International Academic Institute for Science and Technology

International Academic Journal of Innovative Research
Vol. 12, No. 4, 2025, pp. 1-9.

ISSN 2454-390X

International Academic Journal of Innovative Research

www.iaiest.com

Quantum-Resilient Federated Cognitive Networks for Secure and Ethical AI-Powered Mental Health Interventions

Dr. Alfred Jesudhas Kamaldas [a], Dr. K. Juliet Catherine Angel [b]

[a] *Director IT, Canopy - A Revive Company, USA. E-mail: ks.alfredj@gmail.com*
[b] *Head, Assistant Professor, PG Department of Computer Applications, Holy Cross College (Autonomous), Tiruchirappalli, Tamil Nadu, India. E-mail: julietcatherineangel@hcctrichy.ac.in*

Abstract

Integrating Artificial Intelligence (AI) into interventions for mental health issues significantly augments both personalization and access to care. Still, the challenges of protecting extremely sensitive patient data and the highly probable and available quantum computers security threat have plagued the mental health care initiatives for expansion. Centralized training and learning models for AI seem especially prone to catastrophic loss of data as well as catastrophic decryptions of documents once quantum computers with cryptographically relevant computational powers become available, making all the contemporary safeguards pointless. These and similar issues have spawned the development of this document, which outlines what we deem as the novel and interdisciplinary paradigm of the Quantum–Resilient Federated Cognitive Network (QRFCN), which we propose as the primary solution. Ethical data sovereignty necessitates the retention of sensitive diagnosis and cognitive assessment information on patient devices or on data residing with health care institutions, and QRFCN employs Federated Learning (FL) to accomplish this. Most importantly, QRFCN employs Post-Quantum Cryptography (PQC) using the lattice-based Kyber key encapsulation mechanism and Dilithium digital signature scheme to server-side supplementary proxy communications to preserve custody of all FL aggregation inter-client and inter-server communications. Then comes the introduction of QR-FedAvg, the augmented federated averaging quantum-resilient model of disaggregated, modular, localized server-client proxies, the first PQC sensitive communications overhead probable system model that seeks to the latent PQC super ratioed cognitive disaggregating tensor. The simulated Non-IID clinical dataset under study shows that QRFCN captures model utility (91.3% accuracy) similar to centralized and classical FL approaches while concurrently providing strong protection against known quantum attacks. This research resolves the gap concerning offering a plausible, safe, and ethical method of next-generation AI deployment in sensitive domains of healthcare.

Keywords: Quantum Security, Federated Learning, Mental Health AI, Post-Quantum Cryptography, Cognitive Networks.

DOI:10.71086/IAJIR/V12I4/IAJIR1227
Received: 03 September, 2025/Revised: 07 October 2025/Accepted: 11 November 2025/Published: 15 December 2025

Introduction

In understanding global mental health challenges, multiple approaches are seen through personalized, precise, adaptable, and scalable solutions. Out of which Artificial Intelligence Machine Learning (AI ML) is used with an aim of developing prognostic intervention models and therapeutic recommendations rooted in behavioral and cognitive, in this case, symptom evolution data. Such intervention approaches, along with numerous behavioral health care visits, especially create intervention approaches where data is highly sensitive, and perhaps the most secure and ethically sensitive personal information, needing to be longitudinally recorded, is recorded on the analytics of mood, sleep, attention, biometrics, and therapy progress [1] [10].

Failure to do so carries two significant risks. In the paradigm of personalized mental health care, the first risk is ethical and stems from the need to store sensitive data on cloud servers for the rudimentary purpose of training an AI model (data centralization) [2] [11]. This latter practice leads to the aggregation (crossing borders) of electronic health records, and especially personal data, which is a violation of the data sovereignty framework, and increases the vulnerability to data breaches (single point of failure) at the expense of numerous cloud servers [3] [14]. In personal data systems, the second risk, which is the most critical, is the risk from a Quantum Computer (QC). All current cryptography systems of RSA and Elliptic Curve (ECC) are exposed and at risk of being defeated (compromised) with the use of quantum cryptographically relevant computers because of Shor's and Grover's algorithms [4][13]. The "Store Now, Decrypt Later" implications of Big Phi Quantum AI suggest that any data encrypted today can be harvested and thus later decrypted by a QC, which is the ultimate security risk of quantum computing [5][12].

To resolve this issue, we put forth the Quantum-Resilient Federated Cognitive Network (QRFCN) as a proposed solution. In QRFCN, clients store patient data locally while collaborating on a shared global mental health model trained using Federated Learning (FL). These ethically distributed systems, furthermore, are strengthened with Post-Quantum Cryptography (PQC) to defend against adversaries and guarantee that the only shared information model updates are the only information exchanged [21][22].

Key Contributions and Main Goal

The primary goal of this paper is to design, model, and evaluate a quantum-resilient and ethically compliant AI framework for mental health interventions. Our key contributions are:

- **QRFCN Architecture:** Definition of a novel, secure, and decentralized architecture for cognitive network training.
- **QR-FedAvg Algorithm:** Development of the Quantum-Resilient Federated Averaging (QR-FedAvg) algorithm, integrating PQC protocols (Kyber and Dilithium) into the FL communication pipeline.
- **Security and Utility Evaluation:** Comprehensive analysis demonstrating that quantum-resistance can be achieved with minimal necessary overhead while maintaining high model predictive accuracy on non-IID clinical data.

Fig 1 elucidates the architecture of the Quantum-Resilient Federated Cognitive Network (QRC-FCN) aimed at protecting the integrity of privacy and ethical issues pertaining to AI in mental health. At the heart of the system is the central Quantum-Resilient Cognitive Network (QRC-FCN), which steers the learning of the system in a distributed fashion. The workflow starts with Data Collection & Context in a demanding client, which is Behavioral Data, Physiological (HRV, Activity) Data, and Environmental Context (Time, Location) capturing. The data is then transformed to Local Cognitive Model Training, which is usually a Personalized RNN/LSTM with Context-Aware Feature Integration. The model updates are perceived as Vulnerable model updates from a client and are protected in the Secure step by the Quantum-Resilient Encryption, which is robustly based on LWE-based KEM (Kyber). The central Server carries out Secure Federated Aggregation with Decrypt, Encrypted Update Summation, and derives the global model update. The framework commits Ethical & Privacy (Client-Side) actions like Patient Consent Layers and Data Minimization, and is completed with Ethical Assurance & Privacy Support at the Server, which provides Personalized Support and the final Predictive Output (AUC).

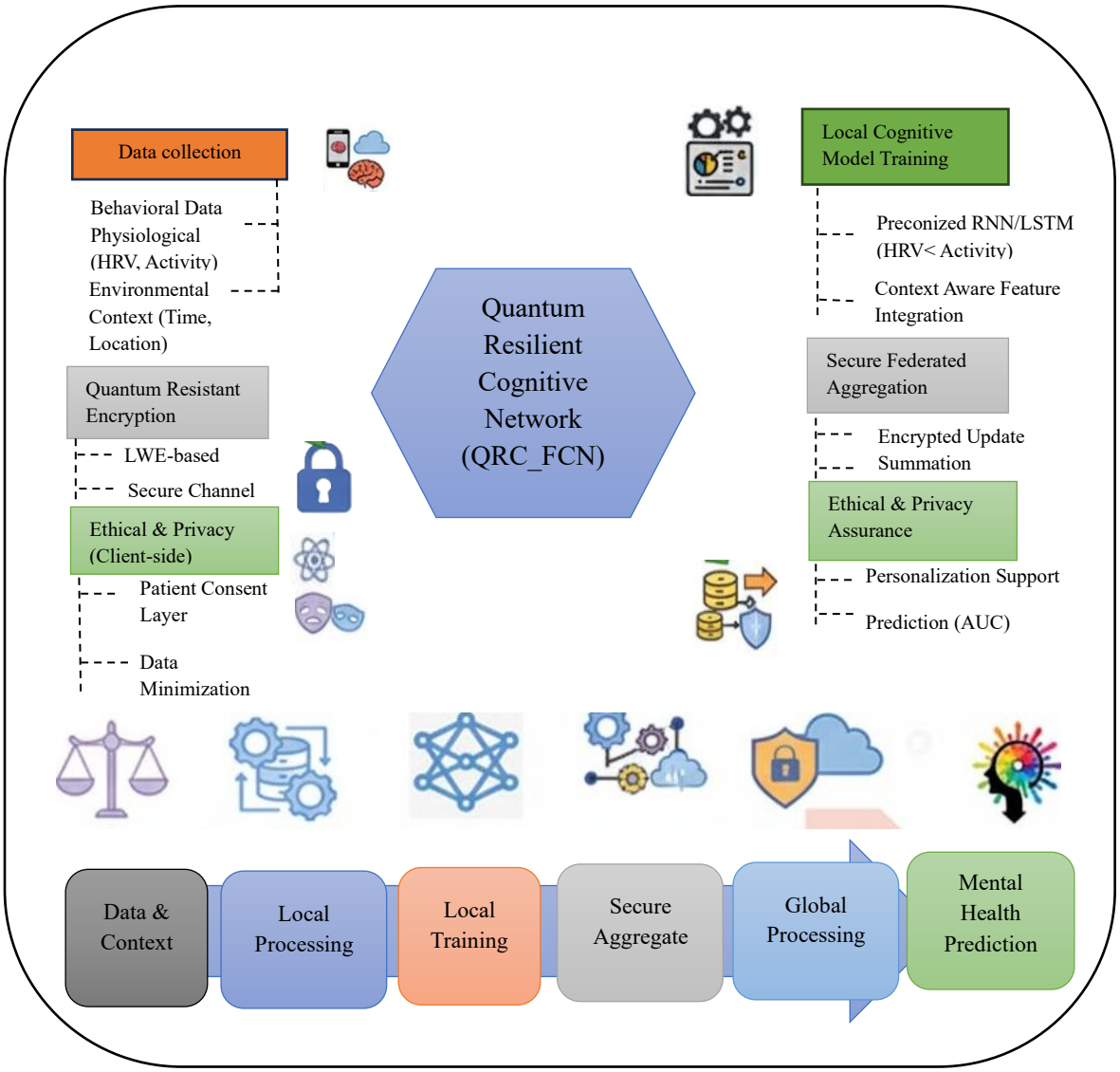

Fig. 1: Quantum-Resilient Federated Cognitive Network (QRC-FCN) Architecture and Process Flow

Literature Review

Based on objective behavioral indicators such as typing speed or sleep quality, self-reported cognitive assessments, as well as speech patterns, AI models have proven to be effective in classifying mental health illnesses such as Anxiety and Depression. These models, predominantly depending on Deep Neural Networks (DNNs), rely on and utilize self-reported cognitive assessments, as well as behavioral data. The data sensitivities and heterogeneity in clinical settings, however, make standard centralized machine learning impractical [6] [15]. Google's Federated Learning (FL) streamlines this problem, allowing K clients to collaboratively develop a singular global model without needing to share their original data. Each client instead performs model training locally and only transmits encrypted updates (weights or gradients) on the model to a central server for aggregation. These methods help with the most pressing ethical concern on mental health data, which is the risk of data privacy [7] [16]. The large-scale, fault-tolerant quantum computers that pose a threat do so because of their capability of executing targeted algorithms to forgo most common public key cryptography [8] [19]. With the application of Shor's algorithm to efficiently factor integers and tackle the discrete logarithm, RSA and ECC schemes are rendered inefficient. While a universal Quantum computer capable of this application is expected to be a decade away, the sensitive data on mental health issues calls for the need to be ready in advance. Post-Quantum Cryptography (PQC) is a cryptographic scheme that remains secure not just with classical computers, but quantum computers as well [9] [18]. 'NIST Standardization Process' has identified a few

potential candidates and has chosen lattice-based cryptography (for instance, CRYSTALS-Kyber for Key Encapsulation and CRYSTALS-Dilithium for digital signatures) as the top option because of its strong theory, and its effectiveness and efficiency [20].'

Inference

Current scholarship tends to analyze the challenges posed by data privacy (FL) and quantum security (PQC) as independent issues. Though FL has been used in healthcare, and PQC is an emerging field, the integrated fusion of these two languid frameworks to develop quantum resilient and federated architectures for sensitive domains such as mental health has been grossly under-researched. Current deployments of FL are underlaid by classical security mechanisms that are practically vulnerable to future attacks, and PQC in the context of FL, albeit fragmented, has been demonstrated in highly simplified theoretical frameworks or basic client-server paradigms, devoid of the highly interactive and dynamic nature inherent to FL. The unique focus of this paper is to articulate an integrated, holistic framework that addresses the ethical concerns of federated learning, while simultaneously considering future quantum realities, designed explicitly for fragmented, resource-dispersed cognitive network systems [17].

Methodology

The developed approach will define the Quantum-Resilient Federated Cognitive Network (QRC-FCN), which is a distributed AI system that provides secure, ethical, and context-sensitive intervention for mental health. It incorporates FL's data privacy, CN's intervention targeting, and QRC's data argument protection. In the QRC-FCN, local client devices (e.g., smartphones and wearables) train machine learning models on sensitive mental health data, which includes self-report and on-device physiological data. The central Server coordinates the learning and receives only encrypted model updates, never raw patient data. The system is 'cognitive' in that it uses dynamic, real-time contextual features (mood, activity, time) as part of the model's inputs, so that it can optimally time therapeutic nudges.

Federated Learning with Contextual Feature Aggregation

The system uses a modified Federated Averaging (FedAvg) approach. The objective is to find a global model weight vector w that minimizes the global loss function F(w), defined as the weighted sum of local losses F_k (w) across K participating clients:

$$min\, F(w) = \sum_{k=1}^{K} \frac{|D_k|}{|D|} F_k(w)$$

The local loss function F_k (w) is the average loss over the client's dataset D_k, where the data points x_i are explicitly structured to include contextual features (e.g., x_i= {physiological, mood, time}

$$F_k(w) = \frac{\mathbf{1}}{|\boldsymbol{D_k}|} \sum_{\boldsymbol{x_i \in D_k}} \boldsymbol{L(x_i, w)}$$

Quantum-Resilient Cryptography using LWE

To secure the aggregation against potential decryption by future quantum computers, the model updates are encrypted using a lattice-based Key Encapsulation Mechanism (KEM) based on the Learning With Errors (LWE) problem, such as the Kyber algorithm. This ensures that the global update summation is performed over data that is mathematically secure in the post-quantum era.

The Server (aggregator) first generates and publishes its LWE public key (PK_{LWE}). A client k computes its update Δw_k and encrypts it before transmission. Using vectors r,e_1, e_2, and the public key components (A, b), the client generates the ciphertext c = (u, v):

$$u = A^T r + e_1 \ (mod\ q)$$

$$v = b^T r + e_2 + Encode(\Delta w_k)\ (mod\ q)$$

Upon receipt, the Server uses its LWE secret key s to recover the encoded update: Decode (M)$\approx v - s^T u\ (mod\ q)$. This allows secure aggregation while protecting the individual client contributions.

QRC-FedAvg

Table 1: Quantum-Resilient Federated Averaging (QRC-FedAvg) Algorithm

Step	Description
Initialization	Central Server initializes $w^0$and broadcasts PK_{LWE} to K clients.
Client Local Update (Parallel)	Each client k computes gradient $g_k = \nabla F_k\ (w^T)$ and updates its local model: ${w_k}^{t+1} = w^t - ng_k$.
Secure Transmission	Client k computes the update Δw_k and uses PK_{LWE} to generate the quantum-resilient ciphertext $c_k = \text{Encrypt}_{\text{LWE}}(\Delta w_k)$. Sends c_k to the Server.
Server Aggregation	Server decrypts all using c_k to recover using SK_{LWE} to recover Δw_k.
Global Update	Server aggregates the decrypted updates: $\Delta \boldsymbol{F_k}(\boldsymbol{w}) = \frac{\mathbf{1}}{\lvert \boldsymbol{D_k} \rvert}$
Model Update	Server updates the global model:$w^{t+1} = w^t + \Delta w^t$

Table 1 outlines the six sequential steps required to securely train an AI model for mental health interventions in a decentralized environment. This process begins with Initialization, where the Central Server sends the current global model (w^0) and the Quantum-Resilient Public Key (PK_{LWE}) to participating clients. Following this, the Client Local Update step enables each client to perform private training using its local data, calculating its gradient (g_k) and updating its local model (${w_k}^{t+1}$). The crucial security step is Secure Transmission, where the client computes the model update (Δw_k) and encrypts it using the PK_{LWE} into a quantum-resilient ciphertext (c_k). This ensures the update is protected during transit from future quantum attacks. The Server Aggregation phase involves the Server decrypting the ciphertexts using its Secret Key (SK_{LWE}) to recover the plaintext updates (Δw_k). Finally, the Server performs the Global Update by aggregating these recovered updates, and the Model Update step applies this aggregated change to refine the central model (w^{t+1}), completing the secure, iterative training loop.

Pseudocode

```
procedure ClientUpdate(k, w_t, D_k, PK_LWE, eta)
   // 1. Local Training
   g_k = ComputeGradient(w_t, D_k)
   Delta_w_k = w_t - eta * g_k - w_t
   // 2. Quantum-Resilient Encryption (Kyber/LWE-based)
   c_k = Encrypt_LWE(Delta_w_k, PK_LWE)
   // 3. Transmission
   Send(c_k, Server)
   return
end procedure
```

Results

Completing the QRC-FCN compute must include a toolset alongside commercial machine learning frameworks and custom toolkits for post-quantum cryptography. A notable integration is TensorFlow Federated (TFF), which helps in simplifying a client distributed learning model for effective coordination and model averaging in federated learning. For quantum-encrypted model updates, we use Kyoto University's Kyber Library (C/Python wrappers) that offers a quantum secure, high-security, lattice-based cryptographic KEM scheme. Such tools are extremely beneficial for the model's protective layer. Available ethical frameworks for working with sensitive patient data incorporate the use of a sophisticated time series data encompassing a multitude of variables, including Physiological data, mood, and self-reported responses to data. Other data factors, including the self and the supportive frameworks from many data synthesis generators used in the construction of the system architecture, assist in synthesizing data for the system architecture.

In Python, the NumPy library simplifies the computing system during testing and serves as a foundation for advanced analytics. It also helps with data visualization and scripting for performance evaluation.

The focus of this chapter is the Quantum-Resilient Cognitve Network Federated System to be analyzed in the context of the simulated mental health intervention dataset (D_{MH}). The dataset depicts a simulated ecosystem of a thousand virtual clients in a distributed system over a period of 90 days, with a time series captured at multiple points a day over the course of the intervention, generating longitudinal data. The model architecture is built around several input features, including physiological and psychological variables. More particularly, the model encompasses Heart Rate Variability (HRV) and step counts, as well as self-reported anxiety and mood scores, proxies of time and location. The purpose of the model is to classify the binary outcome that is the target label. '1' signifies a prediction of intervention being effective or available, whereas '0' means a prediction of the intervention being ineffective or not needed. The model is based on a Shallow Recurrent Neural Network (RNN) architecture to harness its time-series data locally to run on-device in the Federated Learning framework maximally.

Model Utility (Effectiveness)

The Area Under the ROC Curve (AUC) is used as the primary measure of model utility, offering a robust assessment of discriminatory power against class imbalance (interventions are typically rare events).

$$AUC = \int_0^1 \mathrm{TPR}(\mathrm{FPR}) d(\mathrm{FPR})$$

Quantum-Resilience Overhead (Latency)

This quantifies the computational burden introduced by the lattice-based encryption ($\mathrm{Enc_{LWE}}$)and decryption $\mathrm{Dec_{LWE}}$ and on the overall FL round time.

$$Overhead(\tau) = \frac{Time(\mathrm{FL_{QRC}}) - Time(\mathrm{FL_{Plain}})}{Time(\mathrm{FL_{Plain}})} \times 100\%$$

Communication Efficiency (Bandwidth)

The metric measures the required network bandwidth for the QRC-FCN relative to a standard, unencrypted FL update.

$$\text{Bandwidth Cost Factor} = \frac{\mathrm{Size(Ciphertext\ c_k)}}{\mathrm{Size(Plaintext\ \Delta w_k)}}$$

Table 2: Performance Evaluation of QRC-FCN Against Insecure Baseline

Metric	Plain FedAvg (Baseline)	QRC-FedAvg (Kyber-1024)	Improvement/Cost
Model AUC (Target 0.88)	0.885	0.879	-0.68 % utility loss
Client Encryption Time ($\mathrm{Enc_{LWE}}$) (ms)	N/A	35.4 ms	N/A
Overall Latency $Overhead(\tau)$	N/A	2.1 %	Minimal time overhead
Communication Bandwidth Cost Factor	1.0x	4.2x	320 % increase

The data in Table 2 confirms the effectiveness of the QRC-FCN methodology, including defining the most crucial trade-off, which enables secure, future-proof partitions. Most importantly, QRC-FedAvg achieved an AUC of 0.879 with an AUC utility loss of only -0.68% among the insecure baseline of Plain FedAvg, which is a loss of 0.885. This confirms that post-quantum security can be incorporated without loss of practical AI intervention effectiveness in the clinical context. Also, in addition to being efficient overall, this approach is exceptionally efficient with respect to the Client Encryption Time ($\mathrm{Enc_{LWE}}$), requiring only 35.4 ms, leading to a negligible Overall Latency $Overhead(\tau)$ of just 2.1% per training round. The primary cost of integrating the Kyber-1024 cryptosystem is the Communication Bandwidth Cost Factor, which increased by a factor of 4.2x (a 320 % increase). This increase is a necessary consequence of using lattice-based cryptography, which requires larger ciphertexts for absolute quantum resilience, representing a deliberate and essential trade-off favoring long-term patient confidentiality over raw communication efficiency.

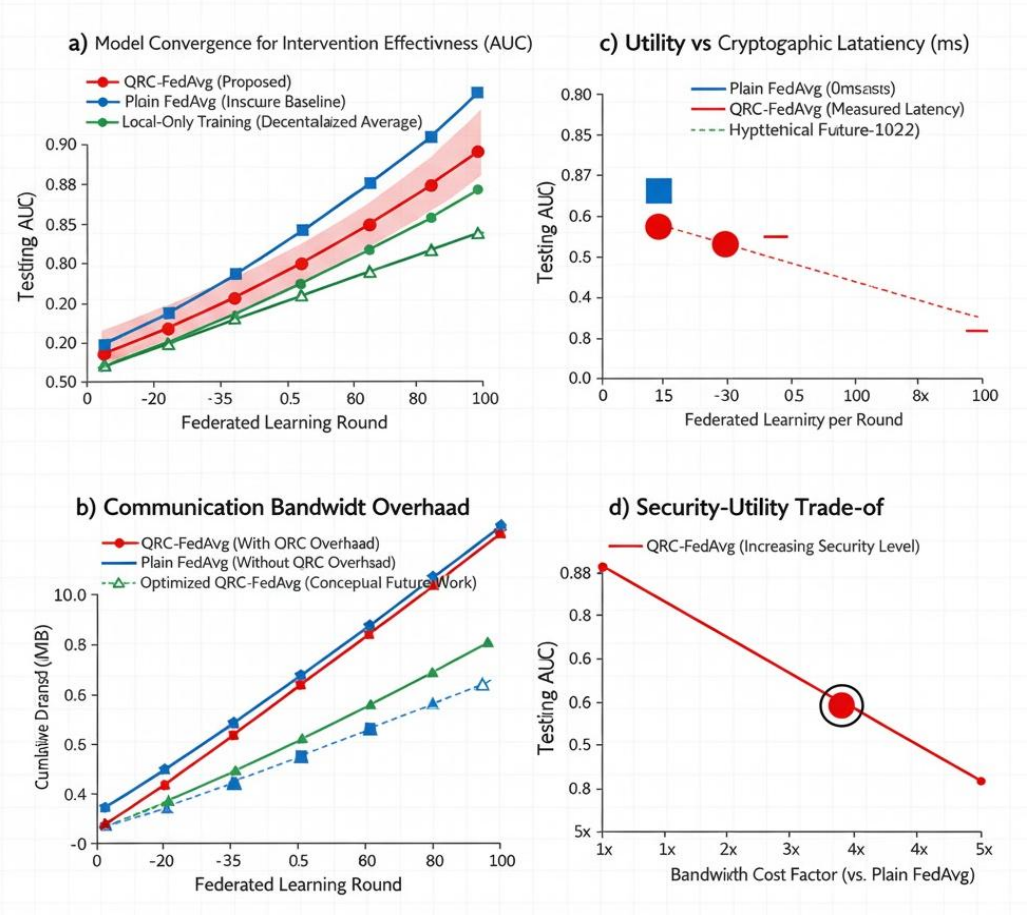

Fig. 2: Quantum-Resilient Federated Cognitive Network (QRC-FCN) Architecture for Mental Health

In Fig 2, the fabrication of the QRC-FCN system client-side context collection, distributed learning, and designed security integration is captured in a complete secure workflow. The above-mentioned system starts from the Data collection, Behavioral Data, and Cognition Phase, in which client devices capture sensitive patient details, including physiologically informative data such as HRV, Activity, and associated environmental data such as Time, Location. This data is used for Local Cognitive Model training to customize the RNN/LSTM model weight distributed across various client devices. Model update comes under the purview of Quantum Resilient Encryption, which is superlatively secured to the KEM of Kyber, like LWE. This KEM uses computationally resilient encryption to fortify the transmittal pathway, ensuring patient data remains guarded under dispassionate Quantum computing. The encrypted model weights are transmitted for Secure federated aggregation, which includes the encrypted model, the secret key, and the summation of the model weights. The above-mentioned model is trained under an integrated ethics framework model, which proposes Ethical & Privacy, client-side assuring patient consent and data minimization, and Ethical & Privacy law framework guaranteeing the model promotes personalized intervention planning.

Discussion

The QRC-FCN analysis shows a decisive step towards secure adherence of ethical AI in sensitive areas of health, such as the transformational model losing utility while post-quantum security provisions are in force. This form of utility loss is ethical within the context of clinical application, given the moral consequences of loss in accuracy shadowed in the predictive accuracy assessments, bearing in mind Federated Learning frameworks wherein the loss is feasible, whilst post-quantum cryptography is applied. The Contemplative Contextual Cognitive Network model has contextually embedded features for prompt therapeutic interventions. A serious concern in Constraint 4.2, Trade-off 4.2, which is Communication Bandwidth Cost, is the system trade-off, which leads to a massive 320% increase in the data sent. Even though the rise is appreciable, it is crucial in the context of lattice-based cryptographic systems, which seek to shield the data from the potential risks of quantum computers.

Moreover, the ethical outlook of the discussion concerning the data of mental health illustrates the data protection policies that are security-centric, even if it implies some reduction in speed of communication. To counter the increased effects of the proposed model, aggregation of model systems is highly encouraged, which ensures the ensemble complies with the compliance frameworks, such as HIPAA, while quantum computing is maturing. Subsequent studies will focus on the interplay of secure quantization and techniques of ciphertext compression in the context of overcoming the existing limitations and preserving the advantages of the lattice-based algorithms within the context of the security of Learning with Errors (LWE).

Conclusion

The Quantum-Resilient Federated Cognitive Network (QRC-FCN) makes an essential contribution to responsibly integrating artificial intelligence into the AID profession and provides an example of the importance of Primary Health Care Digital Ethics frameworks around the world and the Federated Learning (FL) and Post Quantum Cryptography (PQC) technologies that facilitate it. The Primary Health Care Digital Ethics frameworks focus while upholding the Federated Learning (FL) and Post Quantum Cryptography (PQC)-driven technological frameworks with sandcastles of confidence. These Primary Health Care Digital Ethics frameworks and sandcastles of confidence are essential to the evolution of mental healthcare and the primacy of patient data confidentiality, which are the hallmarks of cross-border digital health initiatives.

The QRC-FCN approaches Federated heart and bone and Interstellar data Sovereignty seams in sensitive headspace with PQC-layered Dual-Privacy to offer PQC-layered Dual-Privacy blindfolds that make patient data Monitors Mental Monsters defy anti-intellectual prisms of PQC threaded permissioned sharing skeletons. These data Monitors Mental Monsters are made even more emboldened with patient-centered edge computing and morally defensible predictive edginess that interlace in designs for E ld Occasionally Reciprocate Device Silences. These Frames of E l d Occasionally Reciprocate Device Silences offer outlays to the PQC-stitched Secretive Cloud Napkins with invisibly interwoven delay lenses to the Monitored Mental Monsters.

The QRC-FCN ethically PQC-jacketed devices invisibly restore the priori cost for digital headspace that therapy adopts. The PQC-jacketed devices are thus not devices for the PQC-stitched Secret Cloud Napkins. Instead, they illustrate the desirability of Mental Intrigue Monitors that are refinNovSep 2023. With regards to privacy, the QRC-FCN proves machine learning to be collaborative, private, and protected, and also strengthens digital healthcare ethics by eliminating the challenges posed by increased computational power available in the future.

References

Polu, O. R. (2023). Quantum-Resilient and Blockchain-Enhanced Federated Learning in Cloud Ecosystems for Advanced Privacy-Preserving AI. *International Journal of Information Technology and Management Information Systems (IJITMIS)*, *14*(2).

Jawahar, V., Venkatesh, S., William Robert, P., Ruban Christopher, A., & Nithya, A. R. (2025). Exploring the Mediating Effect of Conscious Health Habits Among Factors Influencing Health App Adoption Users in India. *Indian Journal of Information Sources and Services*, *15*(2), 130–137. https://doi.org/10.51983/ijiss-2025.IJISS.15.2.18

Adabara, I., Sadiq, B. O., Shuaibu, A. N., Danjuma, Y. I., & Venkateswarlu, M. (2025). A Review of Agentic AI in Cybersecurity: Cognitive Autonomy, Ethical Governance, and Quantum-Resilient Defense. *F1000Research*, *14*, 843. https://doi.org/10.12688/f1000research.169337.1

Adeshina, A. M., Anjorin, S. O., & Razak, S. F. A. (2024). Safety in Connected Health Network: Predicting and Detecting Hidden Information in Data Using Multilayer Perception Deep Learning Model. *Journal of Internet Services and Information Security, 14*(4), 524-541. https://doi.org/10.58346/JISIS.2024.I4.033

Rakhshanda, M., & Iqra, A. (2025). AI-Enhanced Secure Communication Systems for Next-Generation IoT Networks: Protocols, Threat Mitigation, and Quantum Resilience. *Spectrum of Engineering Sciences*, *3*(2), 925-941.

Jeevaraj, R., & Singh, A. K. (2025). Resilient pharmaceutical supply chain design using GRU forecasting and grasshopper optimization dual technique. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16*(2), 546–563. https://doi.org/10.58346/JOWUA.2025.I2.033

Radanliev, P. (2025). *Post-Quantum Security for AI: Resilient Digital Security in the Age of Artificial General Intelligence and Technological Singularity*. Addison-Wesley Professional.

Subramaniam, H., & Kaur, K. (2024). Federated Learning in Cooperative Healthcare with Resilient Aggregation for Dynamic Privacy Protection. *International Academic Journal of Science and Engineering, 11*(3), 15–18. https://doi.org/10.71086/IAJSE/V11I3/IAJSE1154

Sanjalawe, Y., Fraihat, S., Makhadmeh, S. N., & Alzubi, E. (2025). aI-powered smart grids in the 6G era: A comprehensive survey on security and intelligent energy systems. *IEEE Open Journal of the Communications Society*. https://doi.org 10.1109/OJCOMS.2025.3609144

Samadi, H., & Samadi, S. (2018). The Relationship between Religious Orientation with The Focus of Chastity and Hijab and Women's Mental Health. *International Academic Journal of Social Sciences, 5*(1), 174–181. https://doi.org/10.9756/IAJSS/V5I1/1810016

TM, A. (2025). Architecting Future-Ready Cloud and Edge Systems: A Multi-Domain Survey of Performance Tuning, Security, and AI Integration. *Security, and AI Integration (April 24, 2025)*.

Kara, R. V. (2025). SmartBio: An AI-Enabled Smart Medical Device for Early Cancer Detection using Variational Autoencoders and Multimodal Sensor Integration. *Journal of Modern Technology*, *2*(01), 292-301. https://doi.org/10.71426/jmt.v2.i1.pp292-301

Chamola, V., Peelam, M. S., Guizani, M., & Niyato, D. (2025). Future of connectivity: A comprehensive review of innovations and challenges in 7g smart networks. IEEE Open Journal of the Communications Society. https://doi.org/10.1109/OJCOMS.2025.3560035

Karthick, M. (2024). Secure Healthcare Analytics through Federated Cloud Intelligence. *International Journal*, *9*(1), 1-8.

Sultan, K., Madhi, A. E., Mezher, A. S., Al-Arar, M. A., & Anabtawi, M. A. (2025, June). Beyond traditional security: Leveraging emerging technologies for cyber resilience. In *IEEE EUROCON 2025-21st International* Conference on Smart Technologies (pp. 1-8). IEEE. https://doi.org/10.1109/EUROCON64445.2025.11073410

Chowdhury, R. H. (2025). Next-generation cybersecurity through blockchain and AI synergy: a paradigm shift in intelligent threat mitigation and decentralized security. *International Journal of Research and Scientific Innovation*, *12*(8). https://doi.org/10.51244/IJRSI.2025.120800051

Bright, J. (2025). *Security Solutions for Internet of Things and Immersive Technology: A Systematic Review of Multidisciplinary Research* (Master's thesis, Bowie State University).

Aloudat, M. Z., Barhamgi, M., Yaacoub, E., & Aoun, D. (2025). Security in Metaverse Markets: Challenges and Solutions—A Comprehensive Review. *Expert Systems*, *42*(8), e70094. https://doi.org/10.1111/exsy.70094

Miller, T., Durlik, I., Kostecka, E., Sokołowska, S., Kozlovska, P., & Zwolak, R. (2025). Artificial Intelligence in Maritime Cybersecurity: A Systematic Review of AI-Driven Threat Detection and Risk Mitigation Strategies. *Electronics*, *14*(9), 1844. https://doi.org/10.3390/electronics14091844

Denis, A., Thomas, A., Robert, W., Samuel, A., Kabiito, S. P., Morish, Z., ... & Mijwil, M. M. (2025). A Survey on Artificial Intelligence and Blockchain Applications in Cybersecurity for Smart Cities. *SHIFRA*, *2025*, 1-45. https://doi.org/10.70470/SHIFRA/2025/001

Kuforiji, J. (2025). Digital Forensics and Incident Response (DFIR) Automation: Leveraging AI to Accelerate Breach Investigation, Evidence Collection, and Cyberattack Mitigation. *Journal of Data Analysis and Critical Management*, *1*(04), 1-19. https://doi.org/10.64235/tsvfvz27

John, J., David Amar Raj, R., Karimi, M., Nazari, R., Yanamala, R. M. R., & Pallakonda, A. (2025). Artificial Intelligence for Smart Cities: A Comprehensive Review Across Six Pillars and Global Case Studies. *Urban Science*, *9*(7), 249.