**An Analysis of Classification Algorithms for Credit Card Fraud Detection**

**STUDENT NAME:** Gearoid Lacey

**STUDENT NUMBER:** C00183380

**COURSE NAME:** Masters in Data Science

**SUBJECT:** Data Analytics

**DEPARTMENT:** Department of Computing and Networking

**COURSE CODE:** CWS07

**DATE OF SUBMISSION:**

Table of Contents

[**Literature Review** 4](#_Toc506999175)

# **Literature Review**

Advances in computing and networking have led to a rise in the occurrence of credit card fraud (Quah and Sriganesh, 2008). The author notes that the increase in online banking and online shopping has also led to the increase in credit card fraud. According to the Banking & Payments Federation of Ireland (BPFI) the total number of online and mobile banking payments in 2014 was approximately 64 million (Banking & Payments Federation of Ireland, 2015).

There are numerous ways fraud can be implemented. One instance where fraud can occur is through the use of social engineering (Atkins and Huang, 2013). Social engineering is the process of manipulating individuals into performing certain actions through deceit. Social engineering can take form in a number of different approaches such as emails ,which on first sight appear to have legitimate credentials and therefore the victim trusts this and enters the required information. The exploitation can also occur through phone calls where the fraudster claims to be someone else generally from a large reputable organisation and ascertains the victims information that way.

Another way credit card fraud can occur is through counterfeit cards (Ghosh and Reilly, 1994). The authors notes that due to the difficulty in counterfeiting credit cards, this approach is more systematic. Another systematic approach documented by the authors is fraudulent applications for credit cards where the fraudster gains access to the victim personal details and requests a credit card using his/her details.

Many financial institutions now use data mining and machine learning to assist there existing measures for fraud the detection. (Ghosh and Reilly, 1994) state that financial institutions have, in the past, detected fraud simply by noting discrepancies in the fraudsters handwriting. In cases where the fraudster has access to a credit card these institutions rely on spotting transaction irregularities. Due to the increasing usage of online banking and payments as outlined previously, these financial institutions rely heavily on machine learning algorithms to alert them to any unusual transactions patterns.

(Ghosh and Reilly, 1994) designed a system which uses a P-RCE Artificial Neural Network (ANN) to classify fraudulent accounts for Mellon Bank. This ANN is a three layer feed forward neural network that makes two passes of the training data and then produces a fraud score.

Their system combined 50 variables to produce 20 features that were then passed to the ANN for account classification. As there were fewer fraudulent transactions than valid transactions, the authors ensure that all fraudulent transactions were included in the sample for training the ANN. When tested using two million transactions, the system vastly improved the fraud detection measures currently in place in Mellon Bank by only requiring a review of 50 accounts per day as opposed to reviewing 750.

Although fraudulent accounts and transactions can largely be classified by data mining and machine learning techniques, there is still a requirement for human verification (Quah and Sriganesh, 2008). Instead of reviewing hundreds or thousands of accounts of transactions, banking personnel only need to verify the accounts or transactions that are flagged as fraudulent by their data mining or machine learning model making the whole process more efficient.

(Quah and Sriganesh, 2008) outline a system for real time fraud detection that uses a neural network to cluster accounts as genuine or fraudulent. In essence the authors have implemented a clustering algorithm such as K Nearest Neighbour (KNN) using a form of ANN that allows for more dynamic relationships in the data.

(Ao and International Association of Engineers, 2011) provide an analysis of three machine learning algorithms for fraud detection. The algorithms analysed are Naïve Bayes, KNN and Logistic Regression (LR). The study was carried out on a dataset with approximately 280,000 transactions that was highly unbalanced. It is worth noting that the KNN algorithm was only .3% less accurate than Naïve Bayes. As the authors used several other methods to evaluate the effectiveness of each algorithm, KNN was actually the optimal algorithm. Noticeably LR provided quite a poor classification accuracy of approximately 54%.

Similarly (Shen et. al, 2007) provide an analysis of three machine learning algorithms for credit card fraud detection. In contrast to the study done by (Ao and International Association of Engineers, 2011), the authors analyse decision trees, neural networks and LR also. In this study neural networks provided the best performance followed by LR and decision trees. Again, the dataset in this study suffers from a highly unbalanced set of classifications as only 0.07% of the training data was labelled as fraudulent.

(Duman et. al, 2013) developed a fraud detection system for a Turkish bank which detects 97% of fraudulent transactions. In addition to the previously mentioned studies, this too suffered from highly unbalanced data where the authors had 978 fraudulent transactions and 22 million valid transactions. Therefore, the authors had to use a stratified sample of the data that included all the fraudulent transactions and only a fraction of the valid transactions. The authors tested multiple existing data mining algorithms as well as some ensembles of these algorithms to determine the best solution for fraud detection. From this analysis, the authors determined that the Migrating Birds Optimisation algorithm was the best option.