International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Credit Card Fraud Detection Using Modern Machine Learning And Deep Learning Approaches

Mrs. Prakruthi G R[1], Preetham Gowda M R[2], Srajan R Aithal[3], Sujith G[4], Vinay S[5]
[1]Assistant Professor, Department of Artificial Intelligence & Data Science
[2]–[5]Students, Department of Artificial Intelligence & Data Science
East West Institute of Technology, Bengaluru, India

The rapid shift toward digital and card-based payment systems has intensified the challenge of detecting fraudulent financial transactions. Static, rule-oriented detection techniques are often unable to recognize newly emerging fraud strategies. This work introduces a data-driven credit card fraud detection framework that leverages machine learning and deep learning algorithms to improve detection accuracy. Transaction records are prepared through feature normalization and class rebalancing using the Synthetic Minority Oversampling Technique (SMOTE). Several supervised classifiers, including Logistic Regression, Random Forest, and XGBoost, are trained and comparatively analyzed. Experimental evaluation highlights the superior performance of ensemble-based models in identifying fraudulent activity. The selected model is deployed through a lightweight Flask web application to enable real-time transaction assessment, making the solution practical for real-world financial systems.

Keywords: Credit card fraud, data-driven security, machine learning, deep learning, XGBoost

I. INTRODUCTION

Electronic payment mechanisms have become central to modern financial operations, offering convenience and speed to users worldwide. However, this growth has also created opportunities for fraudulent misuse, including unauthorized card access and compromised payment terminals. Traditional fraud detection solutions typically rely on predefined rules, which limits their adaptability to evolving fraud patterns. In contrast, machine learning techniques analyze historical transaction data to learn behavioral trends and detect anomalies automatically. This paper focuses on designing an intelligent and adaptable fraud detection system capable of responding to continuously changing transaction behaviors.

II. PROPOSED METHODOLOGY

The proposed approach follows a systematic workflow that includes data preparation, model development, and performance validation. The transaction dataset consists of labeled records classified as either legitimate or fraudulent. Since fraudulent transactions form only a small fraction of the data, feature scaling and SMOTE-based oversampling are applied to improve minority class learning. Multiple supervised learning algorithms are trained alongside a Convolutional Neural Network (CNN) designed to extract complex feature relationships. Model tuning is performed using suitable optimization techniques to reduce misclassification rates.

III. SOFTWARE IMPLEMENTATION

The system is developed using Python and widely used machine learning libraries such as NumPy, Pandas, Scikit-learn, XGBoost, and Imbalanced-learn. Model experimentation and training are conducted in Google Colab using Jupyter Notebook interfaces. Transaction datasets are processed using Pandas, followed by normalization and class balancing through SMOTE. The best-performing model is serialized using Joblib and integrated into a Flask-based web application that supports real-time fraud prediction.

IV. HARDWARE REQUIREMENTS

The proposed fraud detection framework is designed to operate efficiently on standard computing systems. A basic configuration consisting of an Intel Core i3 or equivalent processor, a minimum of 4 GB RAM, and adequate disk storage is sufficient. Although the use of a GPU can speed up model training, the system performs effectively on CPU-based platforms, making it accessible for practical deployment.

V. RESULTS AND DISCUSSION

Performance analysis reveals that XGBoost achieves better fraud detection results compared to traditional classifiers. The inclusion of SMOTE significantly enhances the identification of fraudulent transactions without adversely affecting overall precision. Network-based visualization methods further assist analysts by revealing suspicious

transaction clusters and high-risk payment terminals, thereby improving interpretability and response efficiency.

VI. CONCLUSION

This research presents a reliable credit card fraud detection system based on machine learning and deep learning methodologies. By combining class balancing, ensemble learning, and real-time deployment, the proposed solution enhances fraud detection accuracy and usability. Future enhancements may include the integration of hybrid neural architectures and testing on larger, real-world transaction datasets.

VII. EXPERIMENTAL RESULTS AND VISUAL ANALYSIS

The experimental evaluation is illustrated through transaction dashboards, terminal-level monitoring, and interactive visual representations. These results validate the effectiveness of the proposed learning framework and demonstrate how visual analytics complement predictive modeling in fraud detection systems.

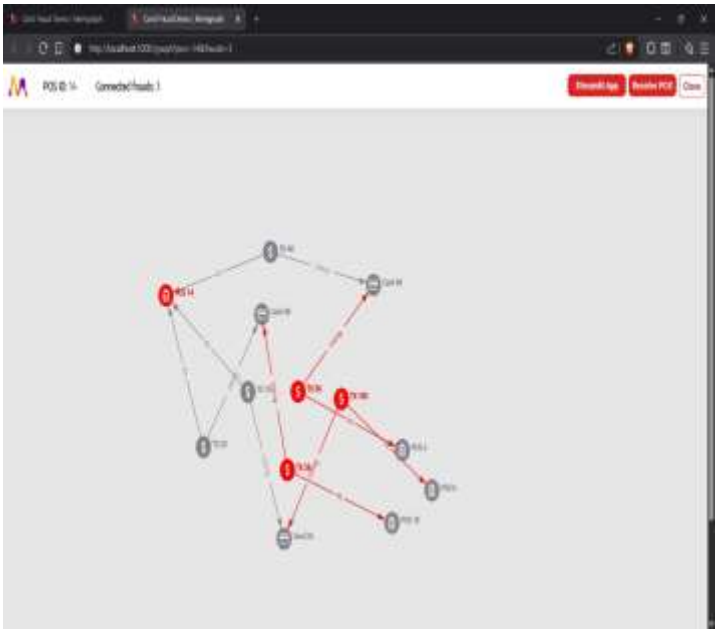

Figure 6.1 This part shows test results from the fraud detection system, using live transactions and map-like visuals to show how well the learning algorithm works with network methods.

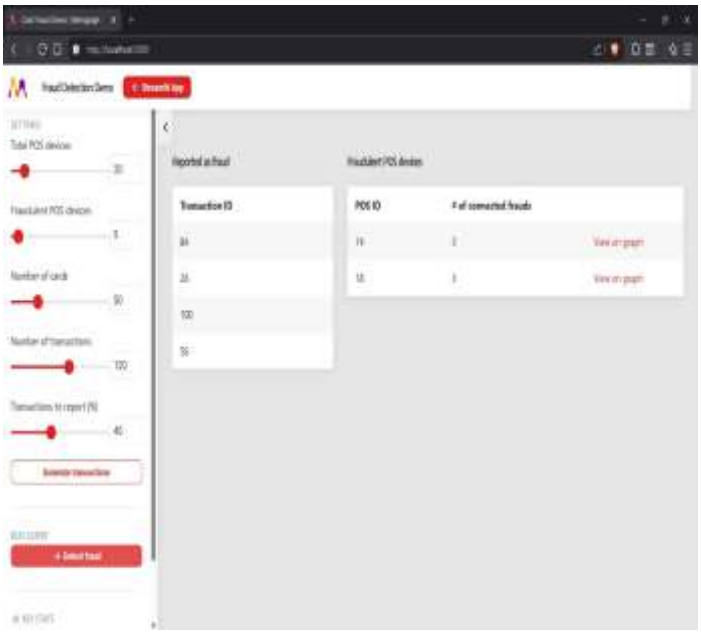

Figure 6.2 This dashboard shows fake transactions and suspicious POS machines, listing each terminal ID with its fraud cases so reviewers can focus on the riskiest ones first..

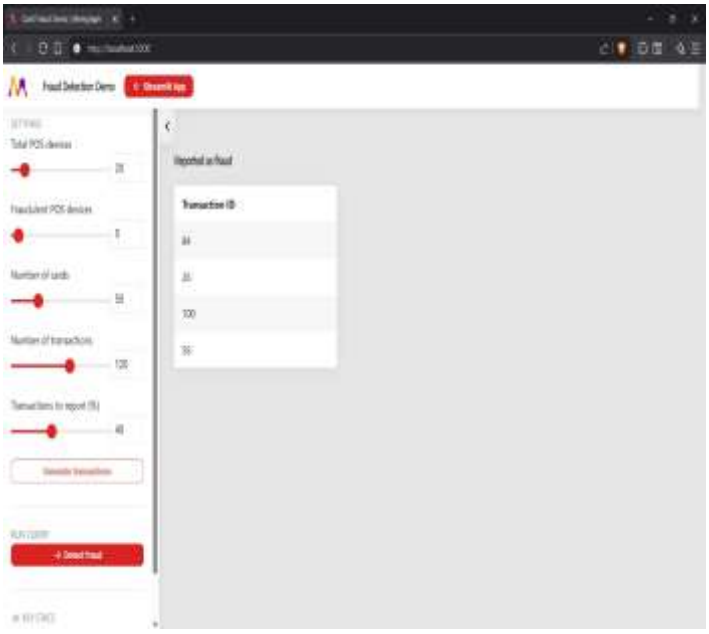

Figure 6.3 This fraud report shows suspicious transaction IDs, proving the system can spot fake activities in large datasets using smart filters instead of guessing.

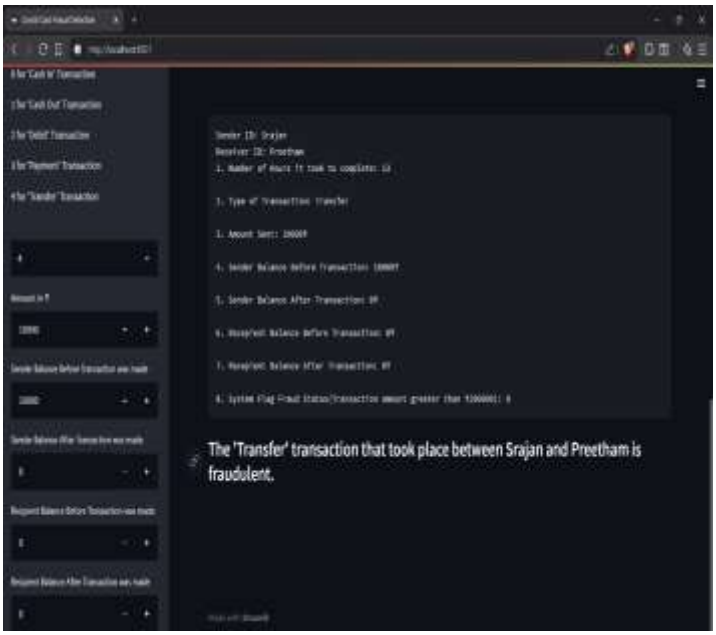

Figure 6.4 A user-friendly interface for spotting fraud at the transaction level—it analyzes your inputs in real time and flags anything suspicious based on patterns from your normal behavior.

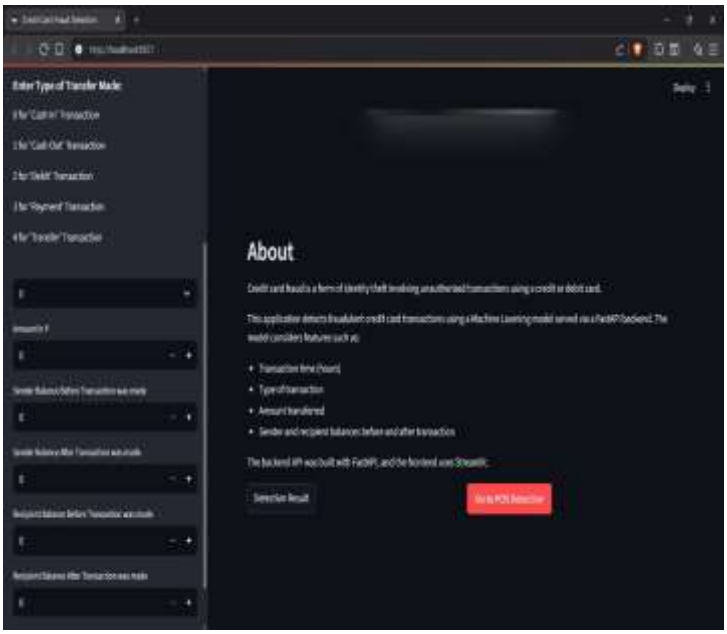

Figure 6.6 The About section explains the transaction attributes analyzed by the ML model, making the fraud detection process easier to understand and more transparent.

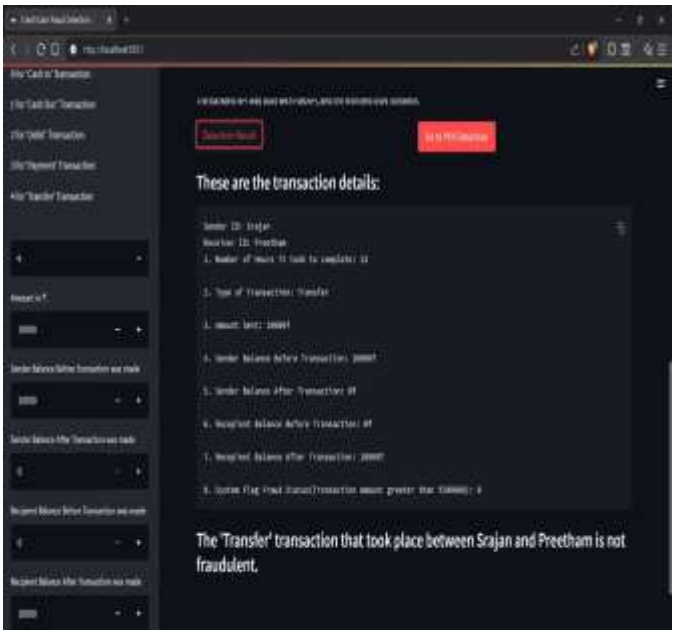

Figure 6.5 The system correctly predicts a legitimate transaction, showing its ability to avoid false fraud warnings and increase user trust.

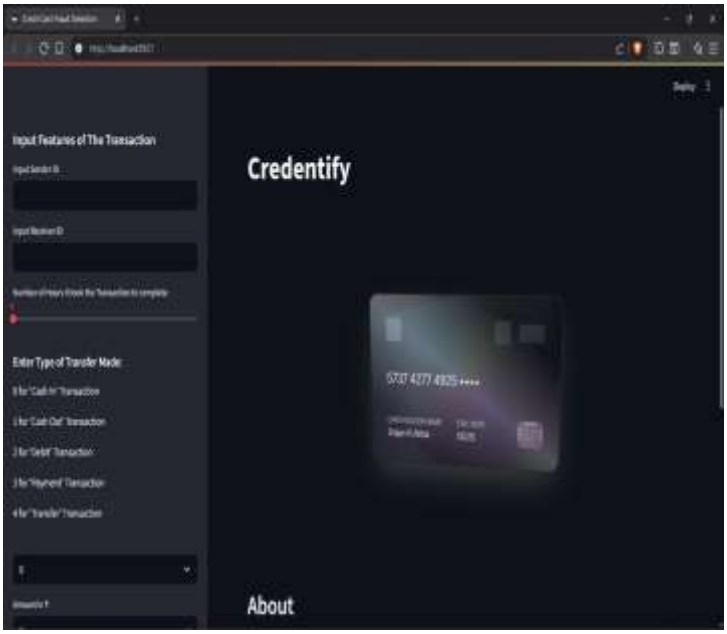

Figure 6.7 The home page of the Credit Card Fraud Detection system allows users to provide transaction inputs and interact with both fraud detection and POS monitoring modules.

VIII. References

1. A. Dal Pozzolo, O. Caelen, and G. Bontempi, Credit Card Fraud Detection: A Realistic Modeling, 2015.
2. F. Carcillo et al., Anomaly Detection in Credit Card Transactions Using Autoencoders, 2019.
3. D. Roy and S. Bhaduri, Machine Learning Techniques for Credit Card Fraud Detection, 2021.
4. A. Bahnsen et al., Decision Trees and Support Vector Machines for Fraud Detection, 2014.
5. A. Singh and A. Sharma, Real-Time Fraud Detection Using XGBoost, 2022.
6. N. V. Chawla et al., SMOTE: Synthetic Minority Over-sampling Technique, 2002.