Joanna Sierra-Mendoza

Professor Werner

Data Mining

25 May 2025

Improving Credit Card Security with Predictive Modeling

Credit card fraud is a growing concern in today’s digital world. With the rise of online transactions and the widespread use of credit cards, fraudulent activity has become prevalent. Detecting fraud effectively is crucial not only for financial institutions but for the consumers they serve. By developing accurate and efficient fraud detection machine-learning models, businesses can save significant amounts of money, prevent loss of trust, and ensure safer financial transactions.

This project aims to discover a way to detect credit card fraud by using machine learning to classify transactions as either fraudulent or legitimate. The importance of solving this problem lies in its potential to reduce financial losses and improve overall consumer confidence in credit card payment systems. Fraud detection solutions also support cost efficiency, regulatory compliance, and customer satisfaction. These outcomes make a strong case for investing in machine learning models that can proactively identify and stop fraud in the future.

The dataset used for this project was obtained from Kaggle. It contains anonymized transaction data, including a binary target variable indicating whether a transaction was fraudulent or not. The dataset includes features such as transaction amount and time, as well as twenty-eight anonymized principal components obtained through PCA for confidentiality purposes.

The first step of the project involved performing exploratory data analysis on the original dataset. During this phase, the class imbalance between non-fraud and fraud transactions became evident. Visualizations such as bar charts comparing class distributions and average transaction amounts helped highlight the differences between the two classes. One key insight is that the average transaction amount was higher for fraud cases compared to non-fraud ones, as shown in the bar chart below. A histogram of one of the unlabeled features, the V2 column specifically, revealed a sharp concentration of values near zero, with a few extreme outliers, as seen in the second image below. Observing this distribution helped to scale features and prepare for sensitivity to rare values when training the models, especially since the V columns were anonymized and required data-driven interpretation. Overall, statistical summaries were used to gain insight into the behavior of both fraud and non-fraud transactions.

A graph of a graph showing a number of different colored squares

AI-generated content may be incorrect.

A graph of a column

AI-generated content may be incorrect.

Following exploratory data analysis, the data was prepared by splitting it into training, testing, and validation sets. Dividing the data this way allowed for model training, performance evaluation, and final testing on previously unseen data. The training set was used to teach the model, the test set was used to adjust and compare performance, and the validation set helped simulate real-world applications. This type of split strengthens the model development process by reducing overfitting and improving performance stability across different data segments.

In the original imbalanced dataset, multiple models were trained and evaluated: logistic regression, random forest, gradient boosting, and a shallow neural network. These models varied in performance, with the validation metrics showing high accuracy but lower precision and recall for the fraud class, which is a common issue when dealing with imbalanced data. To better evaluate model performance in identifying fraud, the dataset was downsized and balanced by sampling an equal number of fraud and non-fraud transactions. The same machine learning models were re-applied to this balanced dataset, following the same training, testing, and validation split. By using a balanced dataset, each model could learn more effectively from the fraud class, which had previously been underrepresented.

Balanced Dataset Classification Report – ordered by f1-score

|  |  |  |  |
| --- | --- | --- | --- |
| **Non-Fraudulent Transactions** | Precision | Recall | f1-score |
| Logistic Regression | 0.89 | 0.97 | 0.93 |
| Random Forest | 0.86 | 1.00 | 0.92 |
| Shallow Neural Network | 0.87 | 0.97 | 0.90 |
| Gradient Boosting | 0.85 | 0.95 | 0.90 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Fraudulent Transactions** | Precision | Recall | f1-score |
| Logistic Regression | 0.97 | 0.89 | 0.93 |
| Random Forest | 1.00 | 0.84 | 0.92 |
| Shallow Neural Network | 0.93 | 0.88 | 0.90 |
| Gradient Boosting | 0.95 | 0.84 | 0.89 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Test Set with**  **Logistic Regression Model** | Precision | Recall | f1-score |
| Not Fraud | 0.94 | 0.97 | 0.96 |
| Fraud | 0.96 | 0.93 | 0.94 |

Performance comparisons on the balanced dataset included logistic regression, two shallow neural networks with different architectures, random forest, and gradient boosting classifier. Results on the validation set showed improved detection of fraud for all models. Among these, logistic regression demonstrated the most consistent and reliable performance in terms of precision, recall, and F1 score. It achieved 95% overall accuracy on the test dataset, with a precision of 96% and a recall of 93% for detecting fraud cases. The logistic regression model demonstrated strong performance in both fraudulent and non-fraudulent transactions. While models such as random forest and neural networks offered competitive results, logistic regression was selected for its simplicity and effectiveness.

Although promising, the model is not ready for production deployment. Further tuning and testing on real-world, imbalanced datasets is necessary. Additional enhancements such as synthetic sampling, cost-sensitive algorithms, or a mix of strategies could further boost performance. Continuous monitoring and updating will also be essential to adapt to evolving fraud patterns. Expanding the system into a fully automated fraud detection pipeline presents a valuable opportunity for future development.