International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Intelligent Credit Card Fraud Detection System using Machine Learning Techniques

Lakshana Shree U.M[1],Mrs.Vanitha K [2]

[1]Undergraduate Student, [2]Assistant Professor, Department of Computer Technology, Dr. N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India

Lakshanamohan479@gmail.com vani.hansa4u@gmail.com

https://doi.org/10.55041/ijsmt.v2i3.216

Cite this Article: U.M, L. S. (2026). Intelligent Credit Card Fraud Detection System using Machine Learning Techniques. International Journal of Science, Strategic Management and Technology, *02*(03). https://doi.org/10.55041/ijsmt.v2i3.216

Abstract

The rapid growth of digital payment systems has significantly increased the risk of credit card fraud. Financial institutions face major challenges in identifying fraudulent transactions due to the highly imbalanced nature of transaction data and the evolving strategies of fraudsters. Traditional rule-based detection systems are no longer sufficient to handle modern fraud patterns.This project presents a web-based Credit Card Fraud Detection System developed using Machine Learning techniques. The system analyzes transaction features such as Time, Amount, and anonymized variables (V1–V28) to classify transactions as legitimate or fraudulent. A supervised machine learning classification model is trained using a real-world dataset and deployed through a Flask-based web application. The system integrates an SQLite database to store transaction details and prediction results. The final application provides real-time fraud prediction with risk percentage, enabling better financial security and decision-making.The proposed system demonstrates how machine learning can be effectively integrated into a scalable web-based architecture for practical fraud detection applications.

Keywords- Fraud Detection, Machine Learning, Classification, Imbalanced Data, Risk Prediction, Web Deployment.

INTRODUCTION

The rapid expansion of digital payment systems has significantly transformed modern financial transactions. Credit cards are now widely used for online shopping, subscriptions, bill payments, and international purchases due to their convenience and speed. However, this growth has also led to an increase in fraudulent activities. Credit card fraud, which involves unauthorized use of card details to perform illegal transactions, results in major financial losses for banks and customers each year. Detecting fraudulent transactions has therefore become a critical challenge for financial institutions, especially as fraud techniques continuously evolve.

Traditional fraud detection systems relied on rule-based methods that flagged transactions based on predefined conditions such as unusual spending patterns or geographic locations. While these systems were useful initially, they lack adaptability and struggle to identify new and complex fraud patterns. With the increasing volume of digital transactions, manual monitoring and static rules are no longer sufficient. Machine Learning (ML) has emerged as an effective solution because it can automatically learn patterns from historical transaction data and identify suspicious behavior with improved accuracy.One of the major challenges in credit card fraud detection is the highly imbalanced nature of transaction data, where fraudulent transactions represent only a small fraction of total transactions. This makes simple accuracy an unreliable performance measure, requiring evaluation metrics such as precision, recall, and F1-score. In this project, a supervised machine learning classification model is developed using transaction features such as Time, Amount, and anonymized

variables (V1–V28). The model is trained to distinguish between normal and fraudulent transactions and is saved for deployment after evaluation.

To make the system practical and usable in real-world scenarios, the trained model is integrated into a web-based application using Flask as the backend framework. A user-friendly interface built with HTML and CSS allows users to enter transaction details, which are processed by the backend and passed to the trained model for prediction. The system displays whether the transaction is normal or fraudulent along with a risk percentage. Additionally, an SQLite database is used to store transaction inputs and prediction results, creating a complete end-to-end fraud detection system that combines machine learning, web development, and database management.

LITERATURE REVIEW

Credit card fraud detection has been widely studied due to its significant financial impact and the continuously evolving strategies of fraudsters. Early approaches relied primarily on statistical and rule-based techniques, where predefined thresholds and manual pattern analysis were used to flag suspicious transactions. Traditional statistical classification methods laid the foundation for fraud detection research [12]. However, these techniques lacked adaptability and struggled to scale with the rapid growth of digital transactions. With the increasing complexity of fraudulent behavior, researchers shifted toward data mining and machine learning approaches to improve detection accuracy and automation [11].

Supervised machine learning models have been extensively explored for fraud detection tasks. Studies have compared algorithms such as Logistic Regression, Decision Trees, Support Vector Machines, and ensemble techniques to determine their effectiveness in identifying fraudulent transactions [6], [7]. Ensemble and feature engineering strategies have been shown to enhance predictive performance by capturing nonlinear relationships within transaction data [9]. Additionally, practical insights from real-world fraud detection systems emphasize the importance of proper feature selection, probability calibration, and model robustness [10]. Sequence-based models and streaming frameworks have also been proposed to address temporal transaction behavior and real-time fraud detection challenges [4], [7].

One of the most critical challenges in fraud detection research is class imbalance, as fraudulent transactions represent only a small fraction of total transactions. Researchers have proposed various imbalance-handling techniques, including undersampling, probability calibration, and cost-sensitive learning to improve minority class detection [5], [8]. Recent benchmarking studies further highlight the importance of using evaluation metrics such as precision, recall, and F1-score rather than relying solely on accuracy [3]. Advances in deep learning and hybrid models have also demonstrated improvements in capturing complex fraud patterns [1], [2]. These modern approaches aim to enhance adaptability and detection sensitivity while maintaining computational efficiency.

Despite significant advancements in algorithm development, many studies focus primarily on offline model comparison rather than real-world deployment. Practical fraud detection systems require integration with scalable architectures capable of real-time prediction and transaction logging [4]. Recent works emphasize the need for systematic evaluation frameworks and deployable solutions that bridge the gap between research and application [2], [6].

The present project addresses this research gap by implementing a complete end-to-end fraud detection system. The supervised classification model is trained using imbalanced transaction data and evaluated using appropriate performance metrics. Unlike many previous works that remain at the experimental stage, the trained model is serialized and integrated into a Flask-based web application, with SQLite database support for transaction storage and monitoring. This deployment-oriented approach aligns with contemporary research trends while demonstrating a practical, user-centric fraud detection solution.

METHODOLOGY

The proposed Credit Card Fraud Detection System follows a structured methodology that integrates data preprocessing, machine learning model development, web deployment, and database integration to create a complete end-to-end solution. The methodology is divided into multiple stages to ensure systematic implementation and reliable fraud prediction.

The first stage involves data collection and preprocessing. A publicly available credit card transaction dataset was used for model training. The dataset contains transaction features such as Time, Amount, and anonymized numerical variables (V1–V28), along with a class label indicating whether a transaction is normal (0) or fraudulent (1). Since fraud detection datasets are highly imbalanced, with fraudulent transactions representing only a small percentage of total records, careful preprocessing was performed. This includes data cleaning, checking for missing values, separating input features and target labels, and performing train-test splitting. Where necessary, feature scaling techniques were applied to normalize the transaction amount and improve model performance. Handling imbalance ensures that the model does not become biased toward predicting only legitimate transactions.

The second stage focuses on model training and evaluation. A supervised machine learning classification algorithm was selected to distinguish between normal and fraudulent transactions. The model learns patterns from historical data by identifying differences in transaction behavior between the two classes. During training, the dataset is divided into training and testing subsets to evaluate generalization performance. Performance metrics such as Accuracy, Precision, Recall, F1-Score, and Confusion Matrix analysis were used to assess the effectiveness of the model. Special attention was given to recall and precision, as missing a fraudulent transaction (false negative) or incorrectly flagging a legitimate one (false positive) can both have serious consequences in real-world applications. Once satisfactory performance was achieved, the trained model was serialized and saved as fraud_model.pkl, enabling reuse without retraining.

The third stage involves model deployment and backend integration. The saved model was integrated into a web application using the Flask framework in Python. Flask serves as the backend server that receives user input, preprocesses it into the required numerical format, and passes it to the trained model for prediction. The model outputs a fraud probability score, which is then interpreted as either a normal transaction or a fraudulent transaction based on a defined threshold. This real-time prediction mechanism ensures immediate decision support when transaction data is entered through the web interface.

The final stage of the system focuses on frontend development and database integration to make the fraud detection model accessible and practical for users. A simple and user-friendly web interface was developed using HTML and CSS, allowing users to easily enter transaction details through a structured form. When the user submits the information, the input data is sent to the Flask backend, where the server processes the data and forwards it to the trained machine learning model for prediction.

To improve system functionality, an SQLite database was integrated to store transaction details along with the corresponding prediction results. Each transaction record is saved in the database, which helps maintain a history of transactions for monitoring and auditing purposes. This stored data can also be useful for future analysis and model improvement, enabling the system to become more accurate over time as more transaction data is collected.

After processing the input data, the system displays the prediction result directly on the web page. The output clearly indicates whether the transaction is legitimate or fraudulent, along with a calculated risk percentage that represents the likelihood of fraud. This clear presentation of results helps users quickly understand the system's decision and take appropriate action if a suspicious transaction is detected. The interface is designed to present the information in a simple and understandable manner, ensuring that users can easily interpret the prediction without technical knowledge.

In addition, the system ensures that the prediction process happens quickly and efficiently, enabling near real-time fraud detection. This is particularly important in financial systems where immediate decisions are required to prevent potential losses. By providing both a classification result and a risk score, the system offers a more informative output that supports better monitoring and decision-making.

Overall, the methodology combines machine learning techniques, web technologies, and database management to create a practical and scalable credit card fraud detection system. Through the integration of intelligent prediction models, an interactive web interface, and reliable data storage, the system demonstrates how technology can be used to improve security and reduce fraudulent financial activities in a real-world environment.

WORKFLOW

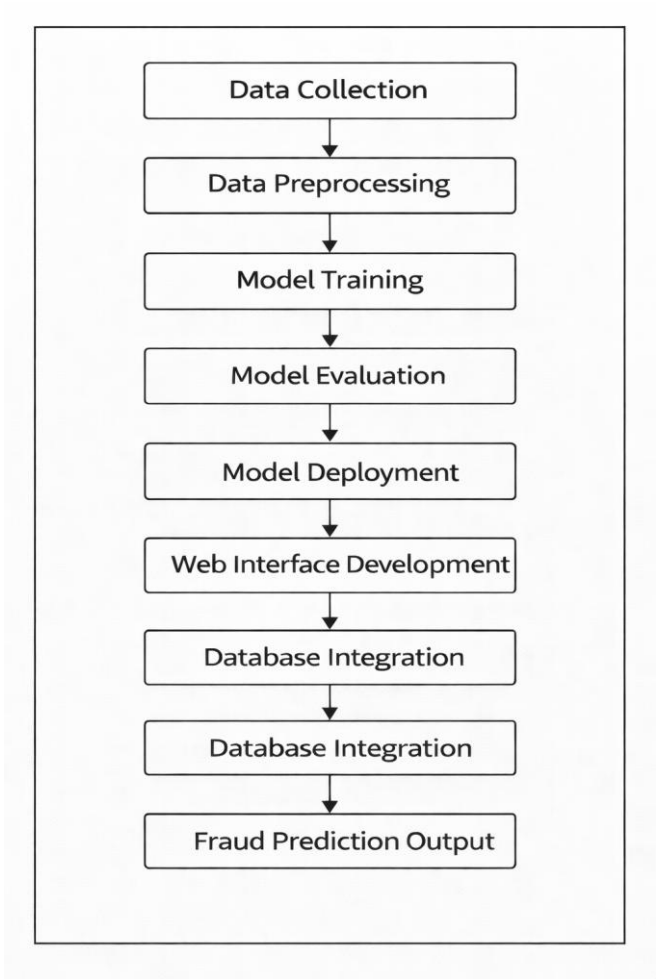

Figure 1: Workflow of proposed methodology.

The operational workflow of the proposed Credit Card Fraud Detection System begins when transaction data is prepared for intelligent analysis and real-time decision making. Instead of functioning only as a static machine learning model, the system operates as an integrated pipeline where each component communicates seamlessly with the next. Once the trained model is made available for use, the application environment is configured so that incoming transaction details can be processed instantly. When a user enters transaction attributes through the web interface, the system converts these inputs into the structured numerical format expected by the trained classifier. This step ensures consistency between the real-time input and the data format used during training. The backend application then activates the saved prediction model to analyze the transaction pattern and calculate the likelihood of fraudulent behavior based on learned feature relationships.

After the prediction is generated, the system performs two important actions simultaneously. First, it presents the classification result to the user in a clear and interpretable format, indicating whether the transaction is legitimate or fraudulent along with a calculated risk percentage. This enhances transparency and supports informed decision-making. Second, the system records the transaction details and prediction outcome in a structured database. This continuous storage mechanism allows the application to maintain a history of analyzed transactions, which can later support auditing, monitoring trends, or improving the model. By combining user interaction, real-time inference, and persistent data logging within a single connected framework, the workflow demonstrates how machine learning can be effectively transformed from a theoretical predictive model into a practical fraud detection solution ready for real-world deployment.

In addition to prediction and storage, the workflow also ensures smooth coordination between the system components to maintain reliability and responsiveness. The backend server continuously manages incoming requests, processes them sequentially, and ensures that each transaction is analyzed independently to prevent conflicts or data overlap. This structured request–response mechanism allows the system to operate efficiently even when multiple transactions are submitted.

Furthermore, by maintaining consistency between training data structure and live input format, the system minimizes prediction errors caused by mismatched feature ordering or scaling differences. This coordinated execution strengthens the robustness of the overall framework and ensures accurate, real-time fraud assessment within a controlled and systematic environment.

CONCLUSION

This project successfully demonstrates the design and implementation of a web-based Credit Card Fraud Detection System using Machine Learning. The system was developed to address the growing challenges of fraudulent financial transactions in digital payment environments. By leveraging transaction features and applying supervised classification techniques, the model effectively distinguishes between legitimate and fraudulent activities. Special consideration was given to handling the imbalanced nature of fraud datasets to ensure reliable detection performance beyond simple accuracy measures.

A significant contribution of this work lies in transforming a predictive model into a deployable application. Instead of limiting the study to model training and evaluation, the system integrates the trained model into a Flask-based web application with a user-friendly interface. The inclusion of SQLite database support enables secure storage of transaction records and prediction outcomes, enhancing traceability and system reliability. This end-to-end implementation demonstrates how machine learning can be practically applied in real-time fraud detection scenarios.

Overall, the proposed system highlights the effectiveness of combining data analytics, backend integration, and web technologies to build a functional and scalable fraud detection solution. The integration of machine learning with a web-based interface allows the system to analyze transaction data efficiently and present results in a clear and user-friendly manner. This approach demonstrates how modern technologies can work together to improve the accuracy and speed of fraud detection in financial systems.

The project not only strengthens financial transaction security but also provides a strong foundation for future improvements. With further development, the system can incorporate more advanced machine learning algorithms to increase prediction accuracy and handle complex fraud patterns. It can also be extended to support real-time transaction streaming, enabling immediate detection and response to suspicious activities. Additionally, deploying the system on cloud platforms would allow it to handle large volumes of transactions, making it suitable for large-scale financial applications and enterprise environments.

REFERENCES

[1] T. Albalawi, “Enhancing Credit Card Fraud Detection Using Machine Learning and Deep Learning Techniques,” Frontiers in Artificial Intelligence, 2025.

[2] N. Baisholan, “A Systematic Review of Machine Learning in Credit Card Fraud Detection,” Computers, vol. 14, 2024.

[3] “Benchmarking Machine Learning Techniques for Credit Card Fraud Detection,” Indian Journal of Science and Technology, 2023.

[4] F. Carcillo, A. Dal Pozzolo, Y.-A. Le Borgne, O. Caelen, Y. Mazzer, and G. Bontempi, “SCARFF: A Scalable Framework for Streaming Credit Card Fraud Detection,” Information Fusion, 2022.

[5] A. Dal Pozzolo et al., “Calibrating Probability with Undersampling for Unbalanced Classification,” IEEE Symposium Series on Computational Intelligence, 2021.

[6] V. N. Dornadula and S. Geetha, “Credit Card Fraud Detection Using Machine Learning Algorithms,” Procedia Computer Science, 2019.

[7] J. Jurgovsky et al., “Sequence Classification for Credit-Card Fraud Detection,” Expert Systems with Applications, 2018.

[8] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, “Calibrating Probability with Undersampling for Unbalanced Classification,” IEEE Symposium on Computational Intelligence, 2017.

[9] A. C. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, “Feature Engineering Strategies for Credit Card Fraud Detection,” Expert Systems with Applications, 2016.

[10] A. Dal Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi, “Learned Lessons in Credit Card Fraud Detection from a Practitioner Perspective,” Expert Systems with Applications, 2015.

[11] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, “Data Mining for Credit Card Fraud: A Comparative Study,” Decision Support Systems, vol. 50, no. 3, 2011.

[12] D. J. Hand and W. E. Henley, “Statistical Classification Methods in Consumer Credit Scoring: A Review,” Journal of the Royal Statistical Society, 1997