THEME: ANOMALY DETECTION (Outliers Detection)

TOPIC: BANK FRAUD PREVENTION STRATEGY

ABSTRACT:

- **Context about theme and problem:**

  Anomaly detection or outliers detection is a part of statistics that enables us to distinguish parts of data that are significantly different from the rest parts of the data or population.
  With some real-world problems such as a bank processing customer transaction in real time, there is the issue of fraudulent transactions which could lead to financial loss. Fraudulent transactions could stand out in bank data if the right strategies are employed, thus having good fraud strategies could help predict potential risky transactions and thereby save the bank and its customers millions of dollars.

- **Research questions:**
  This project seeks to address the following questions:
  a) How does the bank make fraud strategy less reactive and more proactive?
  b) How do you make sure customer experience is not impacted negatively by fraud detection systems?
- **Data:**
  This research will make use of Datasets from the IEEE-Computational Intelligence Society Fraud Detection database (https://www.kaggle.com/c/ieee-fraud-detection/data)
  The dataset consists of customer transactions on their credit card. A training data set and a test data set where the likely fraudulent in the test transactions would be determined using the training data.

- **Techniques:**

  A classification algorithm would be employed to classify the dataset. Some tools to be used are: SAS (data mining tool) and SQL (Relational Database Mgt System)

INTRODUCTION

This research is aimed at proposing a fraud strategy that focuses mainly on two issues:

- **How does the bank make fraud strategies less reactive and more proactive?**
- **How do you make sure customer experience is not impacted negatively by fraud detection?**

To address these problems this research proposes to explore a recent addition to unsupervised learning. Autoencoder. Autoencoders are artificial neural networks in the deep learning Stata and they are able of learning dense proportions. Generally, autoencoders take a dataset (input), compress the dataset into a single vector that quantifies the input and then reproduces an output from the compressed input. Autoencoders are typically applied in machine learning to denoise data and for outlier or anomaly detection.

While some research has been carried out in the area of autoencoders the section there is still room for more research to be carried out from a fraud strategy perspective.

This section will cover the following sub-sections:

- Literature review: a review of similar or related past works in the areas of fraud detection/prevention strategies
- Dataset: this section will explore the attributes and descriptive statistics of the dataset that were used for this research
- Approach: Here we would be presenting a diagrammatic depiction of the steps to be taken during the research.
- A list of references used will also be provided.

LITERATURE REVIEW

This section presents a review of past works in the core topics in this research. We will examine the areas of credit card/debit card fraud and Fraud detection techniques/strategies.

According to the Government of Canada: Credit Card fraud happens when someone steals credit card information belonging to another and uses it without the owner's permission to make transactions which could include online and in-store purchases or cash withdrawals from ATM machines. (https://www.canada.ca/en/financial-consumer-agency/services/credit-fraud.html, 2019.

For years Financial Institutions have adopted different strategies to reduce the risk of credit card fraud. The fallout of customers having fraud on their bank account can be detrimental to a financial institutions reputation as it negatively impacts the customers feeling of trust and security as provided by the financial institution (Krummeck, 2020, cited in Hoffmann and Birnbrich, 2012. PP.391)

Multiple writers over the years have researched on how to fight fraud in the banking sector, however it appears there seems to be a lack of access to near real financial data which could help to possibly give a break through in fraud detection strategies. In 2016 Lopez-Rojas and Axelsson wrote about

MABS (Multi Agent Based Simulation) in their paper entitled A Review of Computer Simulation for Fraud Detection Research in Financial Datasets. Here they reviewed an earlier paper which proposed a simulator that can produce financial data which mirrored the legitimate customer behavior and fraudulent behavior. The writers mention that they receive requests to use their datasets.

Vona (2017, pp. 2-9) in his book 'Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems' wrote that part of fraud data analytics involves analysing data to reveal red flags or outliers that could help understand how to prevent fraud. The author also discusses certain issues to look out for in the process of fraud data analytics some of which are; **False positive (FP)**: a transaction that matches red flags which identify a transaction as being possibly fraudulent based on the fraud profile however the transaction is actually a legitimate transaction. **False Negative (FN)**: a transaction that does not match the red flags based on the fraud profile however is a fraudulent transaction. In response to the foregoing issues the writer suggested that false positives are bound to occur in data analytics and focus should be on minimising the False positives, he also asserts that False negatives can occur as a natural short coming in data analytics, one of his reasons are because sometimes not all test cases are tested/contained in a fraud plan. One of his recommendations is to deal more with false negatives through audit work.

In Another paper by Hoffmann and Birnbrich (2012, pp. 391-392) which was aimed at assessing the impact of a customers understanding of the measures taken by the bank to prevent fraud. The writers argued that there is a direct relationship between a bank's customer base and the banks level of success in proactively managing fraud. The final results of a research conducted by the researchers showed that a majority of customers preferred to receive communications enlightening them about what procedures/systems their bank has in place for fraud detection or how their data is used for fraud detection.

This research will be covering certain customer concerns like a legitimate customer attempting to make a transaction in real time and being declined by a fraud strategy. The ultimate aim is to realise that even though a bank wishes to reduce fraud loss, the bank also stands the risk of having too many false positives which could potentially reduce customer spending, negatively impact customer satisfaction and reduced authorized transactions and profit for the bank.

Kundu et al (2009 pp. 309-315) conducted a short research addressing fraud detection using a specific algorithm which was a hybrid between two variables: time and transaction amounts. Based on the observation of the writers most fraud detection models consider transaction amounts as the most important variable in fraud detection, they also observed that typical fraud detection models usually consider amount and time variables separately, however they were of the option that the most cardholders would make use of their card at a time that is convenient for them and rarely deviate from this pattern and also make purchases which is lower than their credit limits and so fraud profiles or baskets could be built based on a fusion of these two variables , the model however appears rigid and does not take into considerations a change in customer spending behavior pattern or how results could possibly yield a high precision and a less balanced recall because of the focus on only the fraud elements in the training dataset.

In the article, Hybrid approaches for detecting credit card fraud by Kultur and Caglayan (2017 pp.1-13) the writers discussed applying six popular supervised models: decision tree, random forest,

Bayesian network, Naïve Bayes, support vector machine, and K* model to create a fraud detection model. All the models are trained using the same training data, and once the 1st transaction occurs each makes a decision and a final weighted decision is made, on if the transaction is likely to be fraudulent or not, while this approach seems to be highly logical and promising, one possible flaw could be that the hybrid model would be inheriting all the disadvantages of each of the decision models, which could be : overfitting from of decision trees, long training time required for random forest, an underlying assumption by Naïve bays that all attributes are independent, support vector machine and k-nearest neighbors models are not very suitable for large datasets,

Thennakoon et al in 2019, published the research paper Real-time Credit Card Fraud Detection Using Machine Learning. Their model argues that 4 major variables: risky Merchant Standard Industrial Classification code (sic code), Unknown web address, ISO Response Code, Transaction above $100 would be utilized along with a 3 part fraud detection system: API Module, Fraud Detection Model and Data Warehouse. It appears a limitation could be the decision to utilize 4 variables to make a decision on if a transaction is legitimate or fraudulent, it is also not clear if some of these variables like ISO response codes could potentially contribute to predicting fraud.

Patil et al in 2018 (pp. 385-395) proposed a fraud detection model using Hadoop for system design, Hadoop is a solution known for its scalability because it can handle large volume of data over multiple serves however there could be complex number of problems relating to data being processed only in batch as it leads to slowness in performance although this can be improved by using Spark. The researchers also proposed to use decision trees, random forest, and logistic regression classifiers for fraud detection. The research however notes the draw back of overfitting with using random forest.

In 2009, Whitrow et al (pp.30-55) in their paper Transaction aggregation as a strategy for credit card fraud detection proposed a fraud detection model that could used a combination of aggregate transaction amounts and a specific wide time frame of 1, 3 and 7 days to determine risky transactions in conjunction with classifiers like KNN, decision trees and random forest, a possible imitation could be the specificity in the time period, this could generate a large pool of false positives or too high a precision and low performance in the test data results.

A research entitled Feature engineering strategies for credit card fraud detection was conducted by Bahnen et al in 2016. Their research argues that traditional expert systems and machine learning tools may have inadequacies in detecting fraud. The writers used a new method for extracting periodic features to give a proper prediction of if a transaction fell within the confidence interval of previous transactions and also proposed an extended transaction aggregation strategy where they incorporated a combination criteria in transaction grouping. More variables like card holder and transaction type were introduced. A possible limitation could be that the system would take a long time recalculating each feature with every new transaction as a limit is not placed on the number of features that can be calculated.

Some more recent research studies have dealt in the area of concept drift in fraud detection models According to Webb et al in (2016) concept drift is created by the problem of machine learning being static, whereas the world is dynamic and data changes overtime meaning that results from machine

learning models can become inaccurate. From a fraud strategy perspective these inaccuracies could lead to increase in false negatives and false positives or duplications in codes due to constant changes being made in fraud detection strategies. There has been some research into how false positives can be reduced (Baader and Krcmar, 2018 pp. 1-16; Wedge et al, 2018 pp. 372-388) however these research had limitations relating to simulated datasets, and the possible increase in cost based on daily extraction of data for the machine learning.

Somasundaram and Reddy (2018) carried out a research entitled Parallel and incremental credit card fraud detection model to handle concept drift and data imbalance. The research was geared at creating an incremental learning-based parallelized model that could effectively handle concept drifts which are bound to occur in fraud detection following class drift and covariate drift. The results from the model produced higher precision levels (in comparison with a previous fraud detection model proposed by Zareapoor et al which used a balancing strategy to provide effective predictions.) the model however does not account for cyclic recurrence in concept drift. Certain fraud trends are relating to seasons for instance in the summer there may be a surge in fraud relating to airline tickets. If this cannot be accounted for the false negatives may be greater in those periods regardless of this machine learning.

Another paper that proposed the use of a bagging approach for fraud detection model is Cost-sensitive Risk Induced Bayesian Inference Bagging (RIBIB) for credit card fraud detection by researchers Akila and Reddy in 2018 (pp. 247-254). The researchers believed that creating multiple training data sets called bags and then training classifier models with these could improve the accuracy and performance of predictions. They also incorporated a cost-sensitive combiner to align the results with business goals targeted at cost reduction. while their model does provide benefit in terms of cost savings, it does not appear to utilize conventional fraud metrics and as such results could possibly not cover issues like concept drifts at the end of the day.

Another research that was carried out in relation to improving fraud strategies by reducing false positives was from Fiore et al, pp.448-455 (2019) in their paper using generative adversarial networks for improving classification effectiveness in credit card fraud detection. In their research the writers isolated fraudulent transactions from a training dataset, and using a generative adversarial network (GAN) which is an unsupervised machine learning technique that learns to generate new data with the same statistical parameters as the training set, the writers were able to generate a synthetic dataset of fraudulent transactions and then inputted these into the training set and then compared the performance on the same testing dataset used previously. Their results showed a higher precision in comparison with utilizing the training set on the test dataset without the simulated data, while the research may help in the area of creating data for research, possible research could create legitimate transactions as a limitation of the research is that there were no actual legitimate data simulated, the addition of more fraudulent transactions in the dataset would simply have led to be better FP but if this is implemented in real life data it may have a higher false positive.

Chen et al in 2018 pp. 1054-1059, conducted a research entitled Credit Card Fraud Detection Using Sparse Autoencoder and Generative Adversarial Network, the research was similar to the previous

research discussed here however their research made use of an unsupervised is a type of artificial neural network in combination with a GAN. The researchers however generated more legitimate transactions with the GAN thereby training the algorithm with a near realistic situation in real life possibly taking into consideration some accepts of concept drift.

DATASET

This research will be making use of a credit card dataset that depicts and transactions in customer accounts. The Dataset was got from Kaggle (https://www.kaggle.com/jacklizhi/creditcard)

Before we go into to utilizing the dataset, we first need to understand the data. The data contains one file of 31 columns variables and 283726 unique records. It is a highly imbalanced dataset where only over 473 of the records belong to class 1 and the rest 283253 records belong to class 0. This issue will be taken care of by our autoencoder model. The dataset had no missing values but had some duplicates and these were removed. Some descriptive stats were also taken for the dataset and this will be displayed in the initial code and results.

The dataset has 31 variables:

- **Time:** Time variable for the dataset
- **V1-V28**: variables where their real meaning has been masked for privacy reasons
- **Amount**: The transaction amount
- **Class**: denoted by 0 or 1 if the transaction was legitimate or fraudulent

A high-level summary of the attribute types for both datasets is given below:

Binary Attribute:

- Class (Legitimate or Fraud is depicted by 1 or 0)

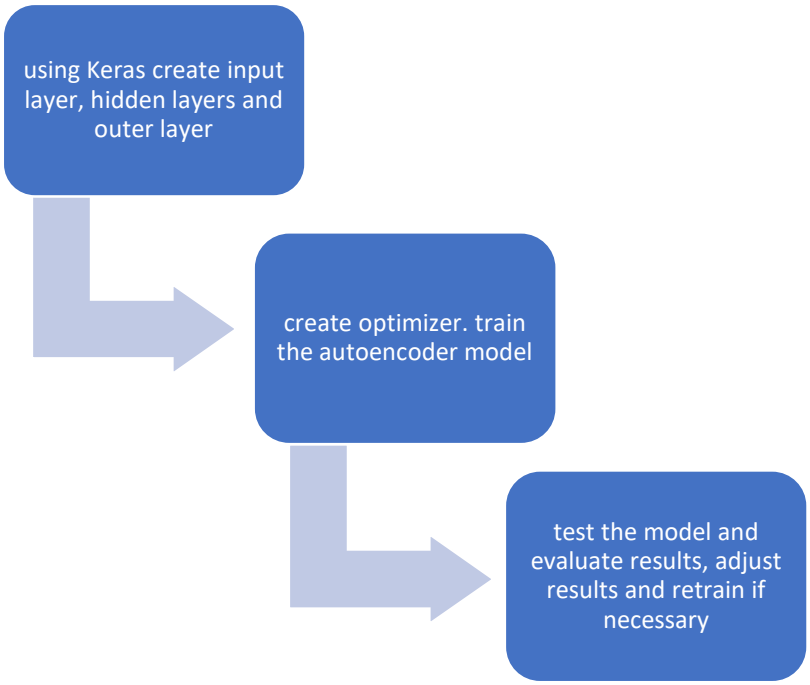
Numeric Attributes:

- Time, V1-V28

Continuous Attribute:

- Amount

APPROACH



Step 1

Using the Keras package in R, we would create our autoencoder model,

Step 2:

We would then compile the model and run it against our already split training dataset

Step 3:

Test the model using the test dataset. We would then evaluate our model results (accuracy and loss) and if we think we can do better we would adjust our model parameter and retrain.

Bibliography

Akila, S., Reddy, U.S., (2018) 'Cost-sensitive Risk Induced Bayesian Inference Bagging (RIBIB) for credit card fraud detection' *Journal of Computational Science, 07/2018, Volume 27*, pp. 247-254.

Baader, G., Krcmar, H., (2018) 'Reducing false positives in fraud detection: Combining the red flag approach with process mining' *International Journal of Accounting Information Systems* 31(1) pp.1-16 [Online] Available at: https://www.sciencedirect.com/science/article/pii/S146708951630077X (Accessed 8 June 2020)

Bahnsen, A.C., Aouada, D., Stojanovic, A., Ottersten, B. (2016) 'Feature engineering strategies for credit card fraud detection' *Expert Systems with Applications / 51(Complete),* pp.134-142 [Online] Available at: https://journals-scholarsportalinfo.ezproxy.lib.ryerson.ca/details/09574174/v51icomplete/134_fesfccfd.xml (Accessed 7 June 2020)

Chen, J., Shen, Y., and Ali, R., (2018) 'Credit Card Fraud Detection Using Sparse Autoencoder and Generative Adversarial Network'. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, 2018, pp. 1054-1059, [Online] Available at: https://ieeexplore-ieee-org.ezproxy.lib.ryerson.ca/stamp/stamp.jsp?tp=&arnumber=8614815 (Accessed 9 June 2020)

Fiore, U., De Santis, A., Perla, F., Zanetti, P., Palmieri, F. (2019) 'Using Generative Adversarial networks for improving classification effectiveness in credit card fraud detection' *Information Sciences* 479 pp. 448-455 [Online] Available at: https://www-sciencedirect com.ezproxy.lib.ryerson.ca/science/article/pii/S0020025517311519?via%3Dihub (Accessed 9 June 2020)

Goodfellow, I.J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y. (2014) 'Generative adversarial nets', *Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2* pp. Pages 2672–2680, [Online] Available at: https://arxiv.org/pdf/1406.2661.pdf

Hoffmann, A.O.I., Birnbrich, C. (2012) 'The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking'. *International Journal of Bank Marketing,* 30(5), pp. 390-407 [Online]. Available at: https://www-emerald-com.ezproxy.lib.ryerson.ca/insight/content/doi/10.1108/02652321211247435/full/pdf?title=the-

impact-of-fraud-prevention-on-bankcustomer-relationships-an-empirical-investigation-in-retail-banking. (Accessed 7 June 2020)

Kultur, Y., Caglayan, M.U. (2017) 'Hybrid approaches for detecting credit card fraud' *Expert Systems* 34(2), pp. 1-13 [Online]. Available at: https://onlinelibrary-wiley-com.ezproxy.lib.ryerson.ca/doi/pdfdirect/10.1111/exsy.12191. (Accessed 7 June 2020)

Kundu, A., Panigrahi, S., Sural, S., Majumdar, A.K., (2009) 'BLAST-SSAHA Hybridization for Credit Card Fraud Detection. *IEEE Transactions on Dependable and Secure Computing,* 6(4), pp.309-315 [Online]. Available at: https://journals-scholarsportal-info.ezproxy.lib.ryerson.ca/pdf/15455971/v06i0004/309_bhfccfd.xml (Accessed 7 June 2020)

Leonard, V. (2017) Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems: John Wiley & Sons, Incorporated. [Online]. Available at: https://ebookcentral-proquest-com.ezproxy.lib.ryerson.ca/lib/ryerson/detail.action?docID=4771464. (Accessed on 7 June 2020)

Lopez-Rojas, E.A., Axelsson, S. (2016) 'A Review of Computer Simulation for Fraud Detection Research in Financial Datasets' *FTC 2016 - Future Technologies Conference 20166-7 December 2016 | San Francisco, United States* [Online] Available at: https://ieeexplore-ieee-org.ezproxy.lib.ryerson.ca/stamp/stamp.jsp?tp=&arnumber=7821715 (Accessed 8 June 2020)

Patil, S., Nemade, V., Soni, P. (2018) 'Predictive Modelling for Credit Card Fraud Detection Using Data Analytics' Procedia *Computer Science, 2018, Volume 132* pp.385-395 [Online] Available at: https://www.sciencedirect.com/science/article/pii/S1877050918309347?via%3Dihub (Accessed 8 June 2020)

Somasundaram, A., Reddy, S. (2018) 'Parallel and incremental credit card fraud detection model to handle concept drift and data imbalance', *Neural Computing and Applications, 01/2019, Volume 31, Issue S1,* pp.3-14 [Online], Available at: https://link-springer-com.ezproxy.lib.ryerson.ca/content/pdf/10.1007/s00521-018-3633-8.pdf (Accessed 7 June 2020)

Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., Kuruwitaarachchi, N. (2019) 'Real-time Credit Card Fraud Detection Using Machine Learning' *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* [Online] Available at: https://ieeexplore-ieee-org.ezproxy.lib.ryerson.ca/stamp/stamp.jsp?tp=&arnumber=8776942 (Accessed 7 June 2020)

Webb, G.i, Hyde, R., Cao, H., Nguyen, H.L, Petitjean, F. (2016) 'Characterizing concept drift' *Data Mining and Knowledge Discovery* 30(4) [Online] Available at:

https://journals-scholarsportal-info.ezproxy.lib.ryerson.ca/pdf/13845810/v30i0004/964_ccd.xml

Wedge, R., Kanter, J.M., Veeramachaneni, K., Rubio, S.M., Parez, S.I. (2018) 'Solving the False Positives Problem in Fraud Prediction Using Automated Feature Engineering' *European Conference, ECML PKDD 2018, Dublin, Ireland, September 10–14, 2018, Proceedings, Part III* pp.372-388 [Online] Available at: http://www.ecmlpkdd2018.org/wp-content/uploads/2018/09/567.pdf (Accessed 8 June 2020)

Whitrow, C., Hand, D.J., Juszczak, P., Weston, D., Adams, N.M. (2009) 'Transaction aggregation as a strategy for credit card fraud detection' *Data Mining and Knowledge Discovery* 18(1) pp.30-55 [Online] Available at: https://journals-scholarsportal-info.ezproxy.lib.ryerson.ca/pdf/13845810/v18i0001/30_taaasfccfd.xml (Accessed 8 June 2020)