# 

# **ESOF 0151 - Large Scale Data Analytics**

# **Date Submitted: October 12th, 2020**

# **Project Progress Report: Stage 2**

# **Contributing Members:**

# **David Adese, Lucas Dillistone, Kevin Genereux**

**Introduction**

The rapid growth of the e-commerce industry has contributed to the exponential increase in online transactions and consequently the surge in fraudulent online activity [1]. Large e-commerce companies are investing significant amounts of resources into detecting fraudulent online activity to prevent a decrease in revenues, legal repercussions, and a loss of reputation. In 2015, the global credit card fraud reached USD $21.84 billion [2]. Machine learning algorithms allow us to extract useful patterns from large datasets that are not easily discernible by humans. This project will explore an automated system for detecting fraudulent online transactions using unsupervised learning classifiers: Artificial Neural Network (ANN), AdaBoost, XGBoost, LightGBM, and a Majority Voting Ensemble Classifier.

Fraudulent transactions are described as being transactions unauthorized by the cardholder or the intentional misrepresentation of some information [3]. Some examples of fraudulent transactions include gaining access to the pin code of the cardholder or vendors charging the user more money for a product than what was agreed upon. During transactions, the merchant provides their card number, card expiration date, and card verification number. Credit card fraud can be accomplished through either physical or digital means. In physical transactions, the credit card is directly involved during the transaction. Most fraudsters complete transactions digitally over the phone or the internet to conceal their identity. When credit card companies lose money due to fraudulent transactions, the cardholder is considered partially (sometimes entirely) responsible for the loss through higher interest rates or reduced benefits. As a result, it is in the best interest of both cardholders and credit card companies to reduce the illegitimate use of credit cards [3].

Designing fraudulent detection models is a complicated task as most related datasets are severely imbalanced with only a small percentage of the transactions being fraudulent. Hence, it becomes important to incorporate undersampling the majority class (fraud transaction) or oversampling the minority class (non-fraud transaction). Transaction datasets typically contain lots of features which makes feature engineering selection (PCA, LDA, correlation analysis, etc.) crucial in reducing model complexity and enhancing overall model performance. In addition, detecting fraudulent transactions is a challenging issue as perpetrators are constantly evolving their fraudulent transaction behaviour to circumvent detection systems. As a result, it is important to develop unsupervised classifiers that extract anomalous patterns in new transactions rather than supervised classifiers that train models entirely based on historical, labelled transactional data.

**Literature Review**

Although automating fraud detection has been extensively researched within the financial industry, there exists limited research on the topic that is publicly available. This is primarily because financial institutions, such as credit card companies, do not want to expose the confidentiality of their customers’ financial data nor the details of their proprietary detection mechanisms to fraudsters [4].

Traditional Classifiers

For credit card fraud detection, *Randhawa et al* [5] used three common supervised learning approaches: Random Forest (RF), Support Vector Machine (SVM), and Logistic Regression (LR). The dataset consisted of one-year transactions where Principal Component Analysis (PCA) was used for feature selection and data under-sampling was used to handle the imbalanced dataset. Their SVM model achieved an AUC score of 0.9503 while their RF model achieved an AUC score of 0.9489. Their results could be improved upon by training their models on a larger dataset as their dataset was relatively small and consisted of only 97,238 transactions from European cardholders. *Marella et al* [6] focused on applying outlier detection strategies, such as Decision Trees, Random Forest, Support Vector Machine (SVM) and KNN to detect fraudulent transactions. On the other hand, *Marella et al* [6] used Linear Discriminant Analysis (LDA) and a correlation matrix to empirically determine the importance of each feature. Their top performing model was RF as it achieved an AUC score of 0.9821. *Bhattacharyya et al* [7]*.* also used RF, SVM, and LR to identify fraudulent transactions. Their research emphasizes the significance of aggregating transaction level behaviour into various groups, such as by Customer ID. An important observation was that only 0.2% of customers within the dataset contain a mix of fraudulent and non-fraudulent transactions. As a result, these researchers considered all transactions to be fraudulent if only one transaction was predicted as fraudulent. Throughout our literature reviews, RF has consistently demonstrated improved performances in comparison to other traditional techniques as [5-7] have shown it to be amongst their highest performing models.

Bayesian Classifiers

According to *Yee et al* [8]*,* Bayesian classifiers are a popular fraud detection technique among researchers due to their demonstrated effectiveness in detecting fraudulence in real-world financial data. In fact, *Maes et al* [3] have determined that their Bayesian Belief Network was capable of detecting 8% more true positives than their top performing Artificial Neural Network model. *Santos and Ocampo,*[9] propose a Baysean method for credit card transaction fraud detection with a built in clustering algorithm. *Santos and Ocampo,*[9]believe that incorporating a clustering algorithm can lead to improved results by only selecting the most important features as input to the Bayesian Classifier. To test their Bayesian classifier, *Santos and Ocampo* [9]selected test data with various ratios of genuine and fraudulent transaction data. The researchers determined that their classifier had obtained an optimal overall accuracy of 90.56% with three clusters. Although the performance of this model lacks when testing more balanced data, it suggests that clustering can be an effective dimensionality reduction strategy to improve performance. While *Santos and Ocampo* [9]created a model that aggregates data together before passing it to a Bayesian Classifier, *de Sá et al* [10]propose a model where data is passed to a Hyper-Heuristic Evolutionary Algorithm (HHEA), which selects components from previous Bayesian Network Classifiers to create a custom algorithm, which better classifies fraudulent data. Using the HHEA *de Sá et al* [10]created an algorithm for a dataset from a popular Brazilian online payment system, and compared the accuracy and economic efficiency to a number of other algorithms used on the same data. The results showed that when dealing with accuracy only the Support Vector Machine and J48 algorithms outperformed the proposed algorithm, and when dealing with economic efficiency the Tree Augmented Naive Bayes (TAN), K2 and Random Forest algorithms performed at a similar or better level than the proposed algorithm. The researchers claim that the model is adequately general to adapt to new transaction datasets.

Deep Learning Classifiers

Deep learning offers powerful techniques for extracting the underlying, anomalous patterns in fraudulent transactions. *Maes et al* [3] have trained their model using a Feed Forward Multi-layer Perceptron Neural Network model. This model obtained an AUC score of 0.9083 and was developed by using three different layers of perceptrons: an input layer, hidden layer, and output layer. As aforementioned, supervised learning classifiers are disadvantageous when identifying fraudulent transactions as they are not as effective in generalizing to the new transaction behaviours of fraudsters. In comparison, *Pumsirirat and Yan* [11] have obtained improved results by using the unsupervised classifiers: deep Autoencoder (AE) and Restricted Boltzmann Machine (RBM). The AE obtained an AUC score of 0.9603 while the RBM obtained an AUC score of 0.9505 in their primary dataset.

*Sadgali et al,* [12] compared a Multilayer Perceptron Neural Network, Convolutional Neural Network, and Simple Neural Network to obtain overall accuracy scores of 87.88%, 82.26%, and 67.58% respectively. While their work was beneficial in comparing the effectiveness of different neural networks, the paper lacked common feature engineering techniques to reduce the complexity of their models and improve performance. In contrast, *Zhang et al,* [13] attempted to make their Neural Network more accurate by including a feature sequencing layer to determine the most effective arrangement . The additional feature sequencing provided *Zhang et al,* [13]more accurate results, and the ability to use lower dimensional data not usually available to Neural Networks. The Convolutional Neural Network created by *Zhang et al,* [13]consistently scored higher over multiple data sets on accuracy, precision and recall than an existing Convolutional Neural Network and Backpropagation Neural Network, with a 26% improvement on precision compared to the existing Convolutional Neural Network. With their work on adding feature sequencing *Zhang et al,* [13]were able to create a Convolutional Neural Network an overall accuracy score of 96% compared to the Convolutional Neural Network created by *Sadgali et al,* [12]with an overall accuracy of 83%. *Zhang et al* [13]highlights the importance of feature sequencing for improving the accuracy of the Convolutional Neural Network model but does not explore the effectiveness in detecting fraudulent transactions of other types of neural networks, such as the Multilayer Perceptron Neural Network.

Gradient Boosting Classifiers

*Randhawa et al,* [5]explored using majority voting by combining AdaBoost with 11 machine learning algorithms, ranging from decision trees to neural network models. The team applied a number of machine learning algorithms to a real world dataset, consisting of 284 087 credit card transactions and compared the results of each model with and without AdaBoost. The addition of AdaBoost to each model showed significant improvements after conducting 10-fold cross validation. The Neural Network and AdaBoost hybrid model attained the highest Matthews Correlation Coefficient score of 0.807. *Zheng et al* [14]*.* explored how their novel Improved Transfer AdaBoost (ITrAdaBoost) can be extended from Transfer AdaBoost to better understand new transaction data as fraudsters adapt their behaviours. This innovative approach involves increasing the weights of instances that are wrongly classified in the training set as they are regarded as being dissimilar to the target domain. The weights are updated according to the distribution distance from an instance to a target domain where the calculation of distance is based on the theory of reproducing kernel Hilbert space. In their dataset, their ITrAdaBoost model achieved an AUC score of 0.9084 compared to an AUC score of 0.8566 with their regular AdaBoost model.

**References Cited:**

[1] S. D. Kavila, “Machine Learning For Credit Card Fraud Detection System,” *International Journal of Applied Engineering Research*, vol. 13, pp. 16819–16824. ISSN 0973-4562.

[2] T. Bhatla, V. Prabhu, and A. Dua, “Understanding Credit Card Frauds,” *Tata Consultancy Services 2002*, Jun. 2003.

[3] S. Maes, K. Tuyls, B. Vanschoenwinkel, and B. Manderick, “Credit Card Fraud Detection Using Bayesian and Neural Networks ,” *Machine Learning Techniques for Fraud Detection*, 2020.

[4] V. V. Vlasselaer, C. Bravo, O. Caelen, T. Eliassi-Rad, L. Akoglu, M. Snoeck, and B. Baesens, “APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions,” *Decision Support Systems*, vol. 75, pp. 38–48, 2015.

[5] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim and A. K. Nandi, "Credit Card Fraud Detection Using AdaBoost and Majority Voting," *in IEEE Access, vol. 6, pp. 14277-14284, 2018, doi: 10.1109/ACCESS.2018.2806420.*

[6] S. T. Marella, K. Karthikeya, S. Myla, M. Mohan Sai, and V. Allam, “Detecting Fraudulent Credit Card Transactions Using Outlier Detection,” *International Journal of Scientific & Technology Research* , Oct. 2019

[7] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, “Data mining for credit card fraud: A comparative study,” *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.

[8] O. S. Yee, S. Sagadevan, and N. H. A. H. Malim, “Credit Card Fraud Detection Using Machine Learning as Data Mining Technique,” 2018.

[9] L. Santos and S. Ocampo,"Bayesian Method with Clustering Algorithm for Credit Card Transaction Fraud Detection," *Romanian Statistical Review, Romanian Statistical Review, vol. 66(1), pages 103-120, 2018.*

[10] A. G.C. de Sá, A. C.M. Pereira, and G. L. Pappa, “A customized classification algorithm for credit card fraud detection,” *Engineering Applications of Artificial Intelligence*, vol. 72, pp. 21–29, Jun. 2018.

[11] A. Pumsirirat and L. Yan, “Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine,” *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 1, 2018.

[12] I. Sadgali, N. Sael, and F. Benabbou, “Fraud detection in credit card transaction using neural networks,” *Proceedings of the 4th International Conference on Smart City Applications - SCA 19*, 2019.Could be higher if that sentence is staying in

[13] Z. Zhang, X. Zhou, X. Zhang, L. Wang, and P. Wang, “A Model Based on Convolutional Neural Network for Online Transaction Fraud Detection,” *2019 International Joint Conference on Neural Networks (IJCNN)*, 2019.

[14] L. Zheng, G. Liu, C. Yan, C. Jiang, M. Zhou, and M. Li, “Improved TrAdaBoost and Its Application to Transaction Fraud Detection,” *IEEE Transactions on Computational Social Systems*, pp. 1–13, 2020.