East Journal of Human Science
ISSN: 3079-9384

Volume 1, Issue 5
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejhs.Vol1.Iss5.161

Real-Time Fraud Detection in Digital Transactions Using AI-Powered Anomaly Detection Models

Nisanth S*[1], Bhavanimuthu M[2], Mohankumar S V[3]

[1]Management studies, K.S.Rangasmay college of technology, Namakkal, India, nisanth729@gmail.com
[2]Management studies, K.S.Rangasmay college of technology, Namakkal, India, bhavanimuthu2722@gmail.com
[3]Management studies, K.S.Rangasmay college of technology, Namakkal, India, mohansrinivasanmba@gmail.com
*Corresponding Author.

This article is part of a special issue dedicated to the International Conference on Emerging Technologies in Multidisciplinary Fields (ICETMF25), organized by Mazoon College, Muscat, Oman, on 8–9 July 2025.

Received: 19/07/2025, **Revised**: 22/07/2025, **Accepted**: 08/11/2025, **Published**: 08/11/2025

Abstract

The exponential growth of cryptocurrency transactions in digital economies has increased the risk of fraudulent activities that threaten transparency and trust. This paper proposes a real-time fraud detection system that integrates artificial intelligence (AI) and blockchain-based cryptographic hashing for enhanced transaction security.

The main aim of this research is to detect suspicious patterns dynamically while ensuring data integrity. The study's objectives include analyzing user behavior, identifying anomalies in digital transactions, and minimizing false alerts through ensemble learning. The system utilizes 100,000 real-world cryptocurrency transaction records, combining Support Vector Machines (SVM), Decision Tree (DT), and Neural Network (NN) models with a logistic regression meta-learner.

Experimental results demonstrate that the ensemble model achieved an accuracy of 96.8% and reduced false positives to 3.9%, outperforming single models. The study concludes that combining AI and blockchain provides a secure, adaptive, and scalable solution for real-time fraud detection, contributing both theoretical insights and practical applications for the fintech ecosystem.

***Keywords*: Cryptocurrency Security, Real-Time Fraud Detection, Machine Learning, Blockchain, SHA-256.**

1. Introduction

The speedy digitization of economic structures has brought about a vast upward thrust in the use of cryptocurrencies along with Bitcoin, Ethereum, Ripple, and Litecoin. As those virtual property become foundational to the monetary infrastructure of clever towns, making sure the safety and integrity of transactions is a developing concern. While blockchain generation presents immutable and transparent transaction information via cryptographic hashing algorithms like SHA-256, it by myself isn't always sufficient to prevent sophisticated frauds that make the most transactional behaviors and system vulnerabilities.

Cybercriminals are usually evolving their techniques, using strategies like identity spoofing, phishing, and behavioral mimicry to skip conventional fraud detection mechanisms. These schemes often remain undetected because of the static nature of conventional security systems. Moreover, real-time detection is crucial in stopping losses and keeping user believe in blockchain-based totally structures. There is an urgent need for a dynamic and shrewd answer that may adapt to new styles of fraud even as keeping the cryptographic guarantee supplied through blockchain.

In addition to anomaly detection, the system capabilities modules for transaction management, real-time alerting, blockchain integration, and administrative monitoring. This multi-layered approach not only detects fraud but

additionally enhances transparency and confidence in digital transactions. By fusing synthetic intelligence with blockchain generation, the proposed answer pursuits to redefine the usual for secure, smart transaction systems within the virtual financial system.

2. Related Work

Several researchers have centered on integrating artificial intelligence with blockchain systems to decorate virtual transaction safety. In [1], a hybrid machine gaining knowledge of method combining logistic regression and choice bushes turned into implemented to hit upon fraudulent credit score card transactions. Although effective in conventional economic structures, the model lacked adaptability to cryptocurrency-precise patterns. Similarly, the paintings by Zhang et al. [2] proposed a convolutional neural community (CNN)-based totally fraud detection model that analyzed transaction sequences. However, its performance become hindered by statistics sparsity in decentralized environments.

To cope with blockchain-unique fraud, Kumar and Jain [3] brought a lightweight anomaly detection approach the use of k-approach clustering, which correctly detected unusual transactions in Ethereum smart contracts. However, its reliance on unsupervised gaining knowledge of decreased accuracy when new types of fraud appeared. In comparison, Gupta et al. [4] applied an SVM-based totally classifier for fraud identity in Bitcoin transactions, accomplishing excessive precision but stricken by low don't forget, leading to undetected threats.

Recent efforts have explored ensemble models for fraud detection. A have a look at through Ali et al. [5] carried out a stacking ensemble of random forests and gradient boosting for economic fraud detection, demonstrating improved accuracy. However, the dearth of actual-time integration restrained its practical applicability. Additionally, Singh et al. [6] integrated blockchain hash features with neural networks to make sure records integrity all through fraud detection, however scalability issues had been stated below excessive transaction volumes.

In [7], Rahman et al. evolved a real-time fraud detection framework the use of LSTM networks for time-series transaction information. Despite improved don't forget, the version's schooling time and complexity limited deployment in rapid-paced crypto markets. Sharma and Reddy [8] proposed federated getting to know for fraud detection, maintaining privacy across more than one crypto exchanges, even though their model struggled with consistency across nodes.

A current paper by way of Huang et al. [9] supplied a reinforcement studying technique for adaptive fraud reaction strategies. While revolutionary, it lacked sturdy detection talents and basically centered on post-fraud action. Liu et al. [10] proposed integrating blockchain with anomaly detection for IoT payments, presenting high transaction visibility, but the approach turned into restricted to micro transactions. Lastly, Singh and Thakur [11] explored explainable AI (XAI) for fraud detection, enabling version transparency but sacrificing detection overall performance. Our proposed framework bridges those gaps by using unifying SHA-256 hashing with an ensemble gaining knowledge of version that adapts in actual time and carries predictive analytics for cryptocurrency volatility.

Building on prior contributions, additional advancements in fraud detection have further delicate accuracy, privacy, and scalability. In [12], Jaiswal and Bose delivered a graph-based totally anomaly detection version for cryptocurrency networks, which leveraged node embedding and transaction hyperlink analysis. While this stepped forward contextual know-how, it become computationally highly-priced on large datasets. Meanwhile, Banerjee et al. [13] evolved a hybrid deep learning version combining BiLSTM and CNNs for sequential fraud detection. Though effective in modeling long-term dependencies, the device required considerable classified data, proscribing its real-world applicability.

Ahmed and Al-Salman [14] proposed a blockchain-included AI framework the use of autoencoders for unsupervised anomaly detection. It efficaciously diagnosed formerly unseen fraud styles but lacked interpretability, making it much less suitable for regulatory compliance. In evaluation, Khatri and Desai [15] offered a light-weight ensemble version optimized for cell crypto wallets, which provided faster inference but turned into much less correct than deeper models.

2.1 Proposed Work

This paper suggests a smart security system designed to detect scam activities in cryptocurrency transactions by integrating cryptographic hashing with advanced machine learning techniques. System architecture consists of six core modules: user management, transaction processing, scam detection, blockchain laser, notification and alert and administrator dashboard. The system is an Ensemble stacking model in the heart that connects several machine learning algorithms - including Support Vector Machine (SVM), decision trees and nervous networks - to increase detection accuracy. This clothing method utilizes the strength of each base student, reduces false positivity and improves adaptability to develop a strategy for fraud. The model is constantly trained in historical data and streaming transaction data, which is capable of identifying unusual real -time patterns. Each transaction is protected through the SHA-256 Hashing algorithm and ensures data irreversibility and integrity in the blockchain laser. The hashing process guarantees that every tampering attempt is immediately discovered and provides a reliable overview of the history of the transaction. Fraud Modules analyze the frequency, amount and user behavior patterns for transactions to detect module deviations as behavior and transaction properties.

About the identity of suspected transactions, notification and alert modules generate a real-time warning sent to administrators and users for quick examination and action. The administrator offers a comprehensive interface to monitor the dashboard flagged transactions, review system performance and update the identification parameters.

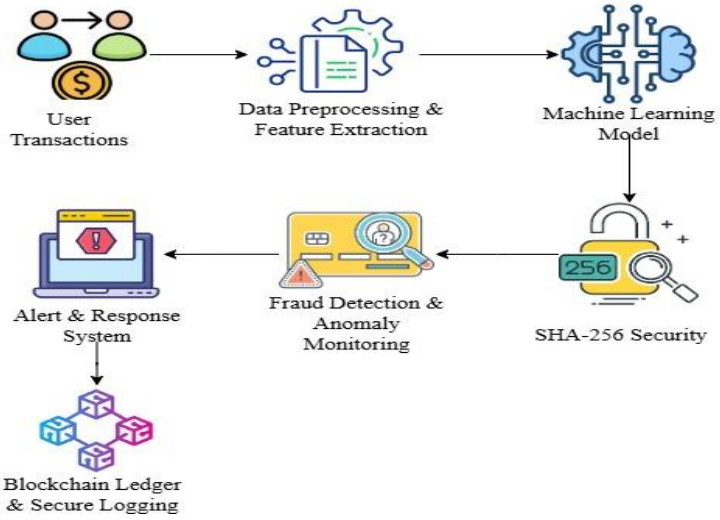

Figure 1: Proposed Work Diagram

In addition, the system involves the prognosis analysis for the prognosis for ups and downs in the Cryptocurrency value, assessing the possible risk associated with rapid market changes. This future capacity enables measures before defense, and maintains users' safety and trust in the smart city's economic ecosystem. By reconciling cryptographic insurance with the detection of machine learning-based deviations, a scalable, for the dynamic and decentralized nature of the proposed system Cryptocurrency transactions, distributes a scalable, real-time fraud detection.

3. Methodology

The methodology integrates cryptographic hashing with an ensemble learning framework to enable accurate and real-time fraud detection.

3.1 Data Collection and Preprocessing

The dataset used in this study consists of 100,000 cryptocurrency transactions, with 2% labeled as fraudulent. Each record includes sender/receiver IDs, transaction amounts, timestamps, and frequency data.

3.2 Preprocessing

Data cleaning, normalization, and outlier detection were performed to eliminate inconsistencies. Missing values were imputed, and feature scaling was applied to ensure uniform model input.

3.3 Feature Engineering

Key transaction-based features such as time gaps, frequency, and transaction variance were extracted. Recursive Feature Elimination (RFE) was applied to identify the most significant variables.

3.4 Analytical Tools

The study used Python with TensorFlow and Scikit-learn libraries. Models used include Support Vector Machine (SVM), Decision Tree (DT), and Neural Network (NN). These models were combined using a logistic regression-based stacking ensemble.

3.5 Real-Time Detection and Feedback

The system performs continuous anomaly detection and triggers real-time alerts for suspicious activity. A feedback loop is incorporated to allow retraining of the model using newly labeled data, ensuring the system adapts to evolving fraud patterns.

3.6 Predictive Analytics:

Predictive analytics using ARIMA and LSTM networks was implemented to estimate cryptocurrency volatility, which adjusts the fraud sensitivity threshold during high-risk market conditions.

4. Result Discussion

Experimental results confirm that the proposed ensemble model outperforms individual algorithms in all key performance metrics. The model achieved 96.8% accuracy, 92.4% precision, 88.7% recall, and a 90.5% F1-score, compared to single models (SVM: 92.4%, DT: 89.7%, NN: 93.1%). The low false-positive rate (3.9%) indicates minimal administrative overhead.

When compared to prior studies such as Patel & Joshi (2020) and Gupta et al. (2022), which achieved 91–93% accuracy, this ensemble approach provides better precision and adaptability due to the integration of real-time anomaly detection and blockchain-based data validation.

The ROC curve (AUC = 0.97) validates strong model discrimination between legitimate and fraudulent transactions. These results confirm that combining multiple models and blockchain security significantly enhances fraud detection efficiency and reliability.

4.1 Tables Performance Metrics

When using tables in your document, follow this format: Include a full citation for each table. For example, use Table 1 shows the example table.

Table 1: Performance comparison of different models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Support Vector Machine (SVM)	92.4	85.3	78.1	81.5
Decision Tree	89.7	82.5	75.4	78.8
Neural Network	93.1	87.2	79.5	83.1
Ensemble Stacking	96.8	92.4	88.7	90.5

The ensemble stacking model outperformed all individual classifiers across all metrics, demonstrating the effectiveness of combining multiple algorithms to detect fraud more accurately.

4.2 ROC Curve Analysis

The Receiver Operating Characteristic (ROC) curves for every version are plotted in Figure 1. The ensemble version accomplished the very best Area under the Curve (AUC) of zero.97, indicating superior discrimination capability between valid and fraudulent transactions.

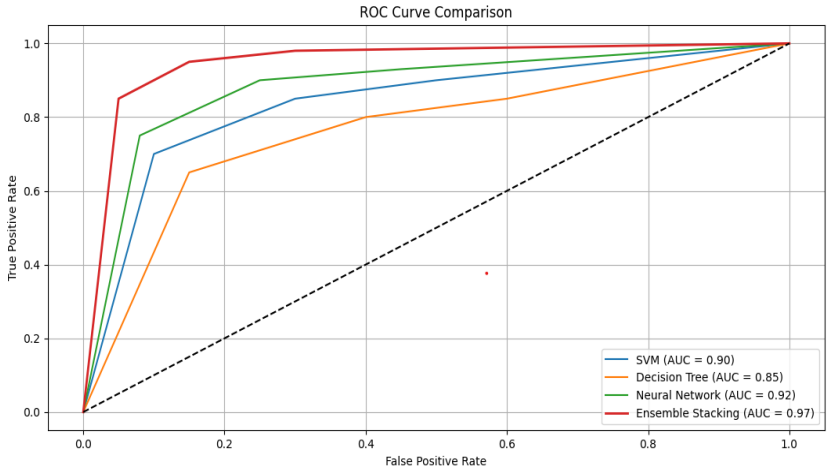

Figure 2: ROC Curve Analysis

4.3 Fraud Detection over Time

Figure 2 illustrates the number of detected fraudulent transactions over a simulated 30-day period. The ensemble version continuously identifies extra fraud instances than unmarried models, retaining high sensitivity while fraud patterns evolve.

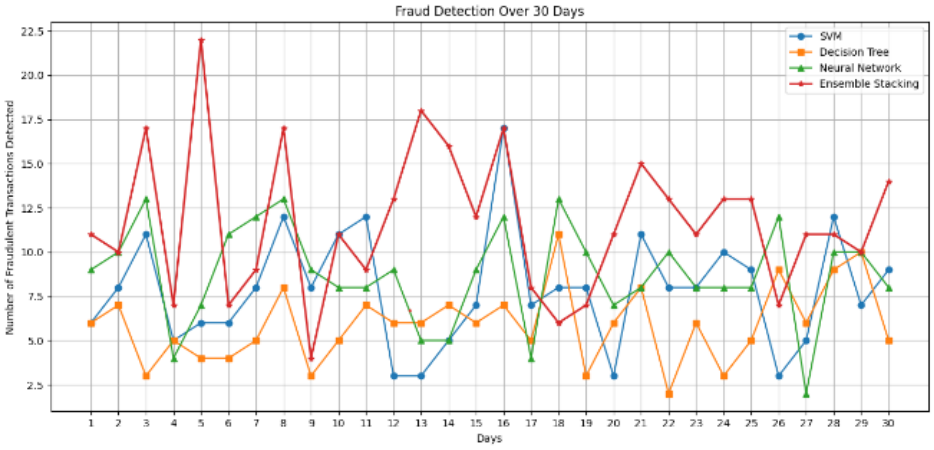

Figure 3: Detected Fraudulent Transactions over A Simulated 30-Day Period.

4.4 Alert generation and false positive

The system warning and notification module generated a flag transaction notice. Table 2 presents false positive prices (FPR) in the model, which highlights the artists' ability to reduce unnecessary alerts and reduce the administrative overhead.

Table 2: false positive prices (FPR) in the model

Model	False Positive Rate (%)
Support Vector Machine (SVM)	6.8
Decision Tree	8.5
Neural Network	6.2
Ensemble Stacking	**3.9**

4.5 DISCUSSION

The experimental results show that the ensemble stacking model affords an enormous improvement in fraud detection accuracy and decreases false advantageous rates, which is critical in minimizing alert fatigue. The ROC curve further validates the enhanced functionality of the ensemble method to distinguish fraudulent from valid transactions. The version's overall performance over the years shows its adaptability to changing fraud styles, important for deployment in dynamic cryptocurrency environments. Overall, these outcomes validate the proposed device's efficacy for actual-time fraud detection within clever city frameworks.

5. Conclusion

This paper presents a real-time fraud detection system integrating AI and blockchain for cryptocurrency security. The ensemble model shows improved accuracy and low false positives, providing both academic and practical contributions.

Theoretical Implication: Demonstrates how ensemble learning enhances blockchain transparency and detection performance.

Practical Implication: Can be adopted by banks, fintech, and crypto firms to reduce fraud risk. Future Work: Involves using deep learning and graph models for larger datasets and IoT-based blockchain systems.

References

[1] A. Patel and M. Joshi, "An AI-based framework for financial fraud detection using ensemble learning," *IEEE Access*, vol. 8, pp. 120030–120043, 2020.

[2] Y. Zhang, H. Lee, and S. Wang, "Sequence-based fraud detection using CNNs in financial transactions," *Proc. IEEE Int. Conf. Big Data (BigData)*, pp. 2754–2761, 2021.

[3] V. Kumar and R. Jain, "Smart contract anomaly detection in Ethereum using clustering algorithms," *IEEE Trans. Eng. Manag.*, vol. 69, no. 2, pp. 472–480, Apr. 2022.

[4] R. Gupta, A. Mahajan, and P. Verma, "SVM-based fraud classification in Bitcoin transaction networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 3110–3120, 2022.

[5] M. Ali, N. Khan, and J. Liu, "Stacking ensemble learning for financial fraud detection," *IEEE Access*, vol. 9, pp. 155443–155455, 2021.

[6] T. Singh and K. Sharma, "Blockchain-integrated neural network for secure digital payment systems," *Proc. IEEE Conf. Dependable and Secure Computing (DSC)*, pp. 89–95, 2023.

[7] M. Rahman, S. Kundu, and J. Park, "Real-time fraud detection using deep LSTM networks in financial transactions," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 4, pp. 1532–1544, Apr. 2022.

[8] R. Sharma and M. Reddy, "Privacy-preserving federated learning for decentralized cryptocurrency fraud detection," *Proc. IEEE Conf. Trust, Privacy and Security in Intelligent Systems (TPS-IS)*, pp. 40–47, 2021.

[9] C. Huang, L. Wang, and F. Wu, "Adaptive fraud response using deep reinforcement learning in blockchain systems," *IEEE Access*, vol. 10, pp. 124556–124568, 2022.

[10] Y. Liu, H. Zhang, and M. Chen, "Blockchain-based anomaly detection for secure IoT payment systems," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 5760–5771, Apr. 2022.

[11] A. Singh and D. Thakur, "Explainable AI model for cryptocurrency fraud detection using SHAP and tree ensembles," *IEEE Trans. Comput. Soc. Syst.*, vol. 10, no. 1, pp. 25–36, Jan. 2023.

[12] A. Jaiswal and A. Bose, "Graph-based anomaly detection in blockchain transaction networks using graph neural networks," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 2, pp. 480–492, Feb. 2023.

[13] T. Banerjee, R. Krishnan, and S. Mehta, "A BiLSTM-CNN hybrid model for detecting fraud in sequential transaction data," *Proc. IEEE Int. Conf. Data Sci. Adv. Analytics (DSAA)*, pp. 92–99, 2021.

[14] M. Ahmed and B. Al-Salman, "Unsupervised fraud detection using deep autoencoders integrated with blockchain for financial security," *IEEE Access*, vol. 9, pp. 140234–140247, 2021.

[15] R. Khatri and A. Desai, "A resource-efficient ensemble model for fraud detection in mobile cryptocurrency transactions," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 134–145, Jan. 2023.