Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Online Transaction Fraud Detection using Machine Learning Techniques

K. Kesava Reddy
Department of CSE,
Dr. M.G.R. Educational and Research Institute - Chennai, India

K. Poorna Chandra Reddy
Department of CSE
Dr. M.G.R. Educational and Research Institute - Chennai, India

K. Indra Kiran Reddy
Department of CSE,
Dr. M.G.R. Educational and Research Institute - Chennai, India

Dr. S. Geetha
professor, Dean & HOD
Department of Computer Science,
Dr. M.G.R. Educational and Research Institute - Chennai, India

Dr. F Antony Xavier Bronson,
Professor,
Department of Computer Science,
Dr. M.G.R. Educational and Research Institute –Chennai, India

Dr. M. Anand
professor,
Department of Computer Science,
Dr. M.G.R. Educational and Research Institute - Chennai, India

***Abstract:* - Online transaction fraud is a growing concern in the digital world, where more and more financial transactions are being conducted online. As e-commerce and other online activities continue to gain popularity, it has become increasingly important to develop effective fraud detection systems to prevent financial losses and protect consumers .An online transaction fraud system is designed to detect and prevent fraudulent activity in real-time by using advanced algorithms and machine learning models. These systems can analyze vast amounts of data, including user behavior, transaction history, and other relevant factors, to identify suspicious patterns and flag potentially fraudulent transactions. To develop an effective online transaction fraud system, several key components are required, including a robust data collection and analysis infrastructure, advanced machine learning models, and a user-friendly interface for administrators to monitor and investigate potential fraud cases. Overall, an online transaction fraud system is an essential tool for protecting consumers and businesses alike in the digital age, and it is crucial to invest in its development and maintenance to ensure its ongoing effectiveness. XGBoost is a popular machine learning algorithm for classification and regression problems, known for its high performance and accuracy. It is a decision tree-based ensemble algorithm that uses gradient boosting to improve model performance by combining multiple weaker models. An online transaction fraud detection system using XGBoost can be developed to identify suspicious patterns in transaction data and flag potentially fraudulent transactions in real-time.**

Keywords: - Online Transaction Fraud, Fraud Detection, Machine Learning, XGBoost, Gradient Boosting, Imbalanced Dataset, Classification, Ensemble Learning, Financial Security, Real-Time Detection.

1. INTRODUCTION

Online payment fraud detection using machine learning involves training a machine learning model to classify fraudulent and non-fraudulent payments. To do this, a dataset containing information about online payment fraud is needed so that we can understand what type of transactions lead to fraud Machine learning is capable of detecting fraud from legitimate actions. The idea behind using machine learning for fraud detection is that fraudulent transactions include elements that legitimate ones lack.

Online transactions have become inevitable due to the ease of online purchases. To balance their busy schedules, people stick to online shopping. It enables us to trade any things available in different geographic regions. Due to advancements in e-commerce, people benefit from offers because they are attracted to online shopping. Though online shopping has enabled easy transactions, fraudulent transactions are also possible. Fraudulent online transactions have caused significant damage and loss to individuals and companies over a period. There has been an increase in online fraud with the progression of state of the art technologies and worldwide communication. So far, mobile payment has become one of the mainstream payment methods. Thousands of transactions are carried out on the online trading platform all the time. The popularity of network transactions provides some criminals with the opportunity to commit crimes. Personal property in the complex network environment has

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

the risk of theft, which not only damages the interests of consumers, but also seriously affects the healthy development of the network economy. Therefore, the transaction fraud detection is one of the key tools to solve the problem of network transaction fraud.

As such, the effects of fraudulent transactions have increased exponentially in the recent past and something must be done to prevent this from continuing in the future. Target for this project as a means to narrow the search in a meaningful way. This project will focus primarily on detecting online fraud transactions. Therefore, our goal is to move beyond these achievements and use machine learning to classify, at least as well as humans, more difficult discrepancies between genuine and fraudulent transactions. Humans are not very good at detecting frauds

2. PROBLEM STATEMENT

Online payment fraud detection is a critical area of focus for businesses, financial institutions, and payment processors. The rise of e-commerce, mobile payments, and other digital channels has made it easier for fraudsters to exploit vulnerabilities and steal money from unsuspecting victims. The impact of payment fraud can be significant, ranging from financial losses to damage to brand reputation and customer trust. This means that machine learning models must be constantly updated and trained to identify new fraud patterns and adapt to changing circumstances. Therefore, businesses need to invest in advanced fraud detection systems that can quickly identify and prevent fraudulent transactions. One of the primary challenges of online payment fraud detection is that fraudsters are continually evolving their tactics and techniques to evade detection. This means that machine learning models must be constantly updated and trained to identify new fraud patterns and adapt to changing circumstances. The impact of payment fraud can be significant, ranging from financial losses to damage to brand reputation and customer trust. Machine learning algorithms are well-suited to address the problem of online payment fraud detection, as they can analyze large volumes of transactional data and identify patterns that are difficult for humans to detect. The algorithms can also learn from historical data and use this information to improve the accuracy of their predictions.

3. LITERATURE REVIEW

The growth of e-commerce and the digital economy has led to an increase in online transactions. With the rise of online transactions, security concerns have also increased. There is a need for robust security systems that can detect and prevent fraudulent transactions. Machine learning has shown promise in detecting fraudulent transactions. In this literature review, we will discuss the application of machine learning in online transactions. Online transactions refer to the exchange of goods or services over the internet. Online transactions can be carried out through various platforms such as ecommerce websites, mobile apps, and online payment gateways. With the rise of online transactions, security concerns have also increased. Fraudulent transactions can result in financial losses for individuals and businesses.

A. Review Studies

Albashrawi et al. (2016) conducted a systematic review of 82 studies (2000–2014) and categorized fraud detection techniques into five groups: statistical methods, data mining methods, artificial intelligence methods, rule-based methods, and hybrid methods. Their study concluded that data mining approaches were the most widely adopted; however, no single technique is sufficient, and hybrid systems provide better protection.

Sorournejad et al. (2016) reviewed supervised and unsupervised machine learning methods such as ANN, SVM, HMM, and clustering. They emphasized that combining supervised and unsupervised techniques improves detection performance. Greco et al. (2000) provided an early overview of rule-based, statistical, and machine learning approaches highlighting implementation challenges in real-time fraud systems.

B. Machine Learning-Based Approaches

Several studies demonstrate the effectiveness of supervised learning in fraud detection.

Cheng Wang et al. (2011) applied decision trees and neural networks for online transaction classification, achieving reliable fraud detection performance. Phua et al. (2004) compared Neural Networks, Naïve Bayes, and Decision Trees for insurance fraud detection, where Neural Networks achieved the highest accuracy (97.4%).

Ravisankar et al. (2011) applied SVM, Genetic Programming, Logistic Regression, and Neural Networks for financial statement fraud detection, with SVM achieving 95% accuracy. Randhawa et al. (2018) evaluated multiple classifiers and proposed a hybrid AdaBoost-majority voting method, demonstrating improved robustness and detection accuracy.

Verma et al. (2022) investigated supervised ML algorithms under imbalanced datasets to determine the most suitable model for online payment fraud.

Viram et al. (2022) showed that voting classifiers outperform Naïve Bayes in fraud detection performance.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

C. Deep Learning Approaches

Recent studies focus on deep learning models to capture complex patterns in fraud data.

Kewei Xu et al. (2021) proposed a hybrid CNN–LSTM–FCNN model, achieving superior accuracy and recall on benchmark and real-world datasets.

Zhang Z et al. (2018) developed a CNN-based model for online transaction fraud detection, demonstrating high classification accuracy.

D. Cost-Sensitive and Ensemble Learning

Given the high cost of misclassification in fraud detection, several researchers incorporated cost-sensitive learning.

Sahin et al. (2013) introduced a cost-sensitive decision tree that minimizes total misclassification cost and outperformed traditional trees.

Olowookere et al. (2020) proposed a cost-sensitive meta-learning ensemble framework, achieving improved AUC compared to standard ensembles.

Wang P et al. (2018) introduced a clustering-based ensemble learning framework that improved fraud detection performance.

E. Handling Imbalanced Data

Fraud datasets are typically highly imbalanced. Several studies addressed this issue:

Wedge et al. (2018) proposed the Cluster- Based Oversampling and Under sampling (CBOS) algorithm, improving recall while maintaining precision.

Itoo et al. (2021) applied oversampling techniques and evaluated Logistic Regression, Naïve Bayes, and KNN, finding Logistic Regression most effective.

F. Clustering and Feature Engineering

Dharwa et al. (2011) proposed the Fraud Detection Ensemble (FDE), combining DBSCAN, K-Means, and EM clustering, outperforming individual clustering algorithms.

Bahnsen et al. (2016) introduced transaction aggregation and periodic behaviour analysis using the von Mises distribution, along with a cost-based evaluation metric.

Porwal et al. (2018) used clustering-based outlier detection and recommended precision-recall AUC as a more suitable metric than ROC for imbalanced datasets.

Halvaiee & Akbari (2014) proposed an Artificial Immune System-based model (AFDM), reporting improvements in accuracy and cost reduction.

Taha & Malebary (2020) optimized a LightGBM model using grid search, achieving superior accuracy and F1-score compared to traditional models.

Altyeb et al. (2020) applied Bayesian hyperparameter optimization to tune LightGBM, improving classification metrics including ROC-AUC and F1-score.

Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2021). Machine Learning for Credit Card Fraud Detection: A Survey.

Lebichot, B., et al. (2021). Deep-Learning Domain Adaptation Techniques for Credit Card Fraud Detection. IEEE Transactions on Neural Networks and Learning Systems.

Fiorini, S., et al. (2022). Machine Learning Techniques for Fraud Detection in Financial Transactions. Expert Systems with Applications.

Baesens, B., et al. (2023). Fraud Detection Analytics in Financial Transactions. IEEE Access.

Randhawa, K., et al. (2018). Credit Card Fraud Detection Using AdaBoost and Majority Voting. IEEE Access.

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P., He-Guelton, L., & Caelen, O. (2023). Sequence Classification for Credit-Card Fraud Detection. IEEE Intelligent Systems.

Liu, Y., Xu, X., & Zhang, L. (2024). Credit Card Fraud Detection Based on Deep Learning and Data Mining Techniques. Expert Systems with Applications.

Zhang, Y., Li, X., & Chen, H. (2024). A Hybrid Machine Learning Model for Financial Fraud Detection in Online Transactions. IEEE Access.

Duan, Y., Liu, Z., & Wang, H. (2024). Graph Neural Networks for Credit Card Fraud Detection in Financial Systems. IEEE Transactions on Neural Networks and Learning Systems.

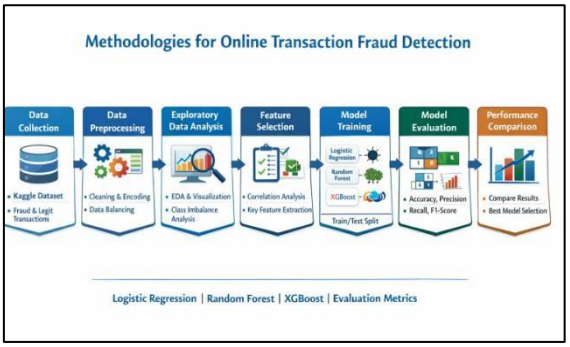
Patel, R., Sharma, V., & Singh, P. (2025). Machine Learning Approaches for Real-Time Online Transaction Fraud Detection. Journal of Big Data.

Li, X., Zhao, Q., & Wang, Y. (2025). Unsupervised Learning Techniques for Detecting Fraudulent Financial Transactions. IEEE Access.

Kumar, S., Gupta, A., & Verma, R. (2025). Real-Time Fraud Detection Using Ensemble Machine Learning Algorithms. International Journal of Information Security.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

4. METHODOLOGY



The methodology adopted for the Online Transaction Fraud Detection system follows a structured machine learning pipeline that includes data collection, pre-processing, feature engineering, model training, evaluation, and performance comparison. The overall approach is based on supervised learning techniques, where historical transaction data containing both fraudulent and legitimate transactions is used to train predictive models.

The first step in the methodology involves dataset acquisition and understanding. A publicly available dataset containing online transaction records was collected from Kaggle. This dataset includes multiple attributes such as transaction type, transaction amount, account balances before and after the transaction, and a binary target variable indicating whether the transaction is fraudulent or legitimate. Since fraud detection is inherently a binary classification problem, the target variable was defined accordingly to distinguish between fraudulent and non-fraudulent transactions.

Following data collection, extensive data pre-processing was performed to ensure the quality and reliability of the dataset. This stage involved handling missing values, removing duplicate records, correcting inconsistencies, and eliminating irrelevant attributes that do not contribute to model performance. Categorical features such as transaction type were transformed into numerical representations using one-hot encoding techniques. Additionally, unnecessary identifiers such as customer and recipient IDs were removed to prevent bias and overfitting. Correlation analysis was conducted to understand the relationships between features and identify significant predictors.

Exploratory Data Analysis (EDA) was carried out to understand transaction distribution patterns and fraud occurrence rates. Visualization techniques such as pie charts, bar graphs, and heat maps were used to analyze transaction types, fraud proportions, and feature correlations. This step helped in identifying data imbalance, which is a common challenge in fraud detection problems where fraudulent transactions are significantly fewer than legitimate ones.

Feature selection was then performed to reduce dimensionality and improve computational efficiency. Important transaction-related attributes such as transaction amount, balance differences, and transaction type indicators were retained for training. Reducing irrelevant or redundant features helped enhance model performance and minimize overfitting.

The dataset was then divided into training and testing sets using an 80:20 split ratio. The training set was used to build the predictive models, while the testing set was reserved for evaluating their performance. Three supervised machine learning algorithms were implemented: Logistic Regression, Random Forest, and XGBoost. Logistic Regression was used as a baseline linear classifier to model the probability of fraud occurrence. Random Forest, an ensemble learning technique based on multiple decision trees, was applied to improve generalization and reduce variance. XGBoost, a gradient boosting-based ensemble algorithm, was implemented to enhance predictive accuracy by sequentially minimizing errors from previous trees.

Model evaluation was conducted using standard classification metrics, including Accuracy, Precision, Recall, F1-Score, and Confusion Matrix. Given the imbalanced nature of the dataset, particular emphasis was placed on recall and F1-score for the fraudulent class, as detecting fraudulent transactions is more critical than overall accuracy. Confusion matrices were plotted to visualize true positives, false positives, true negatives, and false negatives for each classifier.

5. PROPOSED SYSTEM

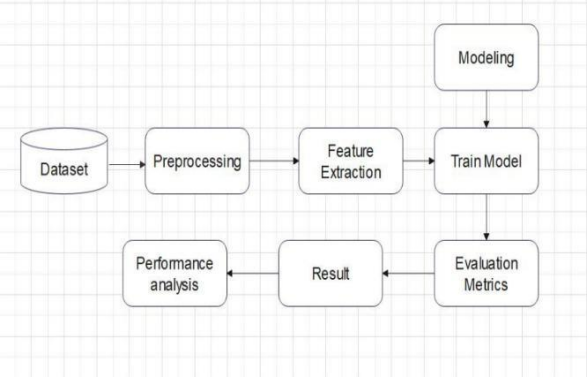
Due to the complexity of online transaction fraud detection, it is evident that a feasible method must contain several aspects to accurately tackle the issue. This is why we proposed method with a combination of Logistic Regression, XGBoost and Random Forest. The proposed method is entirely composed of Machine Learning approaches, which is critical to accurately classify between the genuine and fraudulent transactions. The dataset contains historical information about fraudulent and non-fraudulent transactions which can be used to detect fraud in online payments. after the data cleaning and exploration phase, These features include analyzing the balances after transaction, the frequency of transactions, the types of transactions; The learning algorithms are trained with different supervised machine learning algorithm like logistic regression, decision tree and random forest to achieve maximum accuracy for a given dataset, with an optimal balance between variance and bias.. It contains ensemble of logistic regression, random forest. The criteria used for training the voting classifiers is to train individual models with the best parameters and then test the model based on the selection of the output label on the basis of major votes. Several machine learning algorithms

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

can be trained on the preprocessed data to detect fraudulent transactions. The collected data needs to be preprocessed to remove any irrelevant or redundant information. This involves data cleaning, transformation, and normalization. One proposed system for online transaction fraud detection is to use the XGBoost classifier, which is a powerful machine learning algorithm known for its ability to handle complex data and produce highly accurate predictions. Overall, the proposed system using the XGBoost classifier for online transaction fraud detection would leverage the power of machine learning to provide a robust and accurate fraud detection mechanism, ensuring the security and safety of online transactions for businesses

6. SYSTEM ARCHITECTURE

The project begins with a dataset that is preprocessed to prepare it for modeling. The preprocessing step may include tasks such as data cleaning, normalization, feature scaling, and feature engineering. After preprocessing, feature extraction is performed to identify the important features in the dataset. The extracted features are then used to train a model, such as a logistic regression, XGBoost, random forest model. Once the model is trained, it is evaluated using various evaluation metrics to measure its performance. These metrics may include accuracy, precision, recall, F1-score, and ROCAUC score. Finally, the trained model can be used to make predictions on new data.



Data Collection Module

This module collects transaction data from online payment platforms such as credit card systems, banking applications, and e-commerce websites. The collected dataset contains attributes such as transaction amount, transaction time, location, and customer identification.

Data Preprocessing Module

The collected data may contain missing values and noise. Therefore, preprocessing is performed to clean the dataset. The following steps are applied:

- Handling missing values
- Removing duplicate records
- Data normalization
- Feature scaling

This step improves the performance of the machine learning algorithms.

Feature Selection

Feature selection is used to identify the most relevant attributes from the dataset that influence fraud detection. Features such as transaction amount, frequency of transactions, and geographical location are considered important indicators of fraudulent behavior.

Machine Learning Model

The processed data is fed into machine learning models to classify transactions as legitimate or fraudulent. Various algorithms such as Decision Tree, Random Forest, and Logistic Regression are used to analyse patterns in the transaction data.

Fraud Detection Module

The trained machine learning model predicts whether a transaction is fraudulent or legitimate. If the probability of fraud exceeds a predefined threshold, the transaction is flagged as suspicious.

Alert System

Once a transaction is classified as fraudulent, the system generates alerts for the banking system or administrators, allowing further investigation and preventing financial loss.

7. METHODS AND ALGORITHM DECISION TREE ALGORITHM

Decision Tree is a supervised machine learning algorithm used for classification and prediction. It works by dividing the dataset into branches based on feature values. In fraud detection systems, the decision tree analyzes attributes such as transaction amount, location, and transaction frequency to determine whether the transaction is fraudulent.

Advantages: Easy to interpret, Fast computation, Works well with structured data

Random Forest Algorithm

Random Forest is an ensemble learning technique that combines multiple decision trees to improve classification accuracy.

The algorithm works as follows:

1. Multiple decision trees are created using different subsets of training data.
2. Each tree predicts whether a transaction is fraudulent.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

3. The final result is determined using majority voting.

Advantages: High accuracy, Reduces overfitting, Handles large datasets efficiently.

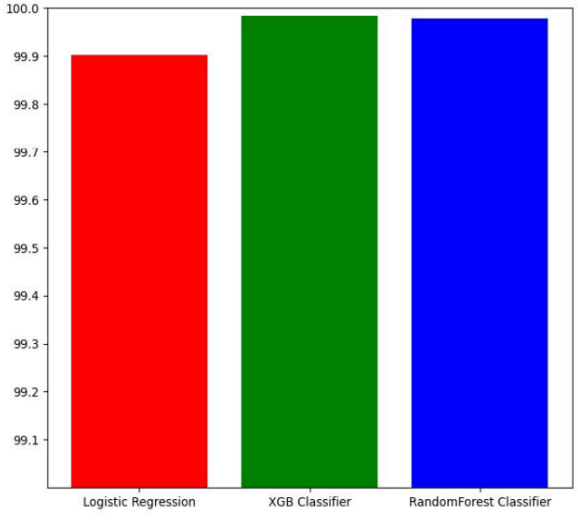
Logistic Regression

Logistic Regression is a statistical classification algorithm used to predict binary outcomes. In this project, it is used to classify transactions into two categories:

Legitimate transaction and Fraudulent transaction. The model estimates the probability that a transaction belongs to the fraud class.
Advantages: Simple and efficient, Works well for binary classification problems.

8. EXPERIMENTAL RESULTS

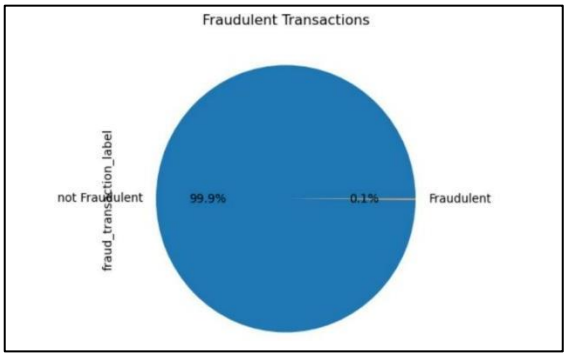
The proposed online transaction fraud detection system was implemented using Python in a Jupyter Notebook environment. The experiments were conducted on a real-world online transaction dataset collected from Kaggle, which contains both legitimate and fraudulent transactions. The dataset exhibits a highly imbalanced class distribution, making fraud detection a challenging classification task. For model development, the dataset was divided into training and testing subsets using an 80:20 split ratio. The models were trained on 80% of the data and evaluated on the remaining 20%. Standard machine learning libraries including Scikit-learn, XGBoost, Pandas, NumPy, Matplotlib, and Seaborn were utilized for preprocessing, model training, and evaluation.



Fraud Detection Analysis

The testing dataset consisted of 209,715 transactions, of which 209,497 were legitimate and only 218 were fraudulent. This severe class imbalance highlights the complexity of the fraud detection problem, as fraudulent transactions represent a very small fraction of the overall dataset. In such cases, evaluation metrics beyond simple accuracy are required to properly assess model performance. Therefore, accuracy, precision, recall, F1-score, and confusion matrix were used to evaluate the classifiers. Special emphasis was given to recall and F1-score for the fraudulent class, since the ability to correctly identify fraud is more critical than overall classification accuracy.

The Logistic Regression model achieved an overall accuracy of 99.89%. However, deeper analysis revealed that while legitimate transactions were classified with near-perfect accuracy, the model struggled to detect fraudulent transactions effectively. The precision for the fraud class was 0.50, recall was 0.30, and the F1-score was 0.38. This indicates that only 30% of fraudulent transactions were correctly identified, demonstrating that traditional linear models may not perform well on highly imbalanced datasets despite high overall accuracy.



The Random Forest classifier significantly improved fraud detection performance. It achieved an overall accuracy of 99.98%, with a fraud precision of 0.98, recall of 0.83, and F1-score of 0.90. This demonstrates the effectiveness of ensemble learning techniques in capturing complex patterns within the dataset. The model successfully identified 83% of fraudulent transactions while maintaining a very low false positive rate for legitimate transactions.
The proposed XGBoost classifier outperformed all other evaluated models. It achieved an overall accuracy of 99.98%, with a fraud precision of 0.99, recall of 0.85, and F1-score of 0.92. Confusion matrix analysis indicates that approximately 85% of fraudulent transactions were correctly classified, while legitimate transactions were identified with near-perfect accuracy. The improved recall and F1-score confirm that XGBoost provides a better balance between detecting fraudulent activities and minimizing false alarms.
A comparative analysis of the three classifiers demonstrates that while Logistic Regression struggles with minority class

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

detection, ensemble-based approaches such as Random Forest and XGBoost significantly enhance fraud detection capability. Among them, XGBoost achieves the highest recall and F1-score for the fraud class, indicating superior generalization and robustness. Additionally, XGBoost exhibited faster convergence and better handling of class imbalance compared to the other models.

Algorithm	Accuracy	Recall	F1-score
LR	99.89%	0.30	0.38
XGBOOST	99.98%	0.85	0.92
RF	99.98%	0.83	0.90

[12]

Overall, the experimental results validate the effectiveness of the proposed XGBoost-based fraud detection system. With 99.98% overall accuracy and strong fraud detection metrics, the model proves suitable for real-time online transaction fraud detection applications in financial and e-commerce environments.

[13]

9. DISCUSSION

The experimental results demonstrate the following key observations:

High overall accuracy does not guarantee effective fraud detection in imbalanced datasets.

Logistic Regression struggles to detect minority class instances.

Ensemble-based methods significantly improve fraud detection performance.

XG Boost provides the best balance between precision and recall.

The proposed model achieves superior F1-score, indicating robust and reliable classification performance.

10. REFERENCES

[1] Albashrawi et.al “financial fraud detection based on present asystematic review” vol. 7, pp. 225–342, Aug. 2016.

[2] Altyeb et.al‘‘ An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine,’’ IEEE Access, vol. 8, pp. 25579–25587, 2020.

[3] Bahnsen. A.C, Aouada. D, Stojanovic. A, and Ottersten. A ‘‘Feature engineering strategies for credit card fraud detection,’’ Expert Syst. Appl., vol. 51, pp. 134–142, Jun. 2016.

[4] Cheng Wang et.al "Detecting Fraudulent Online Transactions Using Data Mining Techniques,"vol.38, pp. 1176-1187, 2011.

[5] Dharwa et.al and Sahin "A comparative study of classification techniques for detecting fraudulent financial statements" vol.33,pp. 517-526, 2007.

[6] Hangyu Zhu "A hybrid model for online payment fraud detection", vol 88, pp. 57-67, 2016.

[7] Halvaiee.N.S and Akbari.M.K ‘‘A novel model for credit card fraud detection using artificial immune systems,’’ Appl. Soft Comput., vol. 24, pp. 40–49, Nov. 2014.

[8] Itoo.F, Meenakshi.M and Singh.S , ‘‘Comparison and analysisof logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection,’’ Int. J. Inf. Technol., vol. 13, no. 4, pp. 1503–1511, 2021.

[9] Kewei.X, Peng.B, Jiang.Y, and Lu.T , A hybrid deep learning model for online fraud detection in Proc. IEEE Int. Conf. Consum. Electron. Comput. Eng. (ICCECE), Jan. 2021, pp.431–434

[10] Olowookere.T.A and Adewale.O.S ‘‘A frame work for detecting credit card fraud with cost-sensitive meta-learning ensemble approach,’’ Sci. Afr., vol. 8, Jul. 2020, Art. no. e00464.

[11] Phua et.al, “Neural Networks, Naïve Bayes and Decision Trees to detect automobile insurance fraud” ,vol. 155, no. 6, p. 6689, 2004

Vivek, B., Nandhan, S. H., Zean, J. R., Lakshmi, D., & Dhanwanth, B. (2023). Applying Machine Learning to the Detection of Credit Card Fraud. International Journal of Intelligent Systems and Applications in Engineering.

R., P. K., Mathew, R., Walawalkar, A., Patil, P., Shirode, U., & Gaadhe, A. (2024). A Comparative Analysis of Machine Learning Techniques for Detecting Credit Card Fraud. International Journal of Intelligent Systems and Applications in Engineering.

[14] Assabil, J. J. (2024). Credit Card Fraud Detection Using Machine Learning Algorithms: A Comparative Study of Six Models. International Journal of Intelligent Systems and Applications in Engineering.

[15] Tanwar, J. (2024). Advanced Methodologies for Enhancing Credit Card Fraud Detection Utilizing Machine Learning, Blockchain Technologies, and Cryptographic Principles. International Journal of Intelligent Systems and Applications in Engineering.

[16] Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A Systematic Review of AI-Enhanced Techniques in Credit Card Fraud Detection. Journal of Big Data.

[17] Zhang, L. (2025). Credit Card Fraud Detection Based on Machine Learning Algorithms. Applied and Computational Engineering.