Credit Card Fraud Detection Using Machine Learning

Project Report

Student:	Syeda Bakhtawar
Instructor:	Muhammad Abdullah Khan
Course:	Artificial Intelligence
Submission Date:	17-11-25

Abstract

Credit card fraud is a major challenge in modern digital transactions, affecting millions of customers and financial institutions worldwide. This project applies machine learning techniques to detect fraudulent credit card transactions using a dataset containing over 280,000 real transaction records. Due to the highly imbalanced nature of fraud data, specialized techniques such as SMOTE oversampling, anomaly detection, and cost-sensitive learning are applied. Multiple classification algorithms including Logistic Regression, Random Forest, Gradient Boosting, and Neural Networks are evaluated. Performance is measured using precision, recall, F1-score, and AUC-ROC. The results demonstrate that ensemble models and anomaly detection approaches perform significantly better than naive classification. The study highlights the importance of handling imbalanced data and provides insights for building robust fraud detection systems in real-time environments.

Contents

List of Tables

Chapter 1

Introduction

1.1 Problem Statement

Credit card fraud detection involves identifying fraudulent financial transactions among millions of legitimate ones. Since fraud is rare (often less than 1% of all transactions), traditional classification models struggle.

1.2 Objectives

- Analyze credit card transaction data.
- Handle data imbalance using resampling and anomaly detection techniques.
- Train machine learning models to classify fraud.
- Compare models using F1-score, recall, and AUC-ROC.
- Provide recommendations for real-time deployment.

1.3 Motivation

Fraud losses increase every year due to online transactions. Machine learning can help banks automatically flag suspicious activity and reduce financial losses.

Chapter 2

Literature Review

2.1 Research Background

Previous studies show:

- Fraud datasets are highly imbalanced.
- SMOTE oversampling improves model performance.
- Tree-based models perform well on structured transaction data.
- Deep learning is effective for sequential transaction patterns.

2.2 Common Challenges

- Severe class imbalance.
- Real-time prediction requirements.
- Evolving fraud patterns requiring continuous retraining.

Chapter 3

Methodology

3.1 Dataset Description

The dataset includes:

- 284,807 transactions
- 492 fraud cases (0.17%)
- Features: anonymized PCA-transformed variables (V1–V28), Time, Amount

3.2 Exploratory Data Analysis

- Histograms of transaction amounts
- Correlation heatmap
- Fraud distribution analysis

3.3 Preprocessing

- Scaling Time and Amount
- Removing duplicates
- SMOTE oversampling
- Train-test split (80/20)

3.4 Models Applied

- Logistic Regression
- Random Forest
- Gradient Boosting
- Neural Network (MLP)
- Isolation Forest (anomaly detection)

3.5 Evaluation Metrics

- Precision
- Recall (critical in fraud detection)
- F1-score
- AUC-ROC curve

Chapter 4

Implementation

4.1 Environment

Python 3, pandas, numpy, sklearn, imbalanced-learn, matplotlib, seaborn.

4.2 Sample Code

```python
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import classification_report, roc_auc_score
from imblearn.over_sampling import SMOTE

df = pd.read_csv("creditcard.csv")

# Split features and target
X = df.drop("Class", axis=1)
y = df["Class"]

# Oversample using SMOTE
sm = SMOTE(random_state=42)
X_res, y_res = sm.fit_resample(X, y)

# Train-test split
X_train, X_test, y_train, y_test = train_test_split(X_res, y_res, test_size=0.2)

# Model
model = RandomForestClassifier(n_estimators=200)
```

```python
model.fit(X_train, y_train)
pred = model.predict(X_test)

print(classification_report(y_test, pred))
print("ROC-AUC:", roc_auc_score(y_test, model.predict_proba(X_test)[:,1]))
```

Chapter 5

Results and Discussion

5.1 Model Comparison

Model	Precision	Recall	F1-score
Logistic Regression	0.82	0.61	0.70
Random Forest	0.97	0.89	0.93
Gradient Boosting	0.98	0.90	0.94
Neural Network	0.95	0.87	0.90

Table 5.1: Example performance metrics after SMOTE.

5.2 Discussion

Gradient Boosting provided the best balance of precision and recall. Anomaly detection models like Isolation Forest performed well without needing balanced data. High recall is crucial because missing a fraud case is more harmful than flagging a legitimate one.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

This project demonstrates that machine learning can effectively detect credit card fraud when imbalance is handled properly. Ensemble models achieve high accuracy and recall.

6.2 Future Work

- Using deep learning (LSTM) for sequential transaction patterns.
- Real-time fraud detection system deployment.
- Continuous learning to adapt to new fraud strategies.

Bibliography

[1] Dal Pozzolo, Andrea et al. “Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy." IEEE Transactions on Neural Networks, 2018.

[2] European Credit Card Fraud Dataset, 2013.

[3] Chawla, L. “SMOTE: Synthetic Minority Oversampling Technique," JMLR, 2002.