Machine Learning Engineer Nanodegree

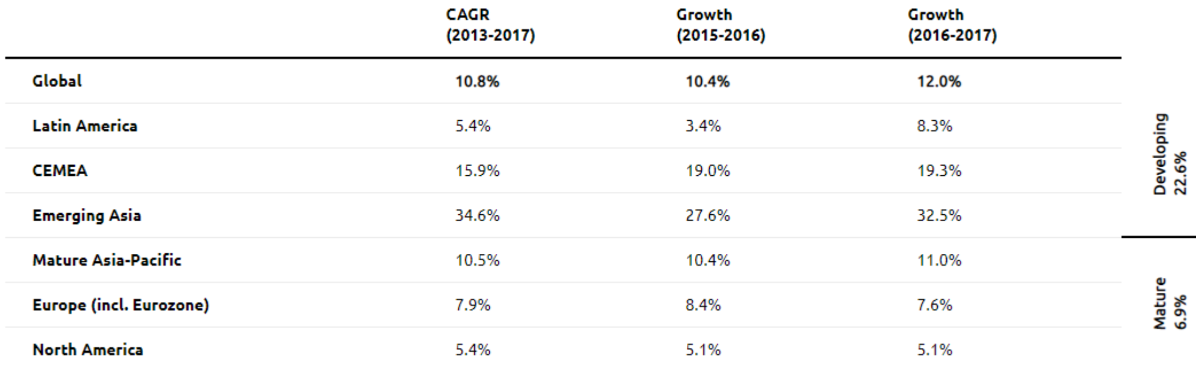
Capstone Proposal

Georgiana Popovici February 10th, 2020

Proposal – Credit Card Fraud Detection

Domain Background

Society's reliance on cash payments has significantly reduced with the growth of contactless payment systems. According to the World Payments Report Global[1], non-cash transaction grew at 12% to reach 539 billion transactions during 2016-2017 and it's expected that in future years there will be a steady growth of non-cash transactions as shown below:



	CAGR (2013-2017)	Growth (2015-2016)	Growth (2016-2017)	
Global	**10.8%**	**10.4%**	**12.0%**	
Latin America	5.4%	3.4%	8.3%	**Developing 22.6%**
CEMEA	15.9%	19.0%	19.3%	
Emerging Asia	34.6%	27.6%	32.5%	
Mature Asia-Pacific	10.5%	10.4%	11.0%	**Mature 6.9%**
Europe (incl. Eurozone)	7.9%	8.4%	7.6%	
North America	5.4%	5.1%	5.1%	

Now, while this might be exciting news, on the other side, fraudulent transactions are on the rise as well.

Fraud[2] is one of the major ethical issues in the credit card industry and it is vital that credit card companies are able to identify fraudulent credit card transactions so that customers are not charged for items that they did not purchase. Depending on the type of fraud faced[3] by banks or credit card companies, various measures can be adopted and implemented.

Problem Statement

Detecting unauthorized credit card transactions is an extremely complex problem, as features are seldom useful if taken individually. The Credit Card Fraud Detection Problem includes modelling past credit card transactions with the knowledge of the ones that turned out to be fraud. This model is then used to identify whether a new transaction is fraudulent or not. The purpose here is to detect 100% of the fraudulent transactions while minimizing the incorrect fraud classifications.

Datasets and Inputs

I have collected my data from a Kaggle dataset[4] which contained 285,000 rows of data and 31 columns, where the most important ones were Time, Amount, and Class (fraud or not fraud). This

[1] https://worldpaymentsreport.com/non-cash-payments-volume/

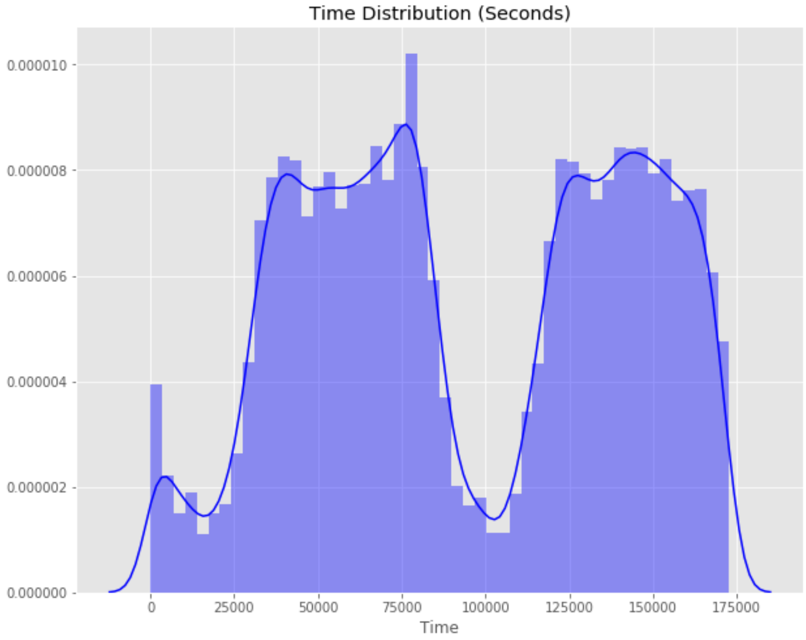
[2] Credit Card Fraud Detection using Machine Learning and Data Science - published by International Journal of Engineering Research & Technology (IJERT)

3 Credit card fraud and detection techniques: a review – published by Linda Delamaire (UK), Hussein Abdou (UK), John Pointon (UK)

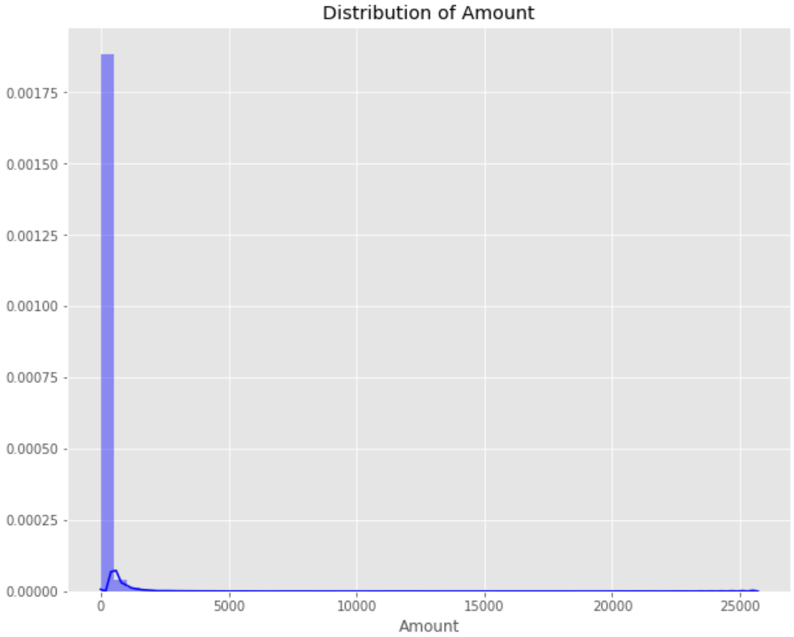
[4] https://www.kaggle.com/mlg-ulb/creditcardfraud

dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced, the positive class (frauds) account for 0.172% of all transactions. The dataset contains only numerical input variables which are the result of a Principal Component Analysis (PCA) transformation.

Feature 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset.



The feature 'Amount' is the transaction Amount, this feature can be used for example-dependant cost-sensitive learning. Feature 'Class' is the response variable and it takes value 1 in case of fraud and 0 otherwise.



Solution

Attempts have been made to improve the alert feedback interaction in case of fraudulent transaction. In case of fraudulent transaction, the authorised system would be alerted and a feedback would be sent to deny the ongoing transaction.

Artificial Neural Network [5]countered fraud from a different direction. It proved accurate in finding out the fraudulent transactions and minimizing the number of false alerts. Traditionally the use of ANN for fraud detection is done using the generated network as a classifier. With this approach, the network is trained with examples of fraudulent and non-fraudulent actions. Once trained, the ANN is able to classify new data as fraudulent or non-fraudulent activities.

Benchmark Model

I will provide a random classifier to compare the scores which should improve as more advanced techniques are introduced. The random classifier will set the worst score benchmark. Later, I will discuss the final scores and plot them using the ROC curve.

Evaluation Metrics

Accuracy is one metric for evaluating classification models. It is the fraction of predictions the model gets right. While accuracy might seem to be a good metric to measure how well a model performs, there is a huge downside when using it in this unbalanced dataset. Since over 99% of the transactions are non-fraudulent, an algorithm that always predicts that the transaction is non-fraudulent would achieve accuracy higher than 99% and it is desirable to obtain the opposite.

Accuracy = (TP + TN) / (TP + TN + FN + FP)

Precision[6] also known as detection rate is the number of transactions either genuine or fraudulent that were correctly classified.

Precision = TP / (TP + FP)

Recall represents the True Positive Rate off all fraudulent transactions cases captured.

Recall = TP / (TP + FN)

The F1 score[7] combines Recall and Precision into one metric as a weighted average of the two. Moreover, F1 takes both false positives and false negatives into consideration**.** In imbalanced classes such as this, F1 is much more effective than accuracy at determining the performance of the model.

F1- Measure = 2 X ((Precision × Recall) / (Precision + Recall))

Project Design

This section will cover the creation of a training data set that will allow the algorithms to pick up the specific characteristics that make a transaction more or less likely to be fraudulent. I have decided to split my data into 60% train, 20% validation, 20% test before creating any models. Since all fraudulent transactions follow a similar pattern, they can be classified considering the following algorithms:

Logistic Regression[8] is a supervised learning technique that is used when the decision is categorical. This means that the result will be either 'fraud' or 'non-fraud' if a transaction occurs.

Decision Tree algorithms in fraud detection are used where there is a need for the classification of unusual activities in a transaction from an authorized user. These algorithms consist of constraints that are trained on the dataset for classifying fraud transactions.

Random Forest uses a combination of decision trees to improve the results. Each decision tree checks for different conditions. They are trained on random datasets and, based on the training

[5] Neural Network Predictor for Fraud Detection: A Study Case for the Federal Patrimony Department by Antonio Serrano(1,2), Lustosa da Costa(1), Carlos Cardonha(3),

[6] "A Comparative Analysis of Various Credit Card Fraud Detection Techniques" Publication - International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-5S2, January 2019

[7] https://towardsdatascience.com/credit-card-fraud-detection-a1c7e1b75f59

[8] https://intellipaat.com/blog/fraud-detection-machine-learning-algorithms/

of the decision tree, where each tree gives the probability of the transaction being 'fraud' and 'non-fraud.' Then, the model predicts the result accordingly.

Isolation Forest[9] is one of the newest techniques and it is an unsupervised learning algorithm for anomaly detection that isolates observations by randomly selecting a feature and then randomly selecting a split value between the maximum and minimum values of the selected feature. Isolating anomaly observations is easier because only a few conditions are needed to separate those cases from the normal observations.

In order to compare these techniques, I will calculate the True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) generated by the above algorithms and use these in quantitative measurements to evaluate and compare their performance.

- True Positive (TP) is number of transactions that were fraudulent and were also classified as fraudulent by the system.
- True Negative (TN) is number of transactions that were legitimate and were also classified as legitimate.
- False Positive (FP) is number of transactions that were legitimate but were wrongly classified as fraudulent transactions.
- False Negative (FN) is number of transactions that were fraudulent but were wrongly classified as legitimate transactions by the system.

The last step would be to print out the model results and the conclusions.

[9] https://en.wikipedia.org/wiki/Isolation_forest