International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 07 | July - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Financial Fraud Detection Using Machine Learning

Trupti Ranjan Behera
Email ID: tbehera2023@gift.edu.in

Asst.Prof. Mohapatra Girashree Sahu
Email ID: girashreesahu@gmail.com

Abstract- Financial fraud poses a significant threat to global economic stability, affecting individuals, institutions, and governments. Traditional fraud detection systems, which often rely on predefined rules and manual inspections, struggle to adapt to evolving fraudulent tactics. In this study, we explore the application of machine learning (ML) techniques to detect and prevent financial fraud with greater accuracy and efficiency. By leveraging supervised and unsupervised learning algorithms, the system can identify complex patterns and anomalies in large volumes of transactional data. We utilize a publicly available credit card fraud dataset to train and evaluate various models, including Logistic Regression, Decision Trees, Random Forest, Support Vector Machines (SVM), and Neural Networks. Performance is assessed using metrics such as accuracy, precision, recall, F1-score, and AUC-ROC. The results demonstrate that machine learning approaches significantly enhance fraud detection capabilities, reduce false positives, and offer real-time predictive analytics. This research highlights the potential of intelligent systems in strengthening financial security and provides insights into future developments in automated fraud prevention.

Keywords- Financial Fraud, Machine Learning, Fraud Detection, Transaction Data, Classification Models, Anomaly Detection, Predictive Analytics, Supervised Learning, Data Mining, Real-time Monitoring.

I. INTRODUCTION

In today's digital age, the rapid growth of financial transactions through online platforms, credit cards, and electronic payments has made the financial sector increasingly vulnerable to fraudulent activities. Financial fraud not only results in significant monetary losses but also undermines consumer trust and damages the reputation of institutions. The dynamic and evolving nature of fraud tactics makes it difficult for traditional rule-based detection systems to effectively identify and prevent such incidents in real-time. Machine Learning (ML) offers a powerful solution to this challenge by enabling systems to automatically learn from data, adapt to new patterns, and make intelligent decisions without explicit programming. By analyzing historical transaction data, ML algorithms can uncover hidden relationships, detect anomalies, and predict fraudulent behavior with high accuracy. Unlike conventional methods, machine learning models can be continuously trained and refined, making them more robust against emerging fraud strategies.

This research investigates the application of machine learning techniques for detecting financial fraud, with a focus on credit card transaction data. Various algorithms, such as Logistic Regression, Decision Trees, Random Forests, Support Vector Machines, and Neural Networks, are evaluated for their performance in identifying fraudulent activities. The objective is to develop an efficient and reliable system that can assist financial institutions in minimizing fraud-related risks through early detection and intervention.

II. LITERATURE REVIEW

The detection of financial fraud has long been a subject of research across disciplines such as computer science, finance, and cybersecurity. With the growing volume and complexity of financial data, researchers have increasingly turned to machine learning techniques for building more adaptive and intelligent fraud detection systems.

Early studies primarily relied on **rule-based and statistical methods** to identify fraud. Although these approaches offered interpretability, they lacked the flexibility to detect novel or evolving fraudulent behaviors. Manual rule updates were time-consuming and often failed to keep up with real-time threats.

Recent advances in machine learning have significantly improved fraud detection performance. **Bhattacharyya et al. (2011)** explored the use of supervised learning algorithms like Random Forests and Neural Networks for credit card fraud detection and found that ensemble methods tend to outperform single classifiers in terms of accuracy and recall. Their study highlighted the effectiveness of feature selection and resampling techniques in handling imbalanced datasets.

Carcillo et al. (2019) emphasized the importance of time-aware modeling and real-time learning in fraud detection systems. They showed that incorporating temporal patterns of transactions can enhance the prediction of future fraud attempts, especially in streaming environments.

In another study, **Pozzolo et al. (2018)** addressed the challenge of class imbalance in financial datasets—where fraudulent transactions represent a tiny fraction of total data—by evaluating various under-sampling and cost-sensitive methods. Their research demonstrated that algorithmic bias can be significantly reduced by balancing the training data or adjusting decision thresholds.

Unsupervised learning techniques such as clustering and autoencoders have also gained attention. These methods do not rely on labeled data and can be effective in **anomaly detection**, where fraudulent activities are rare and diverse. For example, **Fiore et al. (2017)** proposed an autoencoder-based fraud detection framework that achieved high anomaly detection rates without requiring prior fraud labels.

Moreover, the integration of **deep learning** has opened new avenues in detecting more subtle and complex fraud schemes. Recurrent Neural Networks (RNN) and Long Short-Term

Memory (LSTM) networks have been particularly useful in modeling sequential transaction data, capturing temporal dependencies that traditional models might overlook.

In summary, the literature reveals a steady evolution from rule-based systems to sophisticated machine learning models. While supervised algorithms dominate current solutions, the combination of **ensemble learning, anomaly detection, and deep learning** continues to shape the future of intelligent fraud detection systems.

III. RESEARCH GAP

Despite significant progress in the field of financial fraud detection using machine learning, several critical challenges remain unaddressed. A review of existing literature reveals the following key research gaps:

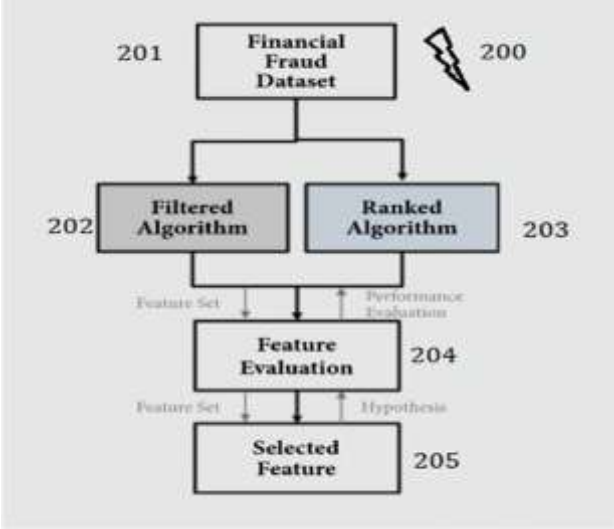
- ✓ **Class Imbalance**: Most financial datasets are highly imbalanced, with fraudulent transactions representing a very small fraction of the total data. Many existing models fail to effectively handle this imbalance, leading to high false negative rates.
- ✓ **Real-time Detection**: A majority of studies focus on offline analysis using historical data. There is limited research on developing real-time or near-real-time fraud detection systems that can respond to threats as they occur.
- ✓ **Dynamic Fraud Patterns**: Fraudsters continuously evolve their strategies to bypass detection systems. Many machine learning models become outdated quickly and lack adaptability to new fraud patterns.
- ✓ **Explainability of Models**: While deep learning models and complex ensembles offer high accuracy, they often act as black boxes. The lack of transparency in decision-making reduces trust and makes regulatory compliance more difficult.
- ✓ **Data Privacy and Security**: Few studies address the ethical and legal challenges of using sensitive financial data, including the need for privacy-preserving machine learning models.
- ✓ **Scalability**: With the growing volume of financial transactions, scalability and computational efficiency become major concerns. Many existing models do not scale well in production environments.

IV. PROBLEM FORMULATION

The primary objective of this research is to develop an efficient and intelligent fraud detection system using machine learning techniques that can overcome the limitations of existing approaches. Specifically, the study aims to:

- ✓ **Detect fraudulent financial transactions** with high accuracy and low false positive rate.
- ✓ **Handle class imbalance** using techniques such as resampling, anomaly detection, or cost-sensitive learning.
- ✓ **Adapt to evolving fraud patterns** through model retraining or incremental learning strategies.
- ✓ **Enable real-time or near-real-time fraud detection**, suitable for deployment in production systems.
- ✓ **Maintain interpretability and transparency**, making the model's decisions understandable to users and regulators.

V. METHODOLOGY



(Figure 1: Design and Approach)

The diagram illustrates a feature selection framework for financial fraud detection using machine learning. Below is a step-by-step explanation of each labeled component:

❖ 200 – Lightning Symbol (Problem Indicator)

This symbol represents a trigger or challenge, indicating the problem of financial fraud which necessitates intelligent detection mechanisms.

❖ 201 – Financial Fraud Dataset

This is the raw dataset containing transaction records, including both legitimate and fraudulent transactions. The dataset typically includes:

- ✓ Transaction ID, time, amount
- ✓ Customer and merchant details
- ✓ Labels (fraudulent or not)

This is the starting point for the feature selection and model development process.

❖ 202 – Filtered Algorithm

The Filtered Algorithm refers to filter-based feature selection methods such as:

- ✓ Chi-square test
- ✓ Information Gain
- ✓ Correlation-based Filtering

These methods evaluate the relevance of features based on statistical characteristics without using a machine learning model. It quickly removes irrelevant or redundant features.

❖ 203 – Ranked Algorithm

The Ranked Algorithm refers to wrapper or embedded feature selection techniques, including:

- ✓ Recursive Feature Elimination (RFE)
- ✓ Feature importance from models like Random Forest, XGBoost
- ✓ LASSO (for embedded feature ranking)

These methods rank features based on their impact on the model's performance.

❖ 204 – Feature Evaluation

This step combines the output from both filtered and ranked algorithms to evaluate:

- ✓ Feature relevance
- ✓ Contribution to model accuracy
- ✓ Redundancy and correlation

Here, features are scored and tested with a performance evaluation metric, such as AUC-ROC, precision, or F1-score.

❖ 205 – Selected Feature

The final output is a refined set of features that are:

- ✓ Highly relevant to fraud detection
- ✓ Non-redundant
- ✓ Optimal for training machine learning models

These features are then used to train, validate, and test the fraud detection models efficiently.

VI. Problem Statement

For many banks, retaining high profitable customers is the number one business goal. Banking fraud, however, poses a significant threat to this goal for different banks. In terms of substantial financial losses, trust and credibility, this is a concerning issue to both banks and customers alike.

In the banking industry, credit card fraud detection using machine learning is not only a trend but a necessity for them to put proactive monitoring and fraud prevention mechanisms in place. Machine learning is helping these institutions to reduce time-consuming manual reviews, costly chargebacks and fees as well as denials of legitimate transactions.

In this project we will detect fraudulent credit card transactions with the help of Machine learning models.
We will analyse customer-level data that has been collected and analysed during a research collaboration of Worldline and the Machine Learning Group.

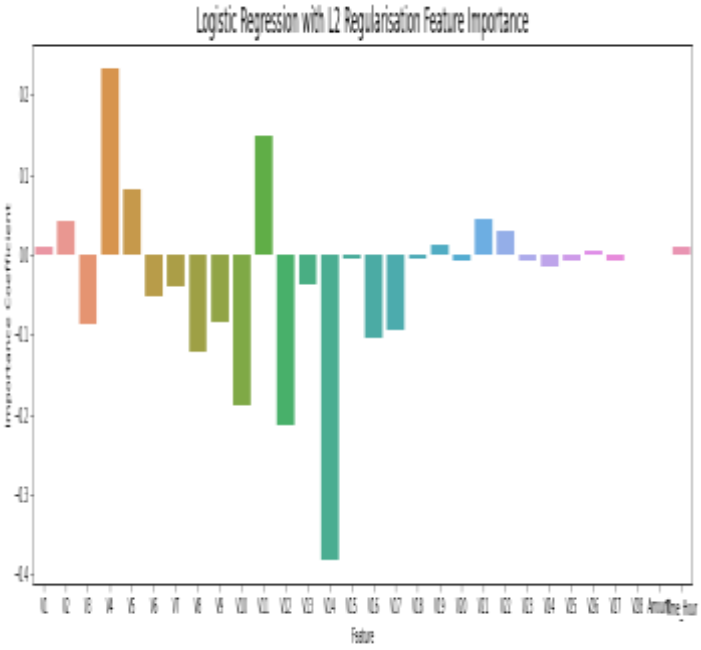
VII. RESULTS AND DISCUSSION

Methodology	Model	Accuracy	roc_value	thershold
Repeated Kfold Cross Validation	Logistic Regression with L2 Regularisation	0.998964	0.969011	0.001423
Repeated Kfold Cross Validation	Logistic Regression with L1 Regularisation	0.998929	0.869289	0.047230
Repeated Kfold Cross Validation	KNN	0.999263	0.864827	0.200000
Repeated Kfold Cross Validation	Tree Model with gini criteria	0.999245	0.874842	1.000000
Repeated Kfold Cross Validation	Tree Model with entropy criteria	0.999087	0.874763	0.010000

(Performance Comparison of Machine Learning Models Using Repeated K-Fold Cross Validation)

The table presents the performance of various machine learning models for financial fraud detection using Repeated K-Fold Cross Validation. The models are evaluated based on accuracy, ROC value, and threshold.

- ✓ Logistic Regression (L2 Regularization) achieved the highest ROC value (0.969) and strong accuracy (99.89%), making it the most reliable model in terms of balanced performance and generalization. The very low threshold (0.0014) suggests it is sensitive to fraud detection.
- ✓ Logistic Regression (L1 Regularization) also performed well (accuracy 99.89%) but had a significantly lower ROC score (0.869), indicating it may not distinguish between classes as effectively as the L2 variant.
- ✓ K-Nearest Neighbors (KNN) gave the highest accuracy (99.93%) but showed a relatively lower ROC value (0.8648), suggesting it might be overfitting or not robust on imbalanced data.
- ✓ Decision Trees (Gini & Entropy) also delivered high accuracy (~99.91%) with moderate ROC values (~0.874). The model with Gini used a threshold of 1.0, which is unusually high and may indicate low sensitivity to minority (fraud) cases.



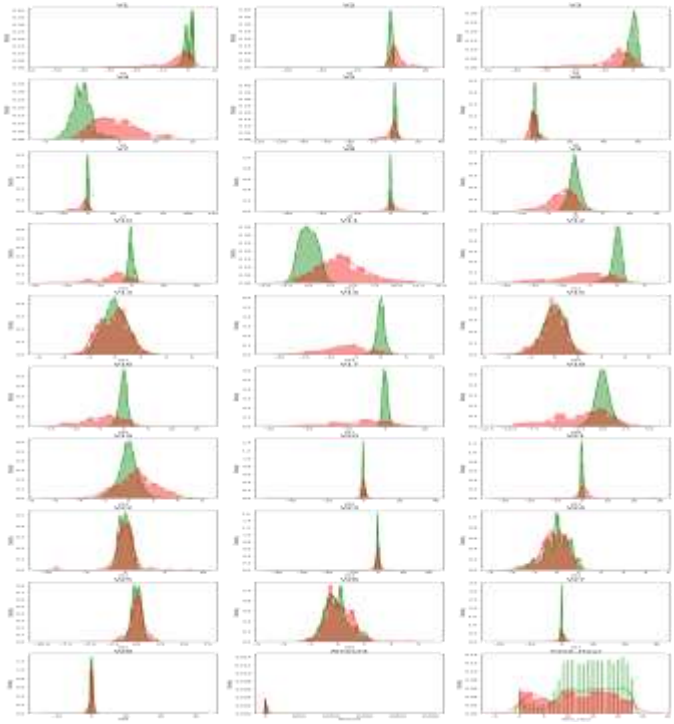
(Figure 2: - Feature Importance Plot from Machine Learning Model for Fraud Detection)

The bar graph visualizes feature importance (likely coefficients or impact scores) from a machine learning model used for financial fraud detection.

❖ **Key Observations:**

- ✓ A few features (left side of the graph) have strong positive or negative contributions, indicating high importance in predicting fraud.
- ✓ Most features on the right have values close to zero, suggesting low or negligible impact.
- ✓ The color gradient likely groups features based on categories or ranges for easier visualization.

This graph helps in identifying which features are most influential in the model's decision-making process. Removing low-impact features (near zero) can simplify the model and reduce computational cost without significantly affecting accuracy.



(Figure 3: - Distribution Plots of Input Features for Fraudulent vs Non-Fraudulent Transactions)

The above figure displays feature distribution plots for different variables in the financial fraud dataset, comparing fraudulent (red) vs non-fraudulent (green) transactions.

❖ Key Insights:

- ✓ Several features show distinct separation between the two classes (e.g., top-left and middle rows), suggesting strong predictive value for fraud detection.
- ✓ Some distributions overlap significantly, indicating limited individual contribution to classification.
- ✓ Features with peaked green distributions suggest dense clustering of legitimate transactions, while red distributions often show longer tails, reflecting the rarity and variability of fraud cases.

These visualizations are crucial for **exploratory data analysis (EDA)**. Features with **clear separation** can be prioritized for model training, while highly overlapping ones may need transformation, combination, or removal.

VIII. CONCLUSION

The Development of a system that can reliably and efficiently predict heart illness is becoming more and more important due to the increasing number of heart disease deaths. The study sought to identify the most effective machine learning method for detecting heart problems. This study examined the accuracy of DT, KNN, RF, SVM, and NB algorithms for heart disease prediction. It analyzes data such as blood pressure, cholesterol, chest pain, alcohol intake, smoking, diet, and stress to help estimate a patient's risk of a heart disease. The dataset needs to be normalized in order to prevent the training model from overfitting and from producing insufficient accuracy when a model is evaluated for real-world data problems, which can differ greatly from the dataset used for training. It was also discovered that statistical analysis plays a significant role in the analysis of a dataset. More datasets can be used to enable deep learning with a variety of additional improvements, potentially yielding more encouraging outcomes. The data can be normalized in more ways, and the outcomes can be contrasted. Additionally, there may be more ways to combine specific multimedia with ML and DL models trained on cardiac diseases for the convenience of physicians and patients.

IX. FUTURE SCOPE

The application of machine learning in financial fraud detection has shown promising results, yet there remains considerable potential for further advancement and real-world implementation. As financial systems continue to evolve, so must the detection mechanisms that safeguard them.

- ✓ **Real-Time Fraud Detection**: Future research can focus on developing models capable of detecting fraud in real time, which is crucial for preventing losses before transactions are completed.
- ✓ **Adaptive Learning Systems**: Implementing models that continuously learn from new patterns and data streams will help in identifying emerging fraud techniques, making the system more resilient and self-improving over time.
- ✓ **Deep Learning and Hybrid Models**: The use of advanced deep learning architectures such as LSTM, CNN, and attention-based models, either standalone or in combination with traditional algorithms, could enhance detection of sophisticated and time-based fraudulent behaviors.
- ✓ **Explainable AI (XAI)**: Enhancing model transparency through explainable AI techniques will help build trust among users and financial regulators, making it easier to understand and validate model decisions.
- ✓ **Privacy-Preserving Techniques**: With increasing concern over data security, future systems can integrate privacy-preserving machine learning methods such as federated learning or homomorphic encryption to protect sensitive financial data.
- ✓ **Multimodal Data Integration**: Combining transactional data with behavioral, biometric, and location-based data can provide a more holistic view of user activity,

increasing the accuracy and robustness of fraud detection systems.

- ✓ **Cross-Border and Multi-Institution Collaboration**: Developing standardized, collaborative fraud detection frameworks across financial institutions and geographic boundaries can help identify fraud rings and shared attack patterns.

REFERENCES

[1] Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[2] Ranshous, S., Bay, C., Cramer, N., Henricksen, M., & Hannigan, B. (2015). Combining Clustering and Classification for Anomalous Activity Detection in Cybersecurity. In Proceedings of the 2015 Workshop on Artificial Intelligence and Security (pp. 49-58).

[3] Bhattacharyya, D., Kalaimannan, E., & Verma, A. (2018). Anomalous Pattern Detection in Enterprise Data Using Hybrid Classification and Clustering Techniques. Procedia Computer Science, 132, 1066-1075.

[4] Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A Comprehensive Survey of Data Miningbased Fraud Detection Research. Artificial Intelligence Review, 33(4), 229-246.

[5] Friedman, J., Hastie, T., & Tibshirani, R. (2001). The Elements of Statistical Learning: Data Mining, Inference, and Prediction. New York, NY: Springer-Verlag.

[6] Brownlee, J. (2020). Master Machine Learning Algorithms. Machine Learning Mastery.

[7] Chollet, F.(2018). Deep Learning with Python. Manning Publications.