International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412001|

Anomaly-Based Intrusion Detection System in Financial Transactions using Ensemble Machine Learning and Blockchain

[1]Shreya M A, [2]Thrupthi K N, [3]Supreetha M S, [4]Refa Samrin, [5]Dr. Rajashekar M B

[1 2 3 4]Department of Computer Science & Engineering,

GSSS Institute of Engineering & Technology for Women, Mysuru, Affiliated to VTU, Belagavi, Karnataka, India

[5]Associate Professor, Department of Computer Science & Engineering,

GSSS Institute of Engineering & Technology for Women, Mysuru, Affiliated to VTU, Belagavi, Karnataka, India

ABSTRACT: With the rapid expansion of digital payment systems, the possibility of financial fraud is also growing fast. Most traditional rule-based Intrusion detection systems lack the ability to identify new and evolving fraud patterns within a real-time context. Therefore, this paper proposes an Anomaly-Based Intrusion Detection System for financial transactions using Ensemble Machine Learning with Blockchain technology. It processes transaction data to learn normal behavior of the users, and detects unusual activities such as unexpected spikes in the amount of transfers initiated or interaction with unknown users. Genuine transactions in this regard go on to be recorded on a blockchain ledger for total transparency of these records against alteration risks. The trials indicated that integrating ensembles with blockchain will enhance the accuracy of detection and reduction of false alerts for a reliable real-time method of protection for the digital financial transaction.

KEYWORDS: Anomaly Detection; Intrusion Detection System (IDS); Financial Fraud Detection; Ensemble Machine Learning; Blockchain Security; Transaction Monitoring; Digital Payments; Real-Time Fraud Prevention; Data Analytics.

I. INTRODUCTION

The rapid digital transition witnessed in the financial segment has brought a change in the manner of conducting transactions. Because of online banking, UPI, mobile wallets, and E-commerce sites, people have been able to carry out transactions at any given time and from anywhere. Although these facilities have accelerated the more number of transactions, they have also made the financial area more vulnerable to cyber threats. Fraudsters and thieves take advantage of weaknesses and ignorance on the part of these people. The rising number depicts the importance of an efficient Real-time Intrusion Detection System.

Conventional intrusion detection systems work on rule-based models and check for specific patterns, like abnormally high transaction values and unusual access locations. Traditional approaches are efficient and capable of detecting existing threats, but they are not effective for identifying new and sophisticated cyber threats, as cyber criminals adapt and change incessantly.

Keeping these problems in mind, there is a proposal for a hybrid solution based on an IDS with Ensemble Machine Learning algorithms, CNN and SVM. These models focus on examining transactional activities and historical data insights.

Adding blockchain technology will help us to safeguard and record transactions effectively and securely. Its decentralized and immutable structure enhances data integrity and transparency.

Together, Machine Learning and Blockchain enable anomaly detection and record-keeping functionalities. The result is an increase in financial security and user trust.

II. LITERATURE SURVEY

The papers surveyed analyze research on applying machine learning and blockchain techniques in intrusion and fraudulent activity detection on finance and blockchain. Some papers highlight the superiority of ensemble learning techniques involving Weighted Random Forests, voting classifiers, and CNN, SVM, Naïve Bayes, and Decision Trees hybrids for improving accuracy on anomaly detection on different feature sets and inductive bias. Other papers deal with streaming analytics involving temporal models RNN and LSTM for online transaction streams for fraud detection. Cost computation, false positives, and drift remain challenges.

A common thread among the articles that emerged here was the implementation of blockchain technologies for secured logging, coordination, and audit trails. The blockchain technologies raise transparency but they also ensure that all efforts within an IDS are validated and enable collaboration but maintain privacy, specifically within federated learning.

Unsupervised methods, clustering, autoencoders, isolation forest, and graph analytics are known for discovering novel attack behaviors but suffer from interpretation and high rates of false positives.

However, some common problems that have been related with all these works include scalability, delay caused by consensus, computational complexity, imbalance in datasets, regulatory compliance, and the need for an explainable and real-time solution.

III. METHODOLOGY

Our system adopts a step-by-step method that analyzes user spending behavior and identifies anything unusual. We start with cleansing and structuring the transaction data into sets with useful and consistent information. We then represent these transactions as sequences so that the model can identify meaningful patterns such as the frequency with which an individual transfers money, the timing associated with these transfers, and the average amount they normally send. We then proceed to feed these sequences into a Convolutional Neural Network.

Once the CNN is done with the extraction of these patterns, these feature extractions are passed on to a Support Vector Machine, which works as a final decision-maker. It assists a transaction classification process as it identifies these discovered patterns. A transaction can be labelled once it undergoes verification. The verified and legitimate ones are then stored within a blockchain ledger. All entries are secured with a cryptographic hash so that no party can make any surreptitious changes to it at a later stage. The above-mentioned mechanism lets an anomalous pattern be detected with precision while also making valid ones tamper-proof and authentic.

IV. EXPERIMENTAL RESULTS

Figures shows the results of Anomaly-Based Intrusion Detection System in Financial Transactions using Ensemble Machine Learning and Blockchain. Figs. (a) Home Page (b) Registration Page (c) Email Validation (d) Email Verified (e) Creating strong Password (f) Registration Successful (g) Detection page (h) Detecting Sender as Fraud (i) Receiver Unknown Alert (j) Transaction Status (k) Blocking the transaction

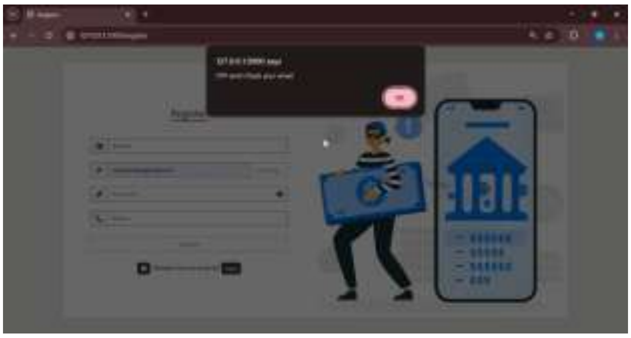
Anomaly-based Intrusion Detection System

(a)

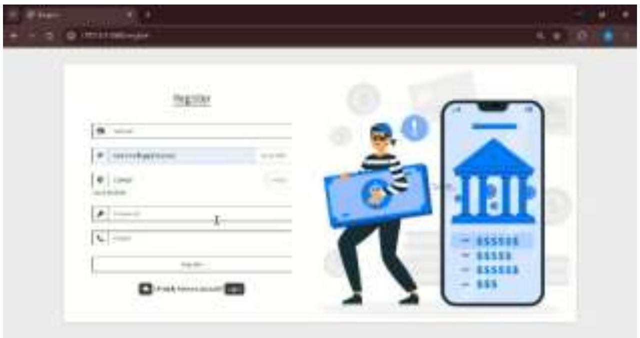
Register

(b)

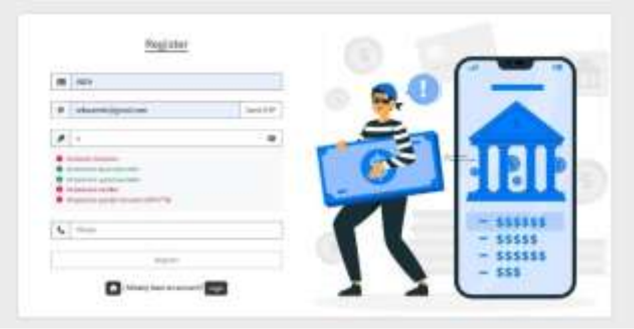
Volume 14, Issue 12, December 2025
|DOI: 10.15680/IJIRSET.2025.1412001|



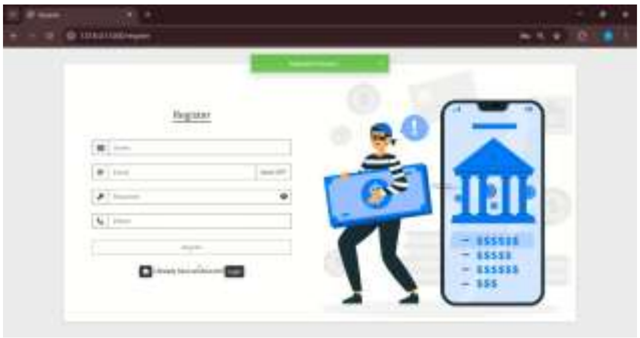
(c)



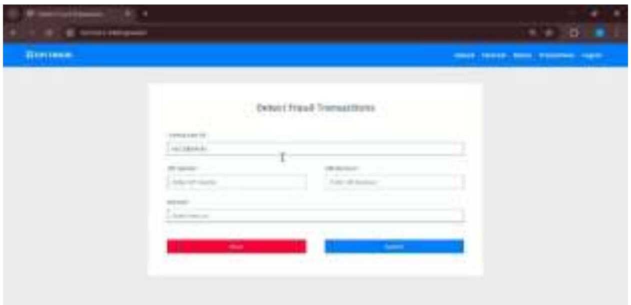
(d)



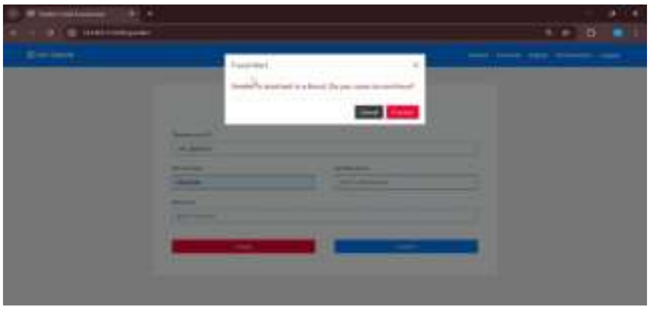
(e)



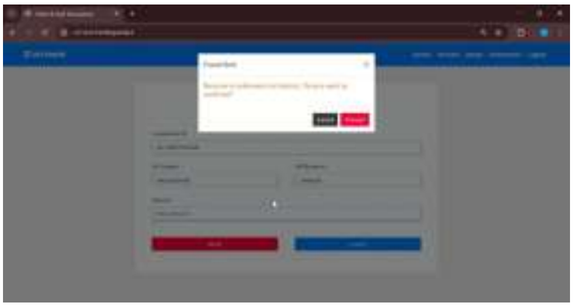
(f)



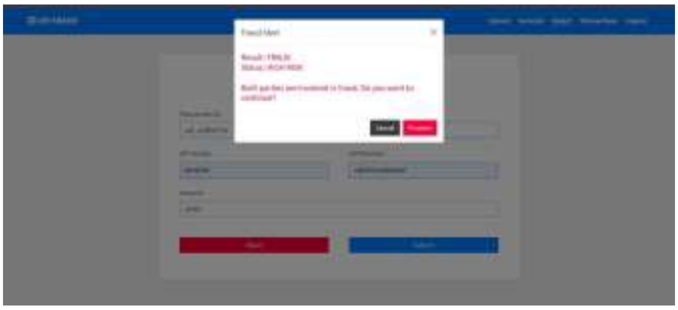
(g)



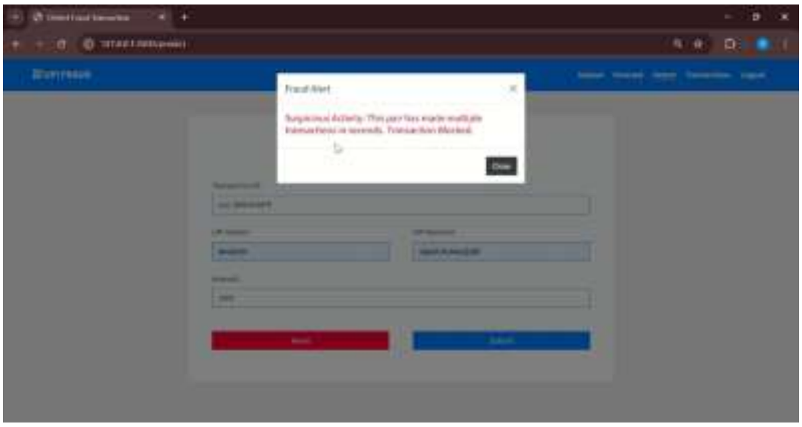
(h)



(i)



(j)


Fraud Alert

Suspicious Activity: This user has made multiple transactions in seconds. Transaction Blocked.

(k)

V. CONCLUSION

As a contribution to research on blockchain and artificial intelligence, we have designed and implemented a system that uses machine learning and blockchain concepts together for flagging unusual/suspicious financial transactions. Our CNN-SVM-based system identifies unusual spending activities based on user regularities not yet experienced and learned before, making it optimized than traditional rule-based systems. By storing legitimate transactions on a blockchain, we have ensured that critical data will not be altered or abused.

REFERENCES

[1] J. Huang, Y. Chen, X. Wang, Z. Ouyang, and N. Du, “Optimization Scheme of Collaborative Intrusion Detection System Based on Blockchain Technology,” Electronics, vol. 14, no. 2, art. 261, 2025.

[2] A. Immadisetty, “Real-Time Fraud Detection Using Streaming Data in Financial Transactions,” Journal of Recent Trends in Computer Science and Engineering (JRTCSE), vol. 13, no. 1, pp. 66–76, 2025. DOI: 10.70589/JRTCSE.2025.13.1.9.

[3] M. Hasan, M. S. Rahman, H. Janicke, and I. H. Sarker, “Detecting Anomalies in Blockchain Transactions Using Machine Learning Classifiers and Explainability Analysis,” Blockchain: Research and Applications, vol. 5, no. 3, art. 100207, 2024. DOI: 10.1016/j.bcra.2024.100207.

[4] A. A. Aliyu, J. Liu, and E. Gilliard, “A Decentralized and Self-Adaptive Intrusion Detection Approach Using Continuous Learning and Blockchain Technology,” Journal of Data Science and Intelligent Systems, Oct. 2024, Online First. DOI: 10.47852/bonviewJDSIS42023803.

[5] S. Siddamsetti, “Anomaly Detection in Blockchain Using Machine Learning,” Journal of Electrical Systems, vol. 20, pp. 619–634, 2024. DOI: 10.52783/jes.2988.

[7] C. Cholevas, E. Angeli, Z. Sereti, E. Mavrikos, and G. E. Tsekouras, “Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey,” Algorithms, vol. 17, no. 5, p. 201, 2024.

[8] R. Lalduhsaka, N. Bora, and A. K. Khan, “Anomaly-Based Intrusion Detection Using Machine Learning: An Ensemble Approach,” International Journal of Information Security and Privacy (IJISP), vol. 16, no. 1, pp. 1–15, 2022.

[9] P. Ramesh, J. K. Lee, and M. González, “Privacy-Preserving Fraud Detection in Financial Systems Using Federated Learning and Blockchain,” International Journal of Secure Financial Computing, vol. 12, no. 3, pp. 145–158, 2021.

[10] W. Zhang, L. Romano, and A. El-Adly, “Graph Neural Networks for Fraud Detection on Transaction Networks,” Journal of Computational Intelligence in Finance, vol. 8, no. 2, pp. 67–84, 2020.