International Journal of Multidisciplinary Engineering in Current Research - IJMEC

Volume 11, Issue 4s, April-2026, http://ijmec.com/, ISSN: 2456-4265

Full Length Article

Enhancing Credit Card Fraud Detection in Banking Using Neural Networks

Syeda Ayesha Atif [1], Noor Ul Jariyah Kulsoom[2] , Tahniyath Unnisa[3], Dr. Md Zainlabuddin[4]

[1,2,3]B.E Students; Computer Engineering Department, ISL College Of Engineering Hyderabad India.
[4]Associate professor, Department of CSE ISL College Of Engineering Hyderabad India.
atifsyedaayesha@gmail.com, nujk1904@gmail.com, Tahniyathunnisa440@gmail.com

Accepted 24-04-2026

Abstract:
Credit card fraud is one of the most serious threats in today's digital banking systems, where thousands of transactions occur every second. Detecting fraudulent transactions in real time is challenging due to the high imbalance between legitimate and fraudulent records and the constantly evolving nature of fraud patterns. In this project, a deep learning-based fraud detection system is developed using the TabNet model, which efficiently handles large-scale, high-dimensional tabular transaction data. The model learns to focus on the most important features of each transaction using sequential attention, achieving high precision and recall while minimizing false alarms. The system integrates advanced pre-processing, balanced data handling, model training, evaluation, and visualization. Finally, a Flask-based web application is built to provide an interactive user interface with modules for registration, login, real-time prediction, and visual analytics of model performance. The proposed system achieves excellent accuracy, faster inference, and robust fraud detection capabilities compared to traditional approaches.

Keywords: *Credit Card, Fraud Detection, Deep Learning, TabNet Model, Machine Learning, Neural Networks, Real-Time Prediction.*

INTRODUCTION:

In the modern digital economy, online and card-based transactions have become the backbone of financial systems, offering convenience and speed to millions of users worldwide. However, this rapid growth has also led to a sharp increase in fraudulent activities, posing severe risks to banks and customers alike. Traditional fraud detection methods often rely on rule-based or conventional machine learning techniques, which struggle to adapt to evolving fraud patterns and large-scale, high-dimensional data. To address these challenges, this project introduces an advanced deep learning approach using the TabNet model, a specialized neural network architecture designed for tabular datasets. TabNet leverages sequential attention to identify the most influential transaction features while maintaining interpretability and computational efficiency. The system processes transactional data, trains the TabNet model to detect anomalies, and provides high-accuracy predictions distinguishing legitimate and fraudulent transactions. A user-friendly Flask web application is integrated to enable real-time fraud prediction, visualization of feature importance, and model performance analytics. This project demonstrates how deep learning-based solutions like TabNet can significantly improve accuracy, reduce false positives, and enhance the overall reliability of fraud detection systems in financial institutions.

LITERATURE REVIEW

The rapid growth of digital banking and online financial transactions has significantly increased the risk of credit card fraud, making fraud detection systems an essential component of modern financial security frameworks. Machine learning and artificial intelligence technologies have emerged as effective solutions for identifying fraudulent activities by analyzing transaction behaviour, detecting anomalies, and predicting suspicious patterns in real time. Numerous researchers have explored different computational techniques, algorithms, and intelligent systems to improve fraud detection accuracy while minimizing false positives. This chapter reviews major studies related to machine learning-based credit card fraud detection systems and highlights their methodologies, findings, and limitations.

Machine Learning-Based Fraud Detection Approaches

Tiwari *et al.* [1] conducted a comprehensive study on the application of machine learning algorithms for credit card fraud detection. The researchers evaluated several classification models, including logistic regression, decision trees, random forest,

https://doi.org/10.63665/IJMEC.1104s.04
ISSN: 2456-4265
IJMEC 2026

and support vector machines, using large-scale transactional datasets. Their study focused on improving fraud detection accuracy through effective feature selection and handling class imbalance problems. Performance metrics such as precision, recall, F1-score, and accuracy were used to compare model efficiency. The findings revealed that ensemble learning approaches, particularly random forest and boosting techniques, provided superior detection accuracy and robustness compared to individual classifiers. The study also emphasized the importance of preprocessing techniques and balanced datasets for improving fraud prediction performance.

Deep learning integration into cybersecurity systems was discussed extensively by Micro [2], who explored the role of artificial intelligence in modern digital security software. The report highlighted how neural network-based architectures can identify abnormal transactional behaviour and adapt dynamically to evolving fraud strategies. The study emphasized the importance of AI-driven systems in real-time fraud prevention, especially in financial institutions handling large-scale transaction streams. The report further explained how deep neural networks, behavioural analytics, and automated anomaly detection systems contribute to reducing unauthorized financial activities. The findings suggested that AI-powered fraud detection systems are more adaptive and scalable than conventional rule-based systems.

Kulatilleke [3] examined the major challenges and complexities associated with machine learning-based credit card fraud detection systems. The study identified critical issues such as severe class imbalance, dynamic fraud behaviour, privacy concerns, and limitations of traditional classification algorithms. According to the author, conventional machine learning techniques such as logistic regression and k-nearest neighbour models often struggle to generalize effectively in highly dynamic transaction environments. The research proposed the adoption of advanced deep learning architectures, hybrid systems, and attention-based models to improve adaptability and fraud detection efficiency. The study concluded that modern fraud detection systems must support continuous learning and real-time adaptability to remain effective against emerging fraud techniques.

Hashemi, Mirtaheri, and Greco [4] investigated the use of supervised machine learning algorithms for fraud detection in banking datasets. Their research, published in *IEEE Access*, compared various algorithms including decision trees, random forests, gradient boosting models, and artificial neural networks. Large-scale banking transaction datasets were used to evaluate model performance under real-world conditions. The findings demonstrated that ensemble and hybrid models achieved higher detection accuracy and lower false-positive rates compared to traditional classifiers. Additionally, the study emphasized the growing importance of explainable artificial intelligence (XAI) in banking applications to ensure transparency, interpretability, and regulatory compliance. The authors suggested that combining high-performing predictive models with explainability mechanisms could improve trust and operational effectiveness in fraud detection systems.

Sulaiman, Schetinin, and Sant [5] presented an extensive review of machine learning approaches used in credit card fraud detection systems. Their study categorized fraud detection methods into supervised, unsupervised, and hybrid learning approaches. The authors analyzed the strengths and weaknesses of various techniques in handling imbalanced datasets and evolving fraud behaviours. The review also examined recent advancements in deep learning, graph-based learning, and attention mechanisms for fraud analysis. The researchers concluded that integrating scalability, interpretability, and adaptive learning capabilities into fraud detection frameworks could significantly enhance overall system performance. Furthermore, the study highlighted the importance of combining traditional statistical methods with advanced deep learning architectures for improved fraud identification.

Comparative Analysis of Literature

The reviewed studies collectively demonstrate that machine learning and deep learning technologies play a significant role in enhancing the efficiency of fraud detection systems. Most researchers agree that traditional statistical methods are insufficient for handling complex and evolving fraud patterns in modern financial systems. Ensemble learning methods, deep neural networks, and hybrid architectures consistently show better performance in detecting fraudulent activities while maintaining lower false-positive rates.

Another major observation from the literature is the challenge associated with class imbalance in fraud datasets. Since fraudulent transactions represent only a small fraction of total transactions, many machine learning models tend to become biased toward legitimate transactions. Researchers have proposed various solutions such as oversampling, undersampling, synthetic data generation, and cost-sensitive learning to address this issue.

The literature also highlights the increasing importance of explainable AI in financial systems. While deep learning models provide high accuracy, they are often criticized for their lack of transparency. Explainability mechanisms are therefore necessary to improve trust, regulatory compliance, and decision-making within banking institutions.

https://doi.org/10.63665/IJMEC.1104s.04
ISSN: 2456-4265
IJMEC 2026

Additionally, several studies emphasize the need for real-time fraud detection capabilities. Fraud patterns evolve rapidly, requiring models that can adapt continuously to changing transactional behaviour. Advanced deep learning systems and adaptive machine learning frameworks have shown promising results in addressing these challenges.

Research Gap

Although significant progress has been made in machine learning-based fraud detection systems, several research gaps still exist. Many existing systems struggle to balance high detection accuracy with low false-positive rates. Some models are computationally expensive and difficult to deploy in real-time financial environments. Additionally, limited research has focused on integrating explainable AI with adaptive deep learning architectures for fraud detection.

Furthermore, evolving cyber threats and dynamic fraud techniques require intelligent systems capable of continuous learning and behavioural adaptation. Existing literature also indicates limited emphasis on scalable hybrid architectures that combine deep learning, ensemble methods, and real-time analytics in a unified framework.

Therefore, the present study aims to address these limitations by developing a robust machine learning-based fraud detection framework that improves detection accuracy, adaptability, scalability, and real-time performance while maintaining operational transparency and efficiency.

METHODOLOGY

Modules Name

The proposed Credit Card Fraud Detection System consists of the following modules: Data Collection and Pre-processing Module, Data Splitting and Balancing Module, TabNet Model Training and Optimization Module, Model Evaluation and Feature Importance Module, Visualization and Result Analysis Module, Flask Web Application Module, and Prediction and Reporting Module.

1. Data Collection and Pre-processing Module

The Data Collection and Pre-processing Module is responsible for importing and preparing the dataset used for fraud detection. The dataset, named *creditcard_2023.csv*, contains approximately 568,630 transaction records with 31 attributes, including anonymized numerical features (V1–V28), transaction amount, and class labels indicating fraudulent or legitimate transactions. During preprocessing, unnecessary columns such as transaction identifiers are removed to reduce redundancy. The module also handles missing and duplicate values to ensure data quality and consistency. Furthermore, normalization and logarithmic scaling techniques are applied to the Amount attribute to improve model learning efficiency and stability. These preprocessing operations convert the raw dataset into a clean and structured format suitable for deep learning model training.

2. Data Splitting and Balancing Module

The Data Splitting and Balancing Module divides the processed dataset into training and testing subsets using an 80:20 ratio while maintaining the original class distribution. Since fraud detection datasets are highly imbalanced, with legitimate transactions greatly outnumbering fraudulent ones, balancing techniques are applied to improve model performance. Methods such as class weight balancing and Synthetic Minority Oversampling Technique (SMOTE) are used to generate additional minority class samples and reduce bias toward majority class predictions. This module ensures that the model learns effectively from both fraudulent and legitimate transaction data, thereby improving fairness, stability, and fraud detection capability.

3. TabNet Model Training and Optimization Module

The TabNet Model Training and Optimization Module forms the core component of the proposed system. In this module, the TabNet deep learning architecture is trained using the balanced and preprocessed dataset. TabNet is specifically designed for tabular datasets and employs a sequential attention mechanism that selectively focuses on the most relevant features during training. This enhances both interpretability and classification accuracy. The training process involves configuring several hyperparameters such as learning rate, number of decision steps, batch size, and sparsity regularization to achieve optimal performance. GPU acceleration available in Google Colab is utilized to speed up the training process and reduce computational time. After successful training and optimization, the model is stored in both *.zip* and *.pkl* formats for future deployment and real-time prediction tasks.

4. Model Evaluation and Feature Importance Module

The Model Evaluation and Feature Importance Module evaluates the effectiveness of the trained TabNet model using standard machine learning performance metrics. The evaluation includes Accuracy, Precision, Recall, F1-Score, and ROC-AUC score to measure the model's predictive capability in detecting fraudulent transactions. A confusion matrix is also generated to visualize the classification results, including true positives, true negatives, false positives, and false negatives. In addition to performance evaluation, this module calculates feature importance scores that identify the most influential attributes affecting the prediction outcome. These insights improve model explainability and help analysts understand the factors contributing to fraudulent transaction behavior.

https://doi.org/10.63665/IJMEC.1104s.04
ISSN: 2456-4265
IJMEC 2026

5. Visualization and Result Analysis Module

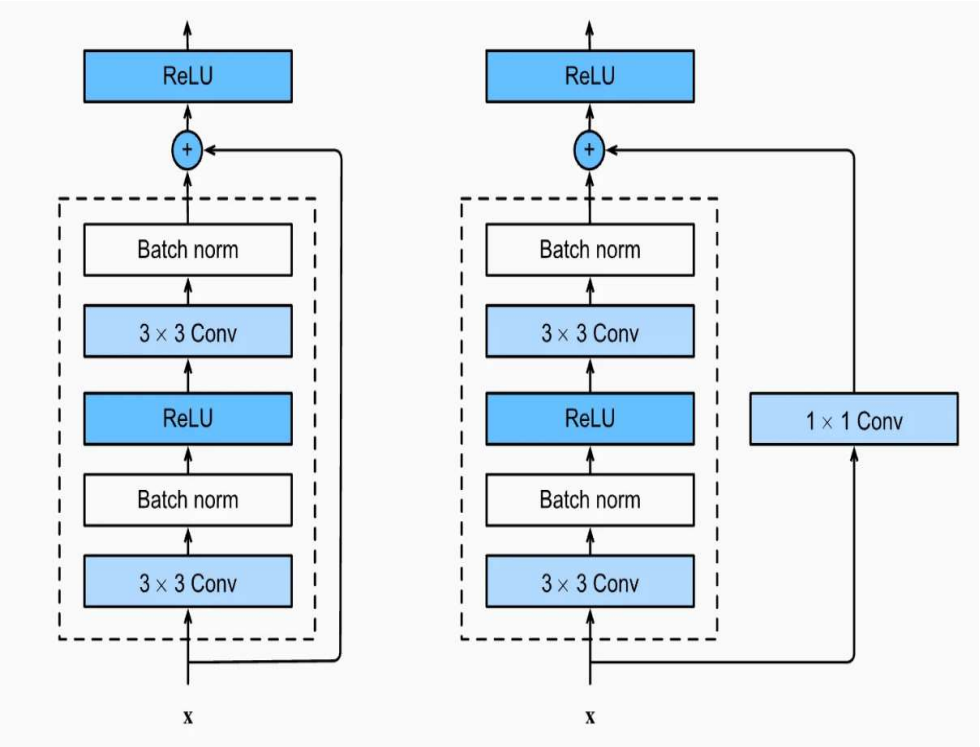
The Visualization and Result Analysis Module generates various graphical representations and analytical reports to provide a better understanding of the model's behavior and performance. The module creates ROC curves, Precision-Recall curves, feature importance bar charts, correlation heatmaps, and training performance graphs. These visualizations assist in evaluating the effectiveness of the fraud detection system and communicating analytical insights clearly. All generated plots, charts, and evaluation results are stored in a dedicated artifacts directory known as *ARTIFACTS_DIR*, enabling easy access for future analysis and integration into the web application dashboard.

6. Flask Web Application Module

The Flask Web Application Module integrates the trained TabNet model into a web-based application that provides an interactive and user-friendly environment for fraud prediction. The Flask application contains several web pages, including a Home Page, User Registration/Login Page, Prediction Page, and Charts Page. Users can manually enter transaction details or upload CSV files for bulk fraud prediction. The backend application loads the trained TabNet model and processes the user inputs in real time to generate prediction results. This module enhances accessibility and enables practical deployment of the fraud detection system for real-world usage.

7. Prediction and Reporting Module

The Prediction and Reporting Module is responsible for performing real-time fraud prediction and presenting the final results to the user. When transaction details are submitted through the web interface, the system preprocesses the input data, applies feature transformation, and performs prediction using the trained TabNet model. The module outputs the classification result as either Fraudulent Transaction (1) or Legitimate Transaction (0), along with the corresponding fraud probability score. Additionally, prediction logs are maintained for monitoring purposes, and detailed analytical reports with visual summaries are generated. These reports assist users and financial analysts in understanding transaction behavior, identifying suspicious activities, and making informed decisions regarding transaction security.



Implementation:

The system is implemented using Python with libraries

Algorithm:

Programming Language: Python

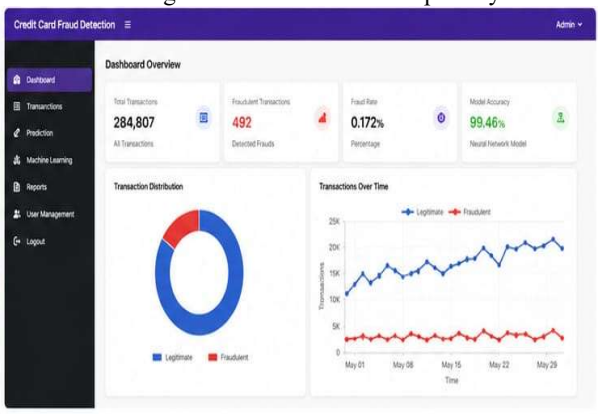
Libraries:NumPy, Pandas, Scikit-learn, TensorFlow / Keras

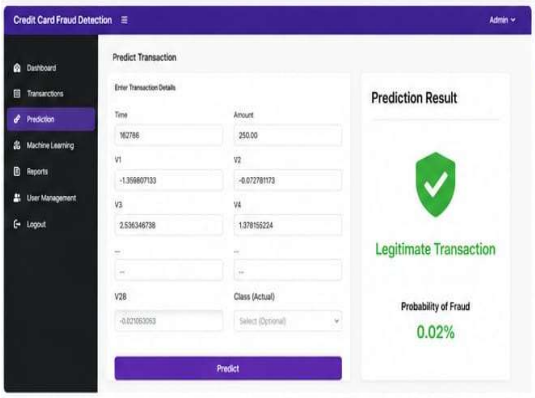
https://doi.org/10.63665/IJMEC.1104s.04
ISSN: 2456-4265
IJMEC 2026

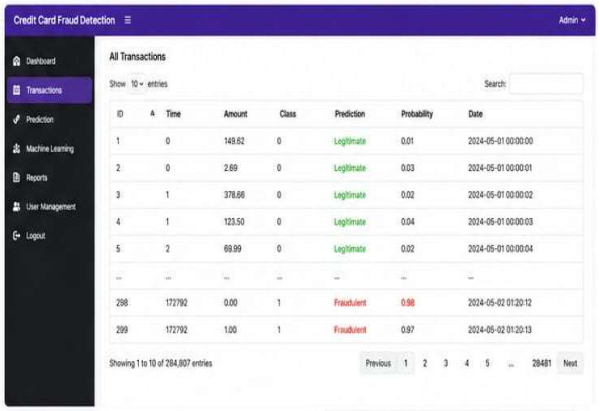
Machine Learning Techniques: Deep Learning, Neural Networks
Oversampling Technique: SMOTE
Development Environment:Spyder IDE
Operating System: Windows

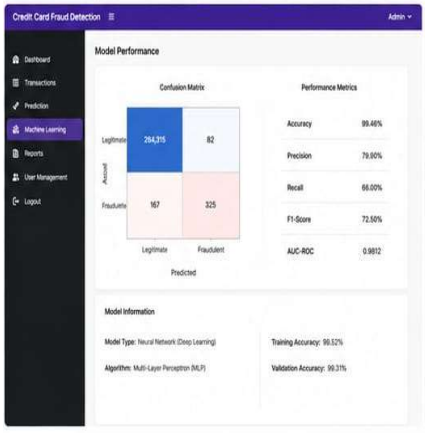
Results

The experimental results show that the proposed ResNet-based model achieves higher accuracy compared to traditional machine learning approaches. The system demonstrates improved recall and precision for fraudulent transactions, indicating better fraud detection capability.

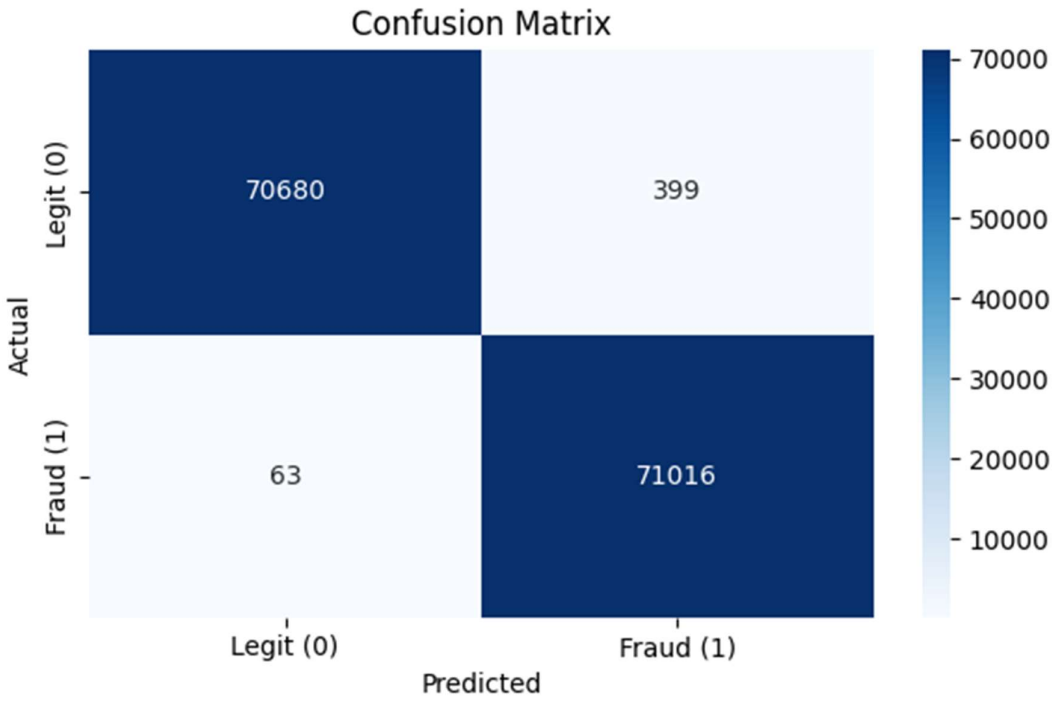


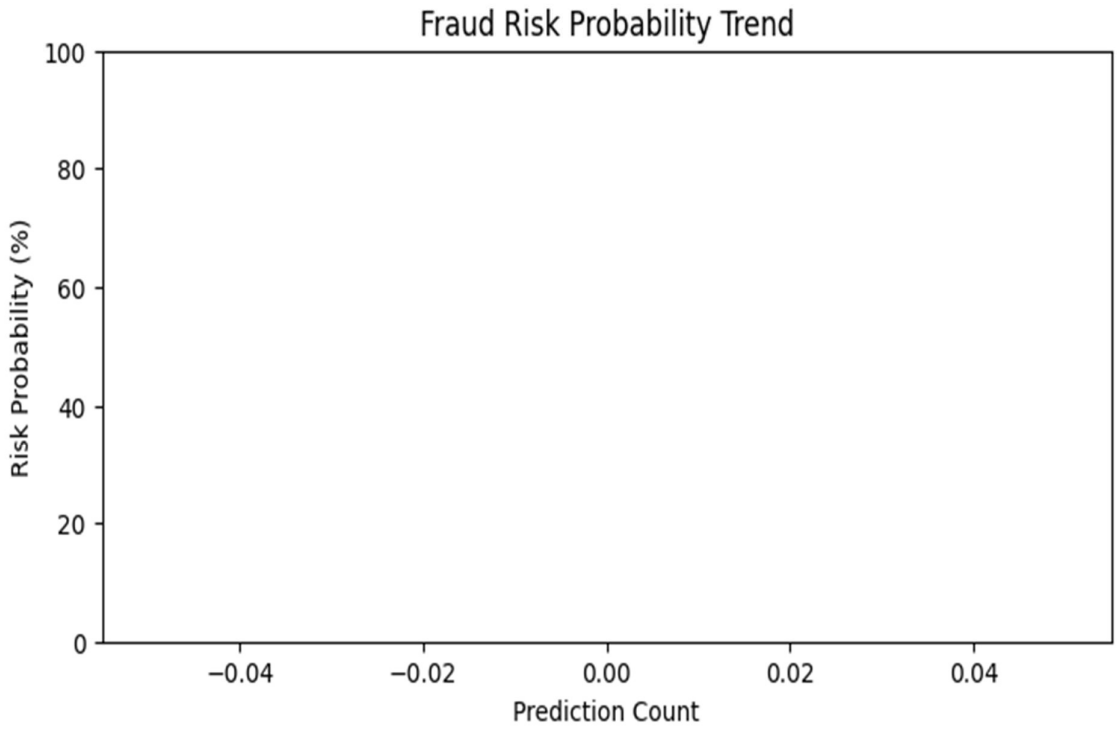




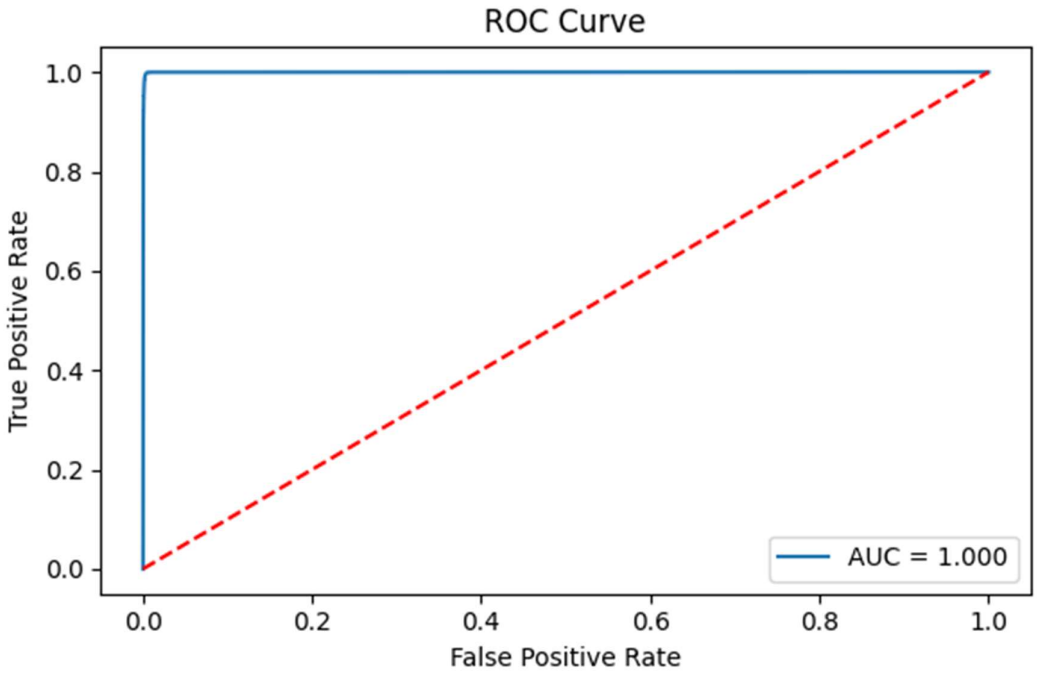


https://doi.org/10.63665/IJMEC.1104s.04
ISSN: 2456-4265
IJMEC 2026





https://doi.org/10.63665/IJMEC.1104s.04
ISSN: 2456-4265
IJMEC 2026



CONCLUSION

This project successfully demonstrates the use of deep learning for credit card fraud detection. By leveraging ResNet architecture, the system achieves improved performance, robustness, and adaptability.

The proposed approach enhances banking security and provides an effective solution for real-world fraud detection challenges. And it presents an efficient deep learning–based approach for credit card fraud detection using a ResNet architecture.

The system successfully addresses challenges such as data imbalance and complex transaction patterns. By leveraging residual learning and proper preprocessing techniques, the proposed model delivers improved accuracy and robustness.

The solution demonstrates strong potential for real-world banking applications and contributes to enhancing financial security.

Future scope:

The system can be further enhanced by integrating real-time fraud detection capabilities in live banking environments. Hybrid models combining multiple deep learning techniques can be explored for better performance.

Future work may also focus on explainable AI techniques to improve model interpretability and deploying the system as a scalable web or mobile application. Additionally, the approach can be extended to detect other types of financial fraud.

Integration with real-time banking systems

Use of hybrid models combining multiple deep learning techniques

Inclusion of explainable AI for better interpretability

Deployment as a web or mobile application

Extension to detect other types of financial fraud

https://doi.org/10.63665/IJMEC.1104s.04
ISSN: 2456-4265
IJMEC 2026

References :

[1] P. Tiwari, S. Mehta, N. Sakhuja, J. Kumar, and A. K. Singh, “Credit Card Fraud Detection Using Machine Learning: A Study,” 2021.

[2] T. Micro, *Deep Security Software*, 2020.

[3] G. K. Kulatilleke, “Challenges and Complexities in Machine Learning-Based Credit Card Fraud Detection,” 2022.

[4] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, “Fraud Detection in Banking Data by Machine Learning Techniques,” *IEEE Access*, 2023.

[5] R. B. Sulaiman, V. Schetinin, and P. Sant, “Review of Machine Learning Approach on Credit Card Fraud Detection,” 2022.