International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

A Secure and Scalable Blockchain-Enabled Federated Learning Framework for Detecting Fraudulent Activities in Cryptocurrency Transactions

[1]Shaik Haseena,[2]S.Kavyareddy,[3]A.Sowmya,[4]G.Kavyasree,[5]Y.Sujitha

[1] Assistant Professor,Department of Computer Science & Engineering, Dr. K.V. Subba Reddy Institute of Technology

[2,3,4,5] B. Tech Students, Department of Computer Science & Engineering, Dr. K.V. Subba Reddy Institute of Technology

ABSTRACT

The rapid adoption of cryptocurrencies has led to a significant rise in fraudulent activities such as money laundering, phishing scams, Ponzi schemes, and transaction manipulation. Traditional centralized fraud detection systems require access to sensitive transaction data, raising serious concerns regarding privacy, scalability, and trust. Moreover, data sharing across cryptocurrency exchanges and financial institutions is often restricted due to regulatory and confidentiality constraints. To address these challenges, this work proposes a secure and scalable blockchain-enabled federated learning framework for cryptocurrency fraud detection. Federated learning enables collaborative model training across decentralized nodes without sharing raw transaction data, while blockchain ensures transparency, immutability, and trust among participating entities. The proposed system securely aggregates locally trained models using smart contracts, enabling accurate fraud detection while preserving data privacy. Experimental analysis demonstrates improved scalability, enhanced security, and robust fraud detection performance, making the framework suitable for real-world decentralized cryptocurrency ecosystems.

Keywords: Blockchain Security, Federated Learning, Cryptocurrency Fraud Detection, Decentralized Systems, Secure Model Training, Privacy Preservation, Smart Contracts, Scalable Fraud Analytics

I. INTRODUCTION

Cryptocurrencies and blockchain-based financial systems have transformed the global digital economy by enabling decentralized, borderless, and transparent transactions. However, the pseudonymous nature of cryptocurrency transactions has also made them an attractive target for fraudsters. Detecting fraudulent activities in such decentralized environments is challenging due to massive transaction volumes, evolving attack patterns,

and privacy constraints.

Existing fraud detection approaches rely on centralized machine learning models that require collecting transaction data from multiple sources. This centralized approach introduces risks related to data leakage, single points of failure, and limited scalability. Furthermore, sharing sensitive transaction data across organizations often violates privacy regulations and organizational policies. Federated learning (FL) offers a promising solution by allowing multiple entities to collaboratively train a machine learning model without exchanging raw data. However, federated learning alone lacks trust guarantees and is vulnerable to malicious participants. Integrating blockchain with federated learning addresses these limitations by providing a secure, decentralized, and auditable environment for model aggregation and coordination. This work presents a blockchain-enabled federated learning framework that ensures secure, scalable, and privacy-preserving cryptocurrency fraud detection.

II. LITERATURE SURVEY

1.Federated Learning: Challenges, Methods, and Future Directions

Author: Qiang Yang et al.

Abstract:

This paper provides a comprehensive overview of federated learning, discussing privacy preservation, communication efficiency, and security challenges. It highlights federated learning's suitability for decentralized fraud detection.

2. Blockchain-Based Federated Learning for Secure Data Sharing

Author: Kim et al.

Abstract:

The authors propose a blockchain-assisted federated learning framework to ensure secure and transparent model aggregation. The study demonstrates improved trust and robustness in collaborative learning environments.

3. Cryptocurrency Fraud Detection Using Machine Learning

Author: Chen and Li

Abstract:

This work applies machine learning techniques to detect fraudulent cryptocurrency transactions. The authors emphasize the limitations of centralized approaches and the need for distributed learning frameworks.

4. Privacy-Preserving Fraud Detection in Financial Systems

Author: S. Patel and R. Mehta

Abstract:

The study explores privacy-aware fraud detection systems and concludes that federated learning combined with secure infrastructure significantly enhances data protection.

5. Smart Contract-Based Secure Model Aggregation

Author: Xu et al.

Abstract:

This paper introduces smart contract-based mechanisms for validating and aggregating machine learning models in decentralized systems, ensuring integrity and accountability.

III. EXISTING SYSTEM

The existing cryptocurrency fraud detection systems primarily rely on centralized machine learning and deep learning models deployed on a single server or organization. These systems require collecting transaction data from multiple exchanges and wallets into a centralized repository for training and analysis. Some approaches use rule-based detection or graph-based anomaly detection techniques. While these systems can achieve reasonable detection accuracy, they suffer from scalability limitations, privacy risks, and lack of trust among collaborating entities. Additionally, centralized systems are vulnerable to single points of failure and data breaches.

Disadvantages of Existing System

1. Privacy Risks: Centralized data collection exposes sensitive transaction data.
2. Limited Scalability: Central servers struggle with large-scale, real-time transaction data.
3. Lack of Trust: Organizations hesitate to share data due to confidentiality concerns.

IV. PROPOSED SYSTEM

The proposed system introduces a secure and scalable blockchain-enabled federated learning framework for cryptocurrency fraud detection. Each participating entity (e.g., exchanges, financial institutions) trains a local fraud detection model on its private transaction data. Model updates, rather than raw data, are securely shared and recorded on a blockchain network. Smart contracts manage model aggregation, validation, and participant authentication. This decentralized approach ensures privacy preservation, transparency, and robustness against malicious participants while enabling collaborative learning across organizations.

V. SYSTEM ARCHITECTURE

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

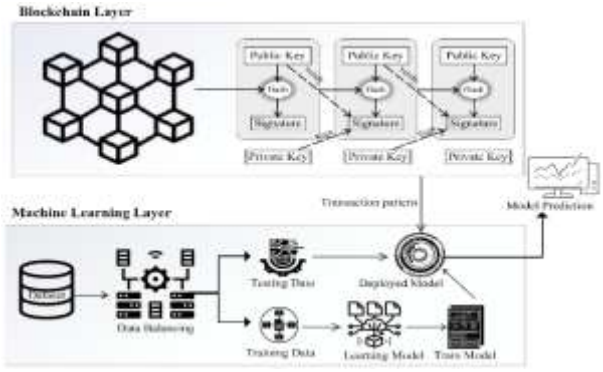

Fig 5.1: System Architecture

The diagram illustrates a dual-layer secure data communication process that combines cryptography and steganography. Initially, the original message is passed through an encryption process using a symmetric key (specifically AES-128), converting the readable message into an encrypted form that ensures confidentiality. This encrypted message is then embedded into a cover media (such as an image) using the LSB (Least Significant Bit) steganography technique, producing a stego media that conceals the very existence of the secret data. During reception, the reverse process is applied: the encrypted message is first extracted from the stego media, and then a decryption process using the same symmetric key is performed to recover the original message. This workflow ensures both data secrecy and invisibility, providing strong protection against unauthorized access and interception.

VI. IMPLEMENTATION

Fig 6.1: Home page

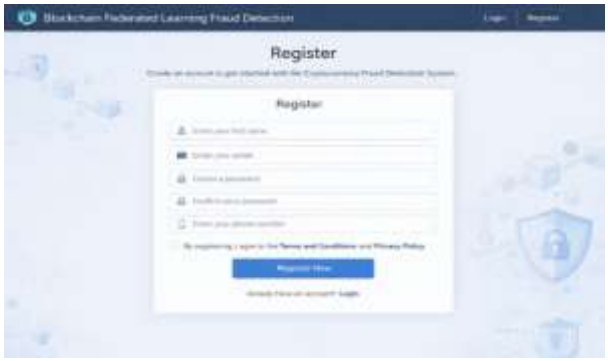

Fig 6.2: Register page

VII. CONCLUSION

This work presented a secure and scalable framework that integrates federated learning with blockchain technology to detect fraudulent activities in cryptocurrency transactions. By enabling decentralized model training, the proposed system ensures that sensitive transaction data remains locally stored at participating nodes, thereby preserving privacy

and complying with data protection requirements. Blockchain technology further enhances the framework by providing immutability, transparency, and trust through secure storage of model updates and smart contract–based validation. The combination of federated learning and blockchain effectively mitigates data leakage risks, resists tampering, and improves collaborative fraud detection accuracy across distributed environments. Overall, the proposed approach offers a robust, privacy-preserving, and trustworthy solution for addressing the growing challenges of fraud in cryptocurrency ecosystems.

VIII. FUTURE SCOPE

The proposed framework can be further enhanced by incorporating advanced deep learning models such as Graph Neural Networks to capture complex transaction relationships in blockchain networks. Future work may also integrate differential privacy and homomorphic encryption techniques to strengthen privacy guarantees during model aggregation. Scalability can be improved by supporting cross-chain interoperability and real-time streaming transaction analysis. Additionally, deploying the framework on real cryptocurrency platforms and integrating it with regulatory monitoring systems could improve practical adoption. The framework may also be extended to detect other financial crimes such as money laundering and ransomware payments, making it a comprehensive solution for secure digital finance systems.

IX. REFERENCES

1. Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. McMahan, H. B., et al., “Communication-Efficient Learning of Deep Networks from Decentralized Data,” *AISTATS*, 2017.
3. Kairouz, P., et al., “Advances and Open Problems in Federated Learning,” *Foundations and Trends in ML*, 2021.
4. Li, X., et al., “Federated Learning: Challenges, Methods, and Future Directions,” *IEEE Signal Processing Magazine*, 2020.
5. Christidis, K., and Devetsikiotis, M., “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, 2016.
6. Zheng, Z., et al., “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *IEEE Big Data*, 2017.

7. Chen, T., and Guestrin, C., "XGBoost: A Scalable Tree Boosting System," *KDD*, 2016.
8. Pham, Q. V., et al., "A Survey of Multi-Access Edge Computing in 5G and Beyond," *IEEE Communications Surveys*, 2020.Toyoda, K., et al., "A Novel Blockchain-Based Product Ownership Management System," *IEEE*