Credit Card Fraud Detection

Mikita Sirosh

Introduction

Credit card fraud is a significant problem in the financial industry, leading to substantial financial losses and undermining trust in electronic payment systems. Detecting fraudulent transactions is challenging due to the highly imbalanced nature of the data and the evolving tactics of fraudsters.

Problem Statement

The goal of this project is to accurately detect fraudulent credit card transactions using a dataset of real-world transactions. The main challenge is to identify as many fraudulent transactions as possible (high recall) while minimizing false alarms (high precision).

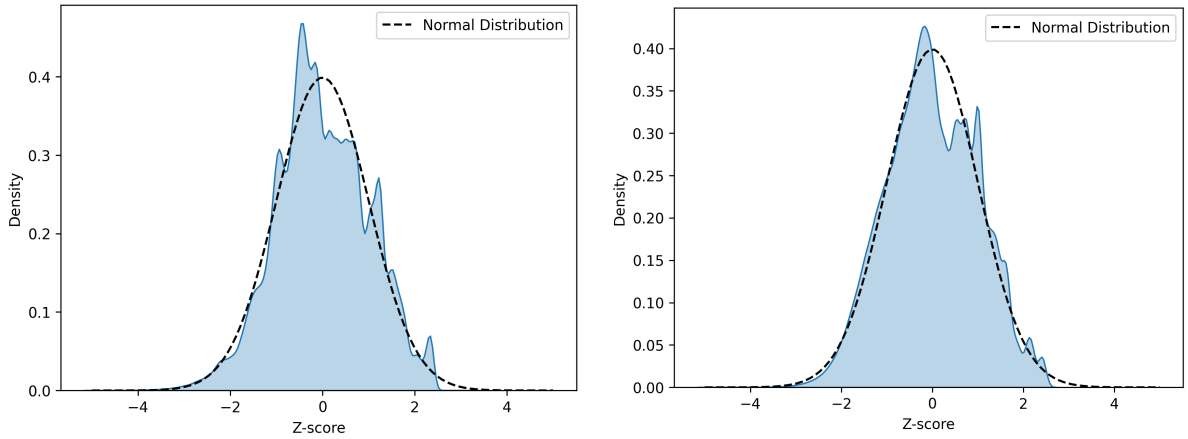
Solution Approach

The proposed solution leverages statistical methods, including normal distributions, the Central Limit Theorem (CLT), and Z-scores, to detect anomalies. The approach consists of the following steps:

1. **Data Acquisition:** The dataset is sourced from Kaggle and loaded into the analysis environment using pandas.
2. **Feature Engineering:** Features are standardized using the mean and standard deviation derived from normal transactions.
3. **Anomaly Scoring:** Each transaction is assigned an anomaly score based on the sum of absolute Z-scores across all features, with the CLT serving as the foundational theorem.
4. **Thresholding:** A threshold is established by determining the quantile of anomaly scores among fraudulent transactions, corresponding to the desired detection rate.
5. **Prediction:** Transactions with anomaly scores exceeding the threshold are flagged as fraudulent.
6. **Evaluation:** Key performance metrics – such as the number of frauds detected, missed frauds, false alarms, and precision – are calculated.
7. **Visualization:** Various plots are generated to illustrate the results and enhance interpretability.

Dataset Overview

The dataset used in this project comprises 28 anonymized numerical features, each representing distinct transaction attributes. These features are standardized, with most following an approximately normal distribution – a key characteristic that supports the statistical robustness of the fraud detection algorithm.



To illustrate the dataset's structure, the figures above display the Z-score distributions for two representative features, V4 and V11.

Evaluation

The following section presents the performance metrics of the algorithm, evaluated using an 85% fraud catch threshold. This threshold was selected to balance fraud detection effectiveness with operational feasibility.

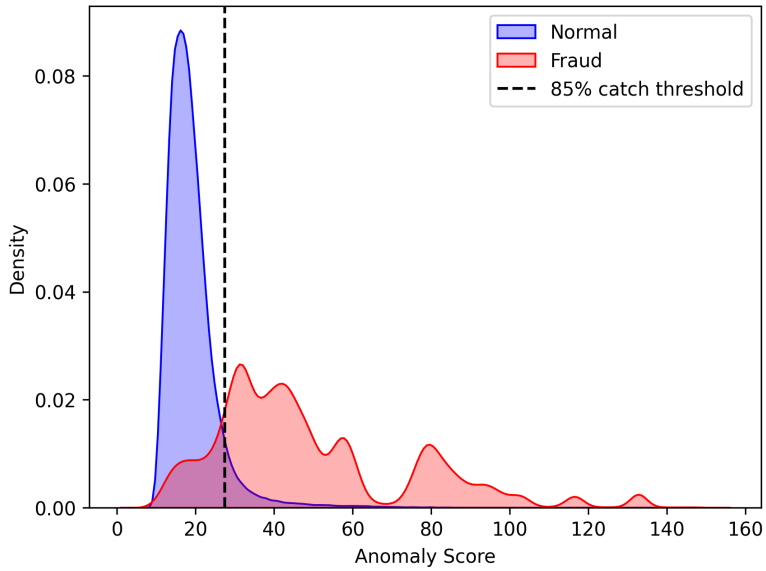
Metric	**Value**
Total Transactions	568 630
Normal Transactions	284 315
Fraud Transactions	284 315
Frauds Caught	241 667
Frauds Missed	42 648
False Positives	20 417
% of Frauds Caught	85.00%
Precision	92.21% (95% CI: 92.11% – 92.31%)

The algorithm demonstrates strong precision at 92.21%, indicating that when it flags a transaction as fraudulent, it is false positive 7.79% of the time. The 95% confidence interval (92.11% – 92.31%) confirms the stability of this performance.

Visualization

Distribution of Anomaly Scores

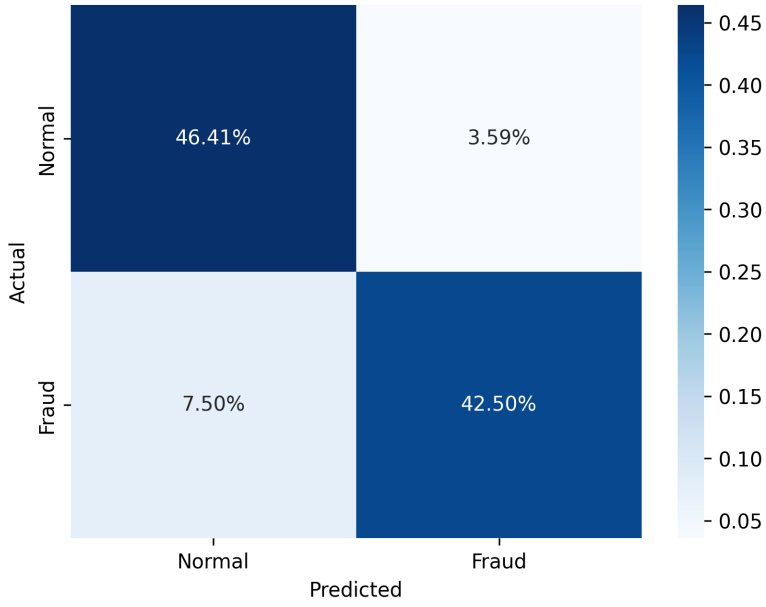
The figure below illustrates the distribution of anomaly scores for both normal and fraudulent transactions, along with the decision threshold (dashed line) used to classify transactions.



This visualization demonstrates that the algorithm's anomaly scores are clearly separated, making it straightforward to identify a "sweet spot" for classification.

Confusion Matrix

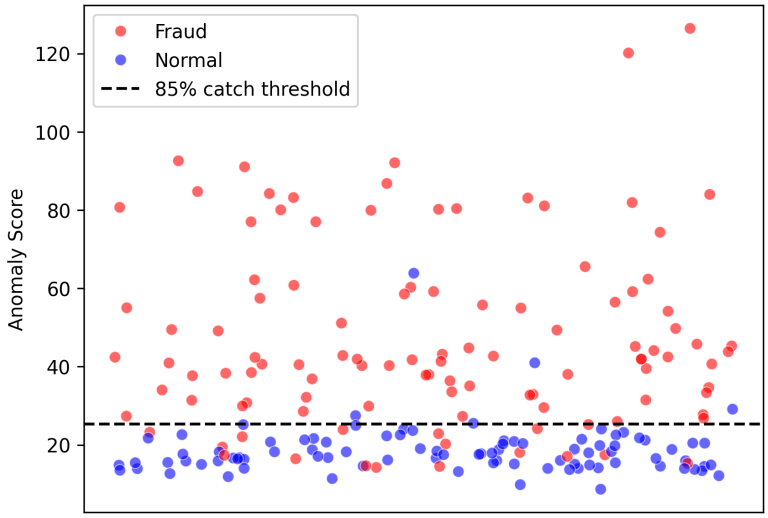
The confusion matrix below provides a detailed breakdown of our algorithm's classification performance, highlighting where mistakes most frequently occur:



It provides clear direction for model refinement, with particular attention needed to reduce missed fraud cases while maintaining reasonable precision.

Simulation

To validate fraud detection system, a simulation was conducted using 200 randomly selected transactions. The results demonstrate the algorithm's ability to distinguish between legitimate and fraudulent activity:



While we see some mistakes (outliers) in the results, the simulation clearly shows our system can reliably tell normal and fraudulent transactions apart in real-world scenarios.

Conclusion

This project demonstrates a proof-of-concept approach to detecting fraudulent credit card transactions using statistical anomaly detection techniques. By standardizing features and setting a threshold based on the desired recall, the method effectively identifies a significant portion of fraudulent transactions while maintaining reasonable precision. The solution prioritizes catching fraud (high recall) but remains adaptable for balancing precision based on business needs.

Source Code

The implementation, including setup instructions and technology stack, is available on GitHub.
Repository: github.com/nikijaz/sigma