International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

AI-Based Fraud Detection System in Online Transactions

Ms. Tirangini Singh Negi[1], Ms. Varsha Chaurasiya[2], Ms. Priyanshi Trivedi[3], Ms. Upma Mishra[4]

[1,2,3,4]Student, Computer Application, Babu Banarasi Das University

Abstract
In the fast-paced digital world, the habit of online transactions has become part and parcel of everyday life. On the other hand, it has also increased the fraudulent factor regarding cybercrime. Artificial Intelligence, in this regard, may help to a great extent in order to detect fraud and prevent it in real time. This research is aimed at the development of an AI-based fraud detection system with an ability to analyze patterns of transactions for the detection of suspicious behavior in order to minimize financial loss. The system learns from previous transaction data using machine learning algorithms to predict whether a new incoming transaction is genuine or fraudulent. Techniques such as data preprocessing, extraction of features, and classification models are combined in the proposed system for effective anomaly detection with accuracy. This study will enhance the security and trustworthiness of online payment systems to help bank, e-commerce platforms, and users to protect their financial information.
Online financial transactions have grown as a crucial part of the digital economy; at the same time, they are facing fraudulent activities related to phishing, identity theft, and payment manipulation. These kinds of threats are complicated and continuously evolving; hence, it is impossible for traditional systems based on rules to handle them. It is here that AI has proven to be a game-changing solution with the incorporation of ML, DL, and other anomaly detection models. The goal is to facilitate adaptive, data-driven fraud detection. This paper is attempt to unify very recent works and present a holistic perspective on AI-driven fraud detection in online transactions by summarizing the current methodologies, models, datasets, challenges and future directions.

Keywords: Artificial Intelligence (AI), Fraud Detection, Online Transaction, Machine Learning, Anomaly Detection, Financial Cybersecurity, Outlier Detection, Credit Card Fraud, Deep Learning.

1. Introduction

The rapid growth in digital payment systems has revolutionized financial services worldwide, but it has also increased the attack surface for cybercriminals. According to [2], the annual estimated global financial losses on account of fraud will exceed $5 trillion due to identity theft, credit card fraud, and money laundering.

The use of traditional methods of fraud detection-rule-based auditing, manual reviews, and fixed thresholds- is limited by static patterns and high levels of false positives. On the other hand, AI-based systems apply ML algorithms that can detect unknown fraud types in real-time by learning dynamic transactional behaviors.

2. Evolution of Online Fraud

This [3] presents a criminological understanding of online fraud typologies: advance fee fraud, romance scams, and phishing attacks are diverse methods that draw on human psychology and technology to deceive victims.

Table 1 summarizes the major online fraud types and their implications for AI-driven detection.

Table 1: Major Types of Online Fraud

Fraud Type	Description	AI Detection Strategy
Phishing	Deceptive emails appearing from banks/institutions.	NLP-based anomaly detection in messages.
Identity Theft	Unauthorized use of personal information.	Pattern recognition and clustering models.
Advance Fee Fraud	Victim pays small "fee" expecting reward.	Behavioral pattern modeling.
Romance Fraud	Emotional manipulation through dating sites.	Sentiment and Social network analysis.

AI works not only to identify suspicious activities but in finding hidden fraud patterns by correlating behavioral and transactional data.

3. AI and Machine Learning Techniques in Fraud Detection

Machine Learning techniques have revolutionized systems designed for the prevention of financial fraud. According to [5], Machine Learning models are categorized into supervised, unsupervised, and deep learning approaches.

3.1 Supervised Learning Models

Models that are supervised rely on labeled data to perform the classification of a transaction into being either legitimate or fraudulent.

- **Logistic Regression:** Although simple, it works effectively for binary fraud classification.
- **Decision Trees and Random Forests:** They are useful for handling nonlinear relationships.
- **Support Vector Machines (SVMs):** Perform well small to medium-sized data with clear margins.

Example: Random Forests achieved a 92% accuracy rate in detecting credit card fraud compared to the traditional model's 75% as noted by Ali et al., 2022, cited in Bello et al., 2023.

3.2 Unsupervised Learning Models

The unsupervised models, such as K-Means clustering and PCA-based outlier detection, are useful in de-

tecting novel fraud cases for which labeled data is not available [4].
Principal Component Analysis (PCA) reduces high-dimensional data and can effectively isolate abnormal transactions with low computational overhead.

3.3 Deep Learning Models

Advanced architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) process sequential transaction data and detect time-series anomalies of Bello et al. (2023).[5]
Deep Learning improves detection accuracy through the identification of complex temporal dependencies in fraud patterns.

4. Comparative Analysis of Traditional and AI-Based Systems

According to the study by [1], AI audits improved detection accuracy by 15-30% and audit time was reduced by 60% compared to manual methods.
Table 2 summarizes the performance comparisons.

Table 2: Comparison between Traditional and AI- Based Fraud Detection

Criteria	Traditional Systems	AI-Based Systems
Data Handling	Manual / rule-based	Automated and Scalable.
Adaptability	Static rules	Dynamic, self-learning
Accuracy	60-70%	85-95%
Detection Time	Delayed / batch	Real time
Maintenance	Manual updates	Self-optimizing

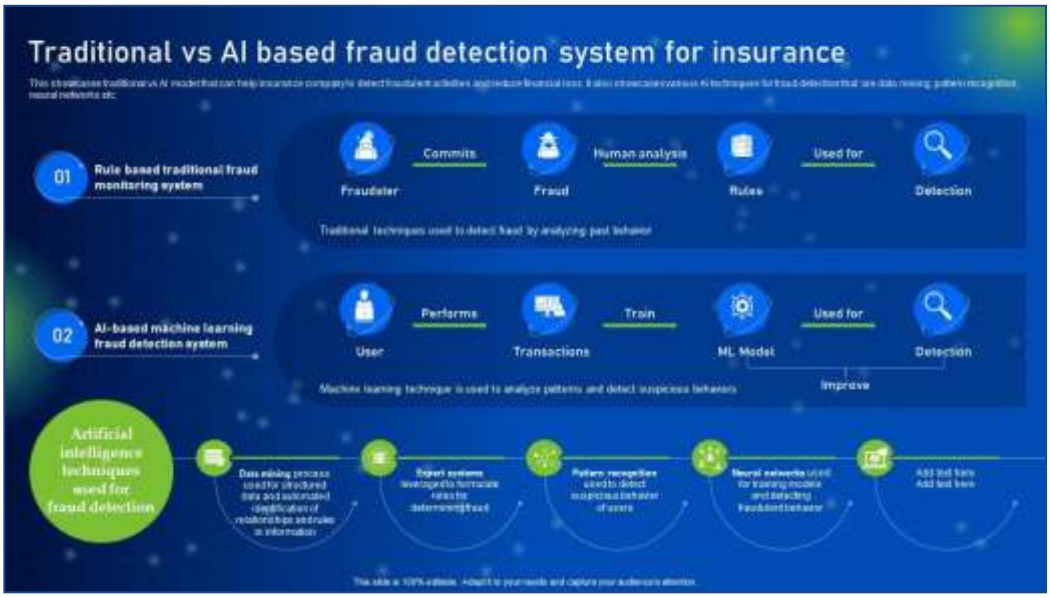

Figure 1 (from slideteam.net) could visualize this accuracy comparison graphically.

5. Outlier Detection and Anomaly Analysis

It finds its main application in outlier detection for credit-card fraud detection.
According to [4] Pawar et al. (2014) classify outlier detection into:
Statistical Methods: Based on probabilistic distributions.
Density-based: Using local outlier factors LOF.
Clustering-based approaches involve the identification of anomalous clusters.
Dimensionality Reduction: Detects anomalies in high-dimensional datasets using Principal Component Analysis (PCA).

6. AI-driven frameworks in Financial Networks

In sum [2] Sarna et al. in 2025, performed a systematic review and presented an AI-driven fraud detection architecture composed of data ingestion, feature engineering, model training, and real-time monitoring.
The AI-Driven Fraud Detection Architecture tells about:
Data Sources: Bank APIs, payment gateways, and e-commerce platforms.
Feature Engineering: transaction frequency, user behavior, device ID
Model Training: ML/DL models (SVM, ANN, CNN, GNN)
Prediction Engine: Classifies transaction as "fraud" or "legit" Feedback Loop: Continuous retraining to reduce false positives.
Graph Neural Networks (GNNs) are powerful tools to detect collaborative and network-based fraud rings since they model relationships between entities. It has been further identified by [2].

7. Ethical, Regulatory, and Practical Challenges

While AI offers unparalleled efficiencies, ethical and regulatory challenges persist.
Data Privacy: AI models often process sensitive personal data, raising compliance issues under GDPR and RBI guidelines.
Model Transparency: Black- box models are not interpretable, which affects trust and auditing (Calestin and Vanith, 2019).
Bias and Fairness: Discrimination can be caused when the data is imbalanced.
Legal Accountability: In as much as fraud detection has been automated, determination of responsibility for errors is not clear.
Kumar (2015) opines that hybrid systems are mandatory, using the efficiency of AI and incorporating human oversight for both accuracy and digital governance.

8. Future Directions

Based on the integrated literature:
Federated Learning: It allows different institutions to cooperate in model training without necessarily sharing sensitive data.
Integration of BlockChain-AI: It enhances transparency and data immutability for secure fraud auditing.
Explainable-AI: It improves the interpretability of models and regulatory compliance.
Edge AI: Brings fraud detection closer to data sources for quicker response time.

9. Conclusion

AI-based Systems greatly enhanced financial institutions' capabilities for fraud detection in online transactions. Supervised, Unsupervised, and deep learning combine to proactively offer scalable and adaptive solutions. However, high-quality datasets, ethical frameworks, and human oversight are needed to ensure the effectiveness of AI systems. The synergy of AI along with blockchain, federated learning, and explainable models is the next frontier in securing the digital financial ecosystem.

10. References

1. Celestin, M., & Vanitha, N. (2019). Artificial Intelligence in Fraud Detection: Are Traditional Auditing Methods Outdated? ICRTASET Conference Proceedings, 180-186.
2. Sarna, N. J., Rithen, F.A., Jui, U. S., Belal, S., Amin, A., & Islam, A. K. M. M. (2025). AI Driven Fraud Detection Models in Financial Networks: A Comprehensive Systematic Review: IEEE Access, 13, 141204-141210.
3. Cross, C. (2019). Online Fraud. Oxford Research Encyclopedia of Criminology. Oxford University Press.
4. Pawar, A. D., Kalavadekar, P. N., & Tambe, S. N. (2014). A Survey on Outlier Detection Techniques for Credit Card Fraud Detection. IOSR Journal of Computer Engineering, 16(2) 44-48.
5. Bello, O. A., Folorunso, A., Ejiofor, O. E., Bundale, F. Z., Adebayo, K., & Babatunde, O.A. (2023). Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions. International Journal of Management Technology, 10(1), 85-109.
6. Kumar, S. (2015). Ethical and Regulatory Challenges of Artificial Intelligence in Auditing: A Review of Emerging Issues. Journal of Accounting and Business Ethics, 12(4), 215-230.