|  |  |
| --- | --- |
|  | |
| Scientific Research + Literature –Assessment 3  TU060 : Literature Review | |
|  | |
| Ciaran Finnegan – Part Time – First Year 2021/2022  MSc in Computer Science (Data Science)  Student No : D21124026  1/5/2022 |  |
|  |  |

Title

**An analysis to compare Machine Learning techniques used in the application of Credit Card fraud detection from 2012-2017 against more recent optimised approaches.**

Abstract

This review describes Machine Learning techniques that were applied from 2012 to 2017 to build models to detect credit card fraud and compares them against emerging approaches documented circa 2020. The review objective is to determine if the more modern ML strategies were delivering significantly better performance, despite possible limitations due to their inherent complexities.

American and European datasets formed the basis of the modelling experiments, and ‘fraud’ was defined as the unauthorised use of card services by a third party.

A significant characteristic of the majority of these datasets is that instances of fraud make up a very small proportion of the total record set. Hence, data resampling considerations are a factor throughout the review.

The two earliest papers employed what the authors themselves described as ‘traditional’ ML Classification approaches. The third paper explained a later ensemble approach to resampling and anomaly detection. The fourth paper detailed experiments in 2020 into more contemporary approaches using Neural Networks. The last paper (also 2020) looked at recent algorithm optimisations to avoid resampling of imbalanced data and circumvent possible data corruption. Further research papers are included in this analysis to add context to the assumptions made by the various authors.

Comparing the findings across the review is challenging as authors use datasets of different sizes and a variety of model comparison criteria. However, F1 Scores, from the best performing models, show a steady increase from 0.729 with enhanced resampling and feature reduction, up to 0.849 when Neural Network approaches are employed, to a score of 0.941 with an Optimised XGBoost (OXGBoost) algorithm.

All metrics in this review need to be considered in the context of their research experiments, but an upward trend in fraud detection rates over time is evident.

The more recent Neural Network approaches performed well and have crucial benefits in terms of computation efficiency.

However, Neural Network predictions can be difficult to audit. The OXGBoost approach has the benefit of both greater transparency and the avoidance of data corruption through resampling. Both techniques are therefore emerging areas of interest for further research.

**Key Words**: Credit Card Fraud Detection, Data Resampling, Feature Engineering, Deep Learning, Neural Network Auditing

Table of Contents

1 Introduction 5

2 Concept A: Addressing the Imbalance and Resampling Challenge 7

3 Concept B: Neural Networks – Handling Volume and Speed for Fraud Detection 8

4 Concept C: Neural Networks and Auditing Fraud Detection Results 9

5 Conclusion: Better ways to capture CC Fraud? 10

6 References 11

# Introduction

* *A concise* ***definition of a topic*** *under consideration (this may be a descriptive or argumentative thesis, or proposal), as well as the* ***scope*** *of the related literature being investigated. (Example: If the topic under consideration is ‘women’s wartime diaries’, the scope of the review may be limited to published or unpublished works, works in English, works from a particular location, time period, or conflict, etc.)*
* *The introduction should also note intentional* ***exclusions****. (Example: “This review will not explore the diaries of adolescent girls.”)*
* *Another purpose of the introduction is to state the* ***general findings*** *of the review (what do most of the sources conclude), and comment on the* ***availability*** *of sources in the subject area.*

Financial analysists such as Whatman (2019) have collated industry statistics to show that credit card fraud remains an evolving multi-billion Euro challenge**[1]**, which threatens global financial institutions with both loss of revenue and reputation.

‘*Fraud’*, in the domain of this literature review, can be defined in terms of an established definition from Bolton (2001) as a historical credit card event, reported to the card provider, in which a third party has conducted a transaction (online or in person) without the permission of the card holder**[2]**.

This report begins by looking at earlier research by Bhattacharyya et al (2011) that emphasized the value of specialist algorithms for fraud detection techniques**[1]**, and which is followed by proposals from Lima and Pereira (2017) for combining more sophisticated resampling in conjunction with selective feature engineering**[2]**. Later research from Nguyen, Tahir, Abdelrazek, and Babar (2020)**[5]** posits that Deep Learning techniques may offer more promising solutions, and ones that will actually be performant enough for the ‘big data’ and real-time requirements of the 2020s. Priscilla and Prabha (2020)**[6]** also propose that resampling itself could be distorting credit card fraud data and that optimising the XGBoost algorithm can sidestep this issue for more contemporary solutions. The criteria for comparison focuses on how the different approaches handle typical fraud dataset imbalances, the need for computation efficiency (both speed and data volumes), and the transparency of the process used to label a transaction as possibly ‘fraudulent’. Obviously, the general accuracy of successive fraud classification approaches is an essential supplementary characteristic.

The historical datasets used in this literature review are sourced from credit card operators providing services in the European and American marketplaces. Therefore, any fraud patterns that are specific to other markets, such as those in Africa and Asia, will not be considered. Neither does any research in this review focus on debit card or prepaid card transactions.

Although the historical fraud datasets in this review vary in size between tens of thousands to more than 10 million rows, the incidents of actual fraud usually constitute less than 1% of any given record set. This characteristic imbalance is one of the defining characteristics of the fraud detection challenge. Researchers such as Sohony, Pratap, and Nambair (2018) have well documented that such a degree of imbalance is a major complication against which learning algorithms must adapt**[7]**.

Due to data confidentiality concerns, there are still relatively few historical credit card fraud datasets upon which to conduct ML experiments for fraud detection. This is a limitation noted in research conducted by Dal Pozzolo et al (2014)**[8]**. Credit Card Fraud Detection is a very active field of research, but the lack of variety in source data requires experimentation with an increasingly sophisticated array of algorithms and parameters.

# Concept A: Addressing the Imbalance and Resampling Challenge

The heavily skewed distribution of data towards ‘non-fraud’ records in many credit card fraud datasets can pose problems for learning algorithms with a possible bias towards the majority class. The 2019 research from Ceronmani Sharmila et almakes a somewhat informal description of applications needing to capture “*fraudulent transactions that take place every once in a while*” **[9]**. In addition, Lima and Pereira (2017) reference the fact that e-commerce systems tend to generate a significant numbers of features for each transaction, and that this combines with the fraud imbalance problem to further complicate the creation of detection models.

*Undersampling* is a technique to remove rows from the majority (non-fraud) class in order to address potential bias in the ML learning process. The earliest research in this review, from Bhattacharyya, Jha, Tharakunnel, and Westland in 2011, determined by experiment that random undersampling contributed to their best detection results, with an F1 Score of *0.787* with RF. However, Lima and Pereira (2017) call out that such a methodology may result in important information being lost. A more elaborate sequence of resampling techniques was proposed, including *oversampling* by artificially creating fraudulent transaction records with the SMOTE method. In these experiments, the best model F1 Score result was *0.729*, but with a much larger dataset and less input data removed than in the 2011 experiments by Bhattacharyya et al.

Despite the positive outcomes in the Lima and Pereira research, later papers in this review declare that oversampling techniques may introduce distortions in the data and cause potential overfitting. Ceronmani Sharmila (2019) and Priscilla and Prabha (2020) both recommend approaches that avoid resampling of credit card fraud data and instead employ enhanced outlier detection (F1 Score: *0.849*) and tree boosting (F1 Score: *0.940*) techniques respectively.

Future credit card fraud research that examines techniques to avoid data resampling will be a key topic of interest.

# Concept B: Neural Networks – Handling Volume and Speed for Fraud Detection

* *There are many ways to organize the evaluation of the sources.* ***Chronological and thematic approaches*** *are each useful examples.*
* *Each work should be critically summarized and evaluated for its* ***premise****,* ***methodology****, and* ***conclusion****. It is as important to address inconsistencies, omissions, and errors, as it is to identify accuracy, depth, and relevance.*
* *Use logical connections and* ***transitions*** *to connect sources.*

# Concept C: Neural Networks and Auditing Fraud Detection Results

# Conclusion: Better ways to capture CC Fraud?

* *The conclusion* ***summarizes the key findings*** *of the review in general terms. Notable commonalities between works, whether favourable or not, may be included here.*
* *This section is the reviewer’s opportunity to* ***justify a research proposal****. Therefore, the idea should be clearly re-stated and supported according to the findings of the review.*

Tabular Comparison 1 – F1 Scores

Tabular Comparison 2 – Size of datasets

Tabular Comparison 3 – Resampling

Bullet point commentary on table..

* General accuracy better with NN and OXGBoost.
* NN capable of processing much larger datasets, at greater speed – with use of GPUs etc.
* OXGBoost works to avoid data distortion

Para…The computation speed demonstrated in the Neural Network experiments has implications in terms of real-time detection applications. This review presents compelling arguments that Neural Networks, more often used for image classification, can deliver solutions that are both more accurate and, crucially, much faster at detection credit card fraud.

Para…Neural Network solutions can be criticised for lack of auditability in terms of classifications, and that remains a problem in this domain, but the potential is obvious. Work could be continued to make NN detection processes more transparent, in line with earlier techniques…

Para… - further work in avoiding resampling would be interesting…

# References

[1] Whatman, P., 2019. *Credit Card Statistics 2020: 65+ Facts For Europe, UK, And US*. [online] Blog.spendesk.com. Available at: <https://blog.spendesk.com/en/credit-card-statistics-2020>

[2] Bolton, R. (2001). Unsupervised Profiling Methods for Fraud Detection. Retrieved 21 April 2022, from https://www.researchgate.net/publication/2407747\_Unsupervised\_Profiling\_Methods\_for\_Fraud\_Detection

[3] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602-613. doi: 10.1016/j.dss.2010.08.008

[4] Lima, R., & Pereira, A. (2017). Feature Selection Approaches to Fraud Detection in e-Payment Systems. *Lecture Notes In Business Information Processing*, 111-126. doi: 10.1007/978-3-319-53676-7\_9

[5] Nguyen, T., Tahir, H., Abdelrazek, M., & Babar, A. (2020). Deep Learning Methods for Credit Card Fraud Detection. Retrieved 25 March 2022, from https://doi.org/10.48550/arXiv.2012.03754

[6] Priscilla, C., & Prabha, D. (2020). Influence of Optimizing XGBoost to handle Class Imbalance in Credit Card Fraud Detection. *2020 Third International Conference On Smart Systems And Inventive Technology (ICSSIT)*, pp. 1309-1315. doi: 10.1109/icssit48917.2020.9214206

[7] Sohony, I., Pratap, R., & Nambiar, U. (2018). Ensemble learning for credit card fraud detection | Proceedings of the ACM India Joint International Conference on Data Science and Management of Data. Retrieved 21 April 2022, from https://doi.org/10.1145/3152494.3156815

[8] Dal Pozzolo, A., Caelen, O., Le Borgne, Y., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems With Applications*, *41*(10), 4915-4928. doi: 10.1016/j.eswa.2014.02.026

[9] Ceronmani Sharmila, V., R., K., R., S., D., S., & R., H. (2019). Credit Card Fraud Detection Using Anomaly Techniques. *2019 1St International Conference On Innovations In Information And Communication Technology (ICIICT)*, *1*(1), 1-4. doi: 10.1109/iciict1.2019.8741421

# Additional Research Topics

* Auditing Neural network solutions for cc fraud detection – or classification problems in general.
* Research on avoiding resampling on highly imbalanced datasets.
* Speed/Big Data benefits of NN with cc fraud detection – or classification