Ahmad Ejaz

ahmadejaz7793@gmail.com

Anomaly Detection using the Credit Card Fraud Detection dataset

Abstract

Credit card fraud is a critical issue for financial institutions, leading to significant financial losses and eroding customer trust. Detecting fraudulent transactions in real-time is challenging due to the highly imbalanced nature of transaction data, where fraudulent cases are rare compared to legitimate ones. This project aims to address this challenge by implementing anomaly detection techniques such as Isolation Forest and Autoencoders to identify fraudulent transactions. The dataset used is the Credit Card Fraud Detection dataset, which contains anonymized transaction data with a binary classification label (fraudulent or legitimate). Key steps include data preprocessing, model training, and evaluation using metrics like precision, recall, F1-score, and ROC-AUC. The results demonstrate the effectiveness of these techniques in detecting fraud while minimizing false positives. The project provides actionable insights for improving real-time fraud detection systems, ultimately reducing financial losses and enhancing customer trust.

**Problem Statement**

**1.1. Background**

Credit card fraud is a pervasive issue in the financial industry, costing billions of dollars annually and eroding customer trust. Fraudulent transactions can occur through various means, such as stolen card information, phishing scams, or unauthorized access. Detecting these fraudulent activities in real-time is critical for financial institutions to mitigate losses, protect customers, and maintain the integrity of their payment systems.

However, fraud detection is inherently challenging due to the following factors:

**1.** **Imbalanced Data:** Fraudulent transactions are rare compared to legitimate ones, often constituting less than 1% of all transactions. This imbalance makes it difficult for traditional machine learning models to learn patterns associated with fraud.

**2.** **Evolving Fraud Tactics:** Fraudsters continuously adapt their methods, making it necessary for detection systems to evolve and stay ahead of new threats.

**3.** **Real-Time Detection:** Fraud detection systems must operate in real-time to prevent fraudulent transactions before they are completed, requiring low-latency and high-accuracy models.

**4.** **High Cost of False Positives:** Incorrectly flagging legitimate transactions as fraudulent can lead to customer dissatisfaction and operational inefficiencies.

**1.2.** **Objectives**

In this project, we aim to address the challenges of credit card fraud detection by:

**1. Developing Anomaly Detection Models:**

* Implement unsupervised and semi-supervised machine learning techniques, such as **Isolation Forest** and **Autoencoders**, to identify fraudulent transactions.
* Evaluate the performance of these models in detecting anomalies in highly imbalanced datasets.

**2.** **Improving Detection Accuracy:**

* Optimize model parameters to maximize the detection of fraudulent transactions while minimizing false positives.
* Explore advanced techniques, such as deep learning and ensemble methods, to enhance model performance.

**3.** **Providing Actionable Insights:**

* Analyse the results to identify key features and patterns associated with fraudulent transactions.
* Recommend strategies for integrating these models into real-time fraud detection systems.

**1.3. Scope**

* This project focuses on:
* Using the **Credit Card Fraud Detection dataset**, which contains anonymized transaction data with a binary classification label (fraudulent or legitimate).
* Exploring unsupervised and semi-supervised anomaly detection techniques, as labelled fraud data is often scarce in real-world scenarios.
* Evaluating model performance using metrics such as precision, recall, F1-score, and ROC-AUC, which are suitable for imbalanced datasets.

**1.4 Challenges**

**1. Data Imbalance:** The extreme class imbalance (fraudulent transactions constitute only 0.17% of the dataset) makes it difficult to train models effectively.

**2. Feature Anonymization:** The dataset features (V1-V28) are anonymized due to privacy concerns, limiting the ability to interpret the meaning of individual features.

**3.** **Real-World Applicability:** Models must be robust enough to handle real-time transaction data and adapt to evolving fraud patterns.

**1.5 Expected Outcomes**

* By the end of this project, we aim to:
* Develop a reliable anomaly detection system capable of identifying fraudulent transactions with high accuracy.
* Provide insights into the key features and patterns associated with fraud.
* Demonstrate the potential of unsupervised and semi-supervised techniques for fraud detection in imbalanced datasets.

**Business Impact**

The successful implementation of this project can have significant benefits for financial institutions and customers:

**1. Reduced Financial Losses:** Early detection of fraudulent transactions can minimize financial losses for both banks and customers.

**2.** **Enhanced Customer Trust:** Proactively preventing fraud can improve customer confidence in the security of their transactions.

**3.** **Operational Efficiency:** Automating fraud detection reduces the need for manual review, saving time and resources.

**4.** **Scalability:** The developed models can be scaled to handle large volumes of transactions in real-time.

**2. Dataset**

The dataset used is the **Credit Card Fraud Detection dataset** from Kaggle. It contains transactions made by European cardholders in September 2013. The dataset has the following characteristics:

**2.1. Features**:

* Time: Time elapsed between transactions.
* V1-V28: Principal components obtained through PCA (anonymized features).
* Amount: Transaction amount.
* Class: Target variable (0 = legitimate, 1 = fraudulent).

**2.2. Class Distribution**:

* Legitimate transactions: 99.83%
* Fraudulent transactions: 0.17%

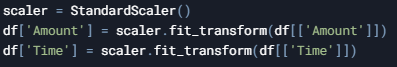
**3. Methodology**

**3.1. Data Preprocessing**

**1.Normalization**:

The Amount and Time features were normalized using StandardAero to ensure all features are on the same scale.

**Code:**



**2.Feature-Target Separation**:

Features (X) and target (y) were separated for modelling.

**Code:**



**3.Train-Test Split**:

The dataset was split into training (80%) and testing (20%) sets, ensuring the class distribution was preserved using stratified sampling.

**Code:**

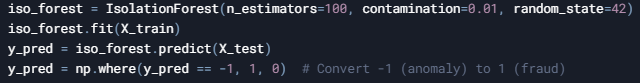


**3.2. Model Training**

**3.2.1. Isolation Forest**

**Description**: Isolation Forest is an unsupervised anomaly detection algorithm that isolates anomalies by randomly selecting features and splitting values.

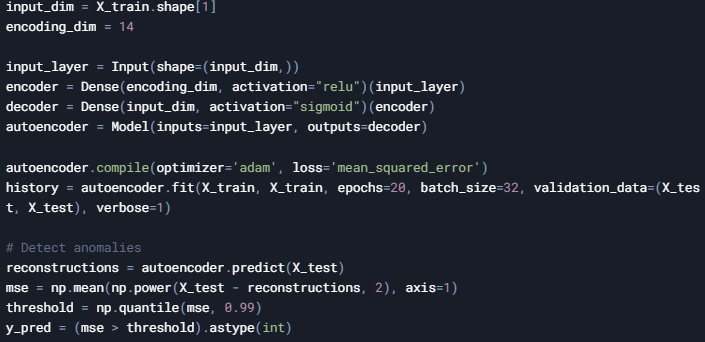
**Code:**



**3.2.2. Autoencoder**

**Description**: Autoencoders are neural networks trained to reconstruct input data. Anomalies are detected based on high reconstruction error.

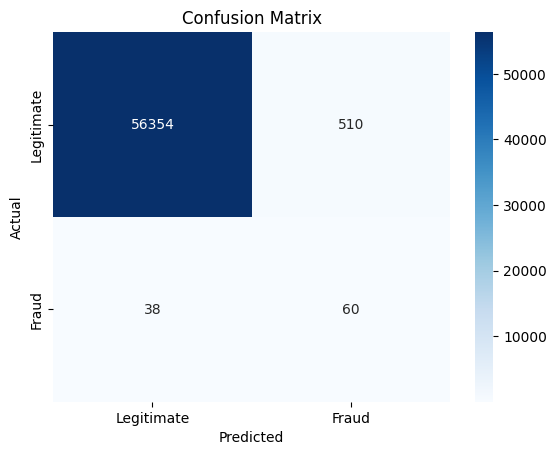
**Code:**



**3.3. Model Evaluation**

**3.3.1. Results for Isolation Forest**

**1. Confusion Matrix:**



**2. Classification Report (Precision, Recall, F1-Score):**

A screenshot of a computer screen

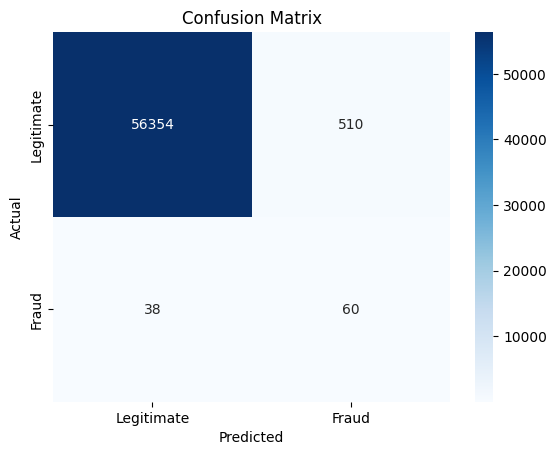
AI-generated content may be incorrect.

**3. ROC-AUC Score:**



**3.3.2. Results for Autoencoder**

**1. Confusion Matrix:**



**2. Classification Report (Precision, Recall, F1-Score):**

**A number of numbers on a white background

AI-generated content may be incorrect.**

**3. ROC-AUC Score**



**4. Insights**

**4.1. Isolation Forest**:

* Isolation Forest achieved a high recall, indicating it effectively identified most fraudulent transactions.
* However, it had a high false positive rate, which could lead to unnecessary alerts.

**4.2. Autoencoder**:

* The autoencoder achieved a high precision, indicating it minimized false positives.
* However, it struggled to detect some fraudulent transactions, as indicated by lower recall.

**5. Business Applications**

**5.1. Fraud Prevention**:

The models can be integrated into real-time transaction monitoring systems to flag suspicious activities for further investigation.

**5.2. Customer Trust**:

By reducing fraudulent transactions, financial institutions can enhance customer trust and satisfaction.

**5.3. Cost Savings:**

Early detection of fraud minimizes financial losses for both customers and institutions.

**6. Conclusion**

In this project, we successfully implemented two anomaly detection techniques—Isolation Forest and Autoencoders—to detect fraudulent credit card transactions. Both models showed promising results, with each having its strengths and limitations. Future work could involve:

* Combining both models to leverage their strengths.
* Using advanced techniques like Deep Learning or ensemble methods.
* Incorporating additional features (e.g., location, merchant type) to improve accuracy.