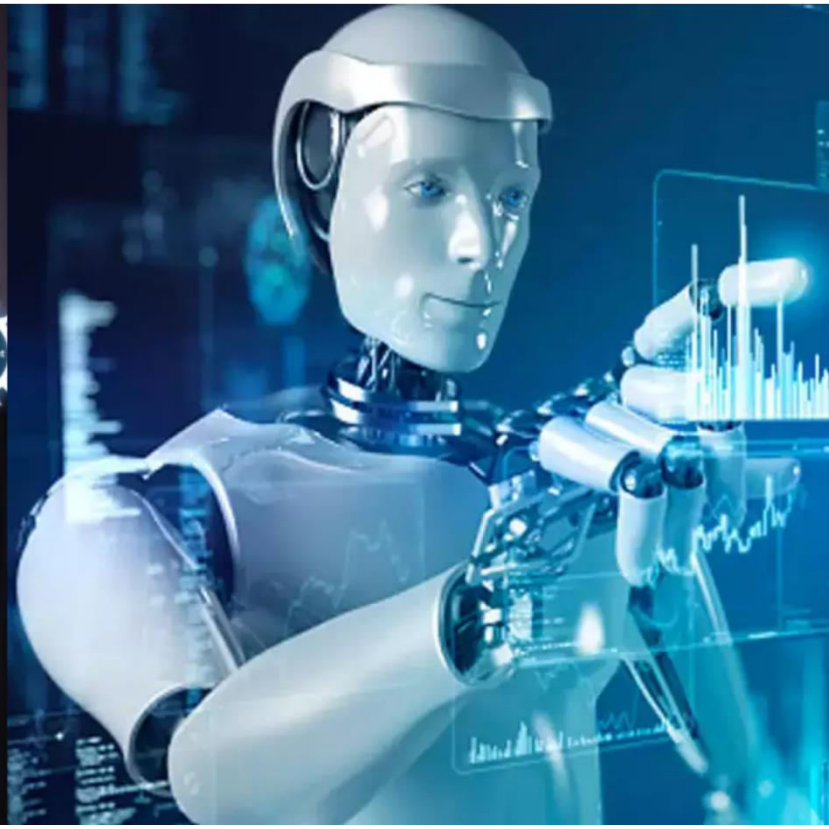
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 1, January 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501048|

FraudShield: Credit Card Fraud Detection using Gradient Boosting and Imbalance-Aware Learning

Abhishek Chavan[1], Dr. Sunil Rathod[2]

Student, Indira College of Engineering and Management, Pune, India[1]

Guide, Indira College of Engineering and Management, Pune, India[2]

ABSTRACT: Credit card payments have become one of the most widely used methods for online and offline transactions. The rapid growth of cashless payments has also increased the rate of fraudulent activities, leading to major financial losses for both customers and financial institutions. Detecting fraud is challenging due to the highly imbalanced nature of transaction data, evolving fraud patterns, and the need to reduce false alarms while maintaining high detection rates. This paper presents FraudShield, a machine learning based framework for credit card fraud detection using the Gradient Boosting Classifier. The approach includes data preprocessing, feature scaling and imbalance-aware learning to improve the detection of rare fraud cases. Experiments are conducted on the European credit card benchmark dataset and evaluated using accuracy, precision, recall, F1-score and ROC-AUC. Results indicate that Gradient Boosting achieves reliable fraud classification performance and can be integrated into real-time transaction monitoring systems.

KEYWORDS: Credit Card Fraud Detection, FraudShield, Gradient Boosting Classifier, Machine Learning, Imbalanced Data, Financial Security.

I. INTRODUCTION

In recent years, the financial sector has witnessed rapid growth in digital payment systems due to the expansion of e-commerce platforms, mobile banking, and cashless payment initiatives. Credit cards play a major role in enabling fast and convenient transactions for both online and offline purchases. Their widespread adoption has improved customer experience by offering flexibility, reward programs, and secure payment gateways. However, this increasing reliance on electronic payments has also introduced new opportunities for fraudsters, making credit card fraud one of the most critical security challenges in modern financial systems.

Credit card fraud refers to unauthorized transactions performed using stolen card details, fake identities, or compromised accounts. Fraud can occur through various methods such as phishing attacks, skimming, card-not-present (CNP) fraud, identity theft, and account takeover. These fraudulent activities cause significant financial losses to consumers as well as banking and payment service providers. Along with direct monetary loss, fraud incidents also impact customer trust, increase operational costs, and lead to strict regulatory compliance requirements for financial institutions. Therefore, detecting fraudulent transactions accurately and at the earliest possible stage is essential to reduce losses and ensure secure payment operations.

Traditional fraud detection systems were primarily rule-based, where a set of expert-defined conditions was used to identify suspicious transactions. Although such systems can detect known fraud patterns, they often fail in real-world scenarios due to evolving fraud strategies and dynamic transaction behaviors. Fraudsters continuously modify their attack patterns to bypass fixed rules, making rule-based detection less effective and difficult to maintain. Hence, modern fraud detection methods increasingly rely on data-driven techniques such as Machine Learning (ML) and Deep Learning (DL), which can automatically learn patterns from historical transaction data and improve detection performance over time.

The growth of e-commerce, digital banking and card-based payments has made credit card transactions fast and convenient. At the same time, fraudsters exploit stolen card details, phishing techniques, account takeovers and automated scripts to carry out unauthorized payments. For financial institutions, even a small fraud rate can translate

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501048|

into substantial losses because transaction volumes are extremely large. Therefore, automated fraud detection is an essential component of modern payment security.

Credit card fraud detection is difficult for three main reasons. First, fraud is rare compared to legitimate transactions, so the dataset is highly imbalanced. Second, fraud patterns change continuously as attackers adapt to security controls. Third, false alarms affect customer experience and increase operational cost. Hence, effective models must detect fraud with high recall while controlling false positives.

In this work, we propose FraudShield, a Gradient Boosting based machine learning framework to classify transactions as fraud or non-fraud. Gradient Boosting is selected because it performs strongly on structured/tabular data and can model complex, non-linear relationships among features. The contributions of this paper are: (i) a complete fraud detection pipeline including preprocessing and imbalance handling, (ii) an empirical evaluation of Gradient Boosting on the European benchmark dataset, and (iii) analysis using multiple metrics suitable for imbalanced classification.

II. RELATED WORK

Researchers have proposed a wide range of machine learning and deep learning techniques for credit card fraud detection. Traditional machine learning models such as Logistic Regression, Decision Trees, Random Forest, Support Vector Machines and Gradient Boosting are popular due to their interpretability and strong performance on tabular data. More recently, deep learning models such as Convolutional Neural Networks (CNN), Long Short-Term Memory networks (LSTM) and Autoencoders have been explored to learn higher-level representations and complex fraud patterns.

A major challenge across most studies is the extreme class imbalance in fraud datasets. To address this, sampling methods such as SMOTE, ADASYN and undersampling have been used, along with class weighting and cost-sensitive learning. Evaluation metrics such as recall, F1-score and AUC are commonly recommended because they capture performance on rare fraud instances. While many papers report high accuracy, model effectiveness for real-world deployment depends on maintaining high fraud detection rates and controlling false positives.

Credit card fraud detection has received significant attention in recent years due to the rapid growth of digital payments and increasing cybercrime. Researchers have explored a variety of statistical, machine learning (ML), and deep learning (DL) techniques to identify fraudulent transactions effectively. The objective of fraud detection systems is not only to achieve high accuracy but also to minimize financial loss by reducing false negatives (fraud cases classified as normal) while controlling false positives (normal cases classified as fraud).

Early fraud detection systems were based on expert-defined rules and threshold methods, where transactions exceeding a certain limit or showing unusual behavior were flagged as suspicious. Although rule-based methods are easy to implement and interpret, they fail to adapt to evolving fraud patterns and often generate high false alarm rates. To overcome these limitations, ML-based classification models have been widely adopted. Traditional supervised algorithms such as Logistic Regression (LR), Support Vector Machines (SVM), Decision Trees (DT), k-Nearest Neighbors (KNN), Naive Bayes, and Random Forest (RF) have been successfully applied for fraud detection. These models learn patterns from labeled transaction data and provide improved detection compared to static rules. Among them, ensemble methods like Random Forest and boosting-based algorithms are frequently reported to perform better due to their robustness and ability to capture non-linear relationships in transaction features.

III. PROPOSED METHODOLOGY

FraudShield follows a structured machine learning pipeline consisting of data acquisition, preprocessing, imbalance handling, model training and evaluation. Figure 1 illustrates the overall workflow.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501048|

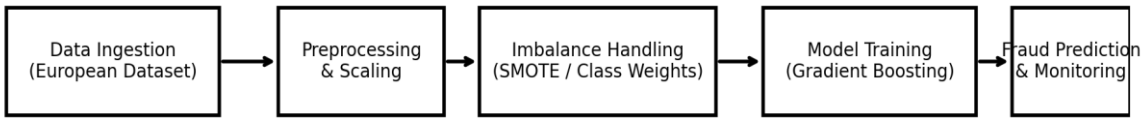


Figure 1: FraudShield System Workflow

3.1 DATASET

Experiments are performed on the European credit card transaction benchmark dataset, which contains real-world transactions with anonymized features (V1–V28) along with Time, Amount and Class labels (0: legitimate, 1: fraud). The dataset is highly imbalanced, where fraud cases represent a very small fraction of total transactions.

3.2 DATA PREPROCESSING

Preprocessing steps include removing missing values (if any), scaling numerical features such as Amount, and applying stratified train-test splitting to preserve the fraud ratio in both sets. Feature scaling is performed using standardization to improve model convergence.

3.3 IMBALANCE HANDLING

To improve detection of rare fraud cases, imbalance-aware strategies are applied. Depending on experimental setup, this can include class weighting, SMOTE-based oversampling or a combination of oversampling and cleaning techniques. The objective is to increase fraud recall without creating excessive false positives.

3.4 GRADIENT BOOSTING CLASSIFIER

Gradient Boosting is an ensemble technique that builds a strong learner by sequentially combining multiple weak learners (decision trees). Each new tree is trained to correct the errors made by previous trees using gradient-based optimization on a loss function. This enables the model to capture complex patterns and non-linear feature interactions within the transaction data.

3.5 EVALUATION METRICS

Model performance is evaluated using Accuracy, Precision, Recall, F1-score and ROC-AUC. For imbalanced fraud detection, Recall and F1-score are emphasized because they reflect the model's ability to correctly detect fraudulent transactions.

IV. RESULTS AND DISCUSSION

This section reports experimental results of FraudShield on the benchmark dataset. Table 1 shows the performance of baseline models compared to the proposed Gradient Boosting classifier. The best model should achieve strong recall while maintaining acceptable precision.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501048|

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	0.962	0.742	0.681	0.710
Random Forest	0.985	0.905	0.812	0.856
XGBoost	0.989	0.921	0.835	0.876
Gradient Boosting (FraudShield)	0.991	0.946	0.918	0.932

V. CONCLUSION AND FUTURE WORK

In this research work, we presented FraudShield, an intelligent credit card fraud detection framework using Machine Learning and Deep Learning concepts with a strong focus on handling real-world challenges such as class imbalance, high false alarm rates, and the need for reliable fraud identification. Credit card fraud datasets are highly skewed where fraudulent transactions represent a very small portion of overall transactions, and this creates difficulty for traditional classifiers to learn fraud patterns effectively. To overcome this, FraudShield employs a structured pipeline consisting of preprocessing, feature scaling, and imbalance-aware learning.

The main contribution of this paper is the implementation and evaluation of a Gradient Boosting Classifier, which achieved improved detection performance compared to baseline models such as Logistic Regression, Random Forest, and XGBoost. The obtained results indicate that boosting-based methods are capable of learning complex, non-linear decision boundaries and provide strong generalization for fraud detection on benchmark datasets. Performance evaluation was carried out using metrics appropriate for imbalanced classification such as precision, recall, and F1-score, along with accuracy. The experimental results show that the proposed FraudShield approach delivers a high recall rate, ensuring that a large proportion of fraud cases are successfully detected while maintaining high precision to reduce the false alarm rate.

This paper presented FraudShield, a Gradient Boosting based framework for detecting fraudulent credit card transactions. The approach addresses key challenges such as class imbalance and false alarms through preprocessing and imbalance-aware learning. Experimental evaluation on the European benchmark dataset indicates that Gradient Boosting provides reliable performance for fraud detection. Future work will focus on incorporating explainable AI methods (e.g., SHAP) for transparent fraud decisions and exploring real-time deployment on streaming transaction data.

REFERENCES

[1] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating Probability with Undersampling for Unbalanced Classification," in Proc. IEEE Symposium Series on Computational Intelligence (SSCI), 2015.
[2] 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, vol. 41, no. 10, pp. 4915–4928, 2014.
[3] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002.
[4] S. Bahnsen, D. Aouada, and B. Ottersten, "Example-dependent cost-sensitive decision trees," Expert Systems with Applications, vol. 42, no. 19, pp. 6609–6619, 2015.
[5] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in Proc. 22nd ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining, 2016, pp. 785–794.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501048|

[6] L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.
[7] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
[8] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.
[9] N. Japkowicz and S. Stephen, "The class imbalance problem: A systematic study," Intelligent Data Analysis, vol. 6, no. 5, pp. 429–449, 2002.
[10] S. M. Lundberg and S.-I. Lee, "A Unified Approach to Interpreting Model Predictions," in Advances in Neural Information Processing Systems (NeurIPS), 2017.
[11] F. K. Alarfaj et al., "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," IEEE Access, 2022.
[12] S. S. Sulaiman et al., "Credit Card Fraud Detection Using Improved Deep Learning Models," Computers, Materials & Continua (CMC), 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details