International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 15, Issue 01, January 2026)

Credit Card Fraud Detection using AI Techniques

Sanskriti Verma[1], Rahul Kumar[2]

[1]*Research Scholar,* [2]*Assistant Professor, Department of CSE, BIT, Meerut, India*

***Abstract*— This paper presents an efficient Credit Card Fraud Detection system using Artificial Intelligence (AI) techniques to identify and prevent fraudulent financial transactions in real time. The proposed approach leverages machine learning and deep learning models to analyze transaction patterns, user behavior, and historical data for distinguishing legitimate transactions from fraudulent ones. Advanced techniques such as anomaly detection, supervised classification, and feature optimization are employed to handle highly imbalanced datasets and evolving fraud strategies. The system aims to improve detection accuracy, reduce false positives, and enhance transaction security, thereby supporting financial institutions in minimizing monetary losses and strengthening customer trust in digital payment systems.**

***Keywords*— Credit Card Fraud, AI, Machine Learning, Anomaly Detection, Transaction Security, Fraud Classification.**

I. Introduction

Credit card fraud has emerged as one of the most critical challenges in the modern digital financial ecosystem due to the rapid growth of online banking, e-commerce platforms, and cashless transactions. With the increasing dependence on credit and debit cards for everyday purchases, fraudsters continuously exploit vulnerabilities in payment systems to perform unauthorized transactions [1]. Credit card fraud typically occurs when sensitive card information such as card number, CVV, or expiration date is stolen or misused, leading to financial losses for both customers and financial institutions. As transaction volumes grow exponentially, traditional manual monitoring and rule-based systems have become insufficient to effectively detect and prevent fraudulent activities in real time[2].

The complexity of credit card fraud detection lies in the dynamic and evolving nature of fraudulent patterns. Fraudsters frequently modify their strategies to bypass security mechanisms, making it difficult to rely on static rules or predefined thresholds. Moreover, genuine customer behavior can vary significantly based on time, location, spending habits, and lifestyle, which increases the chances of false alarms[3]. A system that incorrectly flags legitimate transactions as fraudulent can cause inconvenience to customers and damage trust in financial services. Therefore, achieving a balance between accurate fraud detection and minimal false positives remains a major challenge in credit card fraud management [4].

Another major issue in credit card fraud detection is data imbalance. In real-world transaction datasets, fraudulent transactions represent only a very small fraction compared to legitimate ones [5]. This imbalance makes it difficult for conventional detection techniques to learn fraud patterns effectively, often resulting in biased models that favor non-fraudulent transactions. Additionally, credit card transaction data is high-dimensional and time-sensitive, requiring intelligent analysis to capture hidden patterns, correlations, and anomalies within large-scale datasets [6].

To address these challenges, advanced analytical approaches are increasingly being explored to enhance fraud detection capabilities. Modern credit card fraud detection systems focus on analyzing transaction behavior rather than relying solely on static authentication mechanisms. These systems continuously monitor transaction streams, detect unusual spending patterns, and adapt to changing fraud tactics[7]. Real-time detection has become especially important, as delayed identification of fraudulent transactions can result in significant financial damage and complex recovery processes[8].

Furthermore, credit card fraud not only causes direct monetary losses but also leads to indirect consequences such as reputational damage, legal complications, and reduced customer confidence. Financial institutions are required to invest heavily in fraud prevention infrastructure while complying with strict regulatory and security standards[9]. As digital payments continue to expand globally, the need for robust, scalable, and intelligent credit card fraud detection mechanisms has become more critical than ever[10].

Credit card fraud detection has evolved into a key research and practical domain within financial security systems. The focus is no longer limited to identifying fraud after it occurs, but rather on proactively preventing fraudulent transactions before they are completed[11]. Effective fraud detection systems play a vital role in ensuring secure financial transactions, protecting customer assets, and maintaining the integrity of digital payment ecosystems[12].

II. Literature Survey

Yadlapalli et al., [1] presented a credit card fraud detection framework using multiple machine learning algorithms combined with an Artificial Neural Network.

The study evaluated models such as Logistic Regression, Random Forest, and ANN on real transaction data. Experimental results showed that the ANN model achieved higher detection accuracy of around 97% compared to traditional classifiers. The authors highlighted the effectiveness of neural networks in learning complex transaction patterns. However, the model required careful tuning to handle class imbalance. The study emphasized real-time applicability in banking systems.

Ojugo et al., [2] introduced a spectral-clustering-based fraud detection approach integrated with a genetic algorithm and modular deep learning network. The model focused on improving feature grouping and optimization for fraud classification. Results indicated an improvement of nearly 5–7% in detection accuracy over conventional clustering methods. The genetic algorithm enhanced convergence speed and reduced overfitting. The study demonstrated robustness against noisy transaction data. However, computational complexity was relatively high.

Akande et al., [3] presented a supervised credit card fraud detection system using an artificial neural network. The model was trained on labeled transaction datasets to distinguish fraudulent and genuine activities. Experimental analysis showed an accuracy of approximately 96% with improved recall for fraud cases. The authors emphasized the importance of proper data preprocessing and normalization. The approach performed well on balanced datasets. Limitations were observed when handling highly skewed real-world data.

Ileberi et al., [4] presented a machine learning-based fraud detection framework using a genetic algorithm for feature selection. The GA was used to reduce redundant attributes and improve classifier performance. Results demonstrated that optimized features increased detection accuracy by nearly 4%. The study compared multiple classifiers, including SVM and Random Forest. The proposed method reduced false positive rates significantly. The authors highlighted scalability for large financial datasets.

Shaji et al., [5] developed a fraud detection model using Artificial Neural Networks and Support Vector Machines. The study compared both techniques on transaction datasets to analyze performance differences. Results showed that ANN slightly outperformed SVM with an accuracy of about 95%. The hybrid analysis helped identify strengths of each algorithm. The system effectively detected known fraud patterns. However, adaptability to emerging fraud types was limited.

Bin Sulaiman et al., [6] provided a comprehensive review of machine learning approaches for credit card fraud detection. The paper discussed supervised, unsupervised, and hybrid techniques used in recent research. Comparative analysis indicated that ensemble models generally outperform single classifiers. The review highlighted challenges such as data imbalance and concept drift. Performance metrics across studies ranged between 90% and 98% accuracy. The authors emphasized the need for real-time intelligent systems.

Fara et al., [7] presented a detailed review of machine learning applications in credit card fraud detection along with a practical case study. The study analyzed classification techniques such as decision trees, SVM, and neural networks. Results from the case study showed detection accuracy close to 94%. The paper emphasized model interpretability and explainability. Data imbalance was identified as a major challenge. The author suggested hybrid approaches for improved performance.

Trivedi et al., [8] presented an efficient fraud detection model using multiple machine learning methods. The study evaluated algorithms such as Random Forest, KNN, and Logistic Regression. Experimental results showed Random Forest achieving the best accuracy of around 97%. The authors highlighted reduced false negatives as a key advantage. The model was computationally efficient for large datasets. However, feature engineering played a crucial role in performance.

Adewumi and Akinyelu et al., [9] presented a survey of machine learning and nature-inspired techniques for credit card fraud detection. The paper analyzed evolutionary algorithms, neural networks, and hybrid methods. The survey revealed that bio-inspired models improve optimization and detection rates. Reported accuracies across studies varied between 85% and 99%. The authors discussed strengths and limitations of each approach. The work served as a foundational reference for future research.

Sadgali et al., [10] presented a neural network-based approach for detecting fraudulent credit card transactions. The model focused on learning transaction behavior patterns over time. Experimental results demonstrated an accuracy of approximately 93% on benchmark datasets. The study highlighted the importance of hidden layer tuning. The approach effectively reduced false positives. However, training time increased with larger datasets.

Varmedja et al., [11] analyzed various machine learning methods for credit card fraud detection. The study compared decision trees, neural networks, and ensemble models.

Results showed ensemble techniques achieving superior performance with accuracy above 96%. The authors emphasized evaluation using precision and recall metrics. The study addressed real-world deployment challenges. Data imbalance remained a significant concern.

Lakshmi and Kavilla et al., [12] presented a machine learning-based credit card fraud detection system focusing on classification accuracy. The study applied algorithms such as Naive Bayes and decision trees. Results indicated accuracy levels around 92–95% depending on the classifier. The system effectively identified suspicious transactions. The authors emphasized simplicity and low computational cost. The approach was suitable for small-scale financial systems.

Table 1:
Summary of Literature review

Sr. No	Author	Year	Work	Outcome
1	Yadlapalli et al.	2025	Machine learning and ANN-based credit card fraud detection	ANN achieved ~97% accuracy with improved fraud classification and reduced false alarms
2	Ojugo et al.	2021	Spectral clustering with GA-trained deep learning network	Detection accuracy improved by 5–7% with better feature optimization
3	Akande et al.	2021	Supervised ANN-based fraud detection approach	Achieved ~96% accuracy with strong recall for fraudulent transactions
4	Ileberi et al.	2022	GA-based feature selection with ML classifiers	Feature optimization improved accuracy by ~4% and reduced false positives
5	Shaji et al.	2021	ANN and SVM-based fraud detection model	ANN outperformed SVM with ~95% detection accuracy
6	Bin Sulaiman et al.	2022	Review of ML approaches for fraud detection	Ensemble models showed superior performance (90–98% accuracy range)
7	Faraji	2022	Review with case study on ML-based fraud detection	Case study achieved ~94% accuracy; highlighted data imbalance challenges
8	Trivedi et al.	2020	Efficient ML-based fraud detection model	Random Forest achieved ~97% accuracy with low false negatives
9	Adewumi & Akinyelu	2017	Survey of ML and nature-inspired techniques	Reported accuracy range of 85–99%; highlighted hybrid model benefits
10	Sadgali et al.	2019	Neural network-based fraud detection	Achieved ~93% accuracy with reduced false positive rate
11	Varmedja et al.	2019	Comparative analysis of ML techniques	Ensemble methods achieved >96% accuracy
12	Lakshmi & Kavilla	2018	ML-based credit card fraud detection system	Ensemble methods achieved >96% accuracy

III. CHALLENGES

Credit card fraud detection is a complex and continuously evolving problem due to the rapid expansion of digital payment systems and the increasing sophistication of fraudulent activities. Fraudsters constantly adapt their techniques to bypass security mechanisms, making it difficult to design a system that remains effective over time. At the same time, genuine customer behavior is highly dynamic and unpredictable, which increases the risk of misclassification. A practical fraud detection system must operate in real time, maintain high accuracy, protect user privacy, and comply with strict financial regulations, all while minimizing inconvenience to legitimate users. These conflicting requirements make credit card fraud detection one of the most challenging applications in financial security systems.

1. Imbalanced Transaction Data

In real-world datasets, fraudulent transactions represent only a very small percentage compared to legitimate ones. This severe class imbalance causes machine learning models to become biased toward non-fraudulent transactions, resulting in poor fraud detection rates. Standard classifiers may achieve high overall accuracy but fail to correctly identify fraud cases. Special techniques such as resampling, cost-sensitive learning, or anomaly detection are often required to address this challenge.

2. Evolving Fraud Patterns (Concept Drift)

Fraud strategies change continuously as attackers learn and adapt to existing detection mechanisms. A model trained on historical data may become ineffective when new fraud patterns emerge. This phenomenon, known as concept drift, requires fraud detection systems to be regularly updated or retrained. Failure to handle concept drift can significantly reduce detection accuracy over time.

3. High False Positive Rates

Incorrectly classifying legitimate transactions as fraudulent leads to false positives, which can block genuine customer purchases. Frequent false alerts frustrate customers and reduce trust in financial institutions. Balancing fraud detection sensitivity while minimizing false positives is difficult, as stricter rules may improve detection but harm user experience.

4. Real-Time Detection Requirements

Credit card transactions must be evaluated within milliseconds to allow seamless payment authorization. Complex machine learning models may offer high accuracy but require significant computation time. Designing models that are both accurate and fast enough for real-time decision-making is a major technical challenge in fraud detection systems.

5. Dynamic Customer Behavior

Customer spending behavior varies based on location, time, lifestyle changes, and seasonal factors. A sudden change in spending pattern may be legitimate rather than fraudulent. Capturing such behavioral variations without triggering false alarms requires adaptive and context-aware detection models.

6. Data Privacy and Security Constraints

Credit card transaction data is highly sensitive and subject to strict privacy regulations. Access to detailed data for model training and evaluation is often limited. Ensuring secure data handling while maintaining model effectiveness is a critical challenge, especially when using centralized or cloud-based systems.

7. Limited Availability of Labeled Fraud Data

Obtaining accurately labeled fraud data is difficult, as fraud cases are rare and labeling often requires manual verification. Delayed or incorrect labels can degrade model performance. This limitation makes supervised learning approaches less effective and increases the need for semi-supervised or unsupervised methods.

8. Model Interpretability and Trust

Many advanced fraud detection models, such as deep learning systems, operate as black boxes. Financial institutions and regulators require explanations for why a transaction is flagged as fraudulent. Lack of interpretability reduces trust in automated systems and makes compliance and auditing more difficult.

IV. Strategies

Credit card fraud detection strategies are designed to ensure accurate identification of fraudulent transactions while maintaining smooth and secure payment experiences for genuine users. Due to the increasing volume of digital transactions and the continuously changing nature of fraud techniques, effective strategies must focus on adaptability, accuracy, and real-time performance. These strategies aim to overcome challenges such as data imbalance, evolving fraud patterns, high false positives, and privacy constraints, while ensuring scalability and regulatory compliance in financial systems.

1. *Behavioral Pattern Analysis*--Analyzing customer spending behavior, transaction frequency, location, and merchant usage helps in identifying deviations that may indicate fraudulent activity.
2. *Imbalanced Data Handling Techniques*--Applying resampling methods and cost-sensitive learning ensures that fraud cases are adequately learned despite their low occurrence in transaction datasets.
3. *Hybrid and Ensemble Modeling*--Combining multiple machine learning models improves detection accuracy and robustness by leveraging the strengths of different algorithms.
4. *Real-Time Transaction Monitoring*--Continuous monitoring of transaction streams enables immediate detection and prevention of fraudulent transactions with minimal delay.
5. *Adaptive Learning Mechanisms*--Periodic model updates and online learning help the system adapt to evolving fraud patterns and concept drift.
6. *Feature Selection and Optimization*--Selecting relevant transaction features reduces model complexity and enhances classification performance.
7. *False Positive Reduction Strategies*-- Threshold tuning and risk scoring mechanisms help minimize incorrect fraud alerts and improve customer experience.
8. *Explainability and Compliance Support*--Incorporating explainable decision mechanisms ensures transparency, regulatory compliance, and trust in automated fraud detection systems.

V. Conclusion

Credit card fraud detection has become a critical requirement in today’s digital financial environment due to the rapid increase in online and cashless transactions.

Traditional rule-based systems are no longer sufficient to handle the complexity, scale, and evolving nature of fraudulent activities. Intelligent detection approaches focus on analyzing transaction behavior, managing data imbalance, and adapting to changing fraud patterns while ensuring real-time performance. An effective fraud detection system must balance high detection accuracy with low false positive rates to maintain customer trust and operational efficiency. Overall, robust and adaptive fraud detection mechanisms play a vital role in safeguarding financial transactions, reducing economic losses, and ensuring the security and reliability of modern payment systems.

REFERENCES

[1] P. Yadlapalli, P. Srivatsal, N. Polimera and M. Srinivas, "Credit Card Fraud Detection using Machine learning algorithms and Artificial Neural Network," 2025 International Conference on Artificial Intelligence and Data Engineering (AIDE), Nitte, India, 2025, pp. 539-542, doi: 10.1109/AIDE64228.2025.10987537.

[2] Ojugo, Arnold Adimabua, and Obinna Nwankwo. "Spectral-cluster solution for credit-card fraud detection using a genetic algorithm trained modular deep learning neural network." JINAV: Journal of Information and Visualization 2. 1 (2021): 15 - 24.

[3] Akande, Oluwatobi Noah, et al. "A supervised approach to credit card fraud detection using an artificial neural network." Applied Informatics: Fourth International Conference, ICAI 2021, Buenos Aires, Argentina, October 28–30, 2021, Proceedings 4. Springer International Publishing, 2021.

[4] Ileberi, Emmanuel, Yanxia Sun, and Zenghui Wang. "A machine learning based credit card fraud detection using the GA algorithm for feature selection." Journal of Big Data 9. 1 (2022): 24.

[5] Shaji, Anchana, et al. "Fraud detection in credit card transaction using ann and svm." Ubiquitous Communications and Network Computing: 4th EAI International Conference, UBICNET 2021, Virtual Event, March 2021, Proceedings. Springer International Publishing, 2021.

[6] Bin Sulaiman, Rejwan, Vitaly Schetinin, and Paul Sant. "Review of machine learning approach on credit card fraud detection." Human-Centric Intelligent Systems 2. 1 (2022): 55 - 68.

[7] Faraji, Z. (2022). A review of machine learning applications for credit card fraud detection with a case study. SEISENSE Journal of Management, 5 (1), 49 - 59.

[8] Trivedi, N. K., Simaiya, S., Lilhore, U. K., & Sharma, S. K. (2020). An efficient credit card fraud detection model based on machine learning methods. International Journal of Advanced Science and Technology, 29 (5), 3414 - 3424.

[9] Adewumi, A. O., & Akinyelu, A. A. (2017). A survey of machine-learning and nature-inspired based credit card fraud detection techniques. International Journal of System Assurance Engineering and Management, 8, 937 - 953.

[10] Sadgali, I., Sael, N., & Benabbou, F. (2019, October). Fraud detection in credit card transaction using neural networks. In Proceedings of the 4th international conference on smart city applications (pp. 1 - 4).

[11] Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., & Anderla, A. (2019, March). Credit card fraud detection-machine learning methods. In 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1 - 5). IEEE.

[12] Lakshmi, S. V. S. S., & Kavilla, S. D. (2018). Machine learning for credit card fraud detection system. International Journal of Applied Engineering Research, 13 (24), 16819 - 16824.