IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 12, December 2025

DOI: 10.17148/IARJSET.2025.121217

Payment Fraud Detection-Using Machine Learning Models

Roopa K Murthy[1], Chethana R[2], Dixitha B[3], Harshitha M[4], Swathi A[5]

Assistant Professor, Computer Science and Design, K. S. Institute of Technology, Bengaluru, India[1]

Student, Computer Science and Design, K. S. Institute of Technology, Bengaluru, India[2-5]

Abstract: Fraud detection has emerged as a vital area of research in the era of digitalization, where financial transactions and online services have become increasingly vulnerable to fraudulent activities. With the expansion of e-commerce, online banking, insurance claims, and telecommunication services, identifying and preventing fraud has become a major challenge for organizations. Traditional rule-based systems, while effective for structured and historical data, often fail to detect new and adaptive fraud patterns. As a result, modern fraud detection systems increasingly rely on advanced data-driven approaches such as Data Mining, Machine Learning, Deep Learning and Artificial Intelligence to recognize suspicious behavior and anomalies in real time.

A comprehensive review of current fraud detection techniques, including supervised learning, unsupervised learning, and hybrid models combine these approaches. It highlights widely used algorithms such as Decision Trees, Random Forests, Neural Networks, Support Vector Machines, and anomaly detection frameworks. Furthermore, it discusses key performance metrics like Precision, Recall, and ROC-AUC, which are essential for evaluating detection efficiency. It also addresses major challenges such as data imbalance, privacy concerns, lack of labeled datasets, and the dynamic nature of fraud schemes. Finally, it outlines emerging research trends focused on explainable Artificial Intelligence (AI), Graph-based Detection, and adaptive learning systems, offering insights into future pathway for building more accurate and resilient fraud detection mechanisms.

Keywords: Fraud Detection, Deep Learning, Graph Neural Network (GNN), Real-Time Credit Card Fraud, Banking Security, Artificial Intelligence.

I. INTRODUCTION

Misconduct is a deliberate act to gain illegal or unfair benefits, posing a major threat to financial systems and businesses. With growing online transactions, misconduct has become complex and harder to detect. Credit Card fraud is one of the most common and serious types of financial fraud, resulting in significant financial losses in online shopping, digital payment apps, ATMs, POS terminals, online banking, social media, and email scams. With the rapid increase in online shopping and digital payments, fraudulent transactions have become more frequent and complex making it increasingly challenging for financial institutions to effectively monitor, identify, and prevent such activities. To address this challenge, Fraud Detection in Credit Card systems relies on advanced techniques such as Machine Learning (ML), Deep Learning, and Anomaly Detection to identify unusual transaction behaviors. These models analyze expenditure patterns, transaction frequency, and user profiles to distinguish between genuine and fraudulent activities. The main objective is to ensure secure transactions, minimize financial losses, and maintain user trust.

IMPORTANCE OF FRAUD DETECTION

Financial Protection: Fraud detection is essential for safeguarding organizations and individuals from financial losses caused by illegal or deceptive activities. In sectors such as banking, e-commerce, insurance, and telecommunications, even a single fraudulent transaction can result in significant economic damage. Effective fraud detection systems helps in identifying anomalies and block suspicious transactions before they escalate. By minimizing financial risks, they contribute to the overall stability and profitability of businesses while protecting customers' assets and sensitive data.

Trust and Security: In today's digital economy, maintaining customer trust is as important as preventing financial loss. Fraud detection systems ensure the authenticity and integrity of transactions, strengthening user confidence in online services. Secure and transparent operations enhance an organization's reputation and ensure compliance with data protection and regulatory standards. This trust encourages greater adoption of digital platforms and contributes to the growth of safe and reliable digital ecosystems.

Adaptation to Evolving Threats: Fraudulent activities are constantly evolving, employing new technologies and

This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IARJSET.2025.121217

sophisticated attack patterns. Modern fraud detection leverages Machine learning, Data analytics, and Artificial Intelligence to dynamically learn from new data and adapt changing threat landscapes. This continuous learning capability enables systems to detect previously unseen fraud schemes in real time, making them more resilient and effective in maintaining security across digital and financial environments.

II. LITERATURE REVIEW

SL NO	YEAR OF PUBLICATION	TITLE	DESCRIPTION
1	2025[1]	AI Driven Fraud Detection Models in Financial Networks: A Comprehensive Sytematic Review	A systematic review on AI-driven fraud detection in financial networks, highlighting how Machine Learning, Deep learning, Hybrid Models, and Graph-based techniques significantly enhance fraud identification across banking, insurance, and digital payment systems. The study shows that AI offers major advantages such as higher accuracy, real-time monitoring, scalability, and reduced false positives, especially when integrated with cloud computing, blockchain, and federated learning. However, the authors identify limitations including low explainability in complex models, data privacy risks, algorithmic bias, high implementation costs, and the need for continuous retraining due to evolving fraud patterns. Overall, the review concludes that AI-based approaches outperform traditional detection methods and recommends future development of transparent, ethical, and privacy-preserving.AI frameworks to strengthen global financial security.[1]
2	2025[2]	An Integrated Preprocessing and Drift Detection Approach With Adaptive Windowing for Fraud Detection in Payment Systems	An integrated framework for real-time fraud detection in payment systems. Combines advanced data preprocessing, feature selection (Mutual Information, SelectKBest), and ADASYN for handling class imbalance with Convolutional Neural Networks (CNNs) to capture complex fraud patterns. To address evolving fraud tactics, the model incorporates Early Drift Detection Method (EDDM) and Adaptive Windowing (ADWIN), enabling detection of both gradual and abrupt data drifts. The proposed approach achieved up to 99.99% accuracy, effectively reducing false positives and adapts in changing transaction behaviors. While the system requires high computational resources and expert implementation, it demonstrates exceptional adaptability, scalability, and reliability. Overall, the framework offers a dynamic and drift-aware Deep Learning solution for maintaining consistent, real- time fraud detection performance in modern banking and payment systems.[2]
3	2025[3]	Enhancing Medicare Fraud Detection With a CNN-Transformer-XGBoost Framework and Explainable AI	A hybrid fraud detection framework combining CNNs, Transformers, XGBoost, and domain-specific features uses SHAP(SHapley Additive exPlanations) for explainability and evaluates performance on two Medicare-related datasets. High F1-score (0.92–0.95) and AUC (0.96–0.98); captures complex patterns, explainability via SHAP, scalable and efficient, strong generalization across datasets. Requires high-quality labeled data complexity of Deep Learning components, interpretability of deep modules still

DOI: 10.17148/IARJSET.2025.121217

			limited generalization to other healthcare systems not fully tested. The hybrid model outperforms state-of-the-art methods and offers accurate, interpretable, and scalable Medicare fraud detection. Future improvements include GNNs(Graph Neural Network), semi-supervised learning, and broader dataset validation.[3]
4	2025[4]	FRAUD-X: An Integrated AI, Blockchain, and Cybersecurity Framework With Early Warning Systems for Mitigating Online Financial Fraud: A Case Study From North Macedonia	To detect and prevent online financial fraud A Tested on dataset from Kaggle and North Macedonian banks, the framework achieved an AUC of ~0.99,F1-score improvement of 2–4%, and~90% recall for zero-day threats, all while maintaining real-time performance (~15–16 ms per transaction).FRAUD-X enhances detection accuracy, ensures tamper-proof records, and enables rapid fraud response through its synergy-based approach. However, it demands high computational resources, skilled technical staff, and careful system integration. The study demonstrates that multi-layered synergy significantly outperforms single-method fraud detection, offering a scalable, secure, and efficient model suited for mid-sized banking sectors like North Macedonia.[4]
5	2025[5]	Enhancing Fraud Detection in Banking With Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention	A Deep Learning–based fraud detection framework using Graph Neural Networks and Autoencoders to identify real-time credit card fraud by analyzing both streaming and historical banking data. The approach offers high accuracy, adaptive learning, real-time monitoring, reduced false positives, and strong scalability for large financial datasets. However, it requires significant computational resources which involves complex implementation, faces challenges with imbalanced data, and provides limited interpretability due to its black-box nature. The study concludes that integrating Deep Learning with business intelligence greatly enhances fraud detection efficiency, providing a scalable and reliable solution for identifying both known and emerging fraud patterns in modern banking systems.[5]
6	2024[6]	Quantum Autoencoder for Enhanced Fraud Detection in Imbalanced Credit Card Dataset	The classical methods that combines quantum computing encodes and analyzes transactions, improving anomaly detection accuracy and computational performance. Achieves high performance with G-mean = 0.946 and AUC = 0.947. Effectively handles imbalanced datasets uses only 4 qubits, showing efficient quantum resource utilization. The major drawback is the performance degradation in noisy environments. Increased circuit depth beyond 5 layers leads to overfitting. In Hardware limitations due to NISQ devices. the QAE-FD model surpasses classical and quantum methods in accuracy and efficiency, proving quantum autoencoders enhance fraud detection. The further study suggests work on noise reduction, interpretability, and comparisons with classical Machine Learning models.[6]
7	2024[7]	Machine Learning Methods for Credit Card Fraud Detection: A	A comprehensive and structured analysis of Machine Learning emphasizes the growing need for advanced analytical systems as online transactions continue to

		Survey	expand. It examines core challenges such as severe class imbalance, concept drift, and the limited availability of high-quality public datasets, while offering a systematic comparison of rule-based methods, classical Machine Learning models, and modern Deep Learning techniques. A notable contribution of this review is its well-defined taxonomy that organizes datasets, detection challenges, methodological strategies, and contextual modeling frameworks. Despite its strengths, the work also identifies persistent issues, including inconsistent evaluation metrics and restricted data accessibility, which hinder reproducibility across studies. Ultimately, the review highlights that incorporating contextual information, employing synthetic data generation methods, and adopting robust evaluation frameworks can significantly enhance the performance and reliability of real-world fraud detection systems.
8	2024[8]	Robust Credit Card Fraud Detection Based on Efficient Kolmogorov-Arnold Network Models	This p aper focuses on improving credit card fraud detection by comparing traditional Multilayer Perceptrons (MLPs) with Kolmogorov–Arnold Networks (KAN) and a more optimized version called Efficient KAN. The introduction highlights on how fraud has become more sophisticated, making it essential to use models that are not only accurate but also easy to interpret. The key advantage of KAN is that it offers better transparency and higher detection performance with fewer parameters, while Efficient KAN adds faster training and prediction speeds. However, the standard KAN model has drawbacks such as slower training times and occasional instability during learning. The findings show that both KAN models outperform MLP in accuracy, F1-score, and AUC. This results in KAN that provides a strong, interpretable, and efficient solution for fraud detection systems.[8]
9	2024[9]	OptDevNet: A Optimized Deep Event-Based Network Framework for Credit Card Fraud Detection	This paper explores that older methods like Logistic Regression, SVM, KNN, and Random Forest do not work well when the amount of fraud data is very small. t, the main idea of OptDevNet is to learn how normal transactions usually look and then find tran from this pattern. The model gives each transaction a score and uses this score to the main de if it is fraud or not. Based on the results OptDevNet performs better than all the other models tested and is more reliable for finding fraud. Overall, the study demonstrates that KAN models offer a more transparent and reliable alternative for modern credit card fraud detection.[9]
10	2024[10]	Using Graph Attention Networks in Healthcare Provider Fraud Detection	The healthcare fraud detection by highlighting the limitations of rule-based and traditional Machine-Learning approaches, which fail to capture evolving fraud patterns and the relationships among providers, physicians, and patients. Since many fraud schemes involve collaboration, the authors emphasize the need for relational modeling. Earlier graph-based methods, such as community detection and label propagation,

			considered relationships but could not jointly represent intrinsic provider features and the varying importance of neighboring entities. To overcome this, the study applies a Graph Attention Network (GAT) that embeds both procedure-code features and inter-provider links formed through shared patients and physicians. Experimental results on a public dataset shows that the GAT model achieves higher Recall than XGBoost, Random Forest, and Graph Transformer Networks, making it more effective for identifying fraudulent providers.[10]
11	2024[11]	Financial Fraud Detection Using Value-at-Risk With Machine Learning in Skewed Data	Thus the Value-at-Risk (VaR) with machine learning to detect new bank account fraud in highly imbalanced datasets. VaR treats fraud as a worst-case risk scenario and generates risk-based features that enhance the model's ability to classify rare fraudulent events. Among the tested models, K-Nearest Neighbor (KNN) delivered the highest accuracy and detection rate, demonstrating the effectiveness of combining VaR with ML techniques. The advantages includes improved handling of skewed data, higher fraud sensitivity, the introduction of risk-aware evaluation metrics, and stronger overall detection performance. However, the framework also presents limitations such as high computational cost, reliance on extensive feature engineering, limited dataset availability, and the absence of temporal fraud pattern analysis. The result shows that VaR-based machine learning significantly improves the detection of rare fraud cases and provides a reliable risk-aware framework, though broader datasets and temporal modeling are needed for real-world deployment.[11]
12	2023[12]	Online Payment Fraud Detection Model Using Maching Learning Techniques	A hybrid fraud detection framework that combines a ResNeXt-embedded GRU model with the Jaya optimization algorithm, supported by SMOTE balancing and the EARN feature extraction method. The approach aims to overcome major limitations in financial fraud detection, such as data imbalance, weak feature representation, and poor generalization. The model achieves around 98% accuracy, outperforming traditional machine-learning methods by 10–18%,mainly due to optimized hyperparameters and richer feature learning. However, the framework still faces challenges, including the risk of overfitting the minority (fraud) class, PCA's inability to capture nonlinear features, and limited generalizability across diverse datasets. The study proposed by RXT-J model demonstrates strong efficiency, better scalability, and faster fraud identification. The study highlights that quantum autoencoder–based models like QAE-FD may further enhance accuracy and encourages future work on noise reduction, interpretability, and broader model comparisons.[12]

DOI: 10.17148/IARJSET.2025.121217

III. CONCLUSION

Fraud detection in credit cards and online has evolved substantially with the adoption of Machine Learning, Deep Learning, and hybrid models. Advanced techniques like autoencoders, ensemble learning, and quantum-inspired methods have enhanced detection accuracy, particularly for highly imbalanced datasets. Preprocessing methods such as SMOTE and hyperparameter optimization improve model performance, while real-time deployment ensures timely threat mitigation. Despite these advancements, challenges like overfitting, limited generalizability, and model interpretability persist. Future research should focus on integrating contextual information, explainable AI, and scalable, adaptive frameworks to further strengthen robustness, efficiency, and security against increasingly sophisticated fraudulent activities in financial and digital communication system.

REFERENCES

[1]. NUSRAT JAHAN SARNA, FARZANA AHMED RITHEN, UMME SALMA JUI, SAYMA BELAL, AL AMIN, TASNIM KABIR OISHEE and A.K.M. MUZAHIDUL ISLAM," AI Driven Fraud Detection Models in Financial Networks: A Comprehensive Systematic Review," in IEEE Access, vol.13, pp. 141204 141233, 2025, doi:10.1109/ACCESS.2025.3596060.

[2]. HADI M. R. AL LAWATI, ANAZIDA ZAINAL BANDER ALI SALEH AL- RIMY, (Senior Member, IEEE), MOHAMMAD AL-AZAW, MOHAMADNIZAMKASSIM, SULTAN AHMED ALMALKI, AND TAMI ABDULRAHMAN ALGHAMDI," An Integrated Preprocessing and Drift Detection Approach With Adaptive Windowing for Fraud Detection in Payment Systems." in IEEE Access, vol.13,pp.92036 – 92056,2025,doi: 10.1109/ACCESS.2025.3569609.

[3]. MOHAMMADBALAYET HOSSAIN SAKIL, MDAMIT HASAN, MD SHAHIN ALAM MOZUMDER2, MDROKIBUL HASAN, SHAFIUL AJAM OPEE, M.F. MRIDHA, AND ZEYAR AUNG, "Enhancing Medicare Fraud Detection With a CNN-Transformer-XGBoost Framework and Explainable AI." In IEEE Access, vol.13, pp. 79609- 79622,2025, Doi: 10.1109/ACCESS.2025.3562577

[4]. BEKIM FETAJI, MAJLINDA FETAJI, AFFAN HASAN, SHPETIM REXHEPI, AND GOCEARMENSKI, "FRAUD-X: An Integrated AI, Blockchain, and Cybersecurity Framework With Early Warning Systems for Mitigating Online Financial Fraud: A Case Study From North Macedonia." in IEEE Access, vol.13,pp. 48068-48082, Doi: 10.1109/ACCESS.2025.3547285

[5]. FAWAZ KHALED ALARFAJ and SHABNAMSHAHZADI," Enhancing Fraud Detection in Banking With Deep Learning: Graph Neural Networks and Autoencoders for Real-Time Credit Card Fraud Prevention," in IEEE Access, vol.13, pp.20633 -20646,2025, doi:10.1109/ACCESS.2024.3466288.

[6]. CHANSREYNICH HUOT YOUNGSUN HAN, SOVANMONYNUTH HENG, TAE-KYUNG KIM," Quantum Autoencoder for Enhanced Fraud Detection in Imbalanced Credit Card Dataset," in IEEE Access, vol.12, pp.169671 - 169682,2024, doi:10.1109/ACCESS.2024.3496901.

[7]. KANISHKA GHOSH DASTIDAR, OLIVIER CAELEN, ANDMICHAEL GRANITZER," Machine Learning Methods for Credit Card Fraud Detection: A Survey," in IEEE Access, vol.12, pp. 158939–158965,2024 Doi: 10.1109/ACCESS.2024.3487298.

[8]. THI-THU-HUONG LE AND HOWONKIM, YEONJEONG HWANG, HYOEUNKANG, (Member, IEEE)," obust Credit Card Fraud Detection Based on Efficient Kolmogorov-Arnold Network Models," in IEEE Access, vol.12, pp. 157006 – 157020,2024, Doi: 10.1109/ACCESS.2024.3485200.

[9]. MUHAMMADADIL, ZHANG YINJUN2, MONAM. JAMJOOM, AND ZAHID ULLAH, " Opt DevNet: A Optimized Deep Event-Based Network Framework for Credit Card Fraud Detection." in IEEE Access, vol.12. pp. 132421- 132433,2024, Doi: 10.1109/ACCESS.2024.3458944.

[10]. SHAHLA MARDANI AND HADIMORADI," Using Graph Attention Networks in Healthcare Provider Fraud Detection," in IEEE Access, vol.12, pp. 132786– 132800,2024, Doi: 10.1109/ACCESS.2024.3425892.

[11]. ABDULLAHI UBALE USMAN, SUNUSI BALA ABDULLAHI, YU LIPING, BAYAN ALGHOFAILY, AHMED S. ALMASOUD and AMJAD REHMAN, "Financial Fraud Detection Using Value- at-Risk With Machine Learning in Skewed Data," in IEEE Access, vol.12, pp.64285-64299, 2024, doi: 10.1109/ACCESS.2024.3393154.

[12]. ABDULWAHAB ALI ALMAZROI and NASIRAYUB, "Online Payment Fraud Detection Model Using Machine Learning Techniques," in IEEE Access, vol.11, pp. 137188 - 137203,2023, doi:10.1109/ACCESS.2023.3339226.