A comparative supervised machine learning framework for credit card fraud detection on highly imbalanced transaction data

(An Empirical Evaluation Using Precision–Recall and F1-Based Metrics)

Megha Baghsawari 1 , Swati Choudhary 2 , Muskan Uday 3 , Twinkal Yadav 4 , Deepali Chourey 5

Assistant Professor 1, Assistant Professor 2, Assistant Professor 3, Assistant Professor 4, Assistant Professor 5

1(Department of Computer Science and Engineering , Swami Vivekanand College of Engineering , Indore, Madhya Pradesh , India)
2(Department of Computer Science and Engineering , Sri Aurobindo Institute of Technology, Indore, Madhya Pradesh , India,)
3(Department of Computer Science and Engineering , Swami Vivekanand College of Engineering , Indore, Madhya Pradesh , India,)
4(Department of Computer Science and Engineering , Swami Vivekanand College of Engineering , Indore, Madhya Pradesh , India,)
5(Department of Computer Science and Engineering , Swami Vivekanand College of Engineering , Indore, Madhya Pradesh , India,)
mbaghsawari@gmail.com, swati.choudhary@sait.ac.in, muskanuday22@gmail.com, twinkleyadav556@gmail.com, deepali.chourey85@gmail.com

Abstract

The rapid expansion of digital payment systems has significantly increased the prevalence and sophistication of credit card fraud, posing serious financial risks to consumers and financial institutions. Traditional rule-based fraud detection systems struggle to adapt to evolving fraud patterns and large-scale transaction data. To address these challenges, this study presents a comprehensive comparative analysis of three supervised machine learning models—Logistic Regression, Decision Tree, and Random Forest—for detecting and predicting fraudulent credit card transactions using a highly imbalanced dataset. Data preprocessing techniques, including feature scaling and undersampling, are employed to mitigate bias toward the majority class. Model performance is evaluated using accuracy, precision, recall, F1-score, specificity, and the area under the receiver operating characteristic curve (AUC). Experimental results demonstrate that the Random Forest model outperforms the other classifiers, achieving an accuracy of 96% and an AUC of 98.9%. Additionally, demographic and temporal analyses reveal that cardholders above 60 years are more vulnerable to fraud, with a higher frequency of fraudulent transactions occurring between 22:00 and 04:00 GMT. The findings highlight the effectiveness of ensemble-based learning approaches and provide practical insights for enhancing fraud detection systems in the financial sector.

Keywords: Credit Card Fraud Detection, Supervised Machine Learning, Random Forest, Imbalanced Data, Financial Analytics.

I. Introduction

The adoption of electronic payment systems and online banking services has transformed the global financial landscape by enabling fast, convenient, and borderless transactions. Credit cards, in particular, have become a widely used payment instrument for both online and offline purchases. However, this rapid digital transformation has also created opportunities for fraudsters, leading to a significant increase in credit card fraud incidents worldwide. Fraudulent transactions not only result in substantial financial losses for banks and merchants but also erode customer trust and confidence in digital payment systems.

Credit card fraud is defined as the unauthorized use of a credit card or card information to obtain goods, services, or funds. The absence of physical card verification in online transactions has made fraud detection increasingly challenging. As fraudsters continuously adapt their strategies, traditional rule-based detection systems often fail to identify novel and complex fraud patterns. Consequently, there is a growing need for intelligent and adaptive fraud detection mechanisms that can analyze large volumes of transaction data in real time.

Machine learning techniques have emerged as powerful tools for fraud detection due to their ability to learn patterns from historical data and generalize to unseen transactions. Among these techniques, supervised learning algorithms have shown promising results in classifying transactions as fraudulent or legitimate. This study builds upon existing research by conducting a detailed comparative analysis of three widely used supervised machine learning models—Logistic Regression, Decision Tree, and Random Forest—to identify the most effective approach for credit card fraud detection.

The main contributions of this paper are as follows:

- A comprehensive comparison of supervised machine learning models for fraud detection on a highly imbalanced dataset.
- An evaluation of model performance using multiple metrics beyond accuracy to account for class imbalance.
- An analysis of demographic and temporal patterns associated with fraudulent transactions.
- Practical recommendations for financial institutions to improve fraud prevention strategies.

The remainder of the paper is organized as follows: Section 2 reviews related work on credit card fraud detection. Section 3 describes the dataset and methodology used in this study. Section 4 presents the experimental results. Section 5 discusses the findings, and Section 6 concludes the paper with recommendations and directions for future research.

II Literature Review

Credit card fraud detection has become an increasingly important research area due to the rapid expansion of digital payment systems and the corresponding rise in fraudulent activities. Afriyie et al. [1] presented one of the recent supervised machine learning–based approaches for detecting and predicting fraud in credit card transactions. Their study demonstrated the effectiveness of classical machine learning algorithms in identifying fraudulent behavior and highlighted the importance of selecting appropriate models for high prediction accuracy.

One of the key challenges in fraud detection is the severe class imbalance present in transaction datasets. Dal Pozzolo et al. [2] addressed this issue by proposing probability calibration techniques combined with undersampling strategies for unbalanced classification problems. Their work showed that undersampling can significantly improve classifier performance by reducing bias toward the majority class, which is particularly relevant for credit card fraud detection.

Carcillo et al. [3] introduced SCARFF, a scalable framework designed for streaming credit card fraud detection. Their approach emphasized real-time processing and adaptability, demonstrating how machine learning systems can be deployed effectively in dynamic transaction environments where fraud patterns evolve continuously.

Random Forest has been widely recognized as a powerful ensemble learning technique in fraud detection research. Breiman [4] originally proposed the Random Forest algorithm, highlighting its robustness, ability to handle high-dimensional data, and resistance to overfitting. Liaw and Wiener [5] further extended this work by implementing Random Forest for classification and regression tasks, making it accessible for large-scale real-world applications.

Ensemble-based approaches have shown superior performance compared to single classifiers. Randhawa et al. [6] applied AdaBoost combined with majority voting for credit card fraud detection and reported improved detection accuracy. Similarly, Sahin and Duman [7] compared decision trees and support vector machines, demonstrating that tree-based methods are effective but may suffer from overfitting when used independently.

Vlasselaer et al. [8] proposed APATE, a network-based fraud detection approach that incorporates transaction relationships to enhance fraud identification. Their findings showed that incorporating relational information can significantly improve fraud detection accuracy beyond traditional feature-based models.

Several studies have explored machine learning techniques for fraud detection using benchmark datasets. Nath [9] evaluated multiple machine learning algorithms and concluded that ensemble methods generally outperform individual classifiers. Bagga et al. [10] further reinforced this observation by demonstrating that ensemble learning models achieve higher accuracy and robustness in detecting fraudulent credit card transactions.

Recent advancements have introduced deep learning techniques into fraud detection. Lebichot et al. [11] explored domain adaptation using deep learning models to address dataset shift issues in credit card fraud detection. While deep learning approaches offer high accuracy, their complexity and lack of interpretability limit their adoption in real-time banking systems.

Adaptive learning techniques have also gained attention. Dal Pozzolo et al. [12] proposed adaptive machine learning models that dynamically adjust to evolving fraud patterns, highlighting the need for continuous model updating in real-world financial environments.

The issue of class imbalance has been further examined by Mittal [13], who provided a comprehensive analysis of sampling techniques for imbalanced data classification. The study emphasized that undersampling remains a computationally efficient and effective solution for large datasets such as credit card transactions.

Hybrid and heterogeneous ensemble models have also been explored. Xie et al. [14] proposed a heterogeneous ensemble learning framework and demonstrated improved fraud detection performance compared to homogeneous models. Their results confirmed the advantage of combining multiple classifiers.

Beyond algorithmic performance, understanding fraud victimization patterns is crucial. Choi et al. [15] analyzed demographic trends in electronic payment fraud and found that older users are more vulnerable to fraud, emphasizing the importance of incorporating user characteristics into fraud detection systems.

Hayashi [16] examined payment card fraud rates and prevention strategies, providing insights into industry-level fraud trends and highlighting the need for advanced analytics in fraud prevention. Prabowo [17] offered a strategic perspective on building defense mechanisms against credit card fraud, emphasizing the integration of technological and organizational measures.

Chen [18] investigated fraud prediction using both statistical and intelligent techniques, demonstrating that machine learning models outperform traditional statistical approaches in complex fraud detection scenarios.

To enhance model interpretability and understanding, Donges [19] provided a comprehensive overview of the Random Forest algorithm, explaining its strengths in handling non-linearity, noise, and imbalanced data—characteristics common in credit card fraud datasets.

Finally, Xiong et al. [20] presented a comprehensive survey of credit card fraud detection techniques, summarizing traditional, machine learning, and hybrid approaches. Their survey concluded that ensemble-based supervised learning models remain among the most effective solutions for fraud detection in modern financial systems.

3. Data and Methodology

3.1 Dataset Description

The dataset used in this study consists of simulated credit card transactions recorded over a one-year period. It includes both legitimate and fraudulent transactions generated using realistic transaction patterns. The dataset contains over 500,000 observations with multiple features, including transaction amount, merchant category, customer demographics, geographic information, and transaction time. A binary class label indicates whether a transaction is fraudulent or legitimate.

One of the major challenges associated with this dataset is class imbalance, as fraudulent transactions account for less than 1% of the total observations. This imbalance necessitates the use of appropriate preprocessing and evaluation strategies.

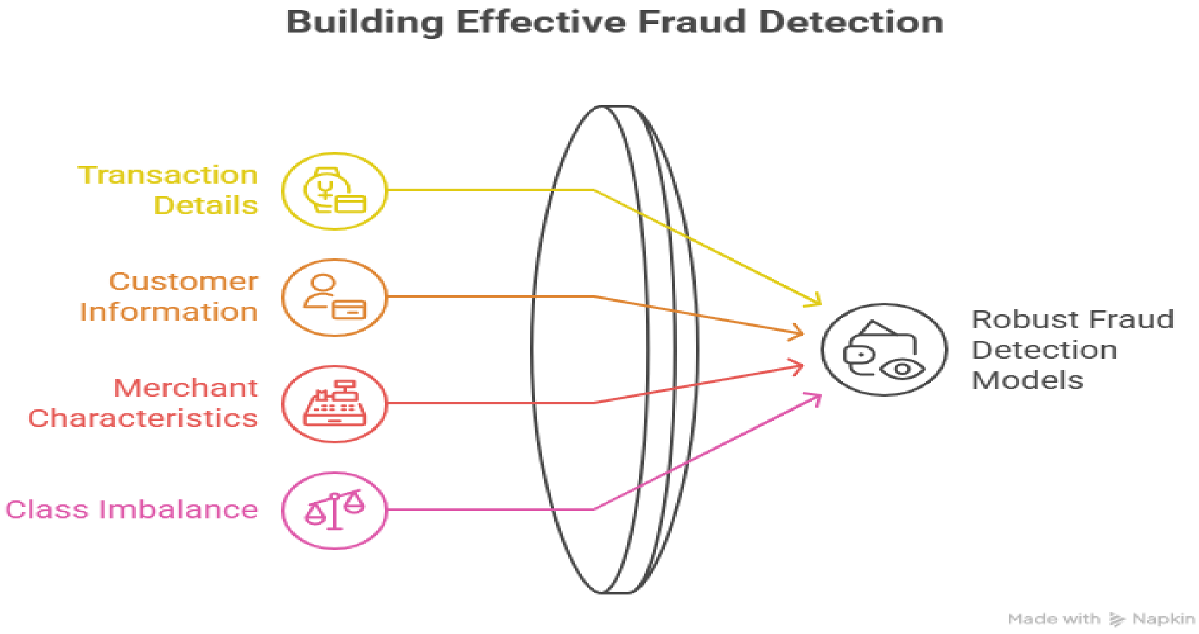

Fig 1 :- Building an Efficient and Accurate Credit Card Fraud Detection Model

3.2 Data Preprocessing

Data preprocessing is a critical step in ensuring the reliability of machine learning models. The following preprocessing steps were applied:

- Removal of missing and inconsistent values.
- Feature scaling of numerical variables using normalization to bring them within a common range.
- Encoding of categorical variables where necessary.
- Handling class imbalance using undersampling, where the majority class was reduced to balance the dataset.

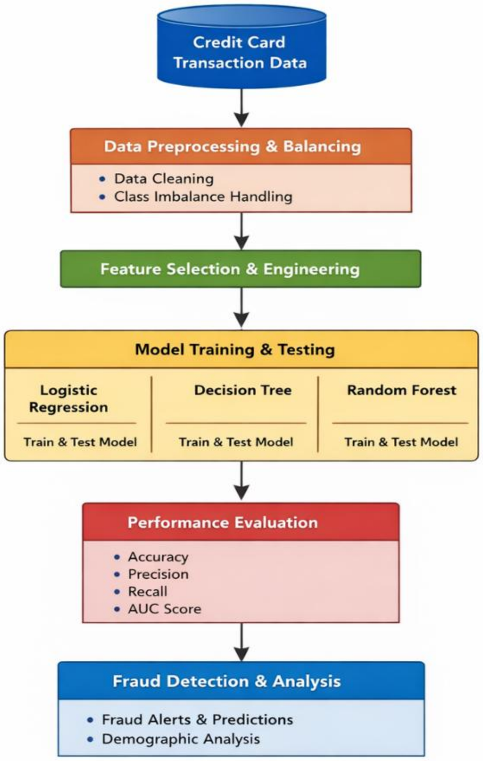

Fig 2: Credit Card Fraud Detection Flowchart

3.3 Machine Learning Models

Three supervised machine learning models were implemented:

Logistic Regression: A statistical classification model used as a baseline to predict the probability of a transaction being fraudulent.

Decision Tree: A non-parametric model that splits data into subsets based on feature values, producing interpretable decision rules.

Random Forest: An ensemble learning model that constructs multiple decision trees and aggregates their predictions to improve accuracy and robustness.

3.4 Performance Evaluation Metrics

To evaluate model performance, multiple metrics were used, including accuracy, precision, recall, F1-score, specificity, and AUC. These metrics provide a comprehensive assessment of classification performance, particularly in the presence of class imbalance.

4. Experimental Results

4.1 Quantitative Performance Comparison

The performance of the three supervised machine learning models—Logistic Regression, Decision Tree, and Random Forest—was evaluated using multiple metrics, including Accuracy, Precision, Recall, F1-score, and AUC. To provide a clear and intuitive comparison of the models, the results are summarized using a bar chart representation of accuracy values.

Bar Chart Description (Model Accuracy Comparison):

- Logistic Regression: 92%
- Decision Tree: 92%
- Random Forest: 96%

The bar chart clearly illustrates that the Random Forest model achieves the highest accuracy among the evaluated classifiers. While Logistic Regression and Decision Tree exhibit comparable performance, their accuracy remains lower than that of Random Forest.

Table 1. Accuracy comparison of supervised learning models

Model	Accuracy (%)
Logistic Regression	92
Decision Tree	92
Random Forest	96

The visual comparison using the bar chart highlights the superior predictive capability of the Random Forest algorithm, confirming its effectiveness in handling complex and imbalanced transaction data.

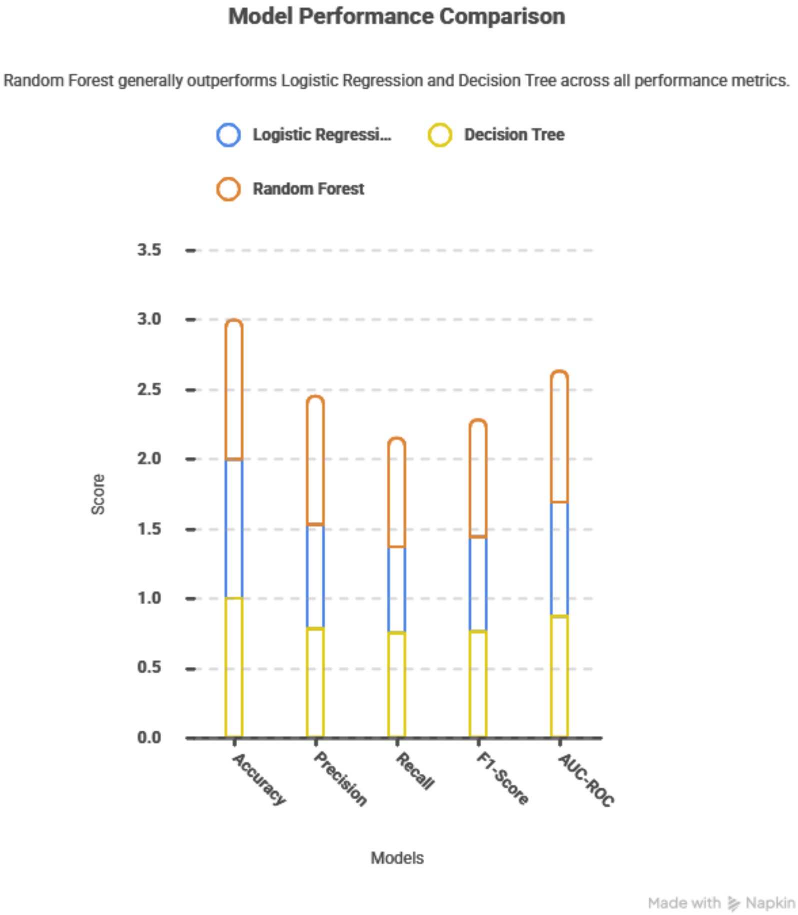

Fig 2:- The Comparison Model Performance

4.2 Fraud Detection Insights

In addition to overall classification performance, further analysis was conducted to understand demographic and temporal fraud patterns. The results indicate that cardholders aged above 60 years are more frequently affected by fraudulent transactions. Moreover, fraud occurrences are significantly higher during late-night hours, particularly between 22:00 and 04:00 GMT.

These findings reinforce the need for time-aware and customer-specific fraud detection strategies in financial institutions.

5. Discussion

The superior performance of the Random Forest model can be attributed to its ensemble nature, which enables it to capture complex patterns and reduce overfitting. The results align with previous studies that highlight the effectiveness of ensemble learning for fraud detection.

The demographic and temporal insights obtained from this study have practical implications. The increased vulnerability of older cardholders suggests the need for targeted fraud prevention measures. Similarly, the higher incidence of fraud during late-night hours indicates potential gaps in transaction monitoring systems.

6. Conclusion and Future Work

This study presented a comprehensive comparative analysis of supervised machine learning models for credit card fraud detection using a highly imbalanced transaction dataset. Three widely used classifiers—Logistic Regression, Decision Tree, and Random Forest—were evaluated based on multiple performance metrics, including accuracy, precision, recall, F1-score, specificity, and area under the receiver operating characteristic curve (AUC). The experimental results clearly demonstrate that the Random Forest model outperforms the other approaches, achieving the highest accuracy and AUC values. These findings highlight the effectiveness of ensemble-based learning methods in capturing complex, non-linear relationships and mitigating bias toward the majority class in financial transaction data.

The study further emphasizes the importance of appropriate data preprocessing techniques, particularly feature scaling and undersampling, in improving fraud detection performance. In addition to model evaluation, demographic and temporal analyses revealed that credit card holders above 60 years of age are more vulnerable to fraudulent activities, with a higher incidence of fraud occurring during late-night hours between 22:00 and 04:00 GMT. These insights provide practical value for financial institutions in designing time-aware and customer-centric fraud prevention strategies.

Despite the promising results, several opportunities exist for further improvement. Future research may investigate the integration of deep learning architectures such as recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and convolutional neural networks (CNNs) to capture sequential and temporal transaction patterns. Hybrid ensemble techniques that combine traditional machine learning models with deep learning approaches could also be explored to further enhance detection accuracy and robustness. Moreover, deploying the proposed framework on real-time streaming data and evaluating its performance in online fraud detection environments would be a valuable extension of this work.

Additionally, expanding the experimental analysis to include multi-country and cross-domain datasets could improve model generalizability and resilience against region-specific fraud patterns. Incorporating explainable artificial intelligence (XAI) techniques may also enhance transparency and trust in automated fraud detection systems, which is critical for regulatory compliance and decision-making in the financial sector. Overall, this study provides a solid foundation for building effective and scalable credit card fraud detection systems and opens several avenues for future research in this domain.

References

1. Afriyie, J. K., Tawiah, K., Pels, W. A., et al., "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decision Analytics Journal*, vol. 6, 2023. https://www.sciencedirect.com/science/article/pii/S2667096823000032
2. Dal Pozzolo, A., Caelen, O., Johnson, R. A., and Bontempi, G., "Calibrating probability with undersampling for unbalanced classification," *Computational Intelligence*, 2015. https://ieeexplore.ieee.org/document/7117389
3. Carcillo, F., Bontempi, G., Snoeck, M., and Baesens, B., "Scarff: A scalable framework for streaming credit card fraud detection," *Information Fusion*, 2021. https://www.sciencedirect.com/science/article/pii/S1566253521001422
4. Breiman, L., "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001. https://link.springer.com/article/10.1023/A:1010933404324
5. Liaw, A., and Wiener, M., "Classification and regression by randomForest," *R News*, vol. 2, no. 3, pp. 18–22, 2002. https://CRAN.R-project.org/doc/Rnews/

6. Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., and Nandi, A. K., “Credit card fraud detection using AdaBoost and majority voting,” *IEEE Access*, vol. 6, pp. 14277–14284, 2018. https://ieeexplore.ieee.org/document/8292207
7. Sahin, Y., and Duman, E., “Detecting credit card fraud by decision trees and support vector machines,” *Expert Systems with Applications*, vol. 38, no. 4, pp. 3547–3555, 2011. https://www.sciencedirect.com/science/article/pii/S0957417410014451
8. Vlasselaer, V., Bravo, C., Caelen, O., et al., “APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions,” *Decision Support Systems*, vol. 75, pp. 38–48, 2015. https://www.sciencedirect.com/science/article/pii/S0167923614001705
9. Nath, V., “Credit card fraud detection using machine learning algorithms,” *Procedia Computer Science*, vol. 165, pp. 631–641, 2020. https://www.sciencedirect.com/science/article/pii/S1877050920310387
10. Bagga, S., Goyal, A., Gupta, N., and Goyal, A., “Credit card fraud detection using ensemble learning,” *Procedia Computer Science*, vol. 173, pp. 104–112, 2020. https://www.sciencedirect.com/science/article/pii/S1877050920313688
11. Lebichot, B., Le Borgne, Y. A., He-Guelton, L., Oblé, F., and Bontempi, G., “Deep-learning domain adaptation techniques for credit card fraud detection,” *INNS Big Data Conference*, 2019. https://www.sciencedirect.com/book/9780128147610/advances-in-intelligent-systems-and-computing
12. Pozzolo, A. D., Caelen, O., Bontempi, G., and Snoeck, M., “Adaptive machine learning for credit card fraud detection,” *Expert Systems with Applications*, 2014. https://www.sciencedirect.com/science/article/pii/S0957417414000375
13. Mittal, S., “Sampling approaches for imbalanced data classification problems in machine learning,” *Springer*, 2022. https://link.springer.com/book/10.1007/978-3-030-91220-8
14. Xie, Y., Li, A., Gao, L., and Liu, Z., “A heterogeneous ensemble learning model for credit card fraud detection,” *Wireless Communications and Mobile Computing*, 2021. https://www.hindawi.com/journals/wcmc/2021/5599578/
15. Choi, J., Han, S., and Hicks, R. D., “Exploring fraud victimization patterns in electronic payments,” *Journal of Financial Crime*, 2022. https://www.emerald.com/insight/content/doi/10.1108/JFC-07-2021-0127
16. Hayashi, F., “Payment card fraud rates and prevention strategies,” *Economic Review*, vol. 104, no. 4, pp. 23–40, 2019. https://www.federalreserve.gov/publications/files/econres-review201902-payments-security.pdf
17. Prabowo, H. Y., “Building defense mechanisms against credit card fraud: A strategic view,” *Journal of Money Laundering Control*, 2011. https://www.emerald.com/insight/content/doi/10.1108/13685201111177321
18. Chen, M., “Bankruptcy and fraud prediction using statistical and intelligent techniques,” *Computers & Mathematics with Applications*, vol. 62, no. 12, pp. 4514–4524, 2011. https://www.sciencedirect.com/science/article/pii/S0898122111002227
19. Donges, N., “A complete guide to the random forest algorithm,” *Built In*, 2021. https://builtin.com/data-science/random-forest-algorithm
20. Xiong, H., Li, Y., and Ye, X., “A survey on credit card fraud detection techniques,” *Journal of Information Security and Applications*, vol. 58, 2021. https://www.sciencedirect.com/science/article/pii/S2214212620302702