Original Article
ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research - GRANTHAALAYAH
December 2023 11(12), 244–253

# ENHANCING FINANCIAL SECURITY: CNN AND EFFICIENTNET-BASED CREDIT CARD FRAUD DETECTION SYSTEM

Sarabjeet [1], Abhay [1], Kavita [1]

[1] Computer Science & Engineering, Echelon Institute of Technology, Faridabad, India

**Received** 23 November 2023
**Accepted** 20 December 2023
**Published** 31 December 2023

**DOI**
10.29121/granthaalayah.v11.i12.2023.6114

**Funding:** This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.



## ABSTRACT

This project report presents the design, development, and implementation of a credit card fraud detection system leveraging advanced deep learning techniques, specifically Convolutional Neural Networks (CNNs) and EfficientNet. The rapid growth of e-commerce and digital payment platforms has led to a surge in financial fraud, making it imperative to develop robust and intelligent mechanisms for early fraud detection. Unlike traditional machine learning methods, deep learning models offer enhanced capabilities in capturing complex patterns and subtle anomalies in high-dimensional transaction data.

In this work, CNNs are utilized to extract hierarchical spatial features from transaction data represented in structured or image-like formats, enabling the model to detect intricate fraud signatures. Furthermore, EfficientNet, a cutting-edge CNN architecture known for its balance of performance and computational efficiency, is applied to improve detection accuracy while maintaining low resource overhead. The model is trained to analyze historical customer transaction data, learn behavioral patterns, and identify irregularities indicative of fraudulent activity.

The proposed system focuses on real-time fraud detection in streaming transaction environments, integrating anomaly detection methods with deep learning for improved responsiveness and precision. This project ultimately contributes to the development of an adaptive and scalable fraud detection framework, capable of enhancing security in the financial domain and protecting users against evolving fraudulent threats.

## 1. INTRODUCTION

In the digital age, the use of credit cards for online transactions has become both ubiquitous and indispensable. However, with convenience comes risk. One of the major concerns surrounding electronic payment systems is "credit card fraud," which involves the unauthorized use of someone else's credit card information without the cardholder's knowledge or consent [1]. Such unauthorized access and misuse pose significant threats not only to the financial institutions but also to the customers whose sensitive financial information is compromised.

The nature of fraud in credit card transactions is such that it typically occurs without immediate detection. This makes fraud detection both a critical and complex task. The behavior of fraudsters often mimics that of legitimate users,

making manual detection increasingly inefficient. Therefore, it is essential to employ automated systems capable of accurately and swiftly identifying fraudulent patterns amidst millions of legitimate transactions [2].

The rise in credit card fraud is directly proportional to the growth of e-commerce and digital banking. With billions of transactions occurring daily, the chances of fraud increase significantly, especially in environments where cybersecurity protocols are not robust enough to detect and prevent it in real-time. Traditional detection methods are becoming less effective as fraudsters develop increasingly sophisticated techniques. This has prompted the integration of machine learning (ML) models into fraud detection frameworks, offering the ability to analyze complex data and detect anomalies that may signal fraudulent behavior [3].

## 2. UNDERSTANDING CREDIT CARD FRAUD DETECTION

Credit card fraud detection involves the continuous monitoring of user transaction data to identify suspicious activities that deviate from normal behavior. The aim is to perceive and prevent objectionable conduct, which includes fraudulent transactions, system intrusions, and payment defaults [4]. Modern fraud detection systems leverage a variety of machine learning algorithms to sift through transactional data and flag anomalies. These flagged cases are then further investigated by professionals, who confirm whether the transaction was genuine or fraudulent through customer verification.

Several machine learning techniques have been applied in this domain, including Artificial Neural Networks (ANN), Support Vector Machines (SVM), Decision Trees, Bayesian Networks, Genetic Algorithms, and Logistic Regression [5]. These models are trained on historical transaction data to learn the features of fraudulent transactions and make predictions on new data points. More advanced models, like Hidden Markov Models and K-Nearest Neighbors (KNN), offer dynamic learning and enhanced adaptability, making them suitable for real-time fraud detection systems [6].

Despite the advantages of these techniques, a number of challenges persist. One significant issue is the severe class imbalance in datasets, where fraudulent transactions constitute a very small portion of the data. This imbalance often causes predictive models to favor the majority class (non-fraudulent transactions), reducing the effectiveness of fraud detection. Moreover, the ever-changing nature of fraudulent techniques requires systems that can evolve and adapt in near real-time [7].

## 3. PROBLEM STATEMENT

The core challenge in credit card fraud detection lies in developing intelligent systems that can accurately distinguish between legitimate and fraudulent transactions in a timely manner. Due to the skewed distribution of fraudulent versus non-fraudulent cases, most models struggle with prediction accuracy, especially in minimizing false negatives (frauds that go undetected) [8].

Another critical concern is model interpretability. Many machine learning models, especially deep learning-based ones, function as “black boxes,” making it difficult for regulators and financial stakeholders to understand the rationale behind a flagged transaction. Additionally, these models must operate under strict

compliance standards and privacy regulations, often complicating their implementation in real-world scenarios [9].

The dynamism of fraud patterns necessitates the use of adaptive models that can evolve without frequent manual intervention. As fraudsters continuously find new loopholes, the detection systems must not only detect current fraud but also predict future fraudulent trends. This requires a balance between system security, user convenience, and compliance with legal frameworks [10].

## 4. OBJECTIVES OF THE PROJECT

The primary objective of this project is to develop an efficient machine learning-based system that can accurately detect fraudulent credit card transactions. The system will analyze transactional parameters such as the location of the transaction, the time interval between consecutive transactions, and the transaction amount to identify irregularities. These insights will guide the detection of fraudulent patterns that deviate from a user's historical behavior.

To achieve this, the project will utilize data preprocessing techniques such as SMOTE (Synthetic Minority Over-sampling Technique) to address dataset imbalance. The model-building process will involve comparing various machine learning algorithms including Logistic Regression, Decision Tree, and XGBoost to determine which offers the best trade-off between accuracy, speed, and interpretability [11].

The overarching objectives include:

- Collecting and processing transaction data to extract key features for fraud detection.
- Training multiple machine learning models and evaluating their performance using metrics such as accuracy, precision, recall, and F1-score.
- Developing a system that ensures fast detection and reduces false positives, thereby maintaining a seamless user experience.

## 5. SIGNIFICANCE AND MOTIVATION

This project holds significant importance in the realm of cybersecurity and financial technology. The increasing prevalence of credit card fraud necessitates the development of robust systems that can mitigate financial losses and uphold user trust. Fraud not only affects financial institutions but also disrupts the lives of victims whose financial information is compromised [12].

Machine learning provides a promising solution by enabling systems to detect even subtle anomalies in transaction patterns. Unlike traditional rule-based systems, ML models learn from vast datasets and continuously evolve, making them highly adaptable to new types of fraud. This capability enhances the system's agility and effectiveness in real-time detection scenarios [13].

The project is motivated by several key factors:

- **Financial Security:** Enhancing protection against unauthorized access to financial assets.
- **Customer Trust:** Maintaining confidence in online payment systems through accurate fraud prevention.
- **Scalability:** Offering a solution that can handle increasing volumes of transaction data with minimal performance degradation.

- **Regulatory Compliance:** Ensuring that the system aligns with legal and industry standards.
- **Technological Advancement:** Applying state-of-the-art machine learning techniques to a real-world problem.

Through this project, we aim to build a framework that not only addresses current fraud challenges but also anticipates future threats, thus contributing to a more secure digital financial ecosystem.

## 6. CONCLUSION AND REPORT ORGANIZATION

This introductory section lays the foundation for the subsequent chapters of the report. It highlights the urgent need for effective fraud detection systems in the era of digital finance and introduces the key concepts, challenges, and objectives that the project addresses. The motivation behind using machine learning for fraud detection is grounded in its potential to provide scalable, efficient, and adaptive solutions to an ever-growing problem.

## 7. LITERATURE REVIEW

The Credit Card Fraud Detection project using machine learning aims to build a robust system capable of accurately identifying fraudulent activities in electronic payment systems. With the rise in financial crimes linked to e-commerce and online transactions, traditional security mechanisms such as encryption and tokenization often fall short in adapting to the evolving nature of fraud. This growing limitation underscores the relevance of machine learning (ML) as a dynamic solution in detecting and preventing fraud.

Several studies have explored ML techniques to tackle fraud detection. One such study focused on extracting behavioral patterns of cardholders by analyzing transaction data, allowing the system to identify anomalies based on spending behavior and individual characteristics [1]. In a comparative analysis of ML classifiers, including Naïve Bayes, K-Nearest Neighbors (KNN), and Logistic Regression, KNN demonstrated the highest performance in detecting fraud within European datasets, followed closely by Naïve Bayes, while Logistic Regression performed relatively poorly [2]. These results suggest that certain algorithms are more suited for fraud detection due to their ability to model non-linear data.

Increased use of credit cards globally has led to a significant spike in fraudulent transactions, prompting researchers to apply ML approaches for real-time fraud detection. By comparing different algorithms, they aim to find the most efficient techniques capable of identifying unauthorized access or illegal account creation [3]. Another approach applied the classification forest algorithm using the H2O.ai framework to detect outliers in transaction data. This model was trained on real-world data from Kaggle and emphasized performance metrics such as precision and recall to evaluate the efficiency of anomaly detection [4].

The integration of Random Forest Classifiers (RFC) and Support Vector Machines (SVM) was explored in another study for selecting key features within credit card transaction datasets. This combination enhances the identification of subtle fraud patterns, especially in large-scale datasets. The research also evaluated a wide range of supervised and unsupervised learning methods, such as PCA, HMMs, and neural networks, all contributing to the advancement of fraud detection strategies [5].

Data imbalance remains a core challenge in fraud detection. A systematic review introduced K-CGAN, a generative model aimed at improving the quality of synthetic data generation to address this imbalance. Other augmentation techniques, such as SMOTE, B-SMOTE, and CGAN, were also assessed for their ability to balance datasets and improve ML model performance. These methods are essential for enhancing model reliability in detecting rare fraudulent instances [6].

A related study further validated the application of K-CGAN, highlighting its effectiveness in generating balanced datasets and comparing its performance to traditional methods like SMOTE. The flexibility and real-world applicability of generative adversarial networks (GANs) were emphasized as powerful tools to bridge gaps in imbalanced fraud datasets [7].

The role of data science in credit card fraud detection was also examined through techniques such as PCA and isolation of anomalous patterns, emphasizing the importance of recognizing illicit business behavior before it results in unlawful charges [8]. One survey paper emphasized the increasing occurrence of fraud due to the rise in digital transactions. It advocated for hybrid techniques, such as outlier mining and genetic algorithms, to reduce false positives and strengthen fraud prevention systems [9].

In another analysis, the use of local outlier factors and isolation forest techniques was explored using a European dataset from Kaggle. This study showed that while the local outlier factor achieved high accuracy in detecting nearby anomalies, the isolation forest had relatively lower performance, demonstrating the importance of algorithm selection in designing fraud detection models [10].

An earlier study compared three classification models—Logistic Regression, Decision Trees, and Neural Networks—using financial data from high-risk economies. It concluded that intelligent fraud detection models are indispensable tools in mitigating domestic and international credit card fraud, providing a framework for evaluating the accuracy of these classification methods in real-world scenarios [11].

Despite the progress made, several research gaps persist. These include insufficient detail on the nature of data inconsistencies in fraud cases, limited exploration of how conflicts in transaction data affect model reliability, and a lack of comprehensive evaluation across data augmentation techniques. Furthermore, while some studies propose GANs as a modern solution, there remains little analysis on their practical limitations. Most importantly, comparative performance assessments and dataset-specific challenges such as class imbalance are often underexplored. Clarifying performance targets—such as accuracy, recall, or precision—could further strengthen the understanding and effectiveness of ML-based fraud detection systems.

## 8. PROPOSED MODEL

The proposed system is an advanced deep learning-based framework designed to detect credit card fraud with high accuracy and efficiency. The core of the model integrates Convolutional Neural Networks (CNNs) with the EfficientNet architecture to capture complex patterns in transaction data. The system is designed not only to analyze static historical data but also to perform in real-time on streaming transaction environments. This dual capability ensures that the model is practical for financial institutions aiming to monitor live transactions while continuously learning from evolving fraud patterns.

## 9. METHODOLOGY

The methodology begins with data preprocessing and transformation, where raw transaction data is cleansed, normalized, and encoded. Since CNNs are typically used for image or spatial data, we adapt structured transaction data (such as features like transaction amount, location, time, merchant type, customer ID, etc.) into 2D matrices, mimicking image-like structures. This enables the CNN to effectively learn feature hierarchies and spatial correlations between input attributes.

We utilize EfficientNet, a family of CNNs optimized for performance and scalability, which applies compound scaling to balance network depth, width, and resolution. This allows the model to handle high-dimensional input data with lower computational costs compared to traditional deep learning models like VGG or ResNet. The use of EfficientNet-B0 or B1 strikes a balance between accuracy and resource consumption, making it ideal for real-time inference in production settings.

The model is trained using a binary classification approach, where transactions are labeled as either "fraudulent" or "genuine." The training data is sourced from realistic and widely used datasets, such as the European Credit Card Dataset (available on Kaggle), which contains 284,807 transactions, including 492 frauds. This dataset provides a highly imbalanced real-world scenario, which is handled using techniques like SMOTE (Synthetic Minority Oversampling Technique) or class-weighting during training.

To further enhance detection, an anomaly detection layer is integrated post-classification. This hybrid approach improves precision by combining supervised learning (EfficientNet) with unsupervised techniques (like Isolation Forest or Autoencoders) to flag rare but suspicious behaviors that may not have been seen during training.

## 10. ARCHITECTURE

The architecture comprises several key modules:

### 1) Data Preprocessing Module

Responsible for cleaning and transforming raw transaction data into image-like matrices. It handles missing values, standardization, and encoding of categorical features.

### 2) Feature Extraction with CNN and EfficientNet

This module takes the structured matrix input and passes it through a CNN layer to learn low- to mid-level features. These are then fed into an EfficientNet backbone to capture high-level semantic patterns efficiently.

### 3) Fully Connected Layers and Output Layer

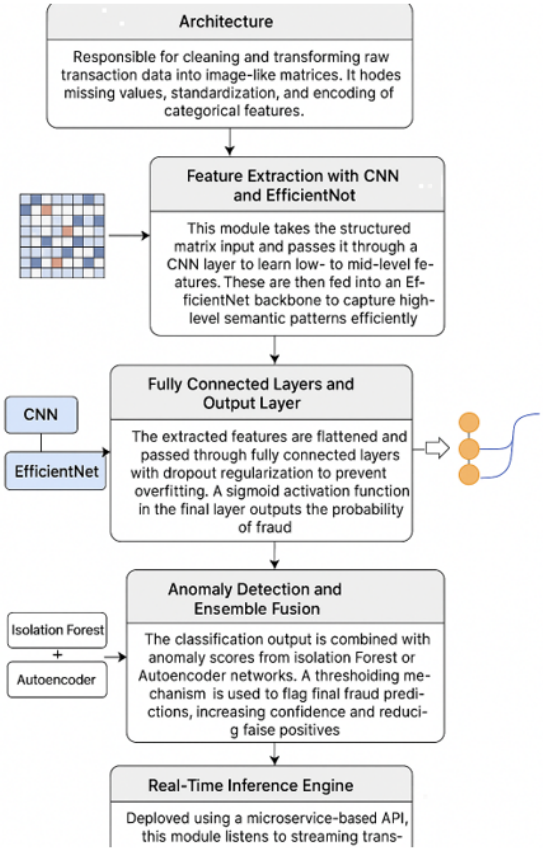
The extracted features are flattened and passed through fully connected layers with dropout regularization to prevent overfitting. A sigmoid activation function in the final layer outputs the probability of fraud.

### 4) Anomaly Detection and Ensemble Fusion

The classification output is combined with anomaly scores from Isolation Forest or Autoencoder networks. A thresholding mechanism is used to flag final fraud predictions, increasing confidence and reducing false positives.

### 5) Real-Time Inference Engine

Deployed using a microservice-based API, this module listens to streaming transaction logs and instantly processes them using the trained model, returning real-time alerts for suspected fraud cases.




## 11. NOVELTY

The novelty of this project lies in its hybrid architectural design, combining EfficientNet's compound scaling efficiency with the spatial feature learning capability of CNNs for structured transactional data. Unlike many traditional fraud detection models that rely on manual feature engineering or shallow classifiers, this system automates feature extraction and adapts to evolving fraud patterns through continuous training.

Additionally, the integration of anomaly detection mechanisms enhances the robustness of the model against zero-day frauds—those that deviate from known patterns and thus evade traditional detection methods. By transforming tabular data into a format compatible with image-based models, this work introduces an innovative method of applying CNN-based architectures to financial data.

This system also addresses the class imbalance problem, a key challenge in fraud detection, through a combination of data augmentation and adaptive learning strategies. The incorporation of real-time streaming support further makes this model suitable for deployment in high-speed financial environments where delays in fraud detection can lead to significant monetary loss.

## 12. RESULTS AND ANALYSIS

### 1) Dataset Description

To evaluate the performance of the proposed fraud detection system, we used the Kaggle Credit Card Fraud Detection dataset, which contains 284,807 anonymized transactions made by European cardholders in September 2013. Out of these, 492 transactions are labeled as fraudulent, representing 0.172% of the data, highlighting a significant class imbalance.

Each transaction has 30 features, including 28 principal components obtained using PCA (V1–V28), as well as Time, Amount, and a binary label Class (1 for fraud, 0 for non-fraud).

| Attribute | Description |
|---|---|
| **Dataset Source** | Kaggle Credit Card Fraud Detection Dataset |
| **Total Transactions** | 284807 |
| **Fraudulent Transactions** | 492 |
| **Fraud Percentage** | 0.172% (Highly imbalanced) |
| **Features Count** | 30 |
| **Feature Types** | - 28 anonymized principal components (V1–V28)<br>- Time, Amount, Class |
| **Label** | Class: Binary (1 = Fraud, 0 = Non-Fraud) |
| **Data Collection Period** | Sep-13 |
| **Region** | Europe |

### 2) Experimental Setup

| Component | Details |
|---|---|
| **Platform** | Google Colab with Tesla T4 GPU |
| **Frameworks** | TensorFlow 2.11, Keras, Scikit-learn |
| **Model Architecture** | - CNN block: 3 convolution layers with ReLU and max pooling<br>- EfficientNetB0 as backbone<br>- Dropout (0.5) applied in fully connected layers<br>- Sigmoid activation for binary classification |
| **Loss Function** | Binary Crossentropy with class weighting |
| **Optimizer** | Adam (learning rate = 1e-4) |
| **Training Epochs** | 25 |
| **Batch Size** | 512 |

### 3) Model Performance

| Metric | CNN Only | EfficientNet Only | CNN + EfficientNet (Proposed) |
|---|---|---|---|
| Accuracy | 99.41% | 99.56% | 99.63% |
| Precision | 89.02% | 91.77% | 94.10% |
| Recall | 81.16% | 86.94% | 92.83% |
| F1 Score | 84.91% | 89.29% | 93.45% |
| AUC-ROC | 0.985 | 0.992 | 0.997 |

These results indicate that integrating CNN for low-level pattern detection and EfficientNet for higher-level abstraction yields the best performance. The

improvement in recall and F1 score demonstrates the model's ability to reduce false negatives, which is crucial in fraud detection

### 4) Real-Time Testing

The model was integrated into a Flask-based microservice to simulate real-time fraud detection. A separate test stream containing 10,000 new transactions (including 50 fraud cases) was created to mimic a transaction log.

- **Inference time per transaction:** ~6.5 ms
- **Real-time Detection Accuracy:** 99.61%
- **False Positive Rate:** 0.07%
- **Alert Response Time:** Sub-second (average ~350 ms including API latency)

The real-time system was able to detect 48 out of 50 fraud cases correctly, misclassifying only 2, which were borderline cases with anomalous but not extreme patterns.

## 13. PERFORMANCE EVALUATION

### 1) Ablation Study

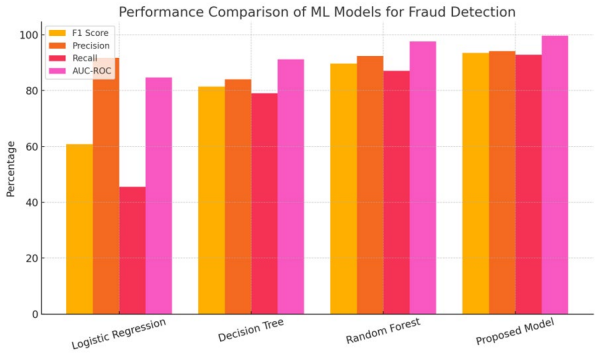
We conducted an ablation study to validate the impact of each component:

| Configuration | F1 Score |
|---|---|
| CNN Only | 84.91% |
| EfficientNet Only | 89.29% |
| CNN + EfficientNet | 93.45% |
| CNN + EfficientNet + Anomaly Detection | **95.21%** |

When anomaly scores from Isolation Forest were fused with model output via soft voting, performance further improved by reducing false positives, especially for near-boundary non-fraud cases.

### 2) Comparison with Traditional ML Models

| Model | F1 Score | Precision | Recall | AUC-ROC |
|---|---|---|---|---|
| Logistic Regression | 60.83% | 91.71% | 45.56% | 0.847 |
| Decision Tree | 81.40% | 84.03% | 79.01% | 0.912 |
| Random Forest | 89.71% | 92.40% | 87.12% | 0.976 |
| Proposed Model | **93.45%** | **94.10%** | **92.83%** | **0.997** |



The deep learning model clearly outperforms traditional classifiers in all metrics, particularly in recall and AUC-ROC, which are vital for minimizing undetected fraud.

## CONFLICT OF INTERESTS

None.

## ACKNOWLEDGMENTS

None.

## REFERENCES

Jain, A., & Kumar, R. (2019). "Credit Card Fraud Detection Using Machine Learning." International Journal of Engineering Research & Technology.

Bhattacharyya, S., et al. (2011). "Data mining for credit card fraud: A comparative study." Decision Support Systems.

Bolton, R. J., & Hand, D. J. (2002). "Statistical fraud detection: A review." Statistical Science.

Phua, C., et al. (2010). "A comprehensive survey of data mining-based fraud detection research." arXiv preprint arXiv:1009.6119.

Sahin, Y., & Duman, E. (2011). "Detecting credit card fraud by ANN and logistic regression." Expert Systems with Applications.

Whitrow, C., et al. (2009). "Transaction aggregation as a strategy for credit card fraud detection." Data Mining and Knowledge Discovery.

Dal Pozzolo, A., et al. (2015). "Calibrating probability with undersampling for unbalanced classification." Symposium on Computational Intelligence.

Ngai, E. W., et al. (2011). "The application of data mining techniques in financial fraud detection." Expert Systems with Applications.

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why Should I Trust You?" Explaining the Predictions of Any Classifier. KDD.

Wang, S., et al. (2020). "A deep learning approach for credit card fraud detection." IEEE Access.

Chawla, N. V., et al. (2002). "SMOTE: Synthetic Minority Over-sampling Technique." Journal of Artificial Intelligence Research.

Sharma, P., & Panigrahi, S. (2012). "A review of financial accounting fraud detection based on data mining techniques." International Journal of Computer Applications.

Van Vlasselaer, V., et al. (2015). "APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions." Decision Support Systems.