IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, May 2026
Impact Factor: 8.2

A Robust Machine Learning Framework for Real-Time Fraud Detection in Banking Transactions

Mr. Gaurav B. Landage[1], Prof. Pragati B. Chandane[2], Dr. Hemantkumar B. Jadhav[3], Prof. Jagruti R. Mahajan[4], Dr. Pradeep M. Patil[5]
[1,2,3,4,5] Department of Computer Engineering
[2,3,4]Assistant Professor, Adsul's Technical Campus, Ahilyanagar
[5]Principal, Adsul's Technical Campus, Ahilyanagar
[1,2,3,4,5] Adsul Technical Campus
gauravlandage.sitcomp@gmail.com[1] , pragatichandane3@gmail.com[2] , hem3577@gmail.com[3]
mahajanjagruti@gmail.com[4] , drpmp66@gmail.com[5]

Abstract: *The rapid expansion of digital banking and online payment systems has resulted in a substantial rise in financial fraud, creating serious security challenges for both customers and financial institutions. Conventional fraud detection methods, which rely heavily on predefined rules, are often ineffective in identifying evolving and complex fraudulent behaviors. To overcome these limitations, this project presents a machine learning–based fraud detection system capable of automatically learning patterns from historical transaction data and detecting fraudulent activities in real time. The proposed system implements and evaluates multiple supervised machine learning algorithms, including Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines (SVM), to classify banking transactions as either legitimate or fraudulent. A publicly available credit card transaction dataset is used for model training and testing, with appropriate data preprocessing and handling of class imbalance. The performance of each model is assessed using standard evaluation metrics such as accuracy, precision, recall, and F1-score. Experimental results indicate that machine learning techniques significantly improve fraud detection accuracy while reducing false positive rates. The system effectively identifies suspicious transactions in real time, enabling timely preventive actions. Overall, the proposed approach enhances the reliability, security, and efficiency of digital banking systems and demonstrates the potential of machine learning as a robust solution for modern financial fraud detection.*

Keywords: Fraud Detection, Banking Transactions, Machine Learning, Supervised Learning, Credit Card Fraud, Anomaly Detection, Financial Security

I. INTRODUCTION

In the modern digital economy, online banking and electronic financial transactions have become essential components of daily life. The widespread adoption of internet banking, mobile payments, and electronic fund transfers has significantly improved convenience and efficiency for users. However, this rapid digital transformation has also led to a substantial increase in financial fraud, posing serious challenges to banks, customers, and regulatory authorities [1]. Fraudulent banking transactions result in massive financial losses every year and negatively impact customer trust and institutional credibility [2].

Traditional fraud detection systems primarily rely on rule-based mechanisms and manually defined thresholds to identify suspicious transactions. While these approaches are simple to implement, they suffer from several limitations, including poor adaptability to evolving fraud strategies and an inability to detect complex or previously unseen fraud patterns [3]. Moreover, rule-based systems often generate a high number of false positives, leading to unnecessary

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, May 2026 Impact Factor: 8.2

transaction declines and customer dissatisfaction [4]. As fraudsters continuously modify their techniques, static rules quickly become outdated and ineffective in real-time transaction environments [5].

To overcome these challenges, machine learning (ML) techniques have emerged as a promising solution for intelligent fraud detection in banking systems. Machine learning models can automatically learn patterns and relationships from large volumes of historical transaction data and use this knowledge to identify anomalous or fraudulent behavior [6]. By analyzing multiple transaction features such as transaction amount, frequency, time, location, and user behavior, ML-based systems can distinguish legitimate transactions from fraudulent ones with greater accuracy than traditional methods [7].

Supervised learning algorithms, including Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines (SVM), have been widely applied in banking fraud detection due to their effectiveness in classification tasks [8]. These algorithms are trained using labeled datasets, allowing them to learn the distinguishing characteristics of fraudulent and non-fraudulent transactions. Additionally, advanced ensemble methods and hybrid approaches have further improved detection performance, particularly in handling highly imbalanced datasets where fraudulent transactions are rare [9].

This project aims to develop a machine learning–based fraud detection system for banking transactions using supervised learning techniques. The proposed system focuses on improving detection accuracy while minimizing false positives through efficient model training and evaluation. By integrating machine learning-driven fraud detection into banking infrastructures, financial institutions can enhance transaction security, reduce financial losses, and provide a safer and more reliable digital banking experience for customers [10], [11].

II. PROBLEM STATEMENT

The rapid advancement of digital banking, online payment platforms, and electronic financial services has transformed the way individuals and businesses perform monetary transactions. While these technologies offer convenience, speed, and accessibility, they have also led to a significant rise in fraudulent activities such as identity theft, unauthorized transactions, account takeovers, and card-not-present fraud. These fraudulent activities cause substantial financial losses to banks and customers and severely impact customer trust and confidence in digital banking systems.

Given these challenges, there is a pressing need for an intelligent and adaptive fraud detection system that can automatically learn from historical transaction data, identify subtle and hidden fraud patterns, and adapt to emerging fraudulent behaviors. Machine learning techniques provide a promising solution by enabling systems to analyze complex transaction features such as transaction amount, frequency, time, location, and customer behavior patterns.

Therefore, the core problem addressed in this project is the development of a robust machine learning–based fraud detection system capable of accurately identifying fraudulent banking transactions from large, imbalanced datasets while minimizing false positives and maintaining real-time efficiency. The proposed solution aims to strengthen financial security, reduce monetary losses, and improve the reliability and trustworthiness of modern digital banking environments.

III. OBJECTIVE

- To study and analyze the patterns of fraudulent and non-fraudulent banking transactions using historical data.
- To preprocess and prepare the dataset, including handling missing values, feature selection, normalization, and addressing class imbalance.
- To implement and evaluate various machine learning algorithms (e.g., Logistic Regression, Decision Tree, Random Forest, SVM, Neural Networks) for detecting fraudulent transactions.
- To compare the performance of these models using evaluation metrics such as accuracy, precision, recall, F1-score, and ROC-AUC.
- To minimize false positives and false negatives, ensuring the model is both sensitive and specific in detecting fraud.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, May 2026
Impact Factor: 8.2

- To develop a prototype fraud detection system capable of detecting suspicious transactions in near real-time.
- To ensure the model's adaptability, allowing for periodic retraining to accommodate evolving fraud patterns.

IV. LITERATURE SURVEY

1. A Machine Learning Based Credit Card Fraud Detection Using the GA Algorithm for Feature Selection
Published: 2022
Publication: Journal of Big Data
Summary: This paper proposes a fraud detection system that combines Genetic Algorithm (GA)–based feature selection with machine learning classifiers such as Decision Tree, Random Forest, Logistic Regression, Artificial Neural Network, and Naive Bayes. The GA selects the most relevant features, improving classifier performance on the imbalanced European credit card transaction dataset. Results demonstrated improved accuracy and detection performance compared to traditional models.

2. Credit Card Fraud Detection Using Machine Learning
Authors: Amit Kumar, Anant Jain, Mohd Ariz, Nitin Kumar
Published: 2022
Publication: Journal of Pharmaceutical Negative Results
Summary: This study compares multiple machine learning algorithms—including Decision Trees, Random Forest, Logistic Regression, Neural Network, and XGBoost—for detecting credit card fraud. The research uses oversampling and undersampling techniques to handle class imbalance and finds tree-based ensemble methods (like Random Forest and XGBoost) to offer superior performance in predicting fraud patterns.

3. Fraud Detection in Banking: A Machine Learning Approach using Credit Card Transaction Data
Author: Karthika Gopalakrishnan
Published: 2023
Publication: Journal of Artificial Intelligence & Cloud Computing
Summary: This article investigates the performance of classic machine learning models such as Decision Tree, K-Nearest Neighbors (KNN), Logistic Regression, SVM, Random Forest, and XGBoost on a publicly available credit card dataset. It evaluates their effectiveness in classifying transactions and discusses practical considerations for real-time implementation in banking systems.

4. Credit Card Fraud Detection Using Machine Learning Algorithms: A Comparative Study of Six Models
Authors: Joseph J. Assabil & Ibidun Christiana Obagbuwa
Published: 2024
Publication: International Journal of Intelligent Systems and Applications in Engineering
Summary: This comparative study evaluates six machine learning models (e.g., Logistic Regression, Decision Trees, KNN, Random Forest, Adaboost, and XGBoost) using resampling techniques like SMOTE to address class imbalance. It highlights how feature engineering and sampling impact performance metrics such as precision, recall, and F1-score in fraud detection.

5. Machine Learning-Based Cyber Fraud Detection: A Comparative Study of Resampling Methods for Imbalanced Credit Card Data
Published: 2026
Publication: Applied Sciences (MDPI)
Summary: This recent paper conducts a comprehensive comparison of machine learning classifiers (e.g., Decision Tree, Random Forest, Logistic Regression, SVM, KNN, XGBoost, CatBoost) with various resampling methods

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, May 2026
Impact Factor: 8.2

(SMOTE, ENN, Tomek Links) to handle the extreme imbalance typical of credit card fraud datasets. It evaluates models using key metrics like accuracy, precision, recall, and ROC-AUC.

V. PROPOSED SYSTEM

The proposed system aims to design and implement an intelligent fraud detection framework for banking transactions using machine learning techniques. The system focuses on accurately identifying fraudulent transactions in real time while minimizing false positives and adapting to evolving fraud patterns. By leveraging historical transaction data and supervised machine learning algorithms, the proposed solution enhances the efficiency, reliability, and security of digital banking operations.

A. System Overview

The proposed fraud detection system consists of multiple stages, including data collection, data preprocessing, feature analysis, model training, fraud classification, and alert generation. A publicly available credit card transaction dataset containing labeled transactions (fraudulent and legitimate) is used to train and evaluate the machine learning models. The system is designed to handle large-scale and highly imbalanced datasets, where fraudulent transactions form a very small portion of the overall data.

The core idea of the proposed system is to replace traditional rule-based detection with a data-driven approach that learns transaction behavior patterns automatically and continuously improves detection performance.

B. Data Collection and Preprocessing

The first stage of the proposed system involves collecting transaction data that includes attributes such as transaction amount, time, frequency, location, and user behavior indicators. Since real-world banking datasets often contain noise, missing values, and redundant features, preprocessing is a crucial step.

Data preprocessing techniques such as data cleaning, normalization, and feature scaling are applied to ensure consistency and improve model performance. Additionally, due to the severe class imbalance between fraudulent and legitimate transactions, appropriate techniques such as undersampling, oversampling, or Synthetic Minority Over-sampling Technique (SMOTE) are employed to balance the dataset and prevent model bias toward majority classes.

C. Feature Selection and Analysis

Feature selection plays an important role in improving fraud detection accuracy and reducing computational complexity. The proposed system analyzes relevant transaction features that contribute most to fraud identification. Correlation analysis and feature importance techniques are used to eliminate irrelevant or redundant features, enabling the models to focus on the most informative attributes.

This step improves learning efficiency and enhances the generalization capability of the machine learning models.

D. Machine Learning Model Training

The proposed system employs multiple supervised machine learning algorithms to classify transactions as fraudulent or legitimate. The algorithms used include Logistic Regression, Decision Tree, Random Forest, and Support Vector Machine (SVM). These models are trained using labeled transaction data and evaluated using standard performance metrics.

Each algorithm offers unique advantages: Logistic Regression provides simplicity and interpretability, Decision Trees offer rule-based decision structures, Random Forest improves accuracy through ensemble learning, and SVM handles high-dimensional data effectively. Model training is performed using a training dataset, while performance evaluation is conducted on a separate testing dataset.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, May 2026
Impact Factor: 8.2

VI. SYSTEM DESIGN

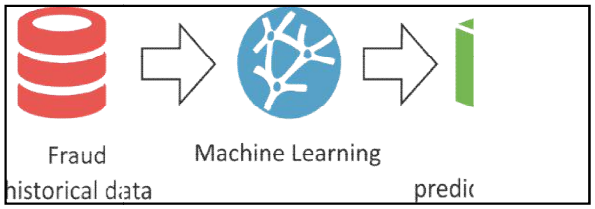


Fig 1: System Architecture

The proposed fraud detection system is designed using a layered architecture to ensure modularity, scalability, and efficient processing of banking transaction data. Each layer is responsible for a specific function, starting from data acquisition and ending with decision-making and model improvement. This layered approach enables seamless integration of machine learning techniques into real-time banking environments while ensuring adaptability to evolving fraud patterns.

A. Data Collection Layer

The Data Collection Layer is responsible for acquiring transaction-related data from various banking and financial sources. This layer serves as the entry point of the system and ensures continuous availability of data for analysis. Data can be collected either in real time during transaction execution or in batch mode for historical analysis.

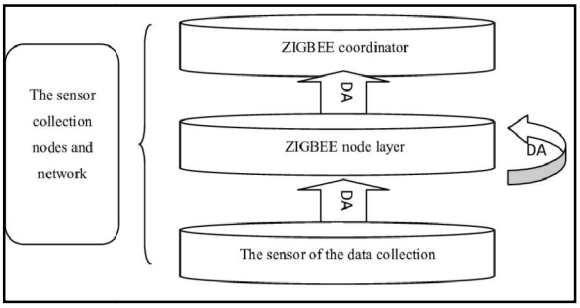


Fig 2: Data Collection

The primary data sources include transaction data such as transaction amount, time, merchant details, payment mode, and user identifiers. In addition, user data including historical transaction behavior, account details, and demographic information are collected to understand normal customer behavior. Device-related data such as IP address, device ID, and browser type are also captured to identify suspicious access patterns. Furthermore, geolocation data is used to track the physical location of transactions, which helps in detecting anomalies such as sudden location changes or transactions from high-risk regions. Once collected, the data is securely transmitted to the preprocessing layer.

B. Data Preprocessing Layer

The Data Preprocessing Layer ensures that raw transaction data is converted into a clean and structured format suitable for machine learning models. Since real-world banking data often contains inconsistencies and noise, preprocessing is a critical step.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, May 2026
Impact Factor: 8.2

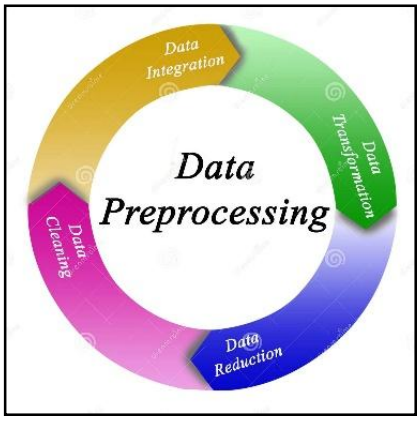


Fig 3: Data Preprocessing

This layer performs data cleaning to handle missing values, duplicate records, and corrupted entries. Numerical features are normalized or standardized to bring them onto a common scale, which improves the performance of algorithms such as Support Vector Machines. Categorical attributes such as merchant type or payment mode are transformed into numerical form using encoding techniques like one-hot encoding or label encoding.

To address the highly imbalanced nature of fraud datasets, techniques such as oversampling, undersampling, or SMOTE are applied. Additionally, outlier detection mechanisms are used to identify extreme values that may indicate either data errors or potential fraud. After preprocessing, the refined data is passed to the feature engineering layer.

C. Feature Engineering Layer

The Feature Engineering Layer enhances the predictive capability of the fraud detection system by constructing meaningful features from raw data. Effective feature engineering helps machine learning models better distinguish between legitimate and fraudulent transactions.

Transaction-based features include transaction amount, frequency, and merchant category. Behavioral features analyze customer spending habits and deviations from historical behavior. Geospatial features calculate the distance between a customer's usual location and the transaction location. Temporal features capture time-based patterns, such as transactions occurring at unusual hours or on weekends. Device and network features analyze device consistency, IP address usage, and network type.

In addition, aggregated features are generated by summarizing transaction activity over different time windows such as daily or weekly periods to identify abnormal spikes in activity. These engineered features are then forwarded to the model training layer.

D. Model Training and Evaluation Layer

In this layer, supervised machine learning models are trained using labeled transaction data, where each transaction is marked as fraudulent or legitimate. Algorithms such as Logistic Regression, Decision Tree, Random Forest, and Support Vector Machine (SVM) are trained to learn fraud patterns from historical data.

The dataset is split into training and testing subsets to evaluate model performance. Performance metrics such as accuracy, precision, recall, F1-score, and confusion matrix are used to assess the effectiveness of each model. Based on these evaluations, the most suitable model is selected for deployment in the real-time fraud detection layer.

In addition, feature engineering and data preprocessing play a crucial role in improving the performance of supervised machine learning models. Raw transaction data is cleaned to handle missing values, remove noise, and normalize numerical attributes such as transaction amount and time. Categorical features like transaction type or merchant category are encoded into machine-readable formats. Important features are then selected or derived to capture behavioral patterns such as transaction frequency, location deviation, and spending trends, which significantly enhance the model's ability to distinguish between fraudulent and legitimate transactions.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, May 2026
Impact Factor: 8.2

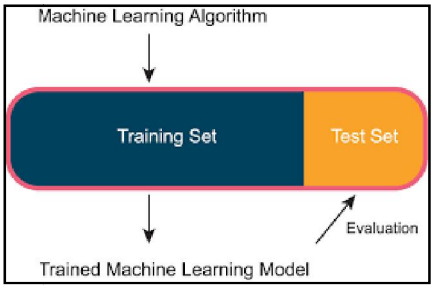
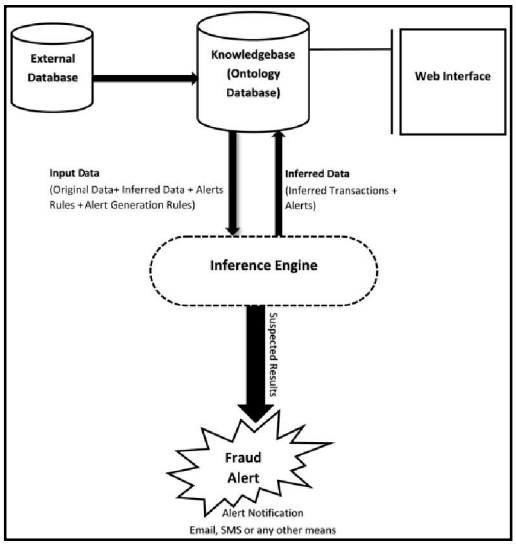


Fig 4: Model Training and Evaluation

E. Fraud Detection Layer (Inference)

The Fraud Detection Layer performs real-time analysis of incoming banking transactions. Each transaction is processed through the trained machine learning model to determine whether it is legitimate or fraudulent.



The model generates a probability score indicating the likelihood of fraud. A predefined decision threshold is applied to classify transactions. Transactions with a probability exceeding the threshold are flagged as suspicious, enabling immediate response and prevention of potential fraud.

F. Decision Support and Alert Layer

This layer is responsible for taking appropriate actions once a transaction is classified as potentially fraudulent. Alerts are generated and sent to fraud analysts or system administrators for further investigation. Each transaction is assigned a fraud risk score to help prioritize cases based on severity.

For high-risk transactions, automated actions such as blocking or reversing the transaction can be triggered to minimize financial losses. Moderate-risk cases may be escalated for manual verification, ensuring a balance between security and customer convenience.

G. Feedback Loop and Model Updating Layer

The Feedback Loop and Model Updating Layer ensures continuous improvement of the fraud detection system. Verified fraud cases and confirmed legitimate transactions are fed back into the system as new training data.

Periodic retraining of models allows the system to adapt to evolving fraud strategies and changing customer behavior. This continuous learning mechanism improves detection accuracy over time and maintains the effectiveness of the system in dynamic banking environments.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, May 2026
Impact Factor: 8.2

VII. RESULT

The proposed machine learning–based fraud detection system was evaluated using a publicly available credit card transaction dataset containing both legitimate and fraudulent transactions. Due to the highly imbalanced nature of the dataset, where fraudulent transactions form only a small fraction of the total data, appropriate preprocessing and class imbalance handling techniques were applied before model training. Multiple supervised learning algorithms, including Logistic Regression, Decision Tree, Random Forest, and Support Vector Machine (SVM), were implemented to analyze their effectiveness in detecting fraudulent transactions.

The experimental results indicate that each algorithm demonstrated varying levels of performance. Logistic Regression provided fast execution and model interpretability but showed limitations in capturing complex and non-linear fraud patterns. The Decision Tree model was able to identify rule-based patterns effectively; however, it exhibited a tendency to overfit the training data. In contrast, the Random Forest model delivered superior performance by combining multiple decision trees, which improved generalization and robustness when handling noisy and imbalanced data. The SVM model also showed strong classification capability in high-dimensional feature spaces but required higher computational resources compared to other models.

VIII. FUTURE SCOPE

The future of fraud detection in banking transactions lies in the development of real-time, large-scale machine learning systems capable of processing millions of transactions with extremely low latency. As digital payment volumes continue to grow, integrating the fraud detection framework with high-performance streaming platforms such as Apache Kafka and Apache Spark can enable instant analysis of transaction streams. This will allow banks to detect and prevent fraudulent activities within milliseconds, significantly reducing financial losses and improving customer trust. Real-time scalability will be essential for supporting global banking systems and high-frequency transaction environments.

Another promising direction for future enhancement is the adoption of deep learning and advanced neural network architectures. Models such as Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Transformer-based architectures can effectively capture sequential, temporal, and behavioral dependencies in transaction data. These advanced models have the potential to detect sophisticated and multi-stage fraud techniques, including synthetic identity fraud, coordinated fraud rings, and mule account activities, which are often difficult to identify using traditional machine learning methods.

REFERENCES

[1]. R. Rambola, P. Varshney, and P. Vishwakarma, “Data mining techniques for fraud detection in banking sector,” 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2018, pp. 1–5, doi: 10.1109/CCAA.2018.8777535.

[2]. N. Malini and M. Pushpa, “Analysis on credit card fraud identification techniques based on KNN and outlier detection,” 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, India, 2017, pp. 255–258, doi: 10.1109/AEEICB.2017.7972424.

[3]. I Sohony, R. Pratap, and U. Nambiar, “Ensemble learning for credit card fraud detection,” Proceedings of the ACM India Joint International Conference on Data Science and Management of Data (CoDS-COMAD ’18), ACM, New York, USA, 2018, pp. 289–294.

[4]. C. Wang, Y. Wang, Z. Ye, L. Yan, W. Cai, and S. Pan, “Credit card fraud detection based on whale algorithm optimized BP neural network,” 2018 13th International Conference on Computer Science Education (ICCSE), Colombo, Sri Lanka, 2018, pp. 1–4.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, May 2026
Impact Factor: 8.2

[5]. J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, 2017, pp. 1–9.

[6]. Y. Caelen, Y. Mazzer, and G. Bontempi, "Scarff: A scalable framework for streaming credit card fraud detection with Spark," Information Fusion, vol. 41, pp. 182–194, 2018.

[7]. Y. Lucas and J. Jurgovsky, "Credit card fraud detection using machine learning: A survey," arXiv preprint arXiv:2010.06479, 2020.

[8]. D. Dal Pozzolo, G. Bontempi, and O. Snoeck, "Adaptive machine learning for credit card fraud detection," Expert Systems with Applications, vol. 41, no. 4, pp. 1294–1304, 2014.

[9]. A Dal Pozzolo, O. Bache, G. Bontempi, and Y. Snoeck, "Calibrating probability with undersampling for unbalanced classification," 2015 IEEE Symposium Series on Computational Intelligence, Cape Town, South Africa, 2015.

[10]. A Whitrow, D. J. Hand, P. Juszczak, D. Weston, and N. M. Adams, "Transaction aggregation as a strategy for credit card fraud detection," Data Mining and Knowledge Discovery, vol. 18, no. 1, pp. 30–55, 2009.

[11]. P. Chan, W. Fan, A. Prodromidis, and S. Stolfo, "Distributed data mining in credit card fraud detection," IEEE Intelligent Systems, vol. 14, no. 6, pp. 67–74, 1999.

[12]. T. Fawcett and F. Provost, "Adaptive fraud detection," Data Mining and Knowledge Discovery, vol. 1, no. 3, pp. 291–316, 1997.

[13]. A Bahnsen, D. Aouada, and B. Ottersten, "Cost-sensitive decision trees for fraud detection," Expert Systems with Applications, vol. 39, no. 12, pp. 10903–10911, 2012.

[14]. S. Carcillo, Y. Bontempi, and G. Snoeck, "Scarff: A fraud detection framework," IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3781–3793, 2018.

[15]. V. Kagita, R. Singh, and R. Sharma, "Credit card fraud detection using decision trees and random forests," International Journal of Computer Applications, vol. 145, no. 8, pp. 15–19, 2016.

[16]. A Srivastava, A. Kundu, S. Sural, and A. Majumdar, "Credit card fraud detection using hidden Markov model," IEEE Transactions on Dependable and Secure Computing, vol. 5, no. 1, pp. 37–48, 2008.

[17]. J. Bolton and D. Hand, "Statistical fraud detection: A review," Statistical Science, vol. 17, no. 3, pp. 235–255, 2002.

[18]. R. Juszczak, D. Weston, and N. Adams, "Predicting fraudulent transactions using dynamic Bayesian networks," Machine Learning, vol. 71, no. 1, pp. 121–144, 2008.

[19]. A Roy and J. Sun, "Fraud detection in financial transactions using deep learning," International Journal of Computer Applications, vol. 179, no. 32, pp. 1–6, 2018.

[20]. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. Westland, "Data mining for credit card fraud: A comparative study," Decision Support Systems, vol. 50, no. 3, pp. 602–613, 2011