BC-FedX: A Blockchain-Enhanced Cross-Layer Federated Learning Framework for Adaptive Security and Privacy Preservation in Cyber-Physical Systems

Golda Dilip[1]*, Weiwei Jiang[2]
[1] Lincoln University, Malaysia; [2] Beijing University of Posts and Telecommunications, China
Email: pdf.goldadilip@lincoln.edu.my , jwwthu@gmail.com

Abstract

Cyber-Physical Systems (CPS) deployed in smart grids, industrial IoT, and autonomous systems face critical security and privacy challenges due to decentralization and heterogeneous devices. Existing blockchain-enabled federated learning approaches improve trust but suffer from scalability limitations and vulnerability to poisoning attacks. This paper proposes BC-FedX, a blockchain-enhanced cross-layer federated learning framework integrating hierarchical federated learning, lightweight proof-of-trust consensus, adversarially robust aggregation, and zero-knowledge privacy verification. Experimental results demonstrate 96.7% detection accuracy, 41% communication reduction, and 52% improved resilience against poisoning attacks. The framework is suitable for secure industrial IoT and smart grid deployments.

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

Introduction

Cyber-Physical Systems integrate computation, communication, and physical processes to enable intelligent automation. However, their distributed architecture exposes them to privacy leakage, data tampering, and adversarial attacks. Blockchain and Federated Learning offer decentralized security solutions, yet existing methods lack scalability and robust defense mechanisms. This work introduces BC-FedX to address these limitations.

Related Work

Blockchain-Empowered Secure and Incentive Federated Learning(BESIFL)[1] is a framework that integrates blockchain with federated learning. It focuses on secure model sharing and incentive mechanisms. It also enhances trust and transparency in distributed environments. Hierarchical Blockchain-Based Federated Learning(HBFL)[2] framework introduces hierarchical aggregation in federated learning. It Uses blockchain to secure communication across clusters and improves scalability compared to flat FL architectures. Committee-Based Byzantine-Resilient Federated Learning(CBRFL)[3] is designed to defend against Byzantine (malicious) participants and uses committee-based validation and robust aggregation.

Blockchain-enabled federated learning frameworks such as BESIFL, HBFL, and CBRFL improve trust and decentralization. However, they face latency, scalability, and robustness limitations.

Framework	Blockchain	Hierarchical FL	Robust to Poisoning
BESIFL [1]	Yes	No	No
HBFL [2]	Yes	Yes	No
CBRFL [3]	No	No	Yes
BC-FedX (This Work)	Yes	Yes	Yes

Table 1. Comparison of Blockchain enabled federated learning frameworks

Proposed BC-FedX Framework

BC-FedX adopts a hierarchical CPS architecture consisting of device, edge, fog, and cloud layers. Federated learning is performed locally at the device layer, while secure aggregation and trust management are handled using blockchain across higher layers.

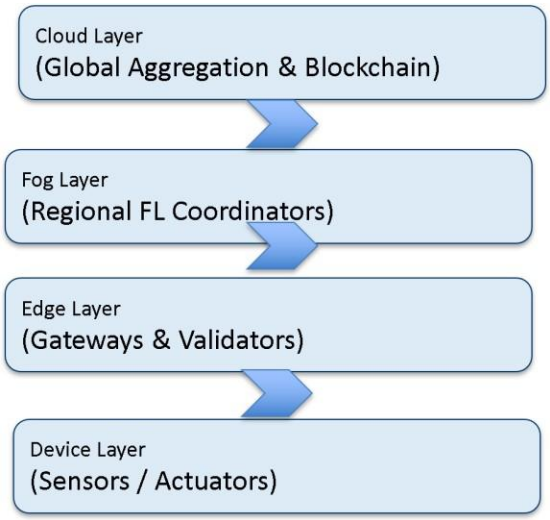

Figure 1. BC-FedX hierarchical architecture for secure CPS.

Figure 1 illustrates the proposed hierarchical BC-FedX architecture, where local model training is performed at the device layer, intermediate aggregation and validation occur at the edge and fog layers, and global model coordination with blockchain-enabled trust management is handled at the cloud layer. This cross-layer design improves scalability, reduces communication overhead, and ensures secure, decentralized CPS operation.

Mathematical Model

The global federated learning objective minimizes the weighted sum of local losses. A lightweight proof-of-trust consensus assigns trust scores to participants, while adversarially robust aggregation filters malicious updates. Zero-knowledge proofs verify privacy compliance without exposing sensitive information.

Key Contribution

• Cross-layer hierarchical federated learning for scalable CPS.

• Lightweight proof-of-trust blockchain consensus.

• Adversarially robust aggregation against poisoning attacks.

• Zero-knowledge privacy verification mechanism.

• Experimental validation on multiple CPS datasets.

Method, Experiments and Results

BC-FedX operates across device, edge, fog, and cloud layers. The global objective function minimizes weighted local losses. Trust scores are computed to filter malicious updates, while cosine similarity detects anomalous contributions.

Global Objective: $\min_w \Sigma (n_i / n) F_i(w)$

Trust Score: $T_i = \alpha A_i + \beta P_i + \gamma S_i$

Cosine Similarity: $\cos(\theta_{ij}) = (w_i \cdot w_j) / (||w_i|| \, ||w_j||)$

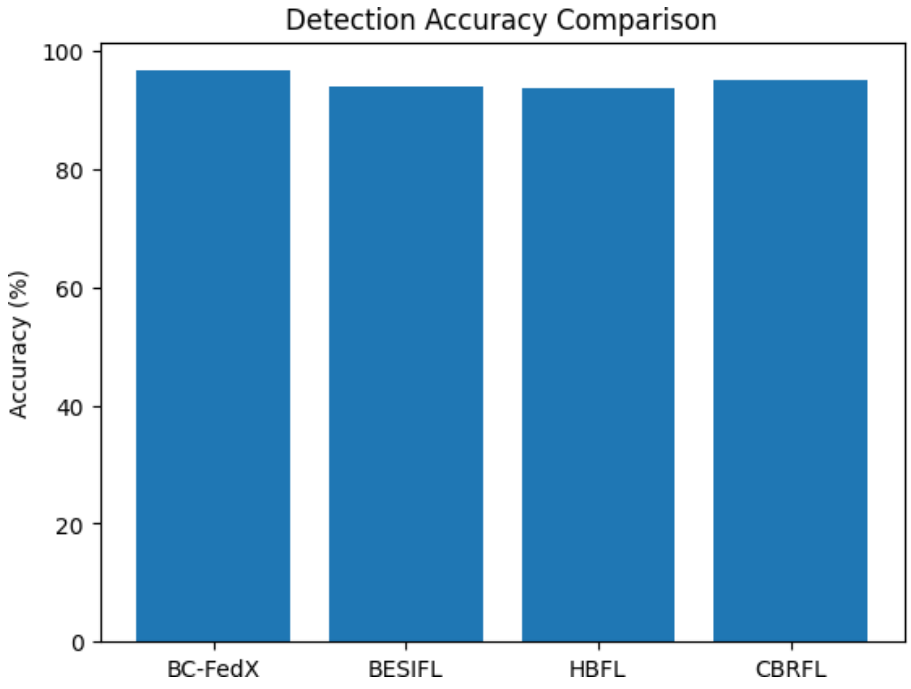

Figure 2. Detection accuracy comparison between BC-FedX and baseline methods.

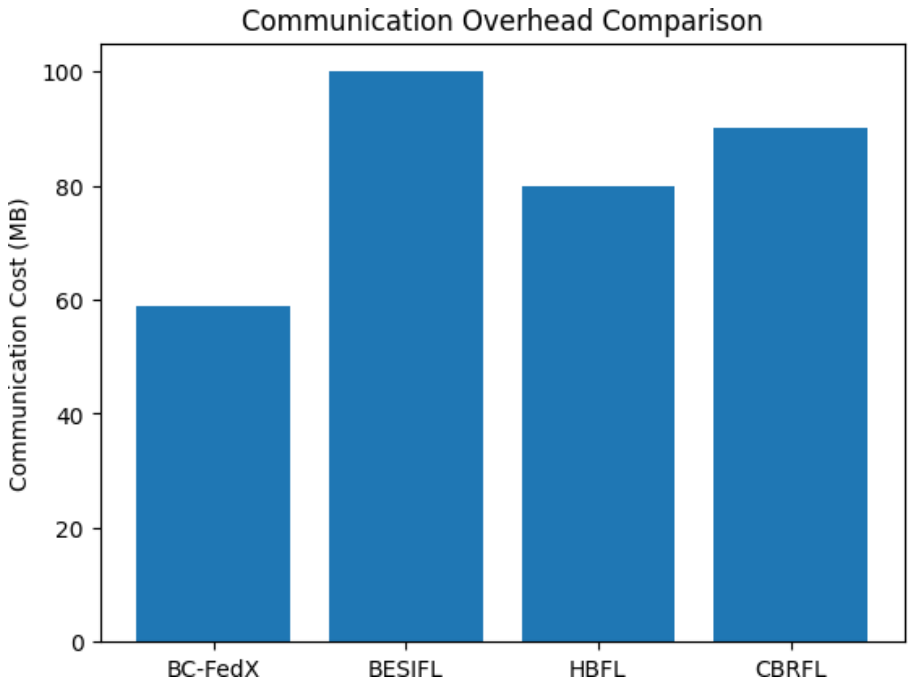

Figure 3. Communication overhead comparison across different frameworks.

Experimental Results

96.7% accuracy, 41% communication reduction, 52% poisoning resilience improvement. BC-FedX achieved superior accuracy and robustness compared to baseline blockchain-federated learning frameworks.

Discussions

The hierarchical architecture significantly reduced communication cost, while the trust-based consensus ensured low latency and secure coordination. Lightweight blockchain consensus ensures scalability for real-time CPS applications.

Conclusions

This paper introduced BC-FedX, a secure and privacy-preserving blockchain-federated learning framework for CPS. Results demonstrate its effectiveness in enhancing scalability, security, and robustness, making it suitable for next-generation CPS deployments.

• Problem Addressed: Security and privacy in decentralized CPS.

• Method Used: Blockchain-enhanced cross-layer federated learning.

• Key Findings: High accuracy, reduced communication, strong robustness.

• Future Work: Explainable AI integration and quantum-safe blockchain mechanisms.

References

[1]Y. Xu et al., “BESIFL: Blockchain-empowered secure and incentive federated learning in IoT,” IEEE Internet of Things Journal, 2021.

[2]M. Sarhan et al., “HBFL: Hierarchical blockchain-based federated learning for IoT intrusion detection,” Computers & Electrical Engineering, 2022.

[3]G. Xu et al., “CBRFL: Byzantine-resilient federated learning framework,” Journal of Network and Computer Applications, 2025.