Daniel Timmermann

Final Report:
Credit Card Fraud Detection

Objective
Build a model that could best predict credit card transactions as fraudulent or not.

Problem
While scrolling through my LinkedIn feed the other day I noticed one of my friends posted some material along with visualizations for fraud committed in 2020. Credit card fraud was not surprisingly among the top three types of identity theft.

Solution
My goal for this project was to build a model that could help decrease credit card fraud by predicting transactions correctly as fraudulent. Once the transactions are flagged then the credit card company can stop the transactions from going through and request verification before proceeding. Yes, this is a tedious process, but customer satisfaction and brand recognition will be greater in the long run for the credit card company.

Data Wrangling
The raw dataset from Worldline and the Machine Learning Group contained 284,807 rows with 31 columns. This dataset was created through principal component analysis so all the features should be numerical. I started by looking at the data types for all the features to verify they were numerical and they were. I also observed the summary statistics for all features such as minimum value, maximum value, standard deviation, average. This is where I first noticed the binary target variable was highly imbalanced with .1727% of the transactions labeled as fraudulent. I then went on to identify and remove 1,081 duplicates, so I ended with 283,726 rows.

Exploratory Data Analysis
I first verified features V1-V28 were normally distributed because this is the result of principal component analysis. I then computed the correlation matrix (Figure 1) to verify there was no correlation between features V1-V28 and discovered V14 and V17 (-0.293375 and -0.313498 respectively) had the highest correlation with the target variable. I explored the values in the 'Amount' column and discovered 75% of transactions were less than or equal to $77.51 and 7 transactions were greater than $10,000. Please see Figure 2 for a boxplot of the values in the 'Amount' column.

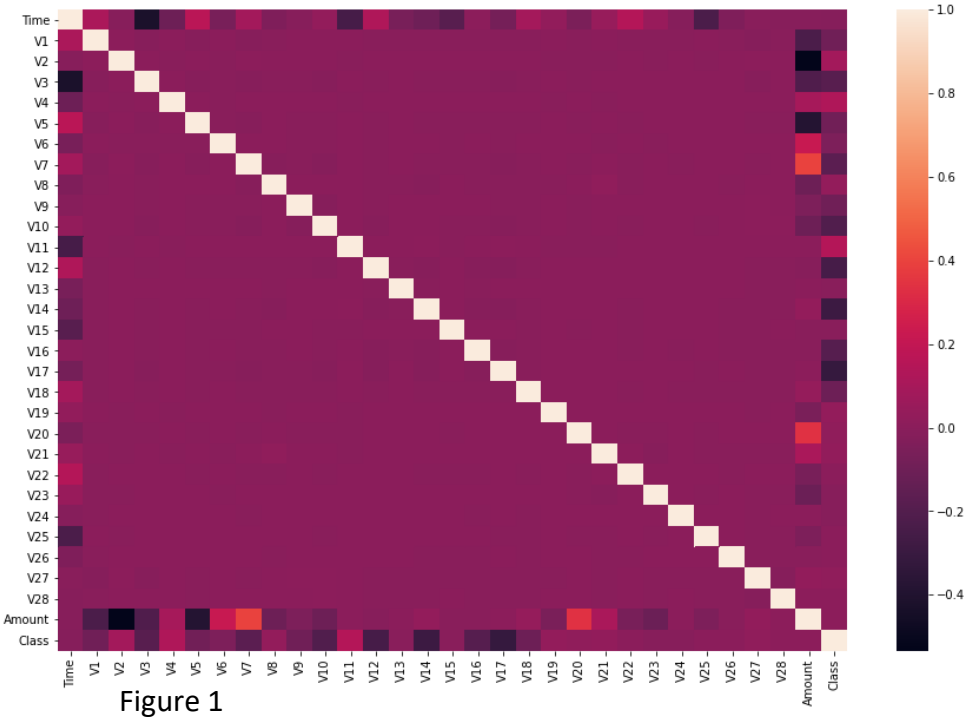

Figure 1

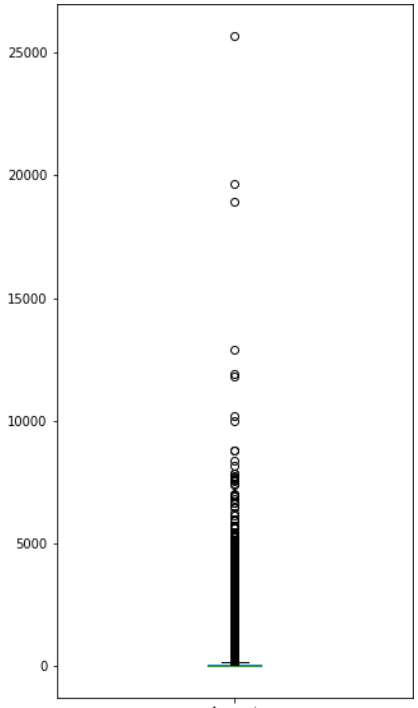

Figure 2

Data Preprocessing

Now with data exploration complete I moved on to preprocessing the data to prepare it for use in machine learning models. With the Time and Amount features having such a wide range of values compared to V1-V28, I first scaled all of the features. I standardized the features, meaning I subtracted the average of the values for each feature and then divided the values by the standard deviation for each feature.

Next I decided how I wanted to handle the highly imbalanced target class. I have 283,253 non-fraudulent and 473 fraudulent transactions. If I were to feed all of the data to the model, then the model will classify almost every if not all transactions as not fraudulent. I had to choose between the following three options: Random Undersampling, Random Oversampling, and Synthetic Minority Oversampling Technique (SMOTE). I decided to implement random undersampling which would collect a sample of 473 non-fraudulent transactions, so there would be an even amount of transactions identified as non-fraudulent to pass into the model. Now I am ready to split my 946 rows of data into training and testing sets.

Modeling

For the modeling step I choose to compare the performance of 3 models.

1. Logistic Regression

2. Random Forest
3. Support Vector Machine

I collected 5 random samples of data to feed into the logistic regression and support vector machine models and then I averaged the scores for each sample. The scores I compared were accuracy, precision, recall, and F1. Both logistic regression and support vector machine were implemented as is and I did not specify and parameters. For the random forest model, I used a grid search method with cross validation to tune the estimators, criterion, and max_depth parameters. Since I used cross validation with 5 folds, this meant I did not need to feed 5 random samples to the model. Every time the model was trained with a different 80% of the 1 random sample I fed to the model and a different 20% was used to test.

After running my models a few times, logistic regression was the clear winner. Figure 3 shows the models scores the first time I tested the models. Logistic regression typically performed better in every scoring category, but the score I wanted to focus on the most was recall. Recall is popular to score to focus on when tackling fraud. One thing you want to minimize with fraud is false negatives. Recall shows how well the model can identify fraudulent transactions without mislabeling transactions as not fraudulent. The impact from credit card fraud will be minimized, but if the model mislabels transactions as not fraudulent then credit card fraud will still be present.

Model	Accuracy	Precision	Recall	F1
Logistic Regression	0.9611	0.9735	0.9469	0.9599
Support Vector Machine	0.9474	0.9883	0.9040	0.9442
Random Forest	0.9421	0.9524	0.9195	0.9357

Figure 3

Final Model Review

Below is what I have concluded from the logistic regression model.

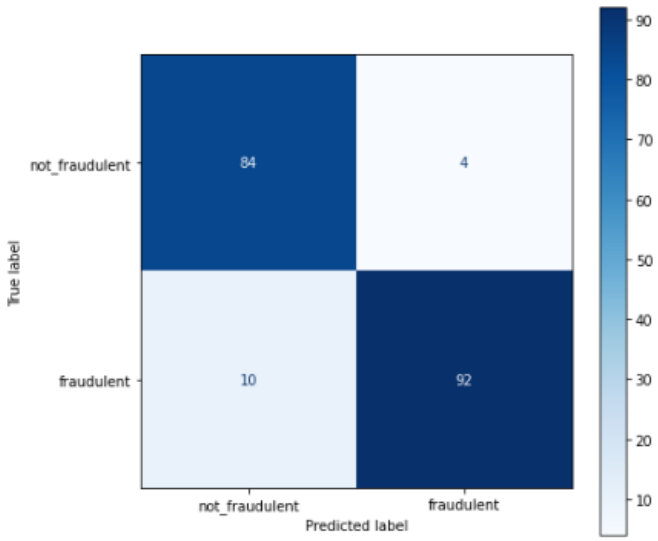

Figure 4

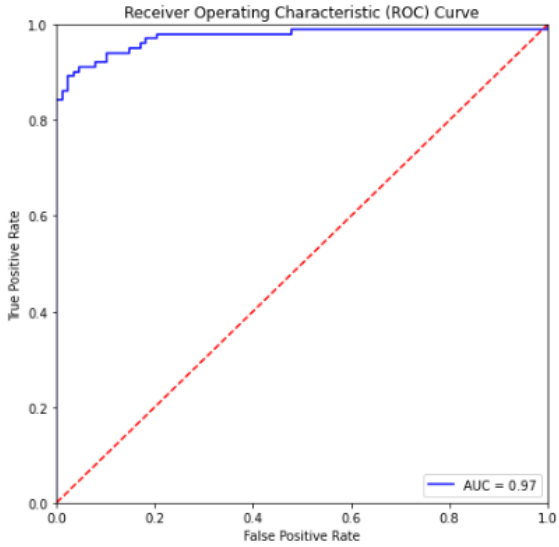

Figure 5

The confusion matrix, seen in Figure 4, can be used to calculate the precision, recall, accuracy, and f1-scores I mentioned before. The model misclassified 10 out of 102 fraudulent transactions. This is something that I would want to continue to improve given more data.

The receiver operating characteristic (ROC) curve, seen in Figure 5, is a visualization used to evaluate the "predictive power" of the model. A curve that is closer to the top left corner means the model has good predictive power. The red dashed line represents a model that has no predictive power. The AUC score in the bottom right corner is the area under the curve represented as a percentage. The higher the score the better the model. Based on the ROC curve and an AUC score of 97%, I can conclude the model has good predictive power.

Now that the overall performance of the model has been assessed I want to view the effect each predictor variable had on the target variable. I created a bar plot, seen in Figure 6, that would visualize the model coefficient for each feature. Later I will mention what can be done with this information to continue to improve the model.

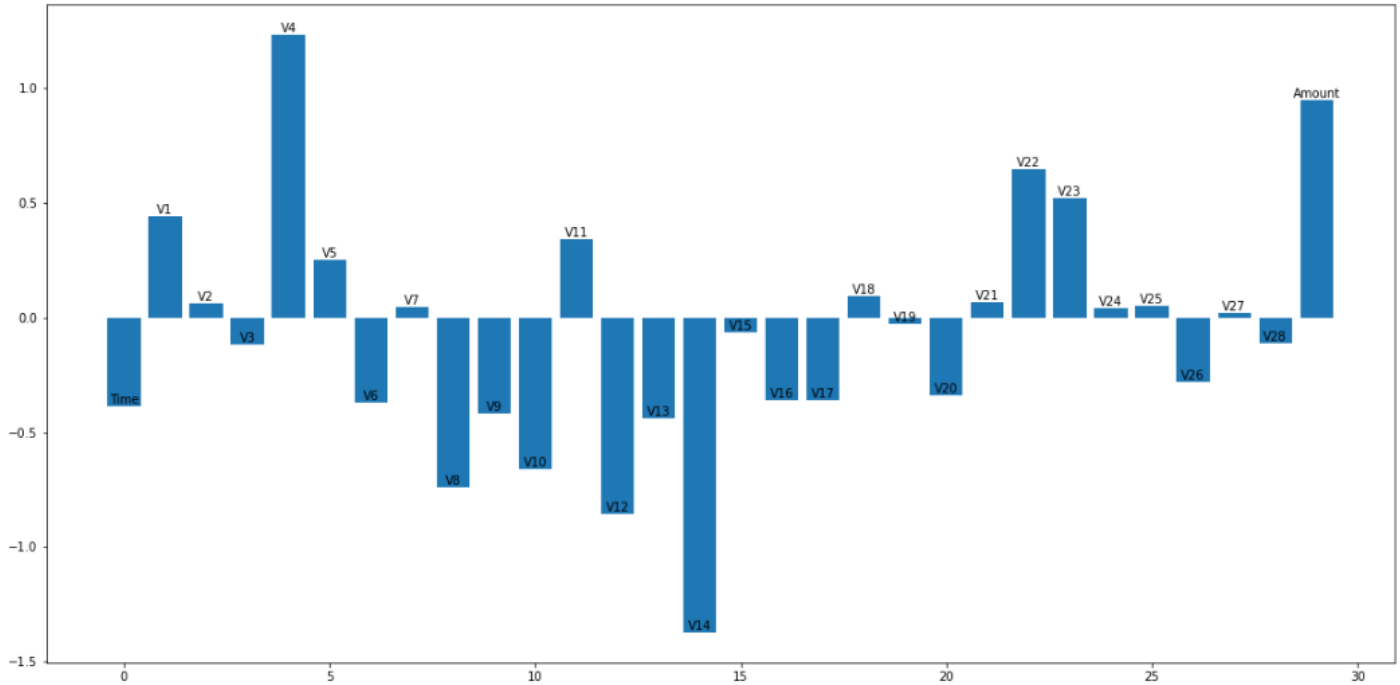

Figure 6

Next I wanted to visualize the decision boundary for this binary classification problem. It is very difficult to do with many features, so I implemented principal component analysis to reduce the features down to 2. Now my visualization for the decision boundary would be 2-dimensional with 473 rows of data and can be seen in Figure 7. Sadly, I do not know which features were kept, so it is difficult to have certain conclusions based on the visualization. I also visualized the decision boundary using the entire dataset to show that, without using an sampling technique

to combat the high class imbalance for the target variable, the model would almost always predict transactions as not fraudulent. This decision boundary can be seen in Figure 8.

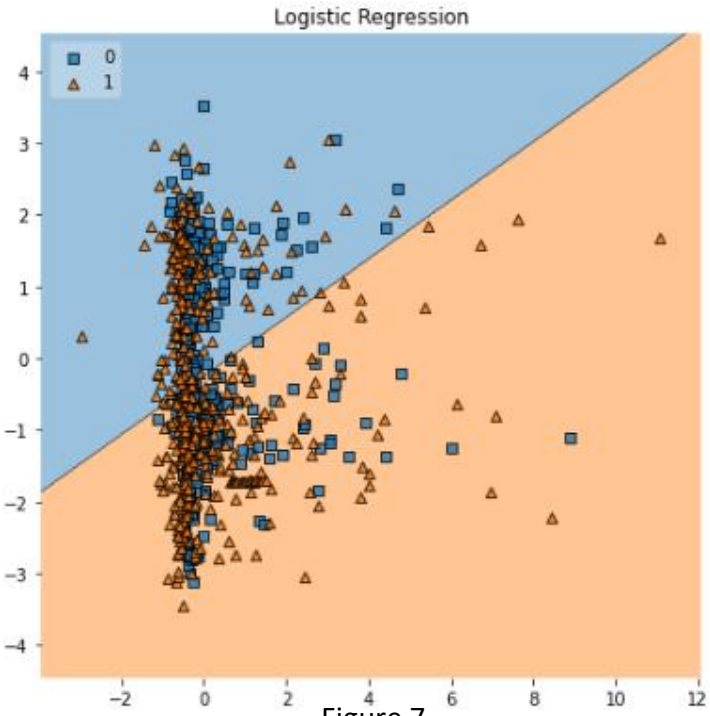

Figure 7

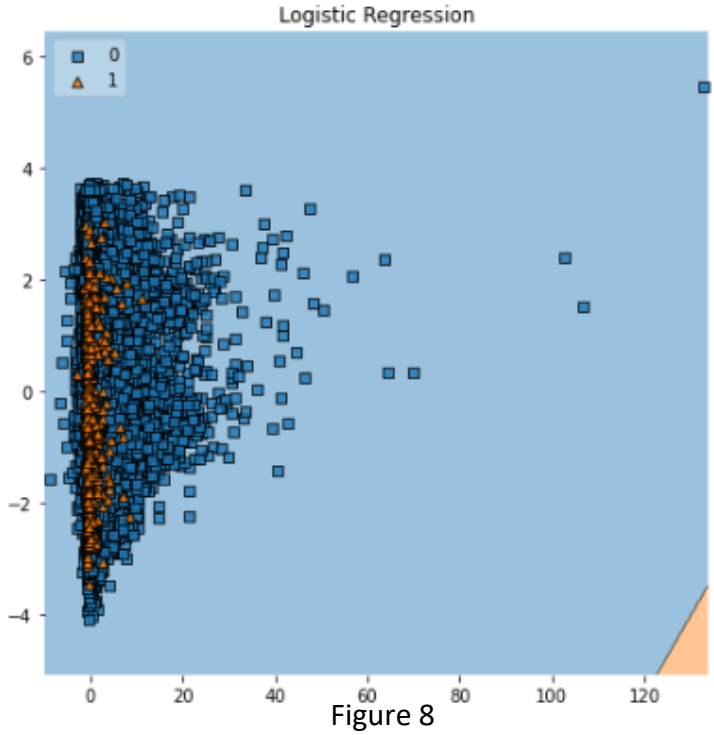

Figure 8

Takeaways and Future Research

As mentioned before, the logistic regression and support vector machine models were used with default parameters. It would be interesting to test and see how all three models compared if I were to do more tuning of the parameters and to include more values in the grid to search from for the random forest model.

Another process that can be attempted to improve model results would be to try out other sampling methods such as random oversampling and synthetic minority oversampling technique.

Lastly, I would like to add more reason to my choice for logistic regression in this project. Logistic regression is the least complex computationally, it would be the easiest to explain to interested stakeholders, and the simplest model to deploy in a business environment.