International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 07 Jul-2026 | Impact Factor: 3.5

Credit Card Fraud Detection using Machine Learning Algorithms

Narkhede Vaishnavi Padmakar[1], Dr. Harsh Lohiya[2], Mr. Manoj Yadav[3]

Research Scholar, Department of Computer Science and Engineering, SSSUTMS, Sehore [1]

Associate Professor, Department of Computer Science and Engineering, SSSUTMS, Sehore [2]

Assistant Professor, Department of Computer Science and Engineering, SSSUTMS, Sehore [3]

How to Cite this Article:

Padmakar, N. V., Lohiya, H. & Yadav, M. (2026). Credit Card Fraud Detection using Machine Learning Algorithms. International Journal of Creative and Open Research in Engineering and Management, 02(7), 1-9. https://doi.org/10.55041/ijcope.v2i7.237

https://doi.org/10.55041/ijcope.v2i7.237

ABSTRACT- Credit cards have become one of the most widely used electronic payment methods, offering users convenient and flexible financial transactions. The rapid growth of e-commerce, digital banking, and online payment systems has significantly increased the incidence of credit and debit card fraud, posing serious financial and security challenges. Effective fraud detection is essential to safeguard consumers, financial institutions, and the stability of the digital payment ecosystem. Machine learning techniques have emerged as powerful tools for identifying fraudulent transactions by analyzing complex patterns and anomalies in transaction data. This study investigates the application of machine learning algorithms, including Random Forest, Support Vector Machine (SVM), and Multilayer Perceptron (MLP), for detecting credit card fraud. The comparative analysis of these models highlights their effectiveness in improving fraud detection accuracy while minimizing false alarms, thereby supporting secure electronic payment systems and enhancing trust in digital financial services.

Keywords: Credit card, Fraud detection, Artificial intelligence, Machine learning, Classification, Imbalance.

I. INTRODUCTION

Fraud refers to any intentional act of deception carried out to obtain unauthorized financial or personal benefits or to cause losses to another individual or organization. With the rapid growth of digital transactions, fraud has become a major concern across various sectors, making effective prevention and detection mechanisms essential. Fraud prevention focuses on implementing proactive security measures to stop fraudulent activities before they occur, such as authentication protocols, encryption, and transaction verification. However, when fraudsters succeed in bypassing these preventive measures, fraud detection systems play a crucial role in identifying suspicious transactions and minimizing potential losses. These systems continuously monitor transaction patterns, assess the likelihood of fraudulent behavior, and generate timely alerts to enable immediate corrective action. The objective of fraud detection is to identify fraudulent activities as early as possible while reducing false positives and ensuring uninterrupted service for legitimate users.

Fraudulent activities are prevalent in numerous domains, including credit card and online payment systems, e-commerce platforms, banking and financial services, healthcare, telecommunications, insurance, and cyber security. Among these, credit card fraud remains one of the most significant challenges due to the widespread adoption of electronic payment methods and the increasing sophistication of cybercriminals. As online shopping and digital banking continue to expand, traditional rule-based detection techniques have become insufficient, leading to the adoption of intelligent machine learning approaches that can recognize hidden patterns and adapt to evolving fraud strategies.

A credit card is a payment instrument issued by a financial institution that allows cardholders to purchase goods and services or withdraw cash within a predefined credit limit. Unlike debit cards, credit cards enable users to make purchases immediately and repay the borrowed amount during a subsequent billing cycle, offering

flexibility and convenience in financial transactions. The security of a credit card depends on the protection of its physical features as well as the confidentiality of sensitive information, such as the card number, expiration date, and verification code. Since unauthorized access to this information can result in fraudulent transactions, robust fraud detection mechanisms are essential. Modern credit card fraud detection systems employ machine learning algorithms to analyze transaction behavior, distinguish legitimate transactions from suspicious ones, and enhance the overall security and reliability of electronic payment systems. The overall workflow of a typical credit card fraud detection system is illustrated in the following figure.

Figure 1: Credit Card Fraud Detection [14].

The remainder of this paper is organized as follows. Section II presents the proposed machine learning-based framework for credit card fraud detection. Section III describes the dataset used in the study along with the evaluation metrics adopted to measure model performance. Section IV discusses the experimental setup, implementation details, and comparative analysis of various machine learning algorithms. Finally, Section V summarizes the key findings and presents the conclusions drawn from the study.

II. PROPOSED MODEL

Machine Learning (ML), a prominent subfield of Artificial Intelligence (AI), has emerged as one of the most influential technologies for solving complex real-world problems through data-driven decision-making. ML enables computer systems to learn patterns and relationships directly from historical data without being explicitly programmed for every possible scenario. Instead of relying on predefined rules, machine learning algorithms automatically build predictive models by identifying hidden structures and meaningful correlations within large datasets. These models continuously improve their performance as more data become available, making them highly effective for dynamic applications such as fraud detection.

Unlike traditional programming approaches, where developers manually define a fixed set of rules to process input data and generate the desired output, machine learning systems learn these rules automatically during the training process. Conventional programs are generally deterministic, procedural, and rule-based, making them less adaptable to changing environments and evolving fraud patterns. In contrast, machine learning algorithms can recognize complex, nonlinear relationships, adapt to new transaction behaviors, and accurately distinguish between legitimate and fraudulent activities. Owing to these capabilities, machine learning has become a preferred approach for credit card fraud detection, where rapidly evolving fraud techniques demand intelligent, scalable, and adaptive detection models..

Figure 2: Architecture of Credit Card Fraud Detection.

This study investigates the effectiveness of several supervised machine learning algorithms for detecting fraudulent credit card transactions. The primary objective is to identify the model that provides the highest detection accuracy while maintaining a low false alarm rate under different transaction scenarios. Machine learning techniques are capable of learning complex transaction patterns from historical data and classifying new transactions as either legitimate or fraudulent. The algorithms evaluated in this research include:

- Logistic Regression (LR)

- Support Vector Machine (SVM)
- Multilayer Perceptron (MLP)

The performance of these classifiers is compared to determine their capability in identifying fraudulent activities efficiently and accurately. The comparative evaluation provides insights into the strengths and limitations of each algorithm for real-world credit card fraud detection applications.

III. DATASET AND PERFORMANCE PARAMETERS

A. Dataset Description

The experiments presented in this study are conducted using the publicly available European Credit Card Fraud Detection dataset obtained from Kaggle. The dataset contains credit card transactions made by European cardholders during September 2013 and is widely used as a benchmark for fraud detection research. Since the dataset is derived from actual financial transactions rather than synthetically generated records, it reflects realistic customer behavior and fraud patterns.

The dataset consists of 284,807 transaction records, of which 284,315 (99.828%) are legitimate transactions and only 492 (0.172%) are fraudulent. This significant imbalance between the two classes makes fraud detection a challenging classification problem. For confidentiality purposes, most transaction attributes have been transformed using Principal Component Analysis (PCA), resulting in anonymized numerical features. The target variable, Class, represents the transaction label, where 0 denotes a legitimate transaction and 1 indicates a fraudulent transaction.

B. Performance Evaluation Parameters

The effectiveness of the machine learning models is assessed using several widely adopted performance metrics for binary classification. These measures provide a comprehensive evaluation of the classifiers, particularly when dealing with highly imbalanced datasets.

Sensitivity (Recall): Sensitivity measures the proportion of fraudulent transactions that are correctly identified by the classifier. A higher sensitivity indicates that the model can successfully detect a larger number of fraud cases while minimizing missed fraudulent transactions.
Specificity: Specificity, also known as the True Negative Rate (TNR), represents the proportion of legitimate transactions that are correctly classified as non-fraudulent. High specificity ensures that genuine customers are less likely to experience unnecessary transaction rejections.
Area Under the ROC Curve (AUC): The Area Under the Receiver Operating Characteristic (ROC) Curve evaluates the overall ability of a classifier to distinguish between fraudulent and legitimate transactions across different decision thresholds. An AUC value closer to 1.0 indicates excellent discrimination capability, whereas a value near 0.5 represents random classification.
F1-Score: The F1-score is the harmonic mean of Precision and Recall, providing a balanced measure of classification performance. It is particularly useful for highly imbalanced datasets because it considers both the ability to detect fraudulent transactions and the accuracy of positive predictions. A higher F1-score reflects a better balance between precision and recall, indicating superior overall model performance.

$$Precision = \frac{TP}{TP + FP}, \quad Recall = \frac{TP}{TP + FN}$$

$$F1 - Score = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

Confusion Matrix Parameters

The evaluation metrics are derived from the confusion matrix, which consists of the following components:

True Positive (TP): A fraudulent transaction that is correctly identified as fraudulent by the classifier.
True Negative (TN): A legitimate transaction that is correctly classified as legitimate.
False Positive (FP): A legitimate transaction that is incorrectly classified as fraudulent, also known as a false alarm.
False Negative (FN): A fraudulent transaction that is mistakenly classified as legitimate, representing an undetected fraud case.

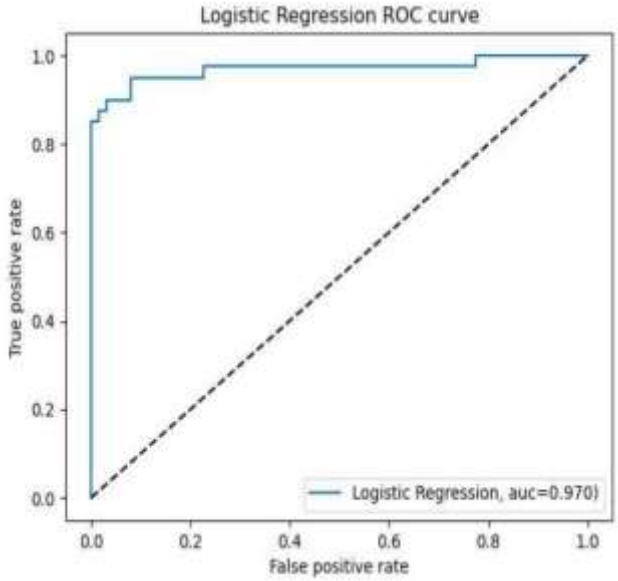

Figure 3: Confusion Matrix.

IV. EXPERIMENTAL RESULT ANALYSIS

Credit card scam finding is while a trade receipts steps to preclude whipped cash, merchandises, or amenities attained via an illegal credit card business. Credit card scam can occur together by the customer or by somebody else. To avoid happening such frauds, there are many techniques invented. If such frauds happen, then how to track the misused transactions are also improvised. Among the many methods, machine learning algorithms make accurate predictions by extracting some underlying information features based on large data samples of different dimensions. To reduce the bias caused by unbalanced data and improve the accuracy of credit card detection, scholars have mainly focused on studied in several aspects, such as data re-sampling, cost-sensitive learning, unbalanced regression, ensemble learning algorithms and deep learning algorithms. Here we used three different machine learning model to compare the performance in the terms of performance parameter as discussed earlier, all the results are simulated with python framework.

		Predicted Value	
		Non-Fraud (NO)	Fraud (YES)
Actual Value	Non-Fraud (NO)	TN	FP
	Fraud (YES)	FN	TP

Figure 4: ROC of logistic regression.

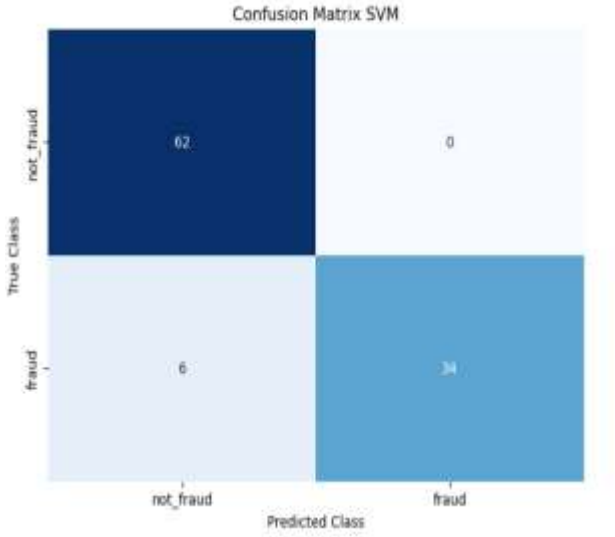

Figure 5: Confusion matrix of support vector machine.

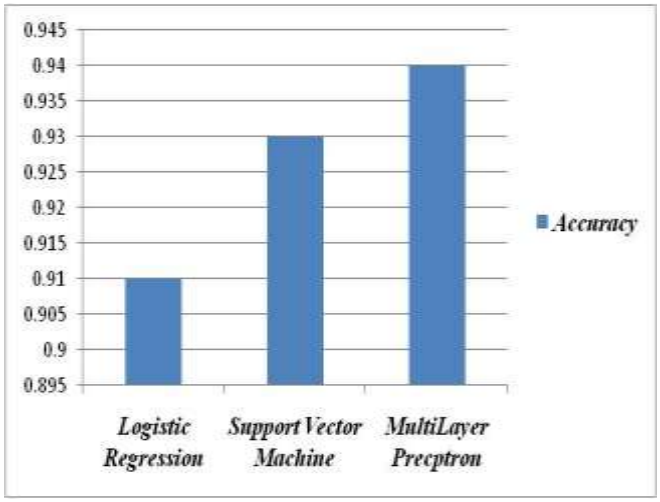

Figure 6: Accuracy using different machine learning approaches.

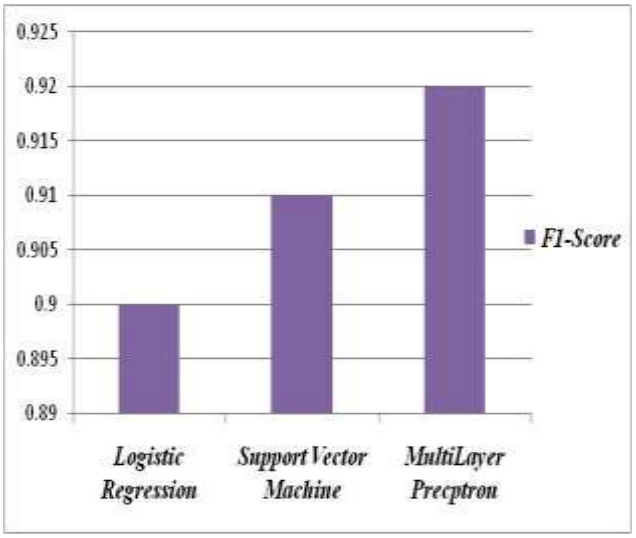

Figure 7: Precision using different machine learning approaches

.

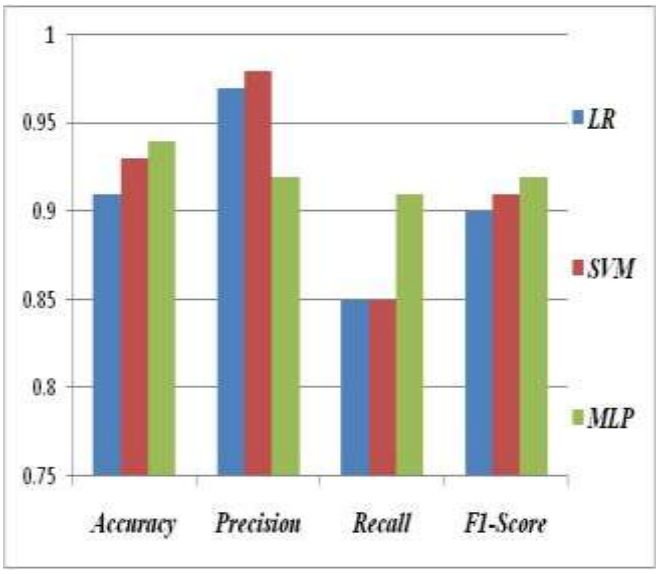

Figure 8: Accuracy, precision, recall, and F1 score using different machine learning approaches.

V. CONCLUSION

This study presented a comparative analysis of several machine learning algorithms for detecting fraudulent credit card transactions using the publicly available European Credit Card Fraud dataset. Logistic Regression (LR), Support Vector Machine (SVM), and Multilayer Perceptron (MLP) were evaluated to determine their effectiveness in identifying fraudulent activities within a highly imbalanced dataset. The performance of these models was assessed using standard evaluation metrics, including sensitivity, specificity, AUC, and F1-score. Experimental results demonstrate that the Multilayer Perceptron outperforms Logistic Regression and Support Vector Machine by achieving superior classification accuracy and improved fraud detection capability. These findings indicate that deep learning-based approaches are more effective in capturing complex transaction patterns and distinguishing fraudulent transactions from legitimate ones. Future work will focus on validating the proposed approach using real-world transaction data from financial institutions, exploring advanced ensemble and deep learning techniques, and incorporating real-time fraud detection mechanisms to further enhance the robustness and practical applicability of credit card fraud detection systems.

REFERENCES

[1] Emmanuel Ileberi, Yanxia Sun, Zenghui Wang, "Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost", IEEE Access, 2021, pp. 165286-165295.

[2] Ebenezer Esenogho, Ibomoiye Domor Mienye, "A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection", IEEE Access, 2022, pp. 16400-16408.

[3] Wei Zhou, Xiaorui Xue, "Credit card fraud detection based on self-paced ensemble neural Network", ITCC 2022, pp. 92-99.

[4] Tzu-Hsuan Lin, Jehn-Ruey Jiang, "Credit Card Fraud Detection with Autoencoder and Probabilistic Random Forest", Mathematics 2021, pp. 1-16.

[5] Gayan K. Kulatilleke, "Credit Card Fraud Detection Classifier selection Strategy", 2022, pp. 1-17.

[6] Deepak Kumar Rathore, Dr. Praveen Kumar Mannepalli, "Recent Trends in Machine Learning for Health Care Sector ", International Journal of Innovative Research in Technology and Management, Vol-5, Issue-2, 2021.

[7] Konduri Praveen Mahesh, Shaik Ashar Afrouz, "Detection of fraudulent credit card transactions: A comparative analysis of data sampling and classification techniques", Journal of Physics: Conference Series, 2021, pp. 1-9.

[8] Dileep M R, Navaneeth A V, "A Novel Approach for Credit Card Fraud Detection

using Decision Tree and Random Forest Algorithms", IEEE, 2021, pp. 1025-1028.

[9] Mosa M. M. Megdad, Bassem S. Abu-Nasser, " Fraudulent Financial Transactions Detection Using Machine Learning", International Journal of Academic Information Systems Research, 2022, pp. 30-39.

[10] Shubham Shah, Dhairya Shah, "Credit Card Fraud Detection System using Machine Learning", International Journal of Research in Engineering and Science, 2022, pp. 9-14.

[11] Deepak Kumar Rathore, Dr. Praveen Kumar Mannepalli, "A Review of Machine Learning Techniques and Applications for Health Care ", International Conference on Advances in Technology, Management & Education, 2021, IEEE proceeding, 978-1-7281-8586-6/21.

[12] Appala Srinuvasu Muttipati, Sangeeta Viswanadham, "Recognizing Credit Card Fraud Using Machine Learning Methods", Turkish Journal of Computer and Mathematics Education, 2021, pp. 3271-3278.

[13] Akhil Songa, Sri Teja Kumar Reddy Tetali, Naga Sai Tanmai Raavi, "Credit Card Fraud Detection using Various Machine Learning Algorithms", International Journal for Research in Applied Science & Engineering Technology, 2022, pp. 1174-1185.

[14] G. Sudha Sadasivam, Mutyala Subrahmanyam and Dasaraju Himachalam, Bhanu Prasad Pinnamaneni, "Corporate governance fraud detection from annual reports using big data analytics", Int. J. Big Data Intelligence, Vol. 3, No. 1, 2016

[15] R Dubey, D Rathore, D Kushwaha, JP Maurya, "An empirical study of intrusion detection system using feature reduction based on evolutionary algorithms and swarm intelligence methods", International Journal of Applied Engineering Research 12 (19), 2017. pp. 8884-8889.

[16] Ophir Gottlieb, Curt Salisbury, Howard Shek, Vishal Vaidyanathan, "Detecting Corporate Fraud: An Application of Machine Learning", December 15, 2006

[17] Renjith, S. Detection of Fraudulent Sellers in Online Marketplaces using Support Vector Machine Approach. International Journal of Engineering Trends and Technology (2018).

[18] Deepak Kumar Rathore, Praveen Kumar Mannepalli, "Diseases Prediction and Classification Using Machine Learning Techniques", AIP Conference Proceedings 2424, 070001(2022); https://doi.org/10.1063/5.0076768.

[19] Roy, Abhimanyu, et al. "Deep learning detecting fraud in credit card transactions." 2018 Systems and Information Engineering Design Symposium (SIEDS). IEEE, 2018.

[20] Pumsirirat, Apapan, and Liu Yan. "Credit card fraud detection using deep learning based on auto- encoder and restricted boltzmann machine." International Journal of advanced computer science and applications 9.1 (2018): 18-25.

[21] Appala Srinuvasu Muttipati, Sangeeta Viswanadham, "Recognizing Credit Card Fraud Using Machine Learning Methods", Turkish Journal of Computer and Mathematics Education, 2021, pp. 3271-3278.

[22] Akhil Songa, Sri Teja Kumar Reddy Tetali, Naga Sai Tanmai Raavi, "Credit Card Fraud Detection using Various Machine Learning Algorithms", International Journal for Research in Applied Science & Engineering Technology, 2022, pp. 1174-1185.