IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Block-chain-Empowered Cyber-Secure Federated Learning for Trustworthy Edge Computing

Mohamed Jahid S[1], Hemnaath R[2], Rajprathap R[3], Sabarivasan P[4],

Department of Computer Science and Engineering, Arasu Engineering College, Tamil Nadu, India.

S.V. Karthik[5], Department of Computer Science and Engineering, Assistant Professor, Arasu Engineering College,
Tamil Nadu, India.

Abstract

This paper proposes a secure federated learning framework enhanced with blockchain technology for use in edge computing environments. The system introduces decentralized trust management, encrypted aggregation of model updates, smart contract-based validation, a reputation-based client scoring mechanism, and tamper-resistant auditing to ensure transparency and security. It effectively addresses major threats such as model poisoning, Sybil attacks, and data integrity issues while maintaining scalability and low latency. Experimental results show that the proposed framework achieves better accuracy and stronger attack resistance compared to traditional federated learning approaches.

1. Introduction

Edge computing supports fast and low-bandwidth applications. Federated Learning (FL) allows multiple devices to train models without sharing raw data, but it faces security and trust issues due to centralized aggregation. This work introduces a blockchain-based secure FL model to improve trust, transparency, and protection against attacks, especially in IoT and distributed AI environments.

2. Background and Preliminaries

This section covers key concepts like distributed learning, blockchain consensus, secure computation, homomorphic encryption, and Byzantine fault tolerance. Federated averaging is used for model updates, while blockchain ensures secure, transparent, and immutable coordination.

3. System Architecture

The system includes edge devices, an aggregation server, blockchain nodes, and smart contracts. Devices train locally and send encrypted updates. Blockchain stores model hashes, and smart contracts validate updates. A reputation system helps identify and reduce malicious participants.

4. Mathematical Formulation

The model uses weighted averaging to update the global model. Security is ensured under adversarial conditions like malicious clients. Data integrity is verified using SHA-256 hashing.

5. Security and Threat Model

The framework ensures confidentiality, integrity, availability, and accountability. It protects against attacks such as model poisoning, Sybil attacks, replay attacks, and gradient manipulation. It remains secure even with up to 30% malicious clients.

6. Performance Evaluation

The proposed model is compared with traditional and secure FL methods using metrics like accuracy, latency, and communication cost. Results show better security and accuracy with manageable overhead. Tested on healthcare and IoT scenarios**.**

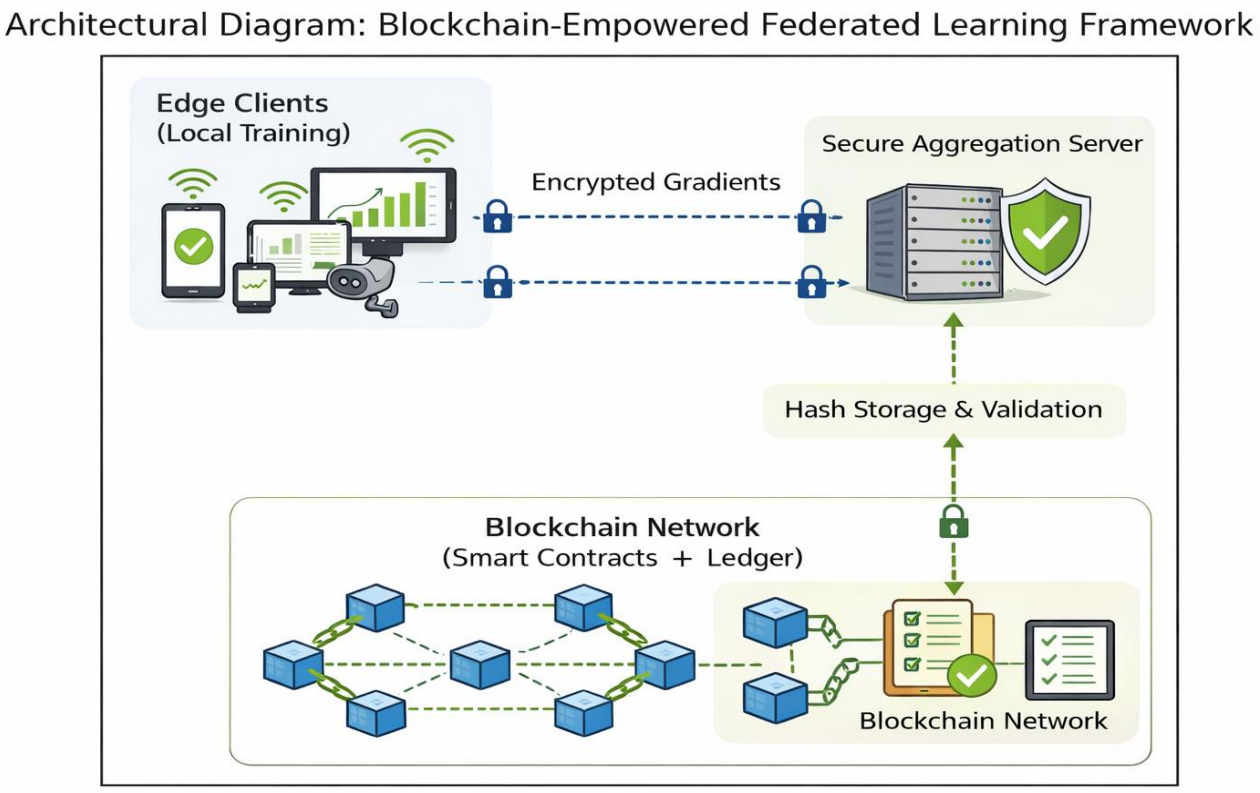
7. Applications and Deployment Considerations

This system can be used in healthcare, autonomous vehicles, industrial IoT, financial systems, and smart cities, where secure and distributed learning is required.

8. Conclusion

Blockchain improves the security and trust of federated learning systems. The proposed framework enhances attack resistance and coordination. Future work focuses on reducing latency and improving cross-chain compatibility.

Figure 1: Proposed Blockchain-Empowered Federated Learning Architecture



HOW FEDERATED LEARNING WORKS

A central server initializes a global model. Edge devices download the model. Each device trains the model using its local dataset. Only model updates (gradients/weights) are shared. The server aggregates updates using algorithms such as Federated Averaging. The updated global model is redistributed.

ADVANTAGES

- Preserves data privacy.
- Reduces communication overhead.
- Complies with data protection regulations.
- Enables collaborative AI across organizations.
- Limitations.

SMART CONTRACTS

Smart contracts are self-executing programs stored on the blockchain that automatically enforce rules and agreements. In federated learning, smart contracts can:

- Validate model updates
- Reward honest participants
- Penalize malicious nodes
- Manage participant authentication

Blockchain eliminates the need for a central aggregation server and builds trust among unknown edge devices.

NEED FOR BLOCK-CHAIN-EMPOWERED CYBER-SECURE FEDERATED LEARNING

In distributed edge networks, participants may not trust each other. Malicious nodes can Inject poisoned model updates. Launch backdoor attacks Submit fake gradients Impersonate legitimate devices.

A centralized FL server becomes a major vulnerability. By integrating block chain into federated learning. Aggregation becomes decentralized Model updates are recorded immutably Participants are authenticated Reputation systems can be implemented Incentive mechanisms ensure fairness.

SYSTEM DESCRIPTION

The proposed system, “Blockchain-Empowered Cyber-Secure Federated Learning for Trustworthy Edge Computing,” is designed to provide a secure, privacy-preserving, and decentralized framework for collaborative machine learning in distributed environments. The system integrates Federated Learning (FL), Blockchain Technology, Edge Computing, and Secure Communication Protocols to ensure trustworthy model training without compromising sensitive data.

BACKGROUND AND CORE CONCEPTS

Federated learning operates on the principle of decentralized data processing. A global model is initially distributed to multiple edge devices, which train the model locally using their private datasets. After training, only the model parameters or gradients are shared with a central aggregator. These updates are then combined using algorithms such as Federated Averaging to produce an improved global model.

Blockchain technology complements this process by introducing decentralization and immutability. It consists of a distributed ledger maintained by multiple nodes, where each transaction is verified through consensus mechanisms. Once recorded, data cannot be altered, ensuring transparency and security. Smart contracts, which are self-executing programs stored on the blockchain, can automate validation processes and enforce rules without human intervention.

In addition to blockchain, several cryptographic techniques are employed to enhance security. Homomorphic encryption allows computations to be performed on encrypted data, ensuring privacy during aggregation. Hashing algorithms such as SHA-256 are used to verify data integrity, while Byzantine fault tolerance mechanisms ensure that the system remains reliable even when some participants act maliciously.

The proposed system architecture consists of four main components: edge devices, blockchain network, aggregation mechanism, and smart contracts. Edge devices are responsible for collecting data and performing local model training. These devices may include smartphones, IoT sensors, or industrial machines.

Once training is completed, the model updates are encrypted and transmitted to the blockchain network. Instead of relying on a central server, blockchain nodes validate and store these updates. Each update is associated with a hash value, ensuring its integrity and preventing tampering. Smart contracts play a crucial role in validating model updates, enforcing participation rules, and managing incentives.

A reputation-based scoring mechanism is also incorporated into the system. Each participant is assigned a reputation score based on their historical behavior. Devices that consistently provide reliable updates are rewarded, while those exhibiting malicious behavior are penalized or excluded. This mechanism helps maintain the overall trustworthiness of the system.

APPLICATIONS AND REAL-WORLD USE CASES

The proposed blockchain-enabled federated learning system has wide-ranging applications across multiple domains. In healthcare, it enables hospitals to collaboratively train predictive models without sharing sensitive patient data. In autonomous vehicles, it supports real-time learning from distributed sensors while ensuring data security.

Industrial IoT systems can benefit from this approach by enabling secure data sharing among machines and devices. Financial institutions can use it for fraud detection and risk analysis while maintaining data confidentiality. Smart cities can leverage this framework to improve services such as traffic management and energy optimization.

The system is particularly suitable for environments where trust is limited and data privacy is critical. By combining blockchain and federated learning, it provides a reliable solution for secure and decentralized artificial intelligence.

REFERENCES

- M. Chen et al., IEEE Access, 2024.
- H. Zhao et al., Journal of Network and Systems Management, 2025.
- S. Rajendran et al., IEEE EDGE, 2025.
- Y. Al-Hassan et al., arXiv, 2025.
- K. Bonawitz et al., Secure Aggregation for FL, 2017.
- McMahan et al., Communication-Efficient FL, 2017.
- S. Nakamoto, Bitcoin Whitepaper, 2008.
- M. Castro and B. Liskov, PBFT, 1999.
- Q. Li et al., IEEE Communications Surveys & Tutorials, 2021.
- J. Kang et al., Incentive Mechanism for Blockchain FL, 2019.
- T. Li et al., Federated Optimization in Heterogeneous Networks, 2020.
- R. Shokri et al., Membership Inference Attacks, 2017.
- Dwork, Differential Privacy, 2006.
- X. Liu et al., Secure Edge Intelligence Systems, 2022.