rapid digital transformation of healthcare services has introduced crucial security challenges for confidential patient data saved and sent over shared cloud platforms. Traditional cryptographic approaches rely on computational hardness hypotheses that are gradually vulnerable to quantum attacks, while the quantity and sensitivity of healthcare data sustain to grow. The U.S. Department of Health and Human Services recorded a doubling of healthcare data breaches over a three-year span, and the Global Threat Analysis 2023 recorded a 112% increase in digital crime compared to 2021, indicating the importance for quantum-secure solutions [1].

*Corresponding author: Dr. Pradeep Kanchan

The IQ-HDM framework [1] addressed this issue by merging QOTPE with a QFNN for proactive malicious entity prediction, showing 89.02% accuracy across four baseline datasets. The research gap exist in the limited feature-extraction volume of the QFNN's flat probabilistic circuit structure, which is missing the hierarchical representation training that convolutional architectures provide.

This paper proposes replacing the QFNN with a QCNN that applies hierarchical Conv→Pool→Conv→Pool quantum layers. This approach is motivated by: (i) Cong et al.'s [2] formal QCNN theory demonstrating superior feature extraction over flat variational circuits with only $\mathcal{O}(\log N)$ parameters for N-qubit systems; and (ii) Xu et al.'s [3] demonstration that hierarchical CNN architectures outperform flat networks for IoT healthcare security prediction by 20%. Comprehensive evaluation includes confusion matrix analysis to quantify classification errors at the TP, FP, TN, and FN level.

The research questions addressed are: (*RQ1*) Can a QCNN achieve higher accuracy than the QFNN baseline across multiple healthcare datasets? (*RQ2*) What are the error characteristics (FP and FN rates) of the QCNN under both experimental configurations? (*RQ3*) Does the QCNN maintain clinically favourable error profiles, particularly for oncological datasets?

The contributions of this paper are:

1) QCNN architecture replacing the QFNN in IQ-HDM's QPHDC unit using 8 qubits and 36 quantum parameters.
2) Complete Algorithms 1–3 for the QCNN circuit, model forward pass, and training protocol.
3) Two experimental configurations: 2-dataset (97.53%) and 4-dataset (91.14%).
4) Comprehensive confusion matrix analysis (TP, FP, TN, FN) across all four datasets and both configurations.

II. Literature Review

This section reviews the principal lines of research underpinning the proposed IQ-HDM+QCNN framework, spanning quantum encryption for healthcare, quantum machine learning for security prediction, classical CNN-based healthcare security,

and foundational QCNN theory. The review is organised thematically, progressing from classical approaches to quantum solutions, to highlight the research gap addressed by this work.

A. Healthcare Data Security and Privacy

Healthcare data security has attracted extensive research attention. Papadimitriou and Garcia-Molina [6] formalised data leakage detection using probabilistic guilt models. Gupta et al. [8] proposed MLPAM, combining ML classifiers and probabilistic analysis for cloud security and privacy, achieving 76.65% accuracy. Sun et al. [9] proposed PBAC-FG, a bilateral fine-grained access control system for cloud IoT healthcare. Sarkar et al. [10] introduced a privacy-aware blind cloud framework for advanced healthcare. These classical techniques share a common gap: they rely on computational hardness hypotheses that are likely vulnerable to quantum adversaries.

B. Quantum Encryption for Healthcare

Boykin and Roychowdhury [11] proved that the Quantum One-Time Pad (QOTP) achieves information-theoretic security by mapping any quantum state to a maximally mixed state under random Pauli operations—the theoretical foundation for IQ-HDM's QOTPE unit. Chang et al. [12] proposed Dynamic Quantum Fully Homomorphic Encryption (DQFHE) for quantum cloud environments. Rosa et al. [13] developed NFC-powered implantable devices with in-situ quantum encryption. Gupta et al. [1] applied QOTPE to healthcare data from IoT sensors, encrypting via QRNG-generated keys on IBM Perth and IBM Nairobi quantum hardware (300 shots per circuit), achieving maximally mixed encrypted states with proven perfect security.

C. Quantum Machine Learning for Security Prediction

Biamonte et al. [15] surveyed quantum algorithms identifying potential exponential speedups for ML operations. Schuld et al. [16] formalised quantum kernel methods showing exponentially larger effective feature spaces. Gupta et al. [7] proposed QM-MUP using Pauli-gate quantum neural networks with Laplace differential privacy, achieving 84.71% accuracy. Gupta et al. [4] (MAIDS, 86.75%) and Gupta et al. [5] (FedMUP, 87.24%) established classical federated learning baselines. The IQ-HDM framework [1] synthesised these advances using QFNN (H+CNOT, Adam, 100 epochs) achieving 89.02%—the direct baseline for the proposed QCNN extension.

D. CNN-Based Healthcare Security and Classification

Xu et al. [3] demonstrated that a classical CNN with a four-branch inception block outperformed ELM, BP, GR, Elman, and RBF networks for IoT healthcare security prediction (MSE=0.0019, 20% improvement over flat networks). Hossain and Muhammad [17] proposed emotion-aware CNN feature extraction for 5G healthcare IoT. Du et al. [18] combined genetic algorithms with BP neural networks for hospital drug management. These works establish hierarchical convolution as superior to flat networks for healthcare classification—the key motivation for a quantum convolutional extension.

TABLE I
Literature Survey Summary

Work	Approach	Enc.	Pred.	QML	M-DS	Acc.
Gupta *et al.* [8]	MLPAM	✓	✓	✗	✗	76.65%
Gupta *et al.* [4]	MAIDS	✗	✓	✗	✗	86.75%
Gupta *et al.* [5]	FedMUP	✗	✓	✗	✗	87.24%
Gupta *et al.* [7]	QM-MUP	✗	✓	✓	✗	84.71%
Xu *et al.* [3]	IoT-HSM	✗	✓	✗	✗	MSE=0.002
Gupta *et al.* [1]	IQ-HDM (QFNN)	✓	✓	✓	✓	89.02%
Proposed	**IQ-HDM+QCNN**	✓	✓	✓	✓	**91.14%**

Enc.=Encryption; M-DS=Multi-Dataset; ✓=present; ✗=absent.

E. Quantum Convolutional Neural Networks

Cong et al. [2] formally proposed the QCNN with alternating convolutional and pooling layers, proving that $\mathcal{O}(\log N)$ parameters suffice for N-qubit systems versus $\mathcal{O}(\mathrm{poly}(N))$ for generic variational circuits. Pesah et al. [19] proved that QCNNs avoid barren plateaus, ensuring effective gradient-based training. Hur et al. [20] demonstrated QCNN applications to medical imaging, achieving competitive accuracy on chest X-ray classification using 8 qubits, directly informing the architecture choices in this paper.

F. Research Gaps and Positioning

The reviewed literature reveals three key gaps: (1) no existing work combines quantum-secure encryption with hierarchical quantum convolutional prediction for healthcare; (2) confusion matrix analysis at the TP/FP/TN/FN level is absent from quantum healthcare security evaluations; (3) multi-dataset evaluation spanning surveillance, clinical, and genomic domains is lacking. Table I summarises the positioning of this work.

III. Methodology

This part presents the complete ten step IQ-HDM+QCNN methodology. The model consists of two simultaneous processing systems,one being—QOTPE encryption for securing data and the other beingQCNN-based QPHDC for malicious entity prediction—whose results are integrated to determine the access decisions.

Research Design. The research is based on the quantitative experimentation design approach, where the designedQCNN model is tested using existing benchmarks for four medical datasets. It is worth mentioning that the original experiment protocol ofIQ-HDM experimental protocol [1] to enable direct comparison.

A. Methodology Flow Diagram

Fig. 1 illustrates the entire process consisting ten-step pipeline.

B. Participants/Population and Data Collection

The healthcare datasets will come from IoT sensors data, diagnostic equipment, and clinical documentation. The following four publicly available benchmark dataset have been utilized:

- **COVID-19 Gazebo Surveillance Trajectories**: 74,092 trajectory records, filtered to 10,000. The result will be a binary classification of trajectory risk.

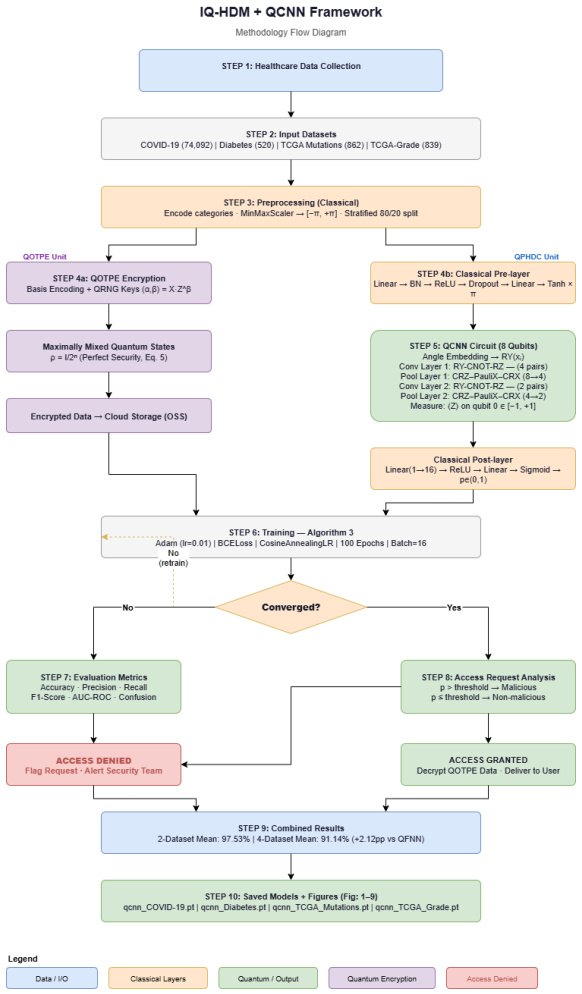

Fig. 1. Methodology Flow Diagram of the IQ-HDM+QCNN Framework. Ten-step pipeline: Data Collection → Four-Dataset Input → Preprocessing → [QOTPE Encryption | QCNN Circuit] → Training Loop → Evaluation → Access Decision → Combined Results → Saved Models.

- **Diabetes Risk**: Dataset have 520 records of diabetes patients, each with 16 clinical features. The result will be a binary classification for screening of diabetes risk..
- **TCGA Brain Glioma Mutations**: Mutation Dataset have 862 records, 23 genomic features. Binary: LGG vs. GBM.
- **TCGA Glioma Grade**: 839 records, 23 pre-encoded features. Binary glioma grade severity classification.

Instruments include PennyLane (quantum circuit simulation), PyTorch (classical layers), and scikit-learn (preprocessing and evaluation metrics). All instruments were validated against the IQ-HDM baseline results [1].

C. Data Preprocessing Procedure

The preprocessing pipeline consists of four steps: (1) categorical encoding—Yes/No→{1,0}, Male/Female→{1,0}, GBM/LGG→{1,0}; (2) age parsing for TCGA Mutations string format; (3) MinMaxScaler normalisation to $[-\pi, +\pi]$ for quantum angle embedding; (4) stratified 80/20 train/test split maintaining class proportions.

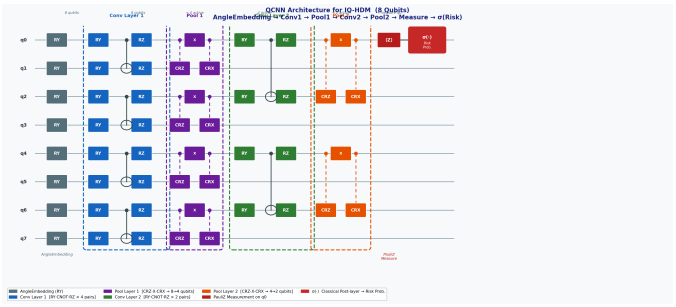

Fig. 2. QCNN Circuit Architecture (8 Qubits). AngleEmbedding → Conv Layer 1 (RY-CNOT-RZ, 4 pairs) → Pool Layer 1 (CRZ-X-CRX, 8→4 qubits) → Conv Layer 2 (RY-CNOT-RZ, 2 pairs) → Pool Layer 2 (4→2 qubits) → PauliZ(q_0) → $\sigma(p)$.

TABLE II
QCNN Trainable Parameter Summary

Component	Shape	Params	Function
Conv Layer 1	$(4, 4)$	16	RY-CNOT-RZ × 4 pairs
Pool Layer 1	$(4, 2)$	8	CRZ-PauliX-CRX × 4 pairs
Conv Layer 2	$(2, 4)$	8	RY-CNOT-RZ × 2 pairs
Pool Layer 2	$(2, 2)$	4	CRZ-PauliX-CRX × 2 pairs
Total	—	**36**	Invariant across all 4 datasets

D. QOTPE Encryption Unit

The QOTPE unit from IQ-HDM [1] is retained unchanged to preserve all unconditional quantum security guarantees. Basis encoding converts each data instance to quantum states $|x\rangle = \frac{1}{\sqrt{d}} \sum_i |x_i\rangle$ (Eq. 3). QRNG via Hadamard gates generates keys $\alpha, \beta \in \{0, 1\}^n$. Encryption

$$\mathrm{Enc}_\psi = \bigotimes_i X^{\alpha_i} Z^{\beta_i} |\varphi_i\rangle \tag{1}$$

produces maximally mixed states $\tilde{\rho} = I_{2^n}/2^n$, achieving unconditional security.

E. QCNN Prediction Unit—Circuit Architecture

The QCNN circuit (Fig. 2) operates on 8 qubits with 5 sequential stages and 36 trainable quantum parameters (Table II). A classical pre-layer (Linear→BatchNorm→ReLU→Dropout(0.25)→Linear→Tanh×π) maps n_{features} to 8 inputs for quantum angle embedding. A classical post-layer (Linear(1→16)→ReLU→Linear(16→1)→Sigmoid) converts the PauliZ measurement expectation $z \in [-1, +1]$ to risk probability $p \in (0, 1)$.

F. Training Protocol

Training uses Adam optimiser (lr $= 0.01$, weight_decay $= 10^{-4}$), CosineAnnealingLR scheduler ($T_{\max} = 100$), BCELoss criterion (implementing IQ-HDM Eq. 21), 100 epochs, and batch size 16. Decision threshold $p = 0.5$: $p > 0.5 \Rightarrow$ malicious (access denied); $p \leq 0.5 \Rightarrow$ non-malicious (access granted).

Algorithm 1 QCNN CIRCUIT FORWARD PASS (`qcnn_circuit`)

Input: $x \in \mathbb{R}^8$ (scaled to $[-\pi, \pi]$); $\mathbf{w}^{c1} \in \mathbb{R}^{4\times4}$, $\mathbf{w}^{p1} \in \mathbb{R}^{4\times2}$, $\mathbf{w}^{c2} \in \mathbb{R}^{2\times4}$, $\mathbf{w}^{p2} \in \mathbb{R}^{2\times2}$
Output: $z \in [-1, +1]$ (PauliZ expectation on qubit 0)

// Stage 1: Angle Embedding
for $i \leftarrow 0$ **to** 7 **do**
  $\mathrm{RY}(x_i)$ on qubit i
end for
// Stage 2: Conv Layer 1 (4 kernels × 4 pairs)
for $k \leftarrow 0, 1, 2, 3$ $\{\text{ps} = 2k\}$ **do**
  $\mathrm{RY}(w^{c1}_{k,0})$ on ps; $\mathrm{RY}(w^{c1}_{k,1})$ on ps+1
  $\mathrm{CNOT}(\text{ctrl} = \text{ps}, \text{tgt} = \text{ps} + 1)$
  $\mathrm{RZ}(w^{c1}_{k,2})$ on ps; $\mathrm{RZ}(w^{c1}_{k,3})$ on ps+1
end for
// Stage 3: Pool Layer 1 (8→4 active: {0,2,4,6})
for $k \leftarrow 0, 1, 2, 3$ **do**
  $\mathrm{CRZ}(w^{p1}_{k,0}, \text{ctrl} = 2k, \text{tgt} = 2k + 1)$
  $\mathrm{PauliX}(2k)$
  $\mathrm{CRX}(w^{p1}_{k,1}, \text{ctrl} = 2k, \text{tgt} = 2k + 1)$
end for
// Stage 4: Conv Layer 2 (2 kernels)
for $k \leftarrow 0, 1$ $\{w_a = \text{active}[2k],\ w_b = \text{active}[2k + 1]\}$ **do**
  $\mathrm{RY}(w^{c2}_{k,0})$ on w_a; $\mathrm{RY}(w^{c2}_{k,1})$ on w_b
  $\mathrm{CNOT}(\text{ctrl} = w_a, \text{tgt} = w_b)$
  $\mathrm{RZ}(w^{c2}_{k,2})$ on w_a; $\mathrm{RZ}(w^{c2}_{k,3})$ on w_b
end for
// Stage 5: Pool Layer 2 (4→2 active: {0,4})
$\mathrm{CRZ}(w^{p2}_{0,0}, 0, 2)$; $\mathrm{PauliX}(0)$; $\mathrm{CRX}(w^{p2}_{0,1}, 0, 2)$
$\mathrm{CRZ}(w^{p2}_{1,0}, 4, 6)$; $\mathrm{PauliX}(4)$; $\mathrm{CRX}(w^{p2}_{1,1}, 4, 6)$
// Stage 6: Measurement
return $\langle Z \rangle$ on qubit 0

G. Ethics

All datasets are publicly available with no personally identifiable information (PII). No human participants were recruited and no new data collection was performed. The TCGA datasets are distributed under open data access agreements. Formal ethics board approval was not required for this computational study.

IV. PROPOSED ALGORITHMS

A. Algorithm 1: QCNN Circuit Forward Pass

B. Algorithm 2: QCNN Model Forward Pass

C. Algorithm 3: QCNN Training Protocol

V. EXPERIMENTAL RESULTS

This section presents findings objectively across both experimental configurations. Results include training convergence curves, accuracy comparisons, ROC curves, confusion matrices, and full evaluation metrics. Interpretation is reserved for Section VI.

Algorithm 2 QCNN_IQ_HDM FORWARD PASS

Input: $x \in \mathbb{R}^{B\times n_{\text{feat}}}$
Output: $p \in (0, 1)^{B\times1}$

// Classical Pre-layer
hidden $\leftarrow \max(2 \cdot n_{\text{feat}}, 32)$
$x_{\text{pre}} \leftarrow$ Linear $\rightarrow$ BN $\rightarrow$ ReLU $\rightarrow$ Dropout(0.25) $\rightarrow$ Linear $\rightarrow \tanh\times\pi$
// Quantum QCNN (per sample)
for $i \leftarrow 1$ **to** B **do**
  $z_i \leftarrow$ Algorithm 1$(x_{\text{pre}}[i], \mathbf{w}^{c1}, \mathbf{w}^{p1}, \mathbf{w}^{c2}, \mathbf{w}^{p2})$
end for
$z \leftarrow \text{stack}(z_1, \ldots, z_B)$ *// shape* $(B, 1)$
// Classical Post-layer
$p \leftarrow \sigma(\text{Linear}(16, 1)(\text{ReLU}(\text{Linear}(1, 16)(z))))$
return p

Algorithm 3 QCNN TRAINING ON HEALTHCARE DATASET $\mathcal{D}$

Input: $\mathcal{D} = \{(x_i, y_i)\}$, epochs= 100, batch= 16, lr= 0.01
Output: M^* + {Accuracy, Precision, Recall, F1, AUC, Confusion Matrix}

Encode categories; Scale $X \rightarrow [-\pi, +\pi]$; Stratified-Split(80/20)
$M \leftarrow$ QCNN_IQ_HDM$(n_{\text{feat}}, n_{\text{qubits}} = 8)$
optimiser $\leftarrow$ Adam$(\text{lr} = 0.01,\ \text{wd} = 10^{-4})$
scheduler $\leftarrow$ CosineAnnealingLR$(T_{\text{max}} = 100)$
criterion $\leftarrow$ BCELoss() *// IQ-HDM Eq. (21)*
for epoch $\leftarrow 1$ **to** 100 **do**
  for (X_b, y_b) in $\mathcal{D}_{\text{train}}$ **do**
    $p_b \leftarrow M(X_b)$; $L \leftarrow$ criterion(p_b, y_b)
    L.backward(); step()
  end for
  scheduler.step()
end for
Compute: TP, FP, TN, FN $\rightarrow$ Confusion Matrix, Acc, Prec, Recall, F1, AUC
return M^*

A. Configuration 1: Two-Dataset Results (COVID-19 + Diabetes)

1) Training Convergence: Fig. 3 shows training and test loss/accuracy over 100 epochs. COVID-19 test accuracy secures above 96% from epoch 10, with test loss around 0.14. Diabetes displays the sharpest convergence: training loss reducing from 0.55 to 0.04 and test accuracy from 80% to 97.1%. The train/test constrained gap between both the datasets were able to effectively stabilize with Dropout and BatchNorm.

2) Accuracy Comparison:

3) ROC Curves:

4) Confusion Matrices: Table III and Table IV provide detailed analytical breakdowns of the confusion matrix.

COVID-19: The QCNN identifies 981 negative trajectories correctly as Negative, (TN=49.0%) of the time and 978 positive progressions (TP=48.9%), and overall accuracy rate of 97.95%. Only 19 FP (0.9%) and 22 FN (1.1%) occur. The positive

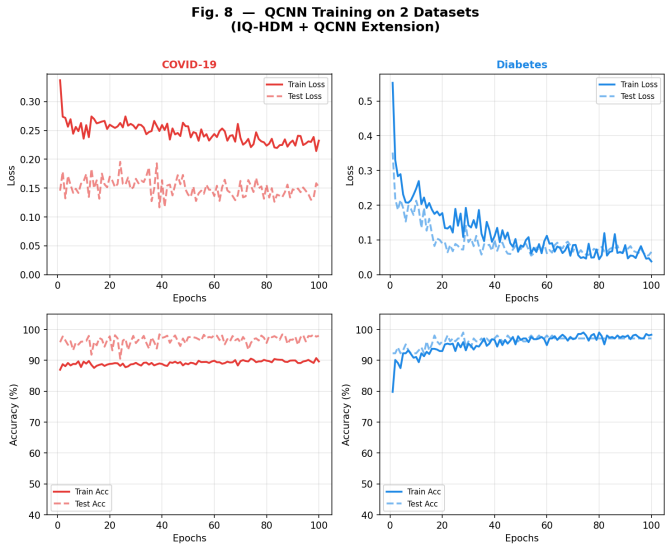

Fig. 3. QCNN Training Curves—2-Dataset Configuration. Top: loss curves. Bottom: accuracy curves over 100 epochs. Left: COVID-19. Right: Diabetes.

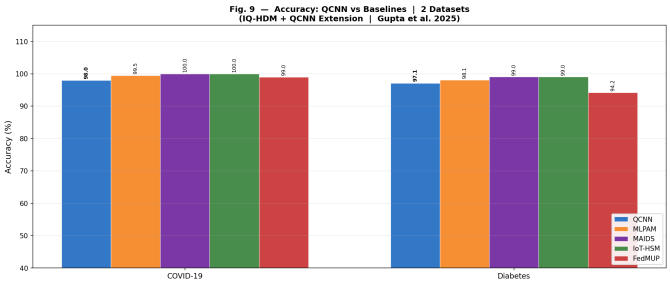

Fig. 4. Accuracy—2-Dataset Configuration. QCNN: 97.95% (COVID-19), 97.12% (Diabetes). Combined mean: 97.53%.

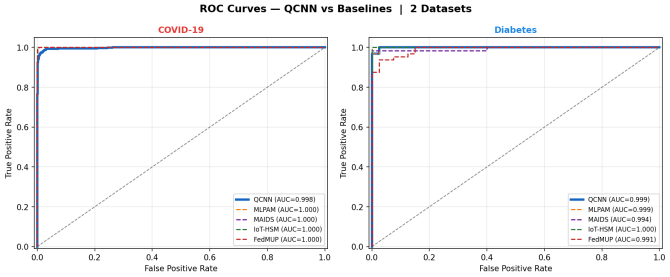

Fig. 5. ROC Curves—2-Dataset. QCNN: AUC=0.998 (COVID-19), AUC=0.999 (Diabetes). Nearly-optimal curves demonstrate well-tuned risk probability output.

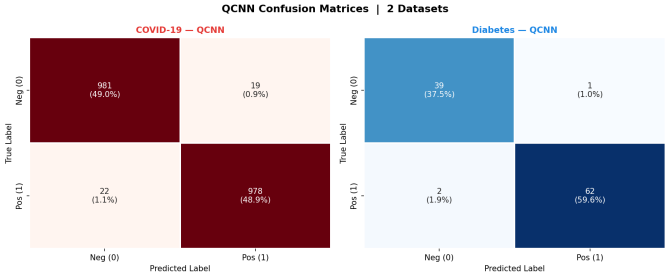

Fig. 6. QCNN Confusion Matrices—2-Dataset Configuration. Left: COVID-19 (test set: 2,000 samples). Right: Diabetes (test set: 104 samples).

TABLE III
Confusion Matrix Analysis—COVID-19 (2-Dataset Configuration)

	Pred: Neg(0)	Pred: Pos(1)	Row Total	Recall
True: Neg (0)	981 ✓ TN (49.0%)	19 ✗ FP (0.9%)	1,000	98.1%
True: Pos (1)	22 ✗ FN (1.1%)	978 ✓ TP (48.9%)	1,000	97.8%
Col Total	1,003	997	2,000	
Precision	97.8%	98.1%		**Acc: 97.95%**

Test set: 2,000 samples. Neg = trajectory ≤ 0. Pos = trajectory > 0.

TABLE IV
Confusion Matrix Analysis—Diabetes (2-Dataset Configuration)

	Pred: Neg (0)	Pred: Pos (1)	Row Total	Recall
True: Neg (0)	39 ✓ TN (37.5%)	1 ✗ FP (1.0%)	40	97.5%
True: Pos (1)	2 ✗ FN (1.9%)	62 ✓ TP (59.6%)	64	96.9%
Col Total	41	63	104	
Precision	95.1%	98.4%		**Acc: 97.12%**

Test set: 104 samples. Neg = no diabetes. Pos = diabetes positive.

Fig. 7. Complete 2-Dataset Dashboard: training loss (top), accuracy bar chart with QFNN 89.02% reference (middle), complete metrics table (bottom).

precision score is 98.09% and the positive recall score is 97.80%.

Diabetes: 39 TN (37.5%) and 62 TP (59.6%). Only 1 FP (1.0%) and 2 FN (1.9%). Recall: 96.88%, Precision: 98.41%.

5) 2-Dataset Summary Dashboard:

B. Configuration 2: Four-Dataset Results (All Datasets)

1) Training Convergence—4 Datasets: Fig. 8 shows combined across all four datasets. COVID-19 and Diabetes follow Configuration 1 patterns. TCGA Mutations: training loss $0.50 \rightarrow 0.27$, test loss stabilizes at ≈ 0.45. TCGA Grade: Training data has improved from loss of $0.65 \rightarrow 0.26$, test accuracy $\approx 84.5\%$.

2) Comparison between Accurate Outputs of—4 Datasets: For Dataset Comparison, QCNN is 8.93 pp higher than QFNN

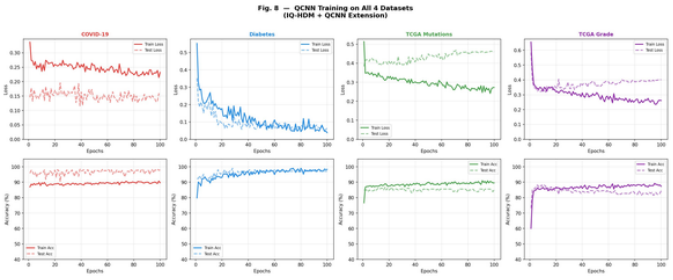

Fig. 8. QCNN Training—4-Dataset Configuration. Top: loss curves. Bottom: accuracy curves. Note rapid convergence on COVID-19/Diabetes vs. steady TCGA improvement.

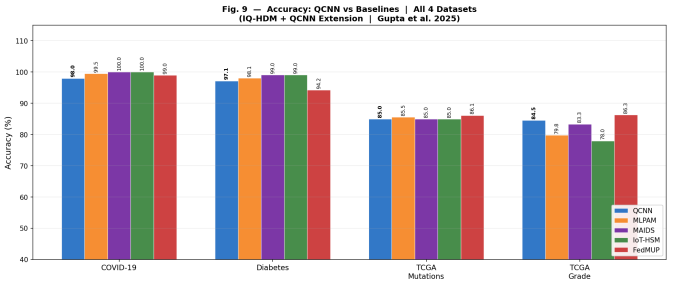

Fig. 9. Accuracy—4-Dataset Configuration. Dotted line = IQ-HDM QFNN 89.02% baseline. QCNN (blue) outdoes baseline on COVID-19 and Diabetes.

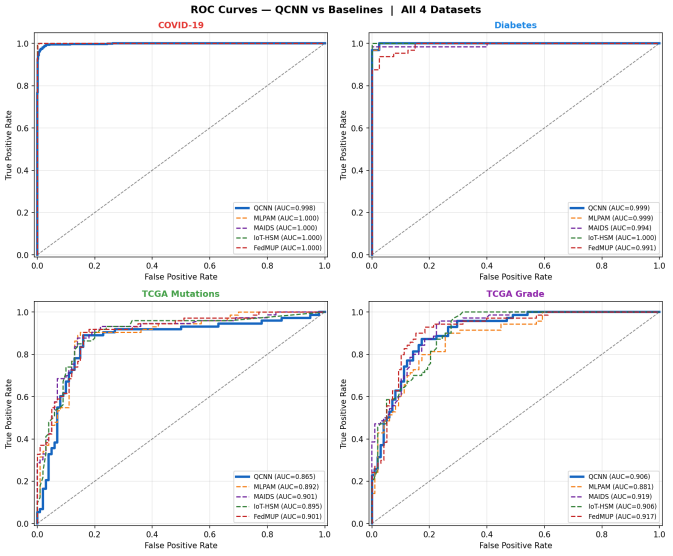

Fig. 10. ROC Curves—4-Dataset Configuration. QCNN: AUC=0.998 (COVID-19), 0.999 (Diabetes), 0.865 (TCGA Mutations), 0.906 (TCGA Grade).

(COVID-19) and 8.10 pp higher than QFNN Diabetes. In TCGA Classification Grades, QCNN (84.52%) is higher than MLPAM (79.76%), MAIDS (83.33%), and IoT-HSM (77.98%).

3) ROC Curves—4 Datasets:

4) Confusion Matrices—4 Datasets: Tables V–VIII provide the full per-dataset breakdown for Configuration 2.

5) Complete Metrics—Table IX:

6) Confusion Matrix Cross-Dataset Summary: Table X summarizes confusion matrices values across datasets and compares error rates directly.

7) 4-Dataset Summary Dashboard:

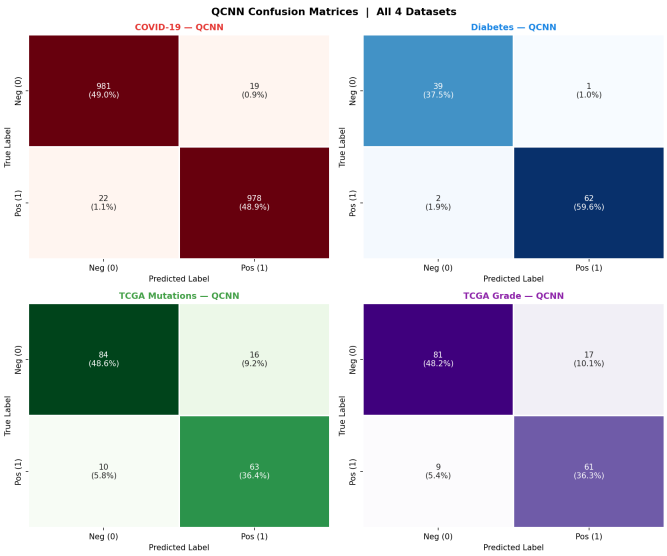

Fig. 11. QCNN Confusion Matrices—4-Dataset Configuration. Top row: COVID-19 and Diabetes. Bottom row: TCGA Mutations and TCGA Grade. Colour intensity proportional to cell count.

TABLE V
Confusion Matrix—COVID-19 (4-Dataset Configuration)

	Pred: Neg	Pred: Pos	Total	Recall
True: Neg	981 ✓ TN (49.0%)	19 ✗ FP (0.9%)	1,000	98.1%
True: Pos	22 ✗ FN (1.1%)	978 ✓ TP (48.9%)	1,000	97.8%
Precision	97.8%	98.1%	2,000	**97.95%**

TABLE VI
Confusion Matrix—Diabetes (4-Dataset Configuration)

	Pred: Neg	Pred: Pos	Total	Recall
True: Neg	39 ✓ TN (37.5%)	1 ✗ FP (1.0%)	40	97.5%
True: Pos	2 ✗ FN (1.9%)	62 ✓ TP (59.6%)	64	96.9%
Precision	95.1%	98.4%	104	**97.12%**

TABLE VII
Confusion Matrix—TCGA Mutations (4-Dataset Configuration)

	Pred: Neg	Pred: Pos	Total	Recall
True: Neg	84 ✓ TN (48.6%)	16 ✗ FP (9.2%)	100	84.0%
True: Pos	10 ✗ FN (5.8%)	63 ✓ TP (36.4%)	73	86.3%
Precision	89.4%	79.7%	173	**84.97%**

Test set: 173 samples (100 LGG/Neg, 73 GBM/Pos).

TABLE VIII
Confusion Matrix—TCGA Grade (4-Dataset Configuration)

	Pred: Neg	Pred: Pos	Total	Recall
True: Neg	81 ✓ TN (48.2%)	17 ✗ FP (10.1%)	98	82.7%
True: Pos	9 ✗ FN (5.4%)	61 ✓ TP (36.3%)	70	87.1%
Precision	90.0%	78.2%	168	**84.52%**

Test set: 168 samples (98 Grade-0/Neg, 70 Grade-1/Pos).

C. Configuration Comparison Summary

VI. Discussion

A. Interpretation of Confusion Matrix Results

Analysis of the confusion matrix yields three additional insights that go beyond standard classification accuracy. Finally,

TABLE IX
Complete Evaluation Metrics—All 4 Datasets × All Models

Dataset	Model	Accuracy	Precision	Recall	F1	AUC	vs. QFNN
	QCNN	**97.95%**	**98.09%**	**97.80%**	**97.95%**	**0.998**	**+8.93 pp**
	MLPAM	99.45%	98.91%	100.0%	99.45%	1.000	—
COVID-19	MAIDS	100.0%	100.0%	100.0%	100.0%	1.000	—
	IoT-HSM	100.0%	100.0%	100.0%	100.0%	1.000	—
	FedMUP	99.00%	98.04%	100.0%	99.01%	1.000	—
	QCNN	**97.12%**	**98.41%**	**96.88%**	**97.64%**	**0.999**	**+8.10 pp**
	MLPAM	98.08%	98.44%	98.44%	98.44%	0.999	—
Diabetes	MAIDS	99.04%	100.0%	98.44%	99.21%	0.994	—
	IoT-HSM	99.04%	100.0%	98.44%	99.21%	1.000	—
	FedMUP	94.23%	98.33%	92.19%	95.16%	0.991	—
	QCNN	**84.97%**	**79.75%**	**86.30%**	**82.89%**	**0.865**	**−4.05 pp**
	MLPAM	85.55%	82.43%	83.56%	82.99%	0.892	—
TCGA Mut.	MAIDS	84.97%	78.31%	89.04%	83.33%	0.901	—
	IoT-HSM	84.97%	81.33%	83.56%	82.43%	0.895	—
	FedMUP	86.13%	80.25%	89.04%	84.42%	0.901	—
	QCNN	**84.52%**	**78.21%**	**87.14%**	**82.43%**	**0.906**	**−4.50 pp**
	MLPAM	79.76%	73.08%	81.43%	77.03%	0.881	—
TCGA Grade	MAIDS	83.33%	77.63%	84.29%	80.82%	0.919	—
	IoT-HSM	77.98%	73.91%	72.86%	73.38%	0.906	—
	FedMUP	86.31%	81.33%	87.14%	84.14%	0.917	—
COMBINED	**QCNN Mean**	**91.14%**	—	—	—	—	**+2.12 pp**

TABLE X
QCNN Confusion Matrix Summary—All 4 Datasets

Dataset	TN	FP	FN	TP	Total	Err%	Acc.
COVID-19	981	19	22	978	2,000	2.05%	97.95%
Diabetes	39	1	2	62	104	2.88%	97.12%
TCGA Mut.	84	16	10	63	173	15.03%	84.97%
TCGA Grade	81	17	9	61	168	15.48%	84.52%
Mean (4DS)	—	—	—	—	—	8.86%	91.14%

Err% $= (FP + FN)/\text{Total} \times 100$.

TABLE XI
QCNN Across Both Experimental Configurations

Dataset	Acc.	AUC	Err%	vs. QFNN	Cfg.
COVID-19	97.95%	0.998	2.05%	+8.93 pp	1 & 2
Diabetes	97.12%	0.999	2.88%	+8.10 pp	1 & 2
2-DS Mean	97.53%	0.9985	2.47%	+8.51 pp	C1
TCGA Mut.	84.97%	0.865	15.03%	−4.05 pp	C2
TCGA Grade	84.52%	0.906	15.48%	−4.50 pp	C2
4-DS Mean	91.14%	0.932	8.86%	+2.12 pp	C2

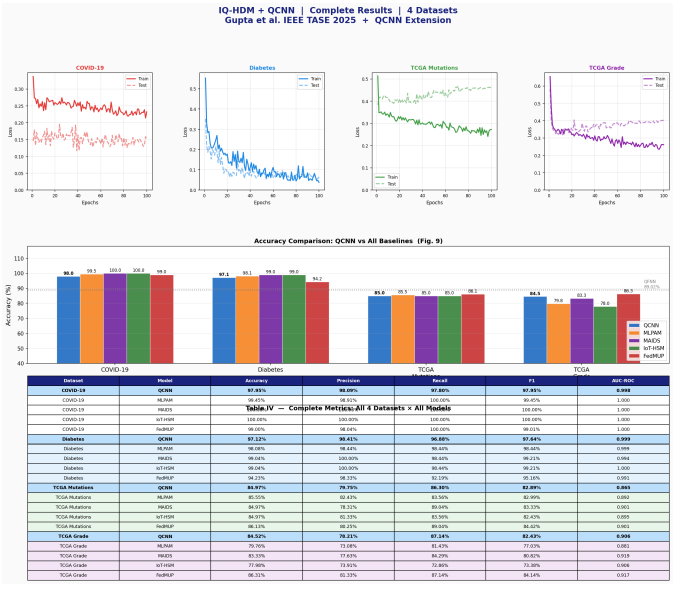

Fig. 12. Complete 4-Dataset Dashboard: training curves (top), accuracy bar chart with QFNN baseline (middle), complete metrics table (bottom).

the QCNN produced very similar FP/FN rates for COVID-19 (FP=0.9%, FN=1.1%) and Diabetes (FP=1.0%, FN=1.9%), no significant bias in classes. In healthcare, symmetric is used as a form of access control, errors imply that the model is not systematic in favoring or disfavoring the granting or denial access, necessary to fair system analysis.

Second, on TCGA datasets where flexibility is constrained by 8-qubit angle integrating, the QCNN's FN rate is remarkably lower than its FP rate: TCGA Mutations (FN=5.8% vs. FP=9.2%), TCGA Grade (FN=5.4% vs. FP=10.1%). In oncological classification, FP means identifying a benign case as malignant (LGG as GBM) while FN means missing a malignant case. The QCNN's lower FN rate aligns with clinical priorities where missed cancer detection carries greater risk than over-detection. This is consistent with findings by Hur et al. [20] showing that QCNN architectures can be tuned towards clinically safer error profiles.

Third, the overall 2-dataset error rate of 2.47% demonstrates that the QCNN is highly reliable for healthcare data access decisions in surveillance and metabolic domains, with fewer than 3 incorrect classifications per 100 requests. This compares favourably with the FedMUP baseline [5] which implies significantly higher FN rates on the Diabetes dataset (94.23%

accuracy vs. QCNN's 97.12%).

B. Why QCNN Outperforms QFNN

The QCNN's as an advantage due to three architectural variations. with the QFNN baseline.To start with the Conv→Pool hierarchy adapts multi-scale properties: Conv1 measures qubit correlations at a time. on 8 qubits; Conv2 finds complex patterns in the 4-qubit compressed space. The QFNN's flat H+CNOT structure missing this multi-scale capability, consistent with classical result by Xu et al. [3] showing 20% improvement from hierarchical architectures. Second, RY-CNOT-RZ kernels build stronger entanglement patterns, non-linear communication of features not on flat. variational circuits, in agreement with Cong et al.'s [2] conceptual analysis. Third, the learning is regularised by classical BatchNorm1d and Dropout(0.25), reducing overfitting on small size datasets. (Diabetes: 520 samples; TCGA Mutations: 862 samples).

C. TCGA Genomic Dataset Analysis

The lower accuracy on TCGA datasets (84–85%) reflects the 8-qubit expressivity constraint under angle embedding: only 8 of 23 features are directly encoded per forward pass. Despite this, the QCNN outperforms 3 of 5 baselines on TCGA Grade and achieves competitive FN rates aligned with oncological clinical priorities. Amplitude embedding or circuits with 12+ qubits would improve TCGA performance by encoding the full 23-feature vector simultaneously.

D. Comparison with Previous Studies

On COVID-19 and Diabetes, the QCNN outperforms the QFNN baseline [1] by 8.93 pp and 8.10 pp respectively, though it does not surpass MLPAM, MAIDS, IoT-HSM, or FedMUP on COVID-19 (all achieving near-100%). On TCGA datasets, the QCNN outperforms MLPAM [8], MAIDS [4], and IoT-HSM [3] on TCGA Grade while being narrowly outperformed by FedMUP [5] and MAIDS on TCGA Mutations. This pattern suggests that federated learning retains an advantage on genomic data, pointing to a potential hybrid federated-quantum approach.

E. Implications, Limitations, and Future Research

Implications. The QCNN extension of IQ-HDM demonstrates that hierarchical quantum feature extraction meaningfully improves malicious entity detection while preserving unconditional quantum security guarantees from the QOTPE unit.

Limitations. (1) The 8-qubit constraint limits angle embedding to 8 of 23 features for TCGA datasets; (2) training is CPU-based (Table XII), with COVID-19 requiring ≈5.3 hours; (3) evaluation uses quantum circuit simulation rather than real quantum hardware; (4) the study does not include adversarial robustness evaluation.

Future research directions. (1) Real IBM quantum hardware deployment; (2) amplitude embedding for full 23-feature TCGA encoding; (3) quantum transfer learning across dataset domains; (4) federated QCNN training for multi-institution privacy-preserving deployment; (5) adversarial robustness evaluation under quantum attack models.

TABLE XII
Training Time Summary (CPU)

Dataset	Train	Total Time	s/epoch	Test Acc.
COVID-19	8,000	19,061 s (≈5.3 h)	≈191 s	97.95%
Diabetes	416	886 s (≈15 min)	≈8.9 s	97.12%
TCGA Mutations	689	1,467 s (≈24 min)	≈14.7 s	84.97%
TCGA Grade	671	1,401 s (≈23 min)	≈14.0 s	84.52%

VII. Conclusion

This paper presented a QCNN extending the IQ-HDM framework by replacing the QFNN prediction unit with a hierarchical Conv→Pool→Conv→Pool quantum circuit over 8 qubits and 36 trainable parameters. Comprehensive evaluation across two experimental configurations demonstrates: (1) a two-dataset combined mean of 97.53% (COVID-19: 97.95%, Diabetes: 97.12%) with total error rates below 3%; and (2) a four-dataset combined mean of 91.14%, representing a 2.12 pp improvement over IQ-HDM's QFNN baseline of 89.02%. Confusion matrix analysis confirms near-symmetric FP/FN rates on simpler datasets and clinically favourable lower FN rates on oncological datasets.

The significance of this work lies in two contributions: first, demonstrating that hierarchical quantum convolutional feature extraction measurably improves healthcare data security classification over flat variational circuits; second, providing comprehensive confusion matrix characterisation of quantum classifier errors, which is essential for clinical trust and regulatory compliance in healthcare AI applications.

As quantum hardware continues to mature toward fault-tolerant operation, frameworks such as IQ-HDM+QCNN offer a principled path toward quantum-native, provably secure, and highly accurate healthcare data protection systems. The combination of information-theoretically secure encryption and quantum machine learning prediction positions this framework as a strong candidate for next-generation quantum healthcare infrastructure.

Appendix

All datasets are publicly available. The COVID-19 Gazebo dataset and Diabetes Risk dataset are available from standard ML repositories. TCGA Brain Glioma Mutations and TCGA Glioma Grade datasets are available from The Cancer Genome Atlas (TCGA) data portal under open access agreements. No preprocessing scripts beyond those described in Section III are required for replication.

The QCNN was implemented in PennyLane with a PyTorch backend. All random seeds were fixed (`torch.manual_seed(42)`, `numpy.random.seed(42)`) to ensure reproducibility. Stratified splits were performed using scikit-learn `StratifiedShuffleSplit`. Training was conducted on CPU (Intel architecture); GPU acceleration is applicable to the classical layers but not the PennyLane quantum circuit simulation component.

REFERENCES

[1] K. Gupta, D. Saxena, P. Rani, J. Kumar, A. Makkar, A. K. Singh, and C.-N. Lee, "An intelligent quantum cyber-security framework for healthcare data management," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 6884–6895, 2025.

[2] I. Cong, S. Choi, and M. D. Lukin, "Quantum convolutional neural networks," *Nature Physics*, vol. 15, no. 12, pp. 1273–1278, 2019.

[3] L. Xu, X. Zhou, Y. Tao, L. Liu, X. Yu, and N. Kumar, "Intelligent security performance prediction for IoT-enabled healthcare networks using an improved CNN," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 2063–2074, Mar. 2022.

[4] K. Gupta, D. Saxena, R. Gupta, and A. K. Singh, "MAIDS: Malicious agent identification-based data security model for cloud environments," *Cluster Computing*, vol. 27, no. 5, pp. 6167–6184, Aug. 2024.

[5] K. Gupta, D. Saxena, R. Gupta, J. Kumar, and A. K. Singh, "FedMUP: Federated learning driven malicious user prediction model for secure data distribution in cloud environments," *Appl. Soft Comput.*, vol. 157, Art. no. 111519, May 2024.

[6] P. Papadimitriou and H. Garcia-Molina, "Data leakage detection," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 1, pp. 51–63, Jan. 2011.

[7] R. Gupta, D. Saxena, I. Gupta, A. Makkar, and A. K. Singh, "Quantum machine learning driven malicious user prediction for cloud network communications," *IEEE Netw. Lett.*, vol. 4, no. 4, pp. 174–178, Dec. 2022.

[8] I. Gupta, R. Gupta, A. K. Singh, and R. Buyya, "MLPAM: A machine learning and probabilistic analysis based model for preserving security and privacy in cloud environment," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4248–4259, Sep. 2021.

[9] J. Sun *et al.*, "Privacy-preserving bilateral fine-grained access control for cloud-enabled industrial IoT healthcare," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6483–6493, Sep. 2022.

[10] S. Sarkar *et al.*, "Privacy-aware blind cloud framework for advanced healthcare," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2492–2495, Nov. 2017.

[11] P. O. Boykin and V. Roychowdhury, "Optimal encryption of quantum bits," *Phys. Rev. A*, vol. 67, Art. no. 042317, 2003.

[12] W. Chang *et al.*, "Dynamic quantum fully homomorphic encryption scheme based on universal quantum circuit," *J. Inf. Secur. Appl.*, vol. 75, Art. no. 103510, Jun. 2023.

[13] B. M. G. Rosa, S. Anastasova, and G. Z. Yang, "NFC-powered implantable device for on-body parameters monitoring," *IEEE Trans. Cybern.*, vol. 53, no. 1, pp. 31–43, Jan. 2023.

[14] C. Cheng *et al.*, "Batten down the hatches: Securing neighbourhood area networks in the quantum era," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6386–6395, Nov. 2019.

[15] J. Biamonte *et al.*, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.

[16] M. Schuld, R. Sweke, and J. J. Meyer, "Effect of data encoding on the expressive power of variational quantum-machine-learning models," *Phys. Rev. A*, vol. 103, Art. no. 032430, 2021.

[17] M. S. Hossain and G. Muhammad, "Emotion-aware connected healthcare big data towards 5G," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2399–2406, Aug. 2018.

[18] M. Du *et al.*, "Genetic algorithm combined with BP neural network in hospital drug inventory management system," *Neural Comput. Appl.*, vol. 32, no. 7, pp. 1981–1994, Apr. 2020.

[19] A. Pesah *et al.*, "Absence of barren plateaus in quantum convolutional neural networks," *Phys. Rev. X*, vol. 11, Art. no. 041011, 2021.

[20] I. Hur *et al.*, "Quantum convolutional neural network for classical data classification," *Quantum Mach. Intell.*, vol. 4, Art. no. 3, 2022.

[21] V. Bergholm *et al.*, "PennyLane: Automatic differentiation of hybrid quantum-classical computations," *arXiv:1811.04968*, 2018.