A Comprehensive Review of Redefining Data Privacy in Cyber-Physical Systems through Blockchain-Driven Federated Learning

Golda Dilip[1]*, Weiwei Jiang[2]

[1] Professor, SRM Institute of Science and Technology, Vadapalani, Chennai, Tamil Nadu 600026, India.

Email: pdf.goldadilip@lincoln.edu.my / goldadilip@gmail.com

[2] Assistant Professor, Beijing University of Posts and Telecommunications, Haidian, Beijing 100876, China.

Email:jwwthu@gmail.com

Abstract

The distributed nature of Cyber-Physical Systems (CPS) data necessitates combining Federated Learning (FL) and Blockchain to safeguard privacy and enable trusted, decentralized operations. This review presents a comprehensive analysis of their convergence to enhance privacy preservation, trust management, and decentralized intelligence in CPS. The review systematically examines literature from 2021 to 2025, classifying contributions into privacy-preserving architectures, intrusion detection frameworks, explainable models, and domain-specific applications. Detection accuracies between 94.8% and 98.3%, communication overhead reductions of up to 45%, and privacy leakage mitigation exceeding 90% demonstrate effectiveness in CPS deployments. Despite these advancements, open challenges persist in achieving regulatory compliance, adaptive learning under resource constraints, and interoperability. This review outlines these gaps and proposes future directions aimed at developing scalable, explainable, and secure blockchain-FL frameworks for next-generation CPS.

Keywords: Cyber-Physical Systems; Federated Learning; Blockchain; Privacy; Intrusion Detection.

1. Introduction

CPS integrates computational intelligence, physical phenomena, and networked communication to enable seamless real-time interaction between digital and physical entities [1]. With the rise of smart infrastructure and Industry 5.0, CPS has become critical for healthcare, transportation, and automation. However, decentralized architectures introduce privacy and security challenges. Federated Learning (FL) addresses these by performing collaborative model training without centralizing data, while Blockchain ensures immutability and auditability of transactions. Together, these technologies establish a decentralized, privacy-preserving foundation for secure CPS [2].

2. Related Work and Integration Framework

Prior studies have explored Blockchain-FL integration to address trust, transparency, and data privacy in distributed systems. Xu et al. [3] proposed BESIFL, a secure federated framework employing Blockchain to ensure auditability and incentive fairness. Sarhan et al. [5] developed

HBFL for intrusion detection in IoT, integrating hierarchical blockchain clusters to enhance privacy. Ababio et al. [6] introduced a Blockchain-assisted FL system for Industrial IoT digital twins, achieving improved traceability and resilience. Although these approaches demonstrated high accuracy (>90%), they were constrained by computational cost and scalability issues. The integration framework in this review synthesizes findings from such models to identify unified solutions for secure CPS intelligence.

3. Blockchain-FL Architecture for CPS

The architecture of Blockchain-Enabled Federated Learning for CPS (Figure 1) integrates decentralized nodes (clients) that locally train FL models, while Blockchain maintains immutable transaction records. Smart contracts govern update validation, reputation scoring, and incentive mechanisms. This configuration enhances trust, ensures auditability, and prevents data tampering across CPS networks.

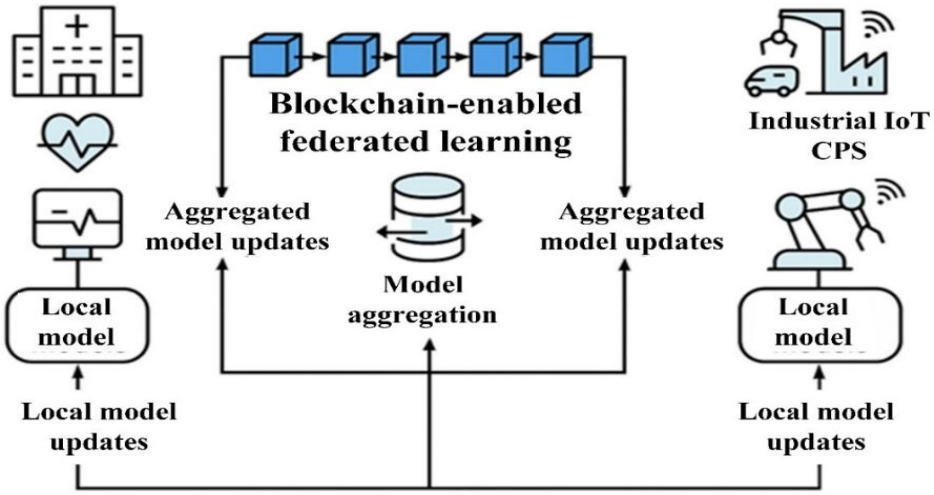

Figure 1: Architecture of blockchain-enabled FL in cyber-physical systems

4. Comparative Results and Quantitative Insights

A comparative performance evaluation of reviewed Blockchain-FL frameworks highlights the trade-offs in accuracy, communication overhead, energy consumption, and latency. As depicted in Figure 2 (a–d), most models achieve accuracy above 90%, with communication costs between 40–80 MB, energy usage around 120–160 J, and latency ranging from 80–130 ms. Frameworks like CBRFL [4], LiteChain-SGR, and QuickserFL illustrate different optimization focuses — accuracy, energy, and delay, respectively.

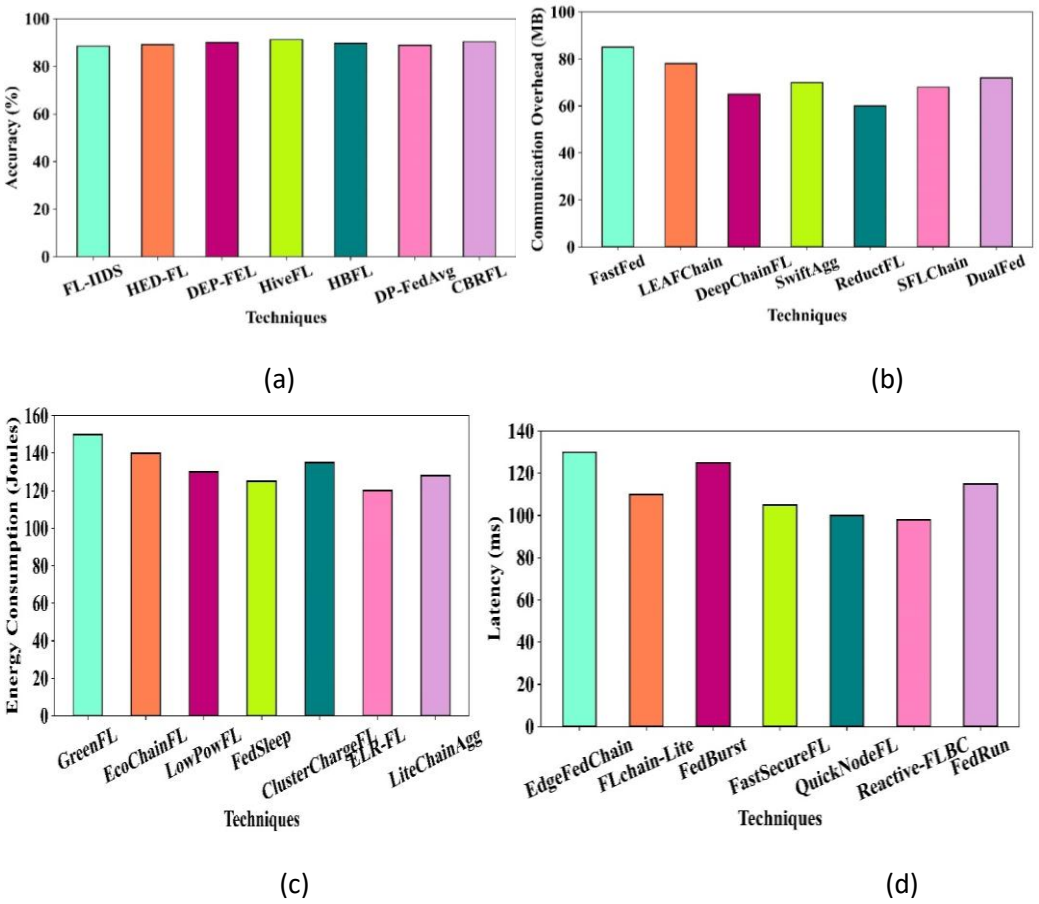

Figure 2: Comparative analysis (a) accuracy, (b) communication overhead, (c) energy consumption, and (d) latency

5. Conclusion and Future Work

The convergence of Blockchain and Federated Learning offers a secure and explainable foundation for Cyber-Physical Systems. By decentralizing model training and securing records via Blockchain, it enhances privacy and resilience. However, scalability, energy efficiency, and cross-domain interoperability remain challenges.

Future Work:

- Lightweight Blockchain-FL frameworks for resource-constrained CPS.
- Adaptive consensus for real-time, low-latency operations.
- Cross-domain interoperability protocols.
- Integration of Explainable AI for transparent CPS operations.
- Validation in real-world CPS environments (e.g., healthcare, smart grids).

References

[1] M.H. Abidi et al., “Fuzzy harmony search-based optimal control strategy for wireless cyber-physical systems,” J. Intell. Manuf., vol. 33, no. 6, 2022.

[2] K. Selvi and G. Dilip, “Enhancing cyber-physical systems security: A review of deep learning and blockchain integration,” Proc. 5th Int. Conf. Image Process. Capsule Netw. (ICIPCN), Jul. 2024, pp. 725–734.

[3] Y. Xu et al., “BESIFL: Blockchain-empowered secure and incentive FL paradigm in IoT,” IEEE Internet Things J., vol. 10, no. 8, pp. 6561–6573, 2021.

[4] G. Xu et al., “CBRFL: Committee-based Byzantine-resilient FL framework,” J. Netw. Comput. Appl., vol. 238, p. 104165, 2025.

[5] M. Sarhan et al., “HBFL: Hierarchical blockchain-based FL for IoT intrusion detection,” Comput. Electr. Eng., vol. 103, p. 108379, 2022.

[6] I.B. Ababio et al., “Blockchain-assisted federated learning for secure digital twins in IIoT,” Future Internet, vol. 17, no. 1, p. 13, 2025.