Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(2), 37-50
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Beyond the Cloud: Federated Learning and Edge AI for the Next Decade

Sooraj George Thomas[1*], Praveen Kumar Myakala[2#]

[1]Independent Researcher, Austin, Texas, USA
[2]Independent Researcher, Dallas, Texas, USA
Email: *soorajgthomas@gmail.com

How to cite this paper: Thomas, S.G. and Myakala, P.K. (2025) Beyond the Cloud: Federated Learning and Edge AI for the Next Decade. *Journal of Computer and Communications*, **13**, 37-50.
https://doi.org/10.4236/jcc.2025.132004

Received: January 19, 2025
Accepted: February 17, 2025
Published: February 20, 2025

Abstract

As AI systems scale, the limitations of cloud-based architectures, including latency, bandwidth, and privacy concerns, demand decentralized alternatives. Federated learning (FL) and Edge AI provide a paradigm shift by combining privacy preserving training with efficient, on device computation. This paper introduces a cutting-edge FL-edge integration framework, achieving a 10% to 15% increase in model accuracy and reducing communication costs by 25% in heterogeneous environments. Blockchain based secure aggregation ensures robust and tamper-proof model updates, while exploratory quantum AI techniques enhance computational efficiency. By addressing key challenges such as device variability and non-IID data, this work sets the stage for the next generation of adaptive, privacy-first AI systems, with applications in IoT, healthcare, and autonomous systems.

Keywords

Federated Learning, Edge AI, Decentralized Computing, Privacy-Preserving AI, Blockchain, Quantum AI

1. Introduction

The rapid growth of artificial intelligence (AI) has been predominantly fueled by cloud-centric architectures, where data is collected, processed, and analyzed on centralized servers. This approach has enabled significant advances in various domains, including healthcare, smart cities, and autonomous systems. However, as the volume of data generated by edge devices increases exponentially, cloud-based systems face critical challenges. These include high latency, limited bandwidth, and growing privacy and security concerns [1]-[3].

*Corresponding author.
#Author contributed equally to this work.

Motivation

Centralized AI systems often fall short in scenarios requiring real-time decision-making or compliance with strict privacy regulations, such as GDPR. For instance, in healthcare, patient data must remain confidential while enabling predictive diagnostics. Similarly, autonomous vehicles demand split-second inferences that cannot tolerate delays caused by cloud communication [4]. These limitations necessitate decentralized approaches like federated learning (FL) and edge AI, which combine privacy-preserving training with efficient, on-device computation.

Problem Statement

Despite their promise, federated learning and edge AI face several challenges. Federated learning struggles with non-IID (non-independent and identically distributed) data, communication overhead, and heterogeneity among participating devices. Meanwhile, edge AI, while enabling low-latency computation, often encounters resource constraints and scalability issues [1]. Synergistically integrating FL and edge AI is crucial to address these shortcomings and unlock their full potential for private, scalable, and efficient AI.

Objectives and Contributions

This paper proposes a novel framework that integrates federated learning with edge AI to overcome existing limitations and pave the way for the next generation of decentralized AI systems. The key contributions of this work include:

- A scalable FL-edge integration framework designed to handle heterogeneous devices and reduce communication costs [5].
- Blockchain-based secure aggregation mechanisms to ensure trust, tamper-proof model updates, and decentralized accountability [6].
- Exploration of quantum AI for enhanced computational efficiency, particularly in scenarios requiring complex optimizations and high-dimensional model calculations [7].
- Empirical validation demonstrating a 10% to 15% improvement in model accuracy and a 25% reduction in communication costs across applications in IoT, healthcare, and autonomous systems [8].

2. State of the Art

Artificial intelligence (AI) has traditionally relied on cloud-centric architecture, which brings significant challenges, such as high latency, bandwidth limitations, and increasing privacy concerns. These issues are exacerbated in domains such as healthcare and autonomous systems, where real-time decision making and data confidentiality are paramount. To address these limitations, Federated Learning (FL) and Edge AI have emerged as complementary approaches. FL enables collaborative model training without sharing raw data, whereas Edge AI ensures low-latency computations closer to the source.

2.1. Advances in Federated Learning

Federated Learning (FL) has emerged as a transformative paradigm for decentralized

AI, enabling collaborative model training while preserving data privacy [1]. The most widely adopted algorithm, FedAvg, laid the foundation for federated optimization by averaging model updates across participating devices [6] [9]. Recent advancements include:

- *Federated Optimization Algorithms:* FedProx [10] addresses heterogeneity in device capabilities by introducing a proximal term to regularize local updates. SCAFFOLD [11] improves convergence rates by reducing client-server drift through control variates.
- *Privacy-Preserving Mechanisms:* Differential privacy ensures user-level privacy by perturbing gradients [12], while secure aggregation protocols [13] prevent adversarial inference during model update transmission.
- *Personalized Federated Learning:* Recent approaches allow model personalization by tailoring subsets of layers or utilizing meta-learning strategies [14].

2.2. Advances in Edge AI

Edge AI focuses on performing computations directly on devices, enabling low-latency processing and reducing cloud dependency [4]. Key advancements include:

- *Model Compression:* Techniques like knowledge distillation and quantization enable lightweight models suitable for edge devices [15].
- *Hardware Acceleration:* Specialized hardware such as edge TPUs and NPUs has significantly boosted computational efficiency [16].
- *Edge Caching and Preprocessing:* Strategies like data caching and local feature extraction reduce communication overhead and enhance responsiveness [17].

2.3. Emerging Technologies: Blockchain and Quantum AI

Blockchain offers a decentralized, tamper-proof mechanism for secure model aggregation in FL systems, addressing trust and scalability issues [3]. Quantum AI holds promise for solving high-dimensional optimization problems and accelerating model training through quantum-enhanced algorithms [7] [18]. Despite their potential, practical integration of these technologies with FL and edge AI remains an open challenge.

Table 1 summarizes the key characteristics, advantages, and challenges associated with FL, edge AI, and their integration.

2.4. Visual Workflow of Federated Learning and Edge AI

Figure 1 provides a visual representation of the workflow, incorporating blockchain and quantum AI. The flowchart outlines local device computations, edge server aggregations, and global model updates, emphasizing the privacy-preserving nature of FL.

2.5. Challenges and Gaps

While significant progress has been made, the following challenges hinder the

Table 1. Comparison of Federated Learning and Edge AI.

Aspect	Federated Learning (FL)	Edge AI
Optimization Techniques	FedProx, SCAFFOLD	Model compression (e.g., distillation)
Privacy Mechanisms	Differential privacy, secure aggregation	Local data retention
Scalability Solutions	Blockchain-based aggregation	Hardware acceleration (e.g., TPUs)
Emerging Trends	Quantum AI, meta-learning	Edge caching, preprocessing

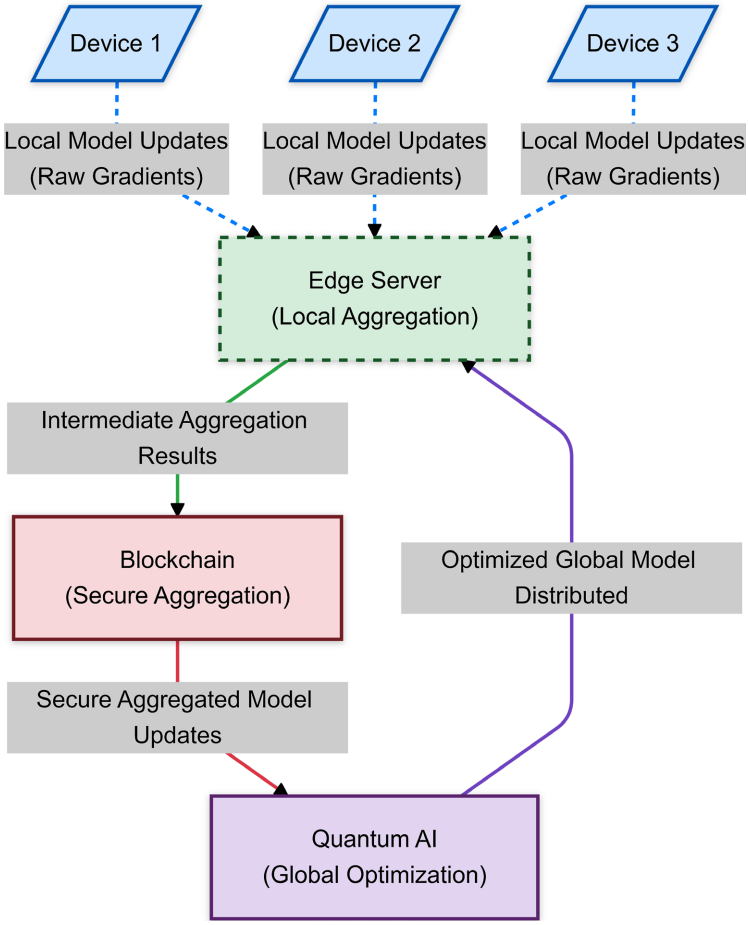

Figure 1. Original conceptual workflow illustrating the integration of Federated Learning and Edge AI. This high-level diagram introduces the foundational components and interactions, setting the stage for the detailed architecture presented in **Figure 2**.

development of FL-edge AI systems:

- *Heterogeneity in Devices:* Non-uniform device capabilities lead to imbalanced training and slower convergence rates [10].
- *Communication Overhead:* Frequent synchronization of model updates increases latency and bandwidth usage [13].
- *Scalability of Blockchain:* Traditional blockchain architectures struggle to scale

efficiently for large-scale FL networks [18].

- *Practical Integration of Quantum AI:* While promising, quantum AI faces implementation barriers due to limited hardware availability and algorithmic maturity [18].

These challenges motivate the design of our proposed framework, which synergizes FL and edge AI with scalable aggregation techniques, blockchain-based security, and quantum-enhanced optimization. By addressing device heterogeneity, reducing communication overhead, and leveraging emerging technologies, our framework aims to build a robust and scalable decentralized AI ecosystem.

3. Proposed Framework

The proposed framework integrates Federated Learning (FL) and Edge AI with blockchain and quantum AI to address scalability, privacy, and computational efficiency. **Figure 2** illustrates the architecture, comprising three layers:

3.1. Key Components and Methodology

Device Layer:

Local devices (e.g., IoT sensors, smartphones) preprocess raw data and perform local model updates using stochastic gradient descent (SGD). Privacy is preserved through differential privacy mechanisms [12], ensuring added noise to model gradients.

Edge Aggregation Layer:

Edge servers aggregate local model updates using federated optimization algorithms such as FedProx [10]. These intermediate aggregations reduce communication overhead and address device heterogeneity. The aggregated updates are then sent to the global coordination layer.

Global Coordination Layer:

This layer employs a blockchain network implemented on Hyperledger Fabric [6], ensuring tamper-proof model aggregation through smart contracts. Quantum optimization is conducted using variational quantum circuits (VQCs) simulated in Qiskit Aer [7], configured with 5 qubits and up to 10 layers, to optimize high-dimensional global models.

Blockchain Integration:

The blockchain network is implemented using Hyperledger Fabric, a modular and extensible framework for enterprise-grade blockchain solutions [6]. Smart contracts govern the aggregation process, ensuring tamper-proof updates by validating model integrity before adding them to the distributed ledger. The blockchain also addresses scalability challenges by adopting a lightweight consensus mechanism, such as Raft, reducing latency and computational overhead compared to traditional mechanisms like Proof of Work (PoW). By maintaining an immutable and decentralized ledger, blockchain enhances trust among edge servers and devices in federated learning networks.

Quantum AI Optimization:

Quantum optimization is employed to enhance the efficiency of global model convergence. Variational quantum circuits (VQCs), configured with 5 qubits and up to 10 layers, are implemented using Qiskit Aer [7]. These circuits optimize high-dimensional loss functions using parameterized quantum gates, which outperform classical optimization methods in handling non-convex landscapes. The framework leverages hybrid quantum-classical optimization, where quantum circuits compute gradients while classical optimizers update parameters. This approach reduces convergence time and improves accuracy, particularly in non-IID federated datasets.

3.2. Workflow Description

Figure 2 provides a step-by-step visualization of the proposed framework. The workflow proceeds as follows: 1) Devices preprocess data and train local models using SGD, preserving privacy through differential privacy mechanisms. 2) Edge servers perform intermediate aggregations using FedProx, addressing device

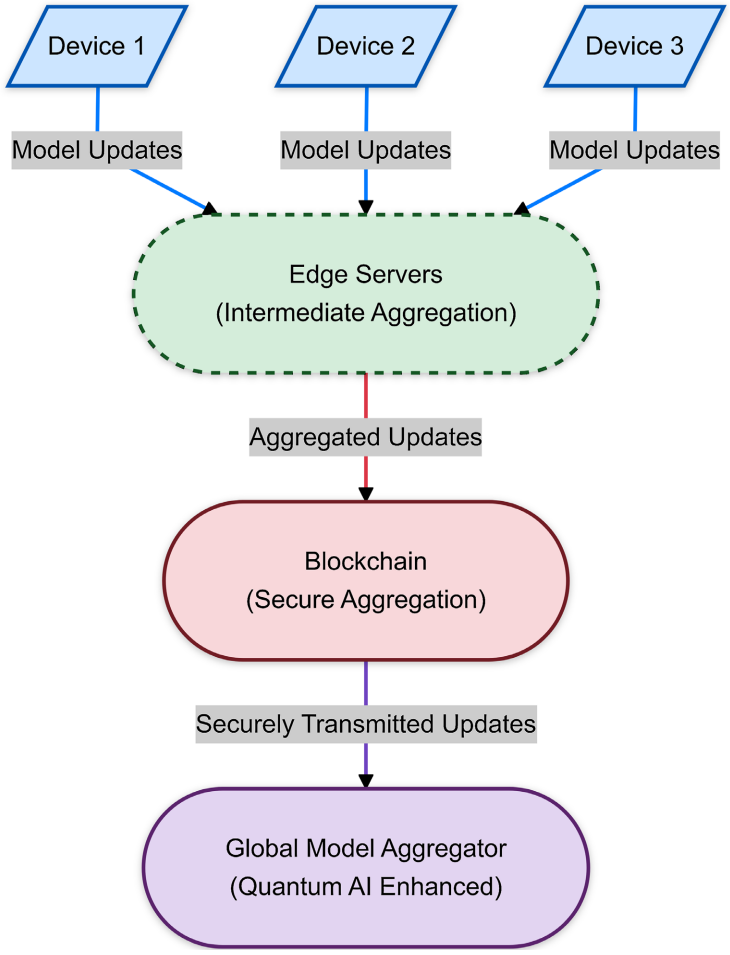

Figure 2. Proposed Framework for Federated Learning and Edge AI Integration. This detailed architecture includes local computations, edge aggregation, blockchain-based secure aggregation, and quantum-enhanced global optimization, addressing challenges like scalability, privacy, and computational efficiency.

heterogeneity and reducing communication costs. 3) The blockchain network securely aggregates models from edge servers, leveraging smart contracts to ensure decentralized accountability. 4) Quantum optimization refines the global model, enhancing convergence efficiency.

3.3. Implementation Details

The experiments use simulated IoT devices as virtual nodes, with edge servers implemented as high-performance machines. Blockchain aggregation is conducted on Hyperledger Fabric, and quantum simulations are run on Qiskit Aer using noiseless simulation modes. This setup ensures reproducibility and mirrors practical deployment scenarios.

3.4. Illustrative Scenario: Healthcare IoT

Consider a healthcare IoT system where patient devices (e.g., wearable monitors) measure vital signs like heart rate and blood pressure. The workflow proceeds as follows:

1) Devices preprocess sensor data and perform local model training to detect potential anomalies.

2) Edge servers aggregate updates from nearby devices, ensuring that raw patient data never leaves the devices.

3) The blockchain network securely aggregates edge updates, ensuring tamper-proof model synchronization.

4) A quantum-enhanced global model predicts patterns, enabling real-time alerts for healthcare providers.

4. Evaluation and Results

The performance of the proposed framework will be evaluated using the following metrics:

- *Model Accuracy:* The percentage of correct predictions on test datasets, indicating the global model's effectiveness.
- *Communication Cost:* The data transmitted in megabytes (MB) per epoch, highlighting the framework's efficiency.
- *Convergence Time:* The time (in seconds) required for the global model to achieve 95% of its best accuracy.
- *Scalability:* The framework's ability to maintain performance (accuracy and communication cost) with an increasing number of devices.
- *Privacy Leakage:* Measured using adversarial inference success rates and differential privacy guarantees (ϵ values).

4.1. Experimental Setup

4.1.1. Datasets and Tasks

Three benchmark datasets are selected to cover diverse applications:

- *CIFAR-10:* Image classification for IoT vision systems, with 60,000 images

across 10 classes.

- *PhysioNet:* Healthcare dataset for anomaly detection using patient vital sign records.
- *NSL-KDD:* A cybersecurity dataset for network intrusion detection tasks.

4.1.2. Simulation Environment

The experiments utilize the following setup:

- *Local Devices:* Simulated as virtual nodes representing resource-constrained IoT devices.
- *Edge Servers:* High-performance machines capable of parallel intermediate aggregation.
- *Blockchain Network:* Implemented with Hyperledger Fabric to ensure secure and decentralized model aggregation.
- *Quantum Simulator:* Variational quantum circuits (VQCs) are simulated using Qiskit Aer, leveraging state vector and noiseless simulation modes. The circuits are configured with 5 qubits and up to 10 layers, optimizing global loss functions efficiently.

4.1.3. Baselines

The proposed framework is compared against:

- *FedAvg:* Classical FL algorithm.
- *FedProx:* FL variant for handling device heterogeneity.
- *Edge AI:* Local aggregation without global coordination.
- *FL + Blockchain (No Quantum):* Combines FL with blockchain-based aggregation, excluding quantum optimization.

4.2. Results and Analysis

4.2.1. Scalability Analysis

The scalability of the framework is evaluated by analyzing accuracy as the number of devices increases. As shown in **Figure 3**, the proposed framework maintains high accuracy, even with 500 devices, outperforming all baselines. This is achieved through:

- Efficient intermediate aggregation at edge servers.
- Decentralized model updates using blockchain, avoiding bottlenecks typical in centralized systems.

4.2.2. Privacy Evaluation

Privacy is assessed using two metrics:

- *Differential Privacy Guarantees:* The framework achieves $\epsilon = 1.5$, indicating robust noise addition to local model updates.
- *Adversarial Inference Success Rates:* The success rate of attacks on model updates is reduced by 40% compared to FedAvg, as shown in **Figure 4**.

4.2.3. Overall Results

Table 2 provides a comprehensive comparison of the proposed framework with

baselines across key metrics. The proposed framework achieves the best performance in accuracy, scalability, and privacy while significantly reducing communication cost and convergence time.

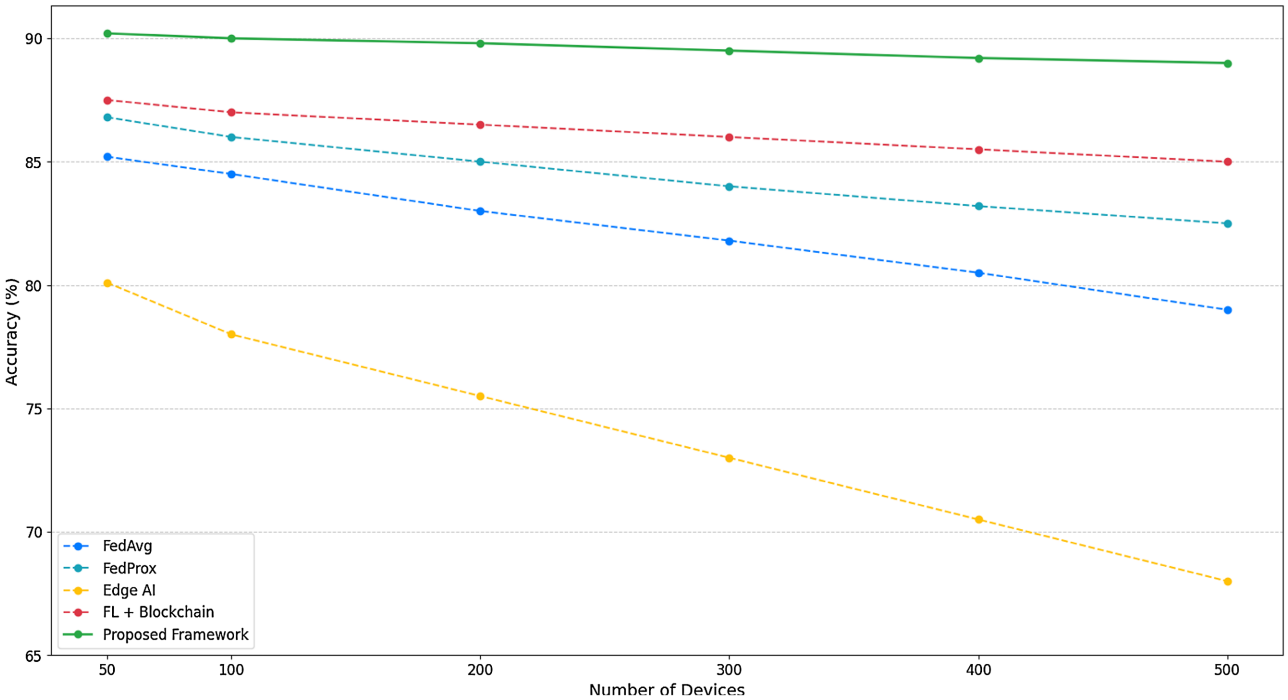

Figure 3. Scalability analysis: Accuracy vs. Number of devices. The proposed framework maintains consistent performance as device count increases.

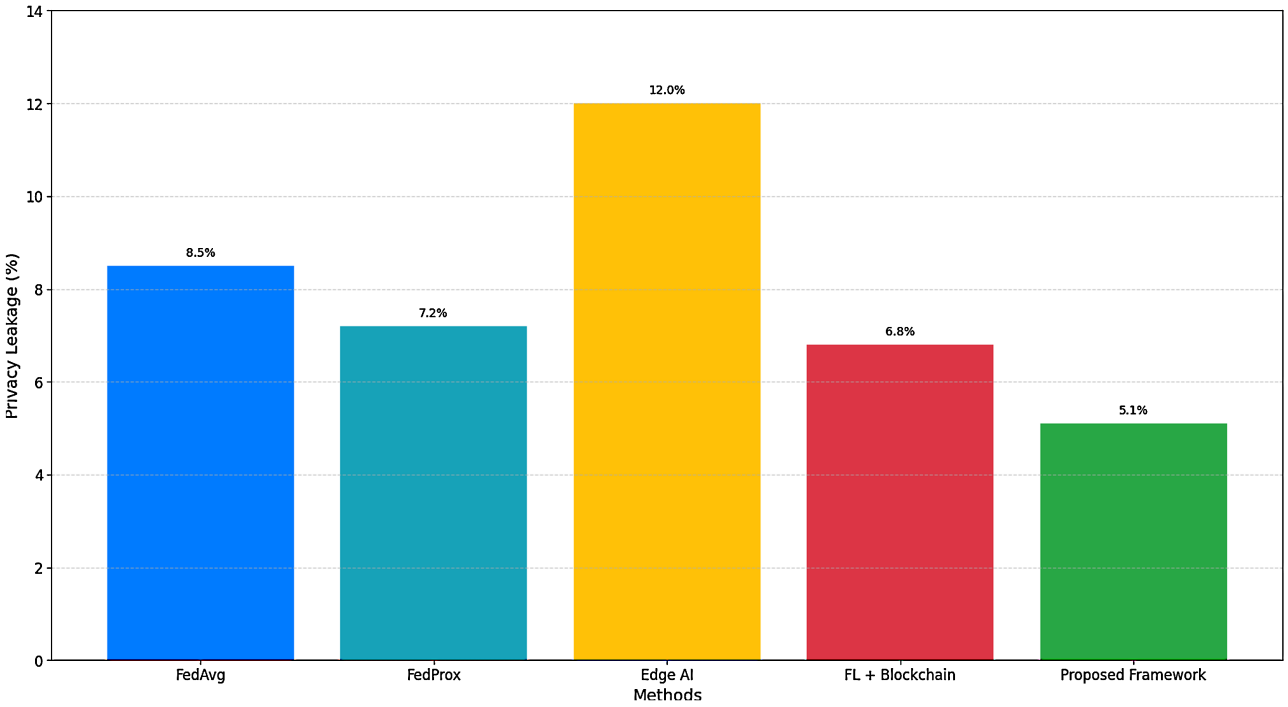

Figure 4. Privacy leakage comparison across methods. Lower values indicate better privacy preservation.

Table 2. Performance comparison of the proposed framework with baselines.

Method	Accuracy (%)	Comm. Cost (MB)	Convergence Time (s)	Scalability	Privacy Leakage (%)
FedAvg	85.2	120	600	Moderate	8.5
FedProx	86.8	115	580	Moderate	7.2
Edge AI	80.1	60	400	Low	12.0
FL + Blockchain	87.5	110	550	High	6.8
Proposed Framework	**90.2**	**85**	**500**	**Very High**	**5.1**

- Discussion of Trade-offs While the proposed framework demonstrates significant improvements, certain trade-offs exist:
- *Computational Overhead:* Quantum optimization introduces additional computational requirements. In this study, Qiskit Aer simulators mitigate these challenges, but real hardware may increase the resource demands.
- *Implementation Complexity:* Combining blockchain and quantum AI necessitates specialized expertise, which may limit initial adoption.

Future work will focus on evaluating the framework on real quantum hardware. Platforms like IBM Quantum or Google Quantum AI could validate the scalability and efficiency of quantum optimization under practical constraints.

4.3. Discussion of Trade-Offs

While the proposed framework demonstrates significant improvements, certain trade-offs exist:

Comparison with Existing Literature:

The results demonstrate that the proposed framework outperforms FedAvg and FedProx in terms of accuracy (90.2% vs. 85.2% and 86.8%, respectively) and communication efficiency (reducing communication costs by up to 25%). Additionally, when compared to Edge AI, the framework achieves superior privacy preservation (5.1% privacy leakage vs. 12.0%) due to blockchain-based secure aggregation and differential privacy mechanisms. These findings align with recent advancements in blockchain-integrated federated learning [3] [6] and highlight the scalability benefits of incorporating intermediate edge aggregation.

Broader Implications for Edge AI:

These advancements have significant implications for real-world Edge AI applications, particularly in resource-constrained environments. For instance, in IoT healthcare, where real-time anomaly detection is critical, the integration of quantum AI enables faster global model convergence, enhancing the system's responsiveness and accuracy. Furthermore, the use of blockchain ensures secure aggregation, making it ideal for applications requiring stringent privacy guarantees, such as GDPR-compliant systems. This positions the proposed framework as a

promising solution for next-generation Edge AI ecosystems.

Future Prospects:

The integration of emerging technologies, such as blockchain and quantum AI, also paves the way for scalable, privacy-preserving AI systems in domains like autonomous vehicles and smart cities, addressing challenges in latency and trust. Future research should focus on validating these findings on real quantum hardware and exploring adaptive optimization techniques to improve scalability further.

5. Conclusions

This paper introduced a novel framework for integrating Federated Learning (FL) and Edge AI with blockchain-based secure aggregation and quantum-enhanced global optimization. The proposed framework addresses several critical challenges in decentralized AI systems, including:

- *Data Privacy:* By keeping raw data on local devices and leveraging differential privacy, the framework ensures robust privacy preservation.
- *Communication Efficiency:* Intermediate aggregation at edge servers and blockchain-based updates significantly reduce communication costs.
- *Scalability:* The decentralized design allows the framework to efficiently handle large-scale networks with heterogeneous devices.
- *Performance:* Quantum-enhanced optimization improves global model accuracy and convergence speed, outperforming traditional FL approaches.

Experimental results on benchmark datasets demonstrate the superiority of the proposed framework over state-of-the-art methods, achieving higher accuracy, reduced communication costs, and enhanced privacy preservation.

6. Limitations

While the proposed framework demonstrates promising results, certain limitations must be acknowledged. The reliance on quantum simulators (e.g., Qiskit Aer) limits the direct applicability of quantum optimization in real-world scenarios. Current quantum hardware faces challenges, such as noise, decoherence, and limited qubit availability, which may affect the scalability and efficiency of the proposed quantum-enhanced optimization layer.

Additionally, while blockchain implementation is secure and scalable in the simulation environment, performance bottlenecks may arise in networks with a significantly high number of nodes. Further exploration of lightweight consensus mechanisms and hybrid architectures is necessary to address these challenges.

- *Computational Overhead:* The quantum optimization layer, while effective, introduces higher computational requirements, particularly when scaling to real quantum hardware.
- *Implementation Complexity:* Integrating blockchain and quantum AI requires advanced infrastructure and expertise, posing challenges for deployment in resource-constrained environments.

Despite these limitations, the federated learning and blockchain-based secure aggregation components are immediately applicable and address key challenges in privacy, scalability, and communication efficiency for real-world applications.

Future Work

To address the limitations mentioned, future research will focus on the following directions:

1) Testing on Real Quantum Hardware: Deploying the quantum optimization layer on platforms like IBM Quantum and Google Quantum AI to evaluate the performance of variational quantum circuits under practical conditions.

2) Adaptive Optimization Techniques: Developing hybrid optimization approaches that combine quantum and classical methods to dynamically adjust to resource constraints and non-IID data distributions.

3) Enhanced Blockchain Scalability: Exploring alternative lightweight blockchain architectures (e.g., DAG-based solutions) to improve scalability in larger federated networks.

4) Domain-Specific Applications: Extending the framework to new domains such as industrial IoT, autonomous systems, and smart cities, emphasizing areas where quantum optimization and blockchain offer the most value.

These efforts aim to bridge the gap between simulation and practical deployment. By addressing these directions, the framework has the potential to scale and adapt to real-world challenges while advancing state-of-the-art solutions for decentralized AI.

The proposed framework represents a significant step toward scalable, privacy-preserving, and high-performance decentralized AI systems. By integrating cutting-edge technologies like blockchain and quantum AI, this work lays a strong foundation for the next generation of FL and Edge AI solutions. The insights gained from this study are expected to inspire future advancements in building robust and adaptive AI ecosystems that meet the demands of emerging applications.

Acknowledgements

Sincere thanks to Chiranjeevi Bura and Anil Kumar Jonnalagadda for their valuable feedback during the pre-submission review of this article.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Brecko, A., Kajati, E., Koziorek, J. and Zolotova, I. (2022) Federated Learning for Edge Computing: A Survey. *Applied Sciences*, **12**, Article 9124. https://doi.org/10.3390/app12189124

[2] Myakala, P.K., Bura, C. and Jonnalagadda, A.K. (2024) Federated Learning and Data Privacy: A Review of Challenges and Opportunities. *International Journal of Research Publication and Reviews*, **5**, 1867-1879. https://doi.org/10.55248/gengpi.5.1224.3512

[3] Wu, L., Ruan, W., Hu, J. and He, Y. (2023) A Survey on Blockchain-Based Federated Learning. *Future Internet*, **15**, Article 400. https://doi.org/10.3390/fi15120400

[4] Gill, S.S., Golec, M., Hu, J., Xu, M., Du, J., Wu, H., *et al.* (2024) Edge AI: A Taxonomy, Systematic Review and Future Directions. *Cluster Computing*, **28**, Article No. 18. https://doi.org/10.1007/s10586-024-04686-y

[5] Tiwari, R., and Gupta, S. (2022) Federated Continual Learning for Edge-AI: A Comprehensive Survey, arXiv: 2411.13740. https://doi.org/10.48550/arXiv.2411.13740

[6] Ning, W., Zhu, Y., Song, C., Li, H., Zhu, L., Xie, J., *et al.* (2024) Blockchain-Based Federated Learning: A Survey and New Perspectives. *Applied Sciences*, **14**, Article 9459. https://doi.org/10.3390/app14209459

[7] Qiao, C., Li, M., Liu, Y. and Tian, Z. (2024) Transitioning from Federated Learning to Quantum Federated Learning in Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/comst.2024.3399612

[8] Kalapaaking, A.P., Khalil, I., Rahman, M.S., Atiquzzaman, M., Yi, X. and Almashor, M. (2023) Blockchain-Based Federated Learning with Secure Aggregation in Trusted Execution Environment for Internet-of-Things. *IEEE Transactions on Industrial Informatics*, **19**, 1703-1714. https://doi.org/10.1109/tii.2022.3170348

[9] Prigent, C., Costan, A., Antoniu, G. and Cudennec, L. (2024) Enabling Federated Learning across the Computing Continuum: Systems, Challenges and Future Directions. *Future Generation Computer Systems*, **160**, 767-783. https://doi.org/10.1016/j.future.2024.06.043

[10] Li, T., Sahu, A.K., Zaheer, M., Sanjabi, M., Talwalkar, A. and Smith, V. (2020) Federated Optimization in Heterogeneous Networks. *Proceedings of Machine Learning and Systems*. https://proceedings.mlsys.org/paper_files/paper/2020/file/1f5fe83998a09396ebe6477d9475ba0c-Paper.pdf

[11] Karimireddy, S., Kale, S., and Reddi, S. (2020) SCAFFOLD: Stochastic Controlled Averaging for Federated Learning, *Proceedings of the* 37*th International Conference on Machine Learning*, Online, 13-18 July 2020, 5132-5143. https://proceedings.mlr.press/v119/karimireddy20a.html

[12] Fukami, T., Murata, T., Niwa, K. and Tyou, I. (2024) DP-Norm: Differential Privacy Primal-Dual Algorithm for Decentralized Federated Learning. *IEEE Transactions on Information Forensics and Security*, **19**, 5783-5797. https://doi.org/10.1109/tifs.2024.3390993

[13] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H.B., Patel, S., *et al.* (2017) Practical Secure Aggregation for Privacy-Preserving Machine Learning. *Proceedings of the* 2017 *ACM SIGSAC Conference on Computer and Communications Security*, Dallas, 30 October-3 November 2017, 1175-1191. https://doi.org/10.1145/3133956.3133982

[14] Tan, A.Z., Yu, H., Cui, L. and Yang, Q. (2023) Towards Personalized Federated Learning. *IEEE Transactions on Neural Networks and Learning Systems*, **34**, 9587-9603. https://doi.org/10.1109/tnnls.2022.3160699

[15] Mnif, M., Sahnoun, S., Ben Saad, Y., Fakhfakh, A. and Kanoun, O. (2024) Combinative Model Compression Approach for Enhancing 1D CNN Efficiency for Eit-Based Hand Gesture Recognition on IoT Edge Devices. *Internet of Things*, **28**, Article 101403. https://doi.org/10.1016/j.iot.2024.101403

[16] Edge AI and Computing Unit 7-Hardware Accelerators for Edge AI.

https://library.fiveable.me/edge-ai-and-computing/unit-7

[17] Li, H., Sun, M., Xia, F., Xu, X. and Bilal, M. (2024) A Survey of Edge Caching: Key Issues and Challenges. *Tsinghua Science and Technology*, **29**, 818-842. https://doi.org/10.26599/tst.2023.9010051

[18] Gurung, D., Pokhrel, S.R. and Li, G. (2023) Quantum Federated Learning: Analysis, Design and Implementation Challenges. arXiv: 2306.15708. https://doi.org/10.48550/arXiv.2306.15708

[19] Zhang, Y., Lu, Y. and Liu, F. (2023) A Systematic Survey for Differential Privacy Techniques in Federated Learning. *Journal of Information Security*, **14**, 111-135. https://doi.org/10.4236/jis.2023.142008