|  |  |
| --- | --- |
|  | |
| 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  1/4/2022 |  |
|  |  |

Title

**An analysis to determine if in the past decade (2012-2022) that the application of Machine Learning techniques for Credit Card Fraud detection have improved in accuracy and performance.**

Abstract

*Objectives*

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

*Methods*

ML detection Models were built based on American and European datasets, where fraud is considered to be the unauthorised use of card services by a third party.

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

The first two papers employed what the authors themselves described as ‘traditional’ ML Classification approaches. The third paper looks at an ensemble approach to resampling and anomaly detection. The fourth paper moves into the more contemporary approach of using Neural Networks. The last paper looks at recent algorithm optimisations to avoid resampling of imbalanced data and circumvent possible data corruption. Further research papers are included in the analysis to add context to the assumptions made by the various authors.

*Results*

Comparing the findings across the review is challenging as authors use datasets of varying sizes and a selection of model comparison criteria. However, F1 Scores, from the best performing models, show a steady increase from 0.767 with enhanced resampling and feature reduction, up to 0.849 when Neural Network approaches are employed, and a score of 0.941 with an Optimised XGBoost (OXGBoost) algorithm.

*Conclusion*

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

The more recent Neural Network approaches perform 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 area 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: Imbalance and Resampling Challenge 7

3 Concept B: Too Many Features 8

4 Concept C: Neural Networks and Auditing 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.*

Credit Card fraud remains an evolving multi-billion Euro challenge, which threatens global Financial Institutions with loss of revenue and reputation.

‘*Fraud’* in the domain of this literature review is defined 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.

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.

A common theme in these research papers is that historical datasets for credit card fraud have a number of challenging characteristics that make it necessary to extend and augment the Machine Learning techniques that would be used in other types of Classification problems;

As of 2021, because of 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 very active field of research, but it is common to see a variety of papers experimenting on the same datasets.

However, the most significant complication is that, although the record sizes in the datasets in this review vary from tens of thousands to more than 10 million, the majority of historical fraud datasets are highly imbalanced, often with less than 1% of records reflecting incidents of actual fraud.

This article looks at a number of major studies, conducted from 2012-2020, which recommend a series of feature engineering and algorithm selections refinements to better detect credit card fraud, and tackle the inherent imbalance challenge.

The findings in the earlier papers emphasize the value of combining sophisticated resampling techniques with specialist algorithms to deliver more effective fraud detection models. Later research from Nguyen, Tahir, Abdelrazek, and Babar (2020)**[1]** posits that Deep Learning techniques may offer more promising solutions, and ones that will actually be performant enough for ‘big data’ and real-time requirements in the 2020s. Priscilla and Prabha (2020)**[2]** 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.

# Concept A: Addressing the Imbalance and Resampling Challenge

* *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.*

The heavily skewed distribution of data towards ‘non-fraud’ records in many credit card fraud datasets can pose problems for learning algorithms and a possible bias towards the majority class. The 2019 research from Ceronmani Sharmila et al **[3]** makes a somewhat informal description of credit card fraud detection applications needing to capture “*fraudulent transactions that take place every once in a while*”. In addition, Lima and Pereira (2017)**[4]** 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**[5]**, determined by experiment that random undersampling contributed to their best detection results. 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, that was shown to drive more effective feature reduction and model performance results.

Despite the positive outcomes in the Lima and Pereira research, later research in this review focuses on the problem that oversampling techniques can introduce distortions in the data and 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 and tree boosting techniques respectively. Future credit card fraud research that examines further techniques to avoid data resampling will be a key topic of interest.

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

# 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.*

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.

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.

# References

[1] 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

[2] 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

[3] 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

[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] 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