Blockchain-Enabled Federated Learning Framework for Privacy-Preserving AI Systems

Abstract

Federated learning (FL) enables collaborative model training across multiple data sources without centralizing data, addressing critical privacy and security concerns in distributed machine learning. However, traditional FL systems face challenges related to trust, data integrity, and secure parameter aggregation. This research proposes a **blockchain-enabled federated learning framework** that integrates decentralized ledger technology with federated AI to enhance transparency, trust, and privacy preservation. Smart contracts will be utilized to ensure secure model parameter exchange, automate validation, and establish auditable data provenance. The proposed system will be evaluated for its privacy guarantees, latency, and model performance across heterogeneous, distributed datasets, demonstrating its potential for deployment in sensitive domains such as healthcare, finance, and IoT.

Keyword

Federated Learning, Blockchain, Privacy Preservation, Smart Contracts, Decentralized AI, Data Provenance, Secure Computation.

OBJECTIVES

1. **To design** a federated learning architecture that enables multiple independent entities to collaboratively train AI models **without sharing raw data**.
2. **To integrate** blockchain as a **decentralized ledger** for secure model parameter exchange, consensus validation, and traceability.
3. **To implement** smart contracts for **auditability, incentive management, and data provenance tracking** within the learning framework.
4. **To evaluate** the proposed system's **privacy guarantees, computational latency, scalability, and model accuracy** using distributed benchmark datasets.