COLLABORATIVE LEARNING FOR ATTACK DETECTION IN TRANSACTIONS AND SMART CONTRACTS

Author's: V. Rajarajeshwari,[1] G. Thilipkumar[2], K. Sujith[3], N. Vanjulavalli[4]

Abstract

Blockchain ecosystems have transformed digital finance, decentralized applications (DApps), and smart contract automation. However, the increasing adoption of blockchain technologies has led to a proportional rise in sophisticated cyber-attacks, including transaction fraud, smart contract exploits, reentrancy attacks, delegatecall abuse, flash loan manipulation, and denial-of-service patterns. Traditional centralized security models struggle to detect such attacks effectively due to privacy constraints, fragmented data ownership, and evolving adversarial tactics. detecting attacks in blockchain transactions and smart contracts. The framework leverages distributed machine learning techniques—specifically federated or collaborative learning—to enable multiple organizations (such as exchanges, banks, blockchain auditors, and decentralized platforms) to jointly train a global threat detection model without sharing raw data. Each participant trains a local model on private data, and model parameters are aggregated to create a robust global model.The system integrates transaction-level features (e.g., gas usage, transaction frequency, entropy metrics) and smart contract behavior indicators (e.g., reentrancy patterns, delegatecall usage, failure rates). The collaborative framework enhances attack detection accuracy while preserving privacy and regulatory compliance. By incorporating explainable machine learning, performance metrics evaluation, and secure aggregation mechanisms, the proposed system offers scalable, privacy-preserving, and adaptive blockchain threat detection.