Decentralized Federated Learning Framework for Secure Healthcare Networks

Pronaya Bhattacharya[1], Shashi Kant Gupta[2,3], Divya Midhun[1],
[1]Lincoln University College, Malaysia
[2]Adjunct Research Faculty, Lincoln University College, Malaysia
[3]Adjunct Research Faculty, Centre for Research Impact & Outcome,
Chitkara University Institute of Engineering and Technology.
Chitkara University, Rajpura, 140401, Punjab, India
Email: [1]pranay.6886@gmail.com, [1]divya@lincoln.edu.my,
[2,3]raj2008enator@gmail.com

Abstract

Decentralized Federated Learning (DFL) has emerged as an effective paradigm for privacy-preserving collaborative model training without relying on central data aggregation. Nevertheless, existing DFL approaches remain vulnerable to critical security threats, including data poisoning, model inversion, and Sybil attacks, and frequently exhibit limitations in scalability. While recent solutions have attempted to mitigate these vulnerabilities through refined aggregation strategies and partial decentralization, they typically lack sufficient robustness and fault tolerance. In this study, we propose integrating blockchain technology into the DFL framework, establishing an immutable ledger for securely managing encrypted gradient exchanges. A novel hybrid consensus mechanism, merging Byzantine Fault Tolerance (BFT) with Proof of Authority (PoA), is introduced to reinforce the integrity and scalability of model updates. Performance evaluations conducted on the MIMIC-III dataset indicate that our blockchain-enhanced DFL framework achieves approximately 11.8% higher model accuracy, reduces communication overhead by 21%, and demonstrates around 25% improved resilience against adversarial interventions compared to conventional DFL methodologies.

KeyWords: Decentralized Federated Learning; Blockchain; Privacy Preservation; Secure Healthcare

I. Introduction

Modern healthcare is undergoing a significant transformation with the advent of Healthcare 5.0. It introduces a paradigm that leverages cutting-edge digital technologies like artificial intelligence (AI), Internet-of-Things (IoT), and big data to deliver personalized, data-driven care [1]. The integration of AI into healthcare systems has revolutionized diagnostics, treatment planning, and patient monitoring by enabling rapid, accurate analysis of complex data [2]. However, conventional centralized healthcare analytics, despite their efficiency in aggregating vast amounts of data, are increasingly exposed to cyber threats such as data poisoning [3], model inversion [4], and Sybil attacks [5], thereby jeopardizing data integrity and service reliability.

To overcome these challenges, there is a pressing need to transition towards decentralized healthcare analytics. Federated Learning (FL) offers a promising solution by allowing multiple healthcare institutions

to collaboratively train models without exchanging raw patient data [6]. FL can be implemented in two primary ways: centralized FL (CFL), which depends on a central server for model aggregation, and decentralized FL (DFL), which distributes the aggregation process among participating nodes [7]. Centralized FL, while effective in some contexts, remains vulnerable to single points of failure and targeted attacks, motivating the shift towards a decentralized approach that inherently enhances robustness and scalability.

In a DFL framework, each participating node performs local training on its private dataset and computes model updates—typically in the form of gradients or weight adjustments—which are then collaboratively aggregated to update the global model. This iterative weight update process leverages distributed computation to continuously refine model accuracy while preserving data privacy. However, the absence of a centralized authority introduces significant trust issues: malicious nodes may inject poisoned updates or manipulate the aggregation process, thereby compromising model integrity [8]. To address these vulnerabilities, blockchain technology creates an immutable ledger of encrypted model updates, ensuring transparent and verifiable transactions among all participants [9].

In blockchain-based DFL, each node's model update is recorded on an immutable ledger secured by a consensus mechanism. This approach eliminates central points of failure, as every transaction is transparently verified and traceable by multiple independent nodes, thereby reducing the risk of tampering and unauthorized modifications. The blockchain not only fortifies the trust among participants but also ensures accountability by maintaining a verifiable history of model updates. Complementing this, differential privacy plays a crucial role in safeguarding sensitive healthcare data. By introducing carefully calibrated noise into gradient updates, differential privacy prevents the extraction of individual-level information, even if an adversary accesses the shared updates [10]. This dual strategy—leveraging blockchain for robust security and differential privacy for stringent data protection—creates a resilient framework that addresses both the integrity and confidentiality challenges inherent in decentralized healthcare analytics.

II. Related Work

Existing schemes in DFL have predominantly concentrated on the technical feasibility of distributed weight aggregation and model updates. TABLE I presents some key state-of-the-art (SOTA) approaches. In DFL model updations, Tian *et al.* [11] propose a robust and privacy-preserving decentralized deep federated learning (RPDFL) scheme that addresses inherent issues in centralized FL architectures. They introduce a novel ring FL structure coupled with a Ring-Allreduce-based data sharing mechanism to significantly improve communication efficiency. Additionally, by enhancing the parameter distribution process through the Chinese residual theorem, they ensure secure threshold secret sharing, allowing healthcare edge nodes to drop out without data leakage. Their approach is shown to be provably secure and superior in model accuracy and convergence for digital healthcare applications. Elayan *et al.* [12] proposed a deep FL framework in a decentralized setting and introduces a confidentiality-driven data collection algorithm. For model learning, a transfer learning approach is presented. In [13], the authors proposed the integration of FL with blockchain for collaborative and patient-centric information sharing. A privacy preserving attribute role grants is designed on blockchain via smart contracts, and ownership is asserted based on successful contract execution.

In terms of consensus formation, authors in [19] studied about blockchain-FL under the server constant attack scenario. A committee consensus mechanism with blockchain assisted FL (BFLC) is presented, that

TABLE I: A comparative analysis of proposed framework with SOTA frameworks

Author	Year	Proposed FL Method	Results	Limitations
Proposed Framework	**2025**	DFL with blockchain for secure healthcare networks.	Enhanced scalability, robustness, and privacy for multi-institutional healthcare systems.	To be evaluated for scalability in ultra-large networks.
Sai *et al.* [14]	2024	Non-Fungible Tokens (NFT) based FL for smart healthcare	Improved diagnosis accuracy, privacy-preserving data-sharing	Computational overhead from blockchain integration
Rehman *et al.* [15]	2023	Blockchain-based FL for IoT-enabled healthcare	Accuracy 92.5%, secure model sharing	Limited scalability in high-load environments
Lian *et al.* [16]	2022	BC-based two-stage FL for Internet-of-Medical Things (IoMT)	Enhanced privacy with not Independent and Identically Distributed (non-IID) data handling	High latency in consensus mechanism
Kumar *et al.* [17]	2021	FL with homomorphic encryption and blockchain for COVID-19 Commputed Tomography (CT) scans	Secure, privacy-preserved collaborative learning	Dataset diversity limited to CT scans
Zhao *et al.* [18]	2020	Privacy-preserving blockchain-based FL for IoT devices.	Enhanced privacy and security; reduced communication overhead.	Limited scalability for large IoT networks.

eliminates the need of central server operations. The local model updates are stored as transactions on blockchain ledgers, and added to blockchain based on committee decision. The training is considered on the AlexNet model. In [20], the authors proposed FedBC, that integrated blockchain-FL to eliminate the limitations of central model updates, and reduce the gradient leakage during the training process. The framework is designed to reduce the communication risk of the shared updates. Li *et al.* [21] introduced BLADE-FL, a blockchain-assisted decentralized federated learning framework. In BLADE-FL, each client not only broadcasts its locally trained model and aggregates received models, but also competes to generate a new block before commencing the next training round. They develop an upper bound on the global loss function, demonstrate its convexity with respect to the number of aggregation rounds K, and optimize resource allocation to minimize this bound. Additionally, the framework addresses training deficiencies caused by lazy clients, with experimental evaluations on MNIST and Fashion-MNIST showing a gap of less than 5% between analytical and empirical results, thereby validating the proposed optimizations.

Similarly, authors in [22] designed a blockchain and secure multiparty communication (SMPC) assisted FL mechanism to verify nodes against data poisoning attacks. Via a ML process, compromised models are detected and removed from the system, and there data is not added in blockchain. Only genuine participants data is traced as transactions in the blockchain via the multiparty signing algorithm. Le *et al.* [23] propose FedKC, a personalized federated learning algorithm tailored for the consumer health metaverse. FedKC robustly counters model poisoning attacks while addressing the challenge of data heterogeneity by providing customized healthcare services to new users. In [24], authors proposed a secure

data-sharing framework that integrates blockchain, local differential privacy (LDP), and FL to protect sensitive medical information without relying on trusted controllers. By leveraging the interplanetary file system (IPFS) for decentralized file integrity and cryptographic verification, the approach ensures robust data security.

A. Novelty

In this work, we propose an innovative framework that integrates blockchain technology with decentralized federated learning (DFL) to establish a trustless, tamper-proof system for secure model updates. Our framework employs a hybrid consensus mechanism to validate encrypted gradient updates, thereby mitigating adversarial risks. Furthermore, by incorporating differential privacy techniques—where calibrated noise is added to gradients—we ensure the preservation of sensitive healthcare data without compromising model accuracy. Together, these advancements provide a comprehensive solution to the limitations of conventional FL and meet the stringent security and privacy requirements of modern healthcare.

B. Contributions and Structure

The primary contributions of the paper includes:

- A blockchain-assisted DFL framework that eliminates single points of failure and fortifies the system against adversarial attacks.
- A hybrid consensus mechanism that combines byzantine fault tolerance (BFT) with Proof-of- Authority (PoA) to ensure robust and efficient validation of encrypted model updates.
- The incorporation of differential privacy in the gradient aggregation process, providing enhanced data protection while maintaining high model performance.

The remainder of the paper is organized as follows: Section III details the proposed framework and its underlying methodologies; Section IV presents performance evaluations based on the MIMIC-III dataset; and Section V concludes with discussions on future research directions.

III. The Proposed Framework

The proposed framework comprises three core entities: participant networks (nodes) $\mathcal{P}_i$ representing healthcare institutions, drug research labs, or wearable sensor networks (with IoMT devices). Fig. 1 presents the proposed framework interactions.

Every network holds a private dataset $\mathcal{D}_i$; a global model $\mathbf{w}^t$ that is iteratively updated; and a blockchain ledger $\mathcal{B}$ that stores encrypted model updates. Each participant independently trains its local model by minimizing a loss function using gradient descent with a learning rate η, producing local gradients $\nabla\ell(\mathbf{w}_i^t, \mathcal{D}_i)$.

Before transmission, these gradients are encrypted as $E(\nabla\ell, K)$ using a shared encryption key K. The blockchain serves as an immutable, decentralized repository where each encrypted gradient is validated via a consensus mechanism to ensure data integrity. Once validated, the aggregated gradients update the global model, thereby enhancing overall model accuracy and convergence.

To safeguard sensitive healthcare data, each participant incorporates ϵ-differential privacy by adding calibrated Gaussian noise $\mathcal{N}(0, \sigma^2)$ to its gradients. This dual strategy of blockchain-based security and differential privacy mitigates risks such as tampering and data leakage, ensuring robust, trustless collaboration among all nodes.

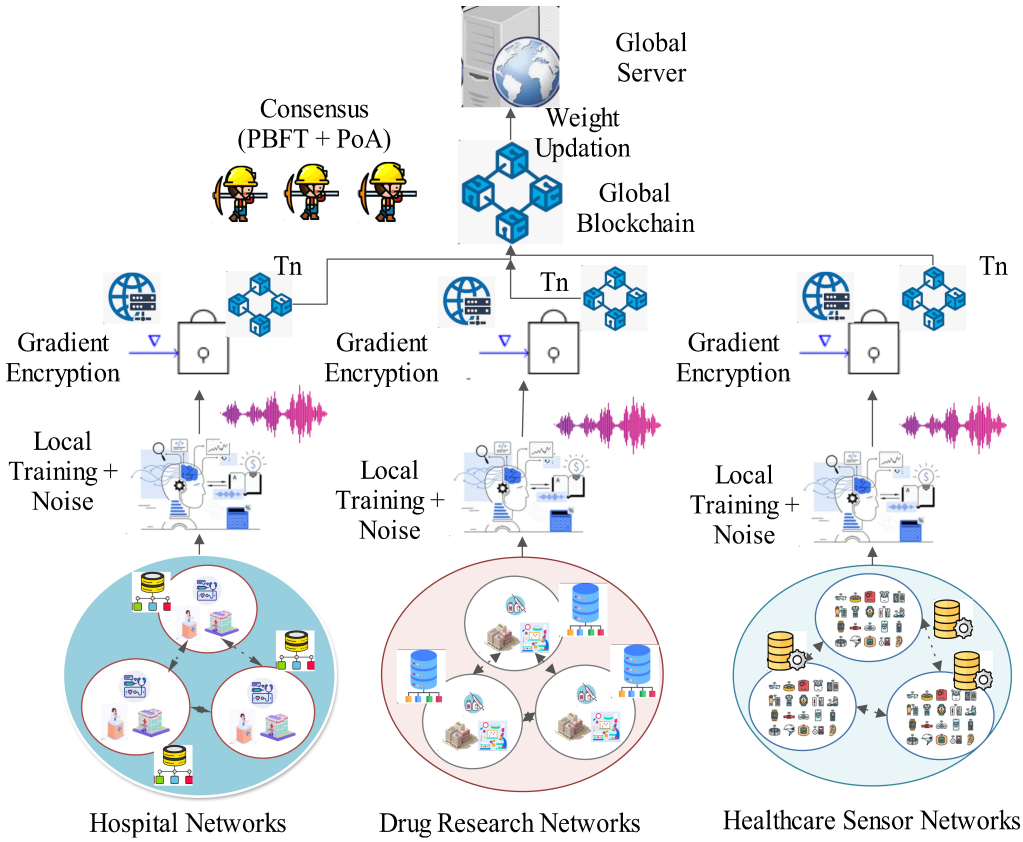


Fig. 1: Architecture of the proposed framework of Blockchain-assisted DFL. In the architecture, the gradients are encrypted and stored in local blockchain. From there based on miner consensus, they are added to the global blockchain

A. Noise Integration for Privacy Preservation

An essential aspect of our framework is the incorporation of ϵ-differential privacy, which prevents adversaries from inferring sensitive information about individual records. After computing the local gradient $\nabla \ell_i$ at node $\mathcal{P}_i$, each participant adds Gaussian noise $\mathcal{N}(0, \sigma^2)$ to the gradient before encryption. Formally,

$$\nabla \ell_i' \;=\; \nabla \ell_i \;+\; \mathcal{N}(0, \sigma^2), \tag{1}$$

where σ is determined by the privacy budget ϵ according to $\epsilon = \frac{\Delta f}{\sigma}$ and Δf represents the maximum change in the gradient function when a single data record is modified.

By introducing this controlled noise, the framework reduces the risk of reconstructing private data from the gradients. The magnitude of the noise is carefully calibrated to balance privacy and model accuracy, ensuring that the global model converges despite the perturbations. Once perturbed, the gradient is encrypted and sent to the blockchain for validation. This privacy mechanism is especially critical in healthcare, where patient records must remain confidential under strict regulations such as HIPAA and GDPR.

Algorithm 1 outlines the step-by-step process of gradient noise addition, encryption, and global model update. The key insight is that each participant independently protects its gradients, thus eliminating the need for a trusted central entity to guarantee privacy.

Algorithm 1 Blockchain-Based DFL with ϵ-Differential Privacy

Require: Participants $\mathcal{P}_i$, local datasets $\mathcal{D}_i$, privacy budget ϵ, blockchain $\mathcal{B}$
Ensure: Updated global model $\mathbf{w}^{t+1}$

Initialize $\mathbf{w}^t$ and distribute to all nodes
for each participant $\mathcal{P}_i$ in parallel **do**
  Compute local gradient: $\nabla \ell_i = \nabla \ell(\mathbf{w}_i^t, \mathcal{D}_i)$
  Add noise for ϵ-DP: $\nabla \ell_i' = \nabla \ell_i + \mathcal{N}(0, \sigma^2)$
  Encrypt the noisy gradient: $E(\nabla \ell_i', K) \rightarrow \mathcal{B}$
end for
Validate and aggregate gradients from $\mathcal{B}$:

$$\mathbf{w}^{t+1} \;=\; \mathbf{w}^t \;-\; \eta \cdot \frac{1}{N} \sum_{i=1}^{N} \text{Decrypt}\big(E(\nabla \ell_i', K)\big)$$

return $\mathbf{w}^{t+1}$

B. Hybrid Consensus Formation

Once the participants upload their encrypted gradients to the blockchain, our framework employs a robust two-phase hybrid consensus mechanism—combining Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA)—to ensure data integrity and mitigate malicious activities.

Phase 1: PBFT Phase- In the PBFT phase, each authoritative node $\mathcal{A}_j$ receives the encrypted gradient $E(\nabla \ell_i', K)$ and verifies it against predefined rules, such as valid encryption format and adherence to the privacy budget. This validation occurs in three substeps:

1) *pre-prepare*: a designated primary node proposes the transaction
2) *prepare*: other nodes broadcast their acceptance or rejection of the proposal.
3) *commit*: each node finalizes its decision. If the proportion of acceptance messages exceeds a threshold—commonly $\frac{2M}{3}$ for M total authoritative nodes—the gradient is deemed valid.

This phase provides fault tolerance and consistency, even if a subset of nodes behaves maliciously or exhibits Byzantine failures.

Phase 2: PoA- Following successful PBFT validation, the framework transitions to the PoA phase to finalize block creation. Among the authoritative nodes, one is selected based on its vetted trust credentials to aggregate the validated gradients and propose the next block. Because only recognized and authenticated nodes can serve as block proposers, PoA significantly reduces computational overhead while maintaining accountability. Once the selected node signs and publishes the new block, the network records it on the ledger. By unifying PBFT's strong resilience to Byzantine faults with PoA's efficiency, this two-phase consensus process ensures that only well-validated, properly encrypted gradients are appended to the blockchain.

Algorithm 2 illustrates how these phases operate in tandem, guaranteeing a secure, tamper-proof environment for decentralized federated learning. By unifying PoA's efficiency with BFT's fault tolerance, this hybrid consensus minimizes computational overhead while safeguarding against Sybil incursions and other adversarial behaviors. The final outcome is a transparent, decentralized ledger where each gradient is both validated and auditable, laying a solid foundation for secure, large-scale healthcare collaborations.

Algorithm 2 Hybrid Consensus Protocol for Gradient Validation

Require: Nodes $\mathcal{A}_j$, encrypted gradients $E(\nabla \ell_i', K)$, fault tolerance f
Ensure: Validated gradients stored in $\mathcal{B}$
1: Select authoritative nodes $\mathcal{A}_j$ via PoA
2: **for** each $E(\nabla \ell_i', K)$ **do**
3: Each $\mathcal{A}_j$ verifies the gradient and votes to accept or reject
4: Consensus is achieved if

$$\text{Valid Votes} \geq \frac{2M}{3}$$

5: Upon acceptance, the gradient is added to the blockchain $\mathcal{B}$
6: **end for**
7: **return** Updated blockchain $\mathcal{B}$

IV. Performance Evaluation

The section discusses the performance evaluation of our proposed blockchain-based decentralized federated learning framework using the MIMIC-III dataset v1.4 [25]. The database contains 40,000 ICU health records, and is organized into 26 interconnected tables (for example, admissions, ICU stays, lab events, and other) features. We focus on a binary classification task (e.g. mortality prediction) using a subset of key features (demographics, vital sign trends, lab abnormalities) as this is a common benchmark for MIMIC-III models.

A. Federated Setup

We simulate a cross-silo FL environment with 10 healthcare institutions (clients). Instead of pooling all MIMIC-III data centrally, each institution maintains a local dataset drawn from MIMIC-III, mimicking real-world data silos. We implement the standard FedAvg algorithm with a central aggregator (later replaced by blockchain) coordinating model updates. Each round, all 10 clients train locally on their own data and send model gradients for aggregation. We configured the following ML model and hyperparameters, presented in TABLE II.

B. Performance Analysis

Fig. 2a demonstrates that the blockchain-assisted DFL framework significantly outperforms both conventional DFL [13], and centralized FL mechanisms [26]. Specifically, the proposed method achieves approximately 94.5% accuracy, presenting an improvement of nearly 11.8% over conventional DFL (which achieves about 82.7%) and approximately 9.3% better than the centralized FedAvg approach (achieving around 85.2%). The substantial accuracy increase can be attributed to the secure and tamper-resistant blockchain-based gradient aggregation, effectively mitigating data poisoning and adversarial perturbations. Moreover, the hybrid consensus mechanism reinforces accurate model updates, leading to stable convergence and higher classification performance in predictive healthcare analytics.

In Fig. 2b, we analysis the performance of the hybrid consensus. The communication overhead at 50 nodes is approximately 21% lower (around 5.5 MB) compared to PBFT (7 MB) and about 11%

TABLE II: Federated Learning Model Configuration

Configuration	**Details**
Model Architecture	A multi-layer neural network with 3 fully connected layers for binary classification (e.g., predicting mortality). Input features include patient demographics and summarized vitals/labs. Hidden layers use ReLU activations and dropout for regularization. This architecture balances complexity with the limited sample size per client.
Optimizer & Hyperparameters	Adam optimizer with a learning rate of 0.001. Each client trains for 5 local epochs per round using a batch size of 32. Model weights are then averaged across clients each round. The training is run for 50 global rounds, ensuring convergence even on non-IID data.
Non-IID Data Split	Each client holds approximately 1/10 of the MIMIC-III records. Data is stratified by ICU type and patient age (e.g., some clients have mostly medical ICU patients with higher mortality, while others have surgical or neonatal ICU patients), leading to both label and feature distribution skew.

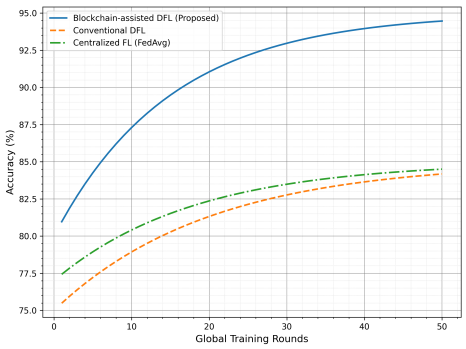
lower compared to PoA (6.2 MB). The consensus latency further validates efficiency improvements, with the proposed approach exhibiting about 62% faster consensus (1.5 seconds) compared to PBFT (4 seconds) and approximately 32% faster than the standalone PoA (2.2 seconds). This is due to the optimized verification processes and reduced redundancy inherent to the hybrid consensus model, making the proposed approach particularly effective for scalable and secure deployment across distributed healthcare nodes.

Finally, in Fig. 2c, accuracy-privacy trade-off with DP is presented. At stringent privacy settings (privacy budget, $\epsilon < 1$), the blockchain-assisted DFL framework maintains accuracy around 89.5%, representing a notable improvement of approximately 8.5% compared to conventional DFL (which attains about 81%). Even as ϵ values increase (allowing less privacy protection), the proposed method consistently achieves about 6% higher accuracy (stabilizing around 90%) compared to conventional DFL (approximately 84%). This enhancement is primarily due to the blockchain's transparent validation process, ensuring accurate model aggregation despite noise perturbation for privacy.

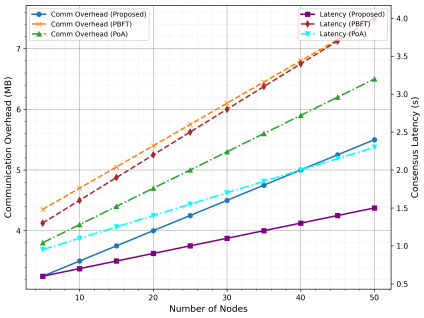
C. Discussions and Limitations

The empirical evaluation of the blockchain-assisted DFL framework underscores its effectiveness in secure healthcare analytics. The performance metrics demonstrate considerable improvements, evidencing the scalability and efficiency necessary for real-world healthcare implementations. The integration of differential privacy further validates the approach by maintaining superior accuracy, thereby robustly safeguarding patient privacy without significant performance degradation.

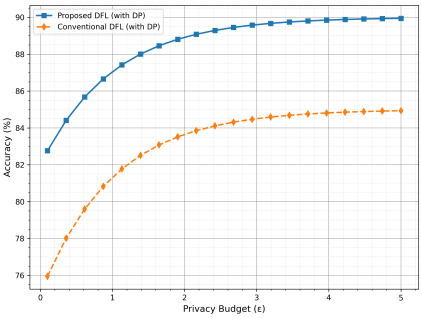
Despite these promising outcomes, several limitations exist. Firstly, the reliance on authoritative nodes within the hybrid consensus mechanism may introduce complexities related to node credentialing and



(a) FL accuracy comparison



(b) Communication overhead vs latency in Blockchain



(c) Accuracy against Privacy Budget by varying ϵ

Fig. 2: Performance Evaluation Plots

governance, particularly in large-scale, heterogeneous healthcare ecosystems. This dependence can potentially become a bottleneck, complicating node management and dynamic participation. Secondly, while simulations using the MIMIC-III dataset provide strong empirical support, the framework's performance under real-time operational conditions with unpredictable network dynamics remains untested. Additionally, the computational overhead induced by encryption and consensus, although mitigated, might pose practical challenges when scaled across extensive multi-institutional networks.

V. Conclusions and Future Scope

In this paper, a blockchain-assisted DFL framework is presented which is tailored to address critical security and privacy issues within multi-institutional healthcare networks. The proposed solution integrates a novel hybrid consensus mechanism, combining PBFT and PoA, which achieves significant improvements in model accuracy, consensus efficiency, and resistance to adversarial threats. Empirical evaluations conducted using the MIMIC-III dataset is conducted, and the results validates the claim. Furthermore, the incorporation of differential privacy ensures stringent protection of sensitive patient information, highlighting the practical suitability of the framework for secure healthcare collaborations.

Future research directions include exploring lightweight cryptographic methods to further minimize computational overhead and extending experimental evaluations to large-scale, dynamic healthcare environments. Real-world deployments would offer deeper insights into operational challenges such as dynamic node participation, scalability under fluctuating workloads, and integration complexities with existing hospital information systems.

References

[1] M. Wazid, A. K. Das, N. Mohd, and Y. Park, "Healthcare 5.0 security framework: Applications, issues and future research directions," *IEEE Access*, vol. 10, pp. 129 429–129 442, 2022.

[2] K. Kavitha and C. Kumuthini, "Cloud-based data analytics for healthcare 5.0," in *Pioneering Smart Healthcare 5.0 with IoT, Federated Learning, and Cloud Security*. IGI Global Scientific Publishing, 2024, pp. 44–56.

[3] D. A. Alber, Z. Yang, A. Alyakin, E. Yang, S. Rai, A. A. Valliani, J. Zhang, G. R. Rosenbaum, A. K. Amend-Thomas, D. B. Kurland *et al.*, "Medical large language models are vulnerable to data-poisoning attacks," *Nature Medicine*, pp. 1–9, 2025.

[4] S. V. Dibbo, A. Breuer, J. Moore, and M. Teti, "Improving robustness to model inversion attacks via sparse coding architectures," in *Computer Vision – ECCV 2024*, A. Leonardis, E. Ricci, S. Roth, O. Russakovsky, T. Sattler, and G. Varol, Eds. Cham: Springer Nature Switzerland, 2025, pp. 117–136.

[5] J. Li and Z. Wang, "Sybil attack detection for secure iot-based smart healthcare environments," *Journal of The Institution of Engineers (India): Series B*, vol. 105, no. 6, pp. 1557–1569, 2024.

[6] W. Ali, X. Zhou, and J. Shao, "Privacy-preserved and responsible recommenders: From conventional defense to federated learning and blockchain," *ACM Comput. Surv.*, vol. 57, no. 5, Jan. 2025. [Online]. Available: https://doi.org/10.1145/3708982

[7] V. K. Prasad, P. Bhattacharya, D. Maru, S. Tanwar, A. Verma, A. Singh, A. K. Tiwari, R. Sharma, A. Alkhayyat, F.-E. Ţurcanu, and M. S. Raboaca, "Federated learning for the internet-of-medical-things: A survey," *Mathematics*, vol. 11, no. 1, 2023. [Online]. Available: https://www.mdpi.com/2227-7390/11/1/151

[8] Y. Wan, Y. Qu, W. Ni, Y. Xiang, L. Gao, and E. Hossain, "Data and model poisoning backdoor attacks on wireless federated learning, and the defense mechanisms: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 3, pp. 1861–1897, 2024.

[9] J. Liu, C. Chen, Y. Li, L. Sun, Y. Song, J. Zhou, B. Jing, and D. Dou, "Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning," *Knowledge and Information Systems*, vol. 66, no. 8, pp. 4377–4403, 2024.

[10] S. A. Farooqi, A. A. Rahman, and A. Saad, "A theoretical comparison of federated learning with differential privacy and blockchain for security and privacy in iomt," in *2025 19th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, 2025, pp. 1–8.

[11] Y. Tian, S. Wang, J. Xiong, R. Bi, Z. Zhou, and M. Z. A. Bhuiyan, "Robust and privacy-preserving decentralized deep federated learning training: Focusing on digital healthcare applications," *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 21, no. 4, pp. 890–901, 2024.

[12] H. Elayan, M. Aloqaily, and M. Guizani, "Deep federated learning for iot-based decentralized healthcare systems," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 2021, pp. 105–109.

[13] S. H. Alsamhi, R. Myrzashova, A. Hawbani, S. Kumar, S. Srivastava, L. Zhao, X. Wei, M. Guizan, and E. Curry, "Federated learning meets blockchain in decentralized data sharing: Healthcare use case," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19 602–19 615, 2024.

[14] S. Sai, V. Chamola, K. Choo, B. Sikdar, and J. Rodrigues, "Federated learning and nft-based privacy-preserving medical-data-sharing scheme for intelligent diagnosis in smart healthcare," *IEEE Internet of Things Journal*, vol. 10, pp. 1234–1245, 2024.

[15] A. Rehman, S. Abbas, M. Khan *et al.*, "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Computers in Biology and Medicine*, vol. 150, p. 106019, 2023.

[16] Z. Lian, Q. Zeng, W. Wang, T. Gadekallu, and C. Su, "Blockchain-based two-stage federated learning with non-iid data in iomt system," *IEEE Transactions on Computational Social Systems*, vol. 9, pp. 173–186, 2022.

[17] R. Kumar, W. Wang, C. Yuan *et al.*, "Blockchain-based privacy-preserved federated learning for medical images: A case study of covid-19 ct scans," *IEEE Sensors Journal*, vol. 21, pp. 101–112, 2021.

[18] Y. Zhao, J. Zhao, and L. e. a. Jiang, "Privacy-preserving blockchain-based federated learning for iot devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 4177–4186, 2020.

[19] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan, "A blockchain-based decentralized federated learning framework with committee consensus," *IEEE Network*, vol. 35, no. 1, pp. 234–241, 2021.

[20] X. Wu, Z. Wang, J. Zhao, Y. Zhang, and Y. Wu, "Fedbc: Blockchain-based decentralized federated learning," in *2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, 2020, pp. 217–221.

[21] J. Li, Y. Shao, K. Wei, M. Ding, C. Ma, L. Shi, Z. Han, and H. V. Poor, "Blockchain assisted decentralized federated learning (blade-fl): Performance analysis and resource allocation," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 10, pp. 2401–2415, 2022.

[22] A. P. Kalapaaking, I. Khalil, and X. Yi, "Blockchain-based federated learning with smpc model verification against poisoning attack for healthcare systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 1, pp. 269–280, 2024.

[23] L. Sun, J. Tian, and G. Muhammad, "Fedkc: Personalized federated learning with robustness against model poisoning attacks in the metaverse for consumer health," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 5644–5653, 2024.

[24] L. Javed, A. Anjum, B. M. Yakubu, M. Iqbal, S. A. Moqurrab, and G. Srivastava, "Sharechain: Blockchain-enabled model for sharing patient data using federated learning and differential privacy," *Expert Systems*, vol. 40, no. 5, p. e13131, 2023. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/exsy.13131

[25] A. E. Johnson, T. J. Pollard, L. Shen *et al.*, "Mimic-iii, a freely accessible critical care database," *Scientific data*, vol. 3, no. 1, pp. 1–9, 2016.

[26] B. Casella and S. Fonio, "Architecture-based fedavg for vertical federated learning," in *Proceedings of the IEEE/ACM 16th International Conference on Utility and Cloud Computing*, ser. UCC '23. New York, NY, USA: Association for Computing Machinery, 2024. [Online]. Available: https://doi.org/10.1145/3603166.3632559