Abstract

Each year organizations lose 5% of revenues to fraud as highlighted in 2014 ACFE (Association of certified fraud examiners) report resulting into nearly $3.7 trillion global fraud loss if applied to 2013 estimated Gross World Product. For the year ending March 2016, 5.8 million incidents of computer misuse and fraud were reported in the Crime Survey of England and Wales (CSEW) wherein the victims were adults aged 16. Similarly, the total losses from online payment fraud for this year are estimated to be $22 billion and could go as high as $48 billion according to a study conducted by Juniper Research. Moreover, as money has evolved over time, financial payment services have a great role to play in moving money around the economy. Therefore, financial institutions need to adapt, to build brand loyalty among consumers who have more options than before to satisfy their financial needs by delivering a safe and seamless user experience. In this data-driven world, one of the ways to tackle this problem is through the application of machine learning techniques in the area of fraud detection. Thus, this project will investigate into the data mining based approach to predict and manage fraud in financial payment services.

This project aims to critically analyze the data of transactions (Cash-In, Cash-Out, Debit, Payment and Transfer) which consists of both normal as well as fraudulent customer behavior in order to build a Classification model that accurately categorize the transactions into fraudulent and genuine categories in the presence of imbalanced data. Consequently, deploying machine learning model as a tool to predict and detect fraud will improve the risk assessment capabilities of the organizations by dynamically conducting fund-flow analytics in real-time which further improve their reputation and customer loyalty.

The two statistical and two ensemble machine learning techniques such as Logistic Regression, Naïve Bayes, Random Forest and Extreme Gradient Boosting algorithms have been experimented with to find the best machine learning algorithm for the problem in question. These techniques have been explained in detail in this project along with detailed data exploration and feature engineering to aid fraud detection research in the field of financial payment services. The results achieved by exploring these supervised classification models were then presented and evaluated using test data on all type of transactions as well as using test data only on fraudulent transactions to conclude with a model which is a best classifier of accurately predicting and classifying the transactions to fraudulent and genuine ones.

The final model suggested to deploy is XGBoost classifier with 96.46% accuracy and low false positives as well as low false negatives which means that the model is capable enough not to treat most of the genuine transactions as fraudulent and real threats won’t be missed out in the form of mistreated fraudulent cases. Furthermore, future work has been discussed followed by limitations and challenges in conducting this study to improve model accuracy in the future.