Volume: 14 Issue: I Month of publication: January 2026

DOI: https://doi.org/10.22214/ijraset.2026.76831

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue I Jan 2026- Available at www.ijraset.com*

# Credit Card Fraud Detection with Advanced Hybrid Deep Learning Algorithm

Sumedha Arya[1], Nirmal Gaud[2]

***Abstract: Progress in the rise of online payments systems has made shopping easier. However, it also increased credit card fraud, with losses expected to exceed $362 billion by 2027. Traditional machine learning algorithms often fail to detect fraud due to complex patterns and unbalanced data. This study uses the IEEE-CIS dataset over which machine learning (ML) and deep learning (DL) algorithms such as Decision Trees, XGBoost, LightGBM, and an advanced Hybrid Deep Learning Model were applied for credit card fraud detection. The proposed model gave the best results, with an ROC AUC of 0.9709 and F1-score of 0.9103. The paper suggests that combining deep learning with explainable AI can improve fraud detection, and future research will aim to make models more transparent and efficient.***

***Keywords: Credit Card Fraud, machine learning, deep learning, imbalanced datasets, ensemble models, SMOTE***

## I. INTRODUCTION

With the rise of online payment systems such as credit cards; global commerce industry has been transformed into speed and convenience. However, this digital growth has multiple challenges, with credit card fraud emerging as a major concern. Fraudulents use techniques such as identity theft, phishing, and hacking to exploit vulnerabilities. In a Juniper study, fraud-related losses were predicted to exceed $362 billion by 2027. Traditional rule-based fraud detection methods generally struggle to identify new fraud patterns in transactions. This occurs because of the presence of highly imbalanced datasets and the need for real-time analysis. In contrast, machine learning (ML) has proven effective in detecting anomalies in large-scale transaction data, adapting to evolving fraud tech- niques over time. However, ML-based systems face challenges such as reducing false positives, handling data imbalance, and maintaining high accuracy in real-time environments. To overcome such challenges, research is now focused on developing robust and scalable algorithms such as hybrid and federated learning models. Given the increasing sophistication of cyber threats, continuous innovation in AI based detection systems is required. This can be done through effective collaboration between banks, tech firms, and regulators to ensure secure digital transactions.

This paper is divided into five sections: Introduction, Lit- erature Review, Research Methodology, Result Analysis, and Conclusion with Future Work.

## II. LITERATURE REVIEW

In this section, we performed a comprehensive review on the detection of credit card fraud. It comprises of different ML and DL techniques used by researchers.

### *A. Literature Review on Credit Card Fraud Detection*

The authors [1] in their research review the challenges of credit card fraud detection. According to them, the credit card dataset faces issues such as class imbalance, feature redundancy, and the need for real-time processing. The study highlights the potential of ML to analyze large datasets and detect fraud patterns. However, there are still various limitations, such as high false positives and computational inefficiencies. The review emphasizes the need for advanced techniques such as SMOTE-ENN, Autoencoders, and ensemble models to overcome these challenges.

A systematic review of 57 studies from 2019 to 2024, is conducted by the authors [2] in their research. They examined advances in deep learning advances in the detection of financial fraud. The review highlights the robustness of models such as CNNs, LSTM, and transformers to address fraud in credit card transactions, insurance claims, and financial audits. In the research, major challenges were identified, such as unbalanced datasets, model interpretability, and ethical concerns. However, the authors noticed progress in feature engineering, data pre- processing, and privacy-preserving techniques for credit card fraud detection. Finally, the study claimed the need for im- proved model interpretability and cross-industry collaboration. In their review, the authors [3], also highlighted the challenges in credit card fraud detection. They emphasized on the need for a detection model with the rise in e-commerce and mobile payments.

Traditional ML algorithms face issues due to dataset insufficiency, caused mainly by privacy concerns and class imbalance, with rare fraudulent transactions. This study highlights the use of Synthetic Minority Oversampling Technique (SMOTE) as an effective solution to balance datasets. Finally, the study inspires for a potential solution by combining Federated Learning with SMOTE and advanced models like LSTM networks to enhance fraud detection accuracy and reliability.

In similar research, the authors [4] also reviewed challenges for credit card fraud detection, due to the increase in electronic payment methods, as global fraud losses reach millions annually. The study highlights the limitations of traditional pattern- matching techniques and supervised ML algorithms. It focuses on class imbalance and mislabelling of fraudulent transactions. Some commonly used sampling techniques, such as random oversampling and undersampling are notified, with SMOTE being the most effective method for balancing datasets. Finally, the review shows high performance of random forests in accuracy over other algorithms such as decision trees and artificial neural networks.

Similarly, the authors [5] also reviewed the challenges in financial fraud detection, due to the significant increase in global credit card fraud losses. In the survey, they identified losses due to financial fraud as $28.4 billion in 2020 to $33.5 billion in 2022, projected to reach $43.47 billion by 2028. Their work shows the limitations of traditional ML models, which behave as black-box in nature. According to them, recent advances, such as ensemble techniques, particularly stacking, improve fraud detection by minimizing overfitting. In addition, XAI methods such as SHAP and LIME can also be used to enhance model interpretability by explaining feature contributions. The review finally highlights the need to combine high-performing models such as XGBoost, LightGBM, and CatBoost with explainable AI to address data imbalance and transparency charges.

The authors [6] also reviewed the challenges in credit card fraud detection, highlighting the increasing economic losses, due to the rise in e-commerce and Card-Not-Present transactions. The research shows that traditional machine learning methods struggle with class imbalance, leading to biased predictions toward the majority class. The review also identified limited applications of deep learning in fraud detection, particularly the use of Continuous-Coupled Neural Networks (CCNN). Also, authors suggested SMOTE as an effective preprocessing method to reduce class imbalance, and enhance model performance on samples of minority classes.

The authors do a comprehensive study on credit card fraud detection [7], focusing on ML algorithms, and emerging techniques. These include federated learning, incremental learning, and NLP to address concerns such as class imbalance, privacy, and evolving fraud patterns. However, limitations still exist, like over-reliance on SMOTE and ADASYN, limited real- world validation, and computational complexity in ensemble models. The authors introduced a novel probability-based kNN approach that replaces traditional distance metrics with logistic regression-derived probabilities. It is a computationally efficient alternative for imbalanced datasets and achieved high performance in diverse datasets.

In their literature review on credit card fraud detection, the authors [8] emphasized the application of ML algorithms to overcome the challenges of fraudulent activities in financial transactions. They evaluated ML models such as logistic re- gression, decision trees, random forest, Naïve Bayes, K-nearest Neighbors, and DL models like simple artificial neural networks. It focused on data preprocessing and model performance through cross-validation. The findings show logistic regression and Naïve Bayes as the best performing models with high accuracy and sensitivity. Meanwhile, decision trees show good interpretability, and random forests show a better response to overfitting through ensemble learning. Cross-validation analysis confirmed the stability and robustness of these models in various folds.

The authors [9] presented a novel framework by integrating AI, blockchain, cybersecurity, and real-time early warning systems to prevent financial fraud in online transactions. Their research combines AI-driven anomaly detection, blockchain for tamper-proof transaction verification, cybersecurity intrusion logs, and real-time alerts. This system achieved a 2–4% F1 score improvement and □90% recall compared to other standalone AI models. It is validated on datasets that include Kaggle Credit Card Fraud, PaySim, and local BFSI logs. The proposed framework offers a scalable and less complex solution, providing a blueprint for improving fraud detection in mid-scale markets.

In their study, the authors [10] enhanced credit card fraud detection using a stacking ensemble model combining XGBoost, CatBoost, and LightGBM, with Logistic Regression as a meta- learner. The model is optimized using Bayesian hyperparameter tuning with an emphasis on imbalanced datasets. Traditional models struggle with bias toward the majority class. While techniques like SMOTE and undersampling reduce imbalance, they are unable to capture complex, non-linear patterns in the data. The study highlights the superiority stacking method, which utilizes multiple base learners to improve predictive performance. The proposed model achieved over training an ROC-AUC score of 0.9887, a recall of 0.86, and an F1-score of 0.87, outperforming compared to single-model baselines.

In a similar study, the authors [11] also proposed an advanced framework for credit card fraud detection. It uses a stacking ensemble technique in combination with K-SMOTEENN to address class imbalance and overfitting challenges. The study emphasized the effectiveness of the stacking model, which combines base learners such as Decision Tree and Random Forest. The proposed model achieved an F1-score of 0.92, precision of 0.95, recall of 0.88, AUPRC of 0.96, and a perfect ROC-AUC of 1.00. By implementing K-SMOTEENN for data resampling and Explainable AI (LIME) for interpretability, the model outperforms standalone models like XGBoost and Decision Tree, and offers a robust solution for real-world fraud detection.

The authors proposed a hybrid deep learning ensemble model for credit card fraud detection in their research [12]. They focused on deep learning techniques, such as Convolutional Neural Networks (CNNs) for spatial feature extraction, Long Short-Term Memory networks (LSTMs) for temporal sequence modeling, and Transformers for better solution. They high- lighted the limitations of individual models as a need for hybrid integration. The study combines CNNs, LSTMs, and Transformers as base learners, while XGBoost was considered a meta-learner. The model achieved a sensitivity of 0.961, a specificity of 0.999, and an AUC-ROC of 0.972 on the European Credit Card Dataset.

This review underscores various ML and DL algorithms along with challenges for credit card fraud detection. Data imbalance, model interpretability, and the evolving nature of fraudulent behaviors proved to be major issues. Traditional ML models performed well, but they are not sufficient to perform fraud detection due to high false positives and poor generalizability. The emerging of hybrid deep learning architec- tures, ensemble stacking, federated learning, and explainable AI (XAI) techniques have shown substantial promising results.

## III. RESEARCH METHODOLOGY

This section represents research that focuses on developing and evaluating ML and DL models for credit card fraud detec- tion. It outlines the systematic approach to data preprocessing, feature engineering, model selection, training, and evaluation to achieve high performance in identifying fraudulent transactions.

### *A. Data Collection*

The dataset used is the IEEE-CIS Fraud Detection dataset, sourced from Kaggle. It consists of:

1) 590,540 transactions with 394 features, including Trans- actionID, isFraud (target variable), TransactionAmt, and various anonymized features (e.g., V1 to V339).
2) 144,233 records with 41 features, including device infor- mation and identity-related features.

The dataset is highly imbalanced, with approximately 3.5% of transactions labeled as fraudulent.

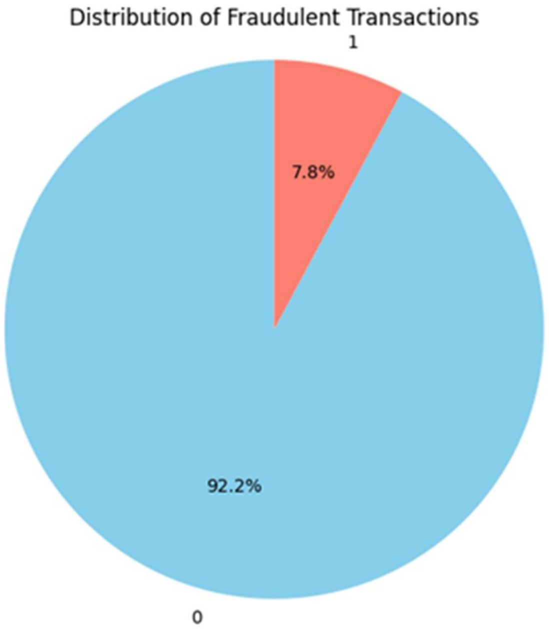

Fig. 1: Distribution of Fraudulent Transactions

### *B. Data Preprocessing*

*1)* The transaction and identity datasets were loaded and merged on TransactionID.
*2)* TransactionID column was dropped post-merge as it served only as a joining key.
*3)* The missing values were replaced with the median of each column. For categorical columns, the mode of each column was used.
*4)* There are no null values present in the dataset.
*5)* LabelEncoder is applied to transform categorical columns into numerical values to maintain model compatibility.
*6)* Resampling is performed to balance the dataset.
*7)* Problematic columns were identified and dropped.
*8)* The top 20 features were selected for model training to reduce dimensionality and improve model efficiency.

### *C. Exploratory Data Analysis (EDA)*

*1)* The distribution of key characteristics was visualized using various plots.
*2)* Its shows the data imbalancing in fraudulent transaction prior to oversampling.

### *D. Model Development*

Multiple machine learning models were developed and evaluated. These are:

*1)* Decision Tree Classifier:
  - Used as a baseline model with max_depth=3 to prevent overfitting.
  - Trained on imputed and scaled data after dropping problematic columns.

*2)* LightGBM Classifier:
  - Configured with parameters: n_estimators=100, max_depth=7, learning_rate=0.1, class_weight=’balanced’.
  - Trained with early stopping to prevent overfitting.
  - Evaluated using ROC AUC and classification report.

*3)* CatBoost Classifier:

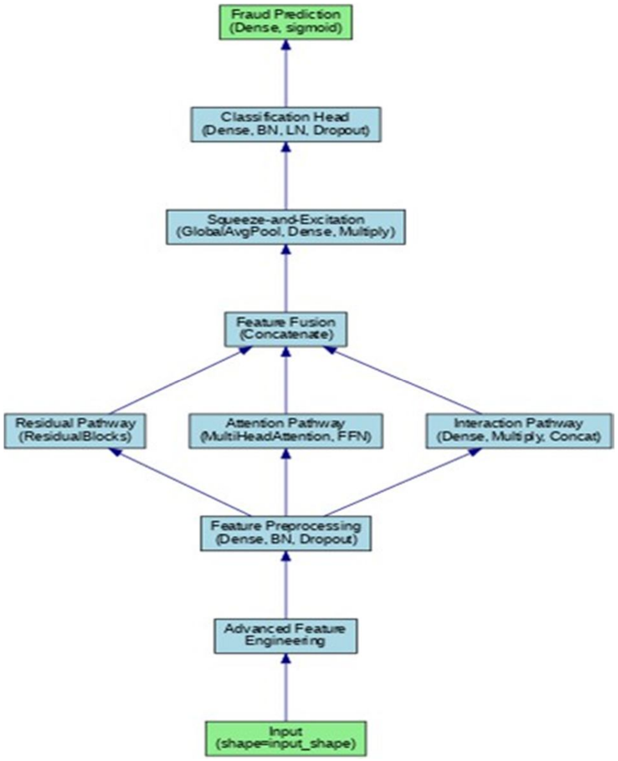

Fig. 2: Proposed Model Architecture

  - Configured with iterations=100, depth=7, learn- ing_rate=0.1, auto_class_weights=’Balanced’.
  - Trained with early stopping and evaluated similarly to LightGBM.

4) XGBoost Classifier:
    - Configured and trained similarly to LightGBM and CatBoost.
5) Enhanced Neural Network Model:
    - Architecture includes dense layers (512, 256, 128, 64 neurons), batch normalization, dropout, multi-head attention, residual blocks, and squeeze-excite blocks.
    - Trained with a combination of specialized loss functions:
        - Focal Loss (70% weight) to focus on hard exam- ples.
        - Class-Balanced Loss (20% weight) to address imbalance.
        - Binary Cross-Entropy (10% weight) as a baseline.
    - Advanced feature engineering layer generates poly- nomial, statistical, interaction, ratio, and binning features.
    - Trained for 50 epochs with early stopping based on validation AUC.
    - Optimal threshold selected to maximize F1-score.

### E. *Model Training and Evaluation*

1) The data is splitted into 80% training and 20% testing sets with stratify to maintain class distribution.
2) Imputation and Scaling:

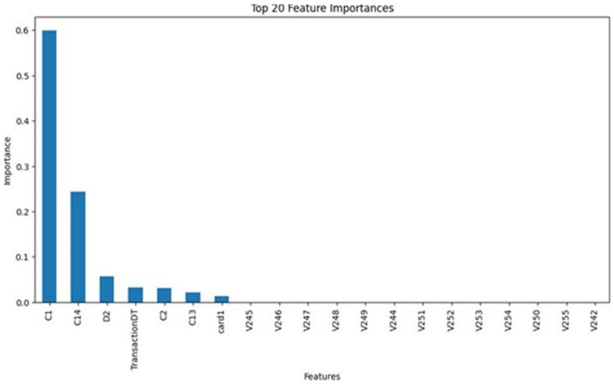

Fig. 3: Top 20 Features Ranked by Importance Scores

3) SimpleImputer is applied to handle any remaining missing values.
4) The features are scaled using StandardScaler for neural network compatibility.

## IV. RESULT ANALYSIS

This section presents a detailed analysis of the results obtained from various models implemented in the research methodology. The models were evaluated using several metrics, including the ROC AUC score, the ROC Curve, the Classifi- cation Report, and the Average Precision Score. In addition, the top contributing features were visualized to interpret their impact on the prediction of the model.

### A. *Decision Tree Analysis*

Served as a baseline model to identify the 20 most important features, helping in initial feature selection.

### B. *Model Performance Summary*

- LightGBM:
    - Achieved a ROC AUC score of 0.9491, with balanced precision and recall ranging from 0.87 to 0.90.
- CatBoost:
    - Reached a ROC AUC score of 0.9407, also maintain- ing strong balance between precision and recall.
- XGBoost:
    - Delivered a ROC AUC of 0.9600, with a precision of 0.90 and a recall of 0.89.
- Enhanced Neural Network:

- Outperformed all other models with a ROC AUC of 0.9709, an average precision score of 0.9713, a F1-score of 0.9103, and an overall accuracy of 91%. The application of advanced feature engineering contributed to a 2–3% performance improvement, while specialized loss functions added another 1–2% gain.

To ensure reliable results, an optimal threshold (0.4380) was chosen for the neural network to improve its F1-score, and a feature importance analysis helped us to understand which inputs contributed the most to the predictions. Oversampling techniques may have added some noise and limited computing power restricted testing of more complex neural network models.

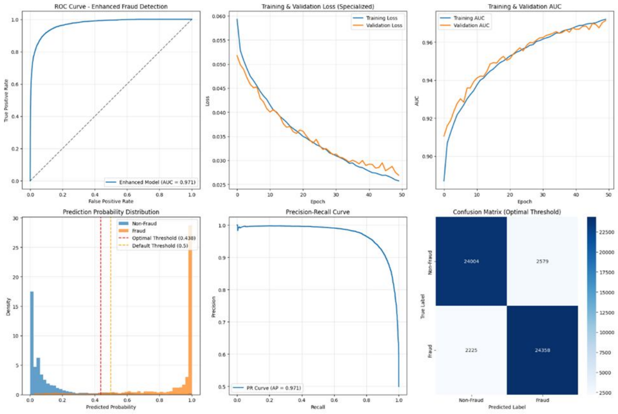

Fig. 4: Proposed Model Results Analysis

## V. CONCLUSION AND FUTURE WORK

In this study, we presented a comprehensive methodology that effectively integrates data preprocessing, feature selection, class balancing, and advanced model development for fraud detection. Among all models evaluated, the enhanced neural network outperformed traditional approaches, achieving the highest ROC AUC score of 0.9709 along with strong precision, recall, and F1-score. The application of advanced feature engineering and specialized loss functions contributed signifi- cantly to this performance increase. Despite promising results, challenges such as feature anonymity, potential oversampling noise, and computational limitations were observed. Future work can focus on exploring more interpretable models, integrating attention mechanisms for better feature attribution, and deploying explainable AI (XAI) frameworks to improve transparency.

## REFERENCES

[1] R. K. Gupta, A. Hassan, S. K. Majhi, N. Parveen, A. T. Zamani, R. Anitha, B. Ojha, A. K. Singh, and D. Muduli, “Enhanced framework for credit card fraud detection using robust feature selection and a stacking ensemble model approach,” Results in Engineering, vol. 26, p. 105084, Apr. 2025.

[2] Y. Chen, C. Zhao, Y. Xu, and C. Nie, “Year-over-year developments in financial fraud detection via deep learning: A systematic literature review,” Jan. 2025.

[3] W. Mohamedhen, M. Charfeddine, and Y. Hadj Kacem, “Enhanced credit card fraud detection using federated learning, lstm models, and the smote technique,” in Proc. 17th Int. Conf. Agents Artif. Intell. (ICAART), vol. 3, 2025, pp. 368–375.

[4] M. Gostkowski, A. Krasnode¸bski, and A. Niedziółka, “Credit card fraud detection using machine learning techniques,” European Research Studies Journal, vol. 27, no. 2, pp. 571–585, 2024.

[5] F. Almalki and M. Masud, “Financial fraud detection using explainable ai and stacking ensemble methods,” May 2025.

[6] Y. Wu, L. Wang, H. Li, and J. Liu, “A deep learning method of credit card fraud detection based on continuous-coupled neural networks,” Mathematics, vol. 13, no. 5, p. 819, Feb. 2025.

[7] R. V. Karunya, S. Ganesh, D. Muralidharan, G. R. Brindha, and M. Thiruvengadam, “Credit card fraud data analysis and prediction using machine learning algorithms,” Security and Privacy, vol. 8, no. 3,

[8] p. e413, Apr. 2025.

[9] S. F. Farabi, M. Prabha, M. Alam, M. Z. Hossan, M. Arif, M. R. Islam, A. Uddin, M. Bhuiyan, and M. Z. A. Biswas, “Enhancing credit card fraud detection: A comprehensive study of machine learning algorithms and performance evaluation,” Journal of Business and Management Studies, vol. 6, no. 4, pp. 1–10, 2024.

[10] B. Fetaji, M. Fetaji, A. Hasan, S. Rexhepi, and G. Armenski, “Fraud-x: An integrated ai, blockchain, and cybersecurity framework with early warning systems for mitigating online financial fraud: A case study from north macedonia,” IEEE Access, vol. 13, pp. 35 472–35 485, Mar. 2025.

[11] A. El Bazi, M. Chrayah, N. Aknin, and A. Bouzidi, “Enhancing credit card fraud detection using a stacking model approach and hyperparameter optimization,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 15, no. 10, pp. 1080–1087, 2024.

[12] N. Damanik and C.-M. Liu, “Advanced fraud detection: Leveraging k-smoteenn and stacking ensemble to tackle data imbalance and extract insights,” IEEE Access, vol. 13, pp. 35 280–35 290, Jan. 2025.

[13] E. Ileberi and Y. Sun, “A hybrid deep learning ensemble model for credit card fraud detection,” IEEE Access, vol. 12, pp. 175 829–175 842, Nov. 2024.