A Hybrid Approach for Fraudulent Transaction Detection: SMOTE-Autoencoder Framework

1st Yathartha Patankar
Department of Computer Science
California State University, Fullerton
Fullerton, USA
yatharthapatankar@csu.fullerton.edu

2nd Kanika Sood
Department of Computer Science
California State University, Fullerton
Fullerton, USA
kasood@fullerton.edu

***Abstract*—Fraudulent transactions represent a formidable challenge across diverse industries, with particularly profound implications within finance industry, where they can yield significant financial losses and precipitate reputational harm. Traditional rule-based approaches to fraud detection exhibit notable deficiencies in adapting to the dynamic nature of fraudulent behaviors, resulting in elevated rates of false negatives. This paper introduces a pioneering methodology for detecting fraudulent transactions, leveraging the integration of the Synthetic Minority Over-sampling Technique (SMOTE) and autoencoder-based anomaly detection. Given the prevalent class imbalance inherent in real-world transaction datasets, SMOTE plays a pivotal role in rectifying this imbalance, mitigating false negatives. The deployment of autoencoder architecture facilitates the discernment of latent patterns and the identification of anomalies indicative of fraudulent conduct. The efficacy of the proposed framework is rigorously evaluated by employing a principal component analysis (PCA) transformed dataset, meticulously crafted to emulate authentic transactional environments. The empirical assessment unequivocally substantiates the framework's proficiency in accurately identifying fraudulent transactions while concurrently minimizing false positives and false negatives. The ensuing experimental findings underscore profound enhancements in detection performance when contrasted with conventional methodologies, thereby underscoring the transformative potential of the proposed approach in fortifying fraud detection systems. This research engenders substantive contributions to the evolutionary trajectory of fraud detection methodologies, engendering invaluable insights conducive to mitigating fraudulent activities pervading financial transactions.**

***Index Terms*—Fraudulent transactions, Fraud detection, Synthetic Minority Over-sampling Technique (SMOTE), Autoencoder-based anomaly detection, Class imbalance, Principal Component Analysis (PCA), False positives, False negatives, Machine learning, Anomaly detection, Data imbalance, Dynamic fraud behaviors**

I. Introduction

Fraudulent transactions pose a pervasive and intricate challenge across various industries, with the finance sector bearing particularly profound implications. These deceitful activities encompass a range of fraudulent behaviors, including but not limited to unauthorized purchases, identity theft, and money laundering. Such nefarious acts not only inflict significant financial losses but also precipitate detrimental repercussions on the reputation and trustworthiness of the institutions involved. Within the realm of financial transactions, fraudulent activities manifest in diverse forms. One prevalent type is credit card fraud, wherein perpetrators exploit stolen or compromised credit card information to make unauthorized purchases or cash withdrawals. Another common form is account takeover fraud, wherein fraudsters gain unauthorized access to individuals' accounts through various means, including phishing attacks or malware. While once considered practical, traditional rule-based approaches to fraud detection exhibit notable inadequacies in adapting to the dynamic and evolving nature of fraudulent behaviors. These approaches rely on predefined rules and thresholds to identify suspicious transactions, often resulting in elevated rates of false positives and false negatives. False positives refer to legitimate transactions erroneously flagged as fraudulent, while false negatives denote fraudulent transactions that go undetected. In light of these challenges, this study introduces a novel and thorough approach to identifying fraudulent transactions, particularly analyzing data related to credit card transactions. The approach integrates two advanced techniques: the Synthetic Minority Over-sampling Technique (SMOTE) and autoencoder-based anomaly detection. SMOTE, renowned for its efficacy in addressing class imbalance inherent in real-world transaction datasets, plays a pivotal role in rectifying this disparity, notably mitigating false negatives. Concurrently, autoencoder architecture enables the discernment of latent patterns within transactional data, facilitating the identification of anomalies indicative of fraudulent conduct. The proposed methodology is meticulously evaluated using a principled approach involving assessing its performance on a principal component analysis (PCA) transformed dataset. This dataset, tailored to simulate authentic credit card transactional environments, is a rigorous testbed for evaluating the framework's efficacy and robustness. Through extensive experimentation and analysis, the empirical findings unequivocally substantiate the proficiency of the proposed framework in accurately identifying fraudulent transactions while minimizing the incidence of false negatives.

II. Literature Review

Credit card fraud detection is a critical concern for financial institutions due to the increasing prevalence of fraudulent activities, especially with the rise of online transactions. Various studies have explored the application of machine learning algorithms for fraud detection in credit card transactions.

Aditi Singh, Anoushka Singh, and others in the year 2022 [1] comprehensively analyzed different machine-learning algorithms for credit card fraud detection. Their study evaluated four algorithms: logistic regression, decision tree, random forest, and CatBoost, using a dataset sourced from Kaggle. Through data preprocessing and resampling techniques, they addressed issues such as imbalanced datasets, aiming to enhance the accuracy of fraud detection models. Their findings indicated that CatBoost outperformed other algorithms, achieving an accuracy of 99.87 percent. This study highlights the significance of machine learning in mitigating financial risks associated with credit card fraud.

Kanika and Jimmy Singla[2] emphasize the adverse impact of data imbalance on learning model accuracy, necessitating the development of strategies to mitigate bias and prevent inaccurate outcomes. Despite the burgeoning interest in deep learning techniques for fraud detection, the scarcity of access to confidential transactional data has hampered research progress, resulting in insufficient exploration of the class imbalance problem.

Another research work was done To tackle the class imbalance issue[3] by Dilip Singh Sisodia, Nerella Keerthana Reddy, and Shivangi Bhandari (2022), who propose the utilization of resampling techniques, focusing on both oversampling and undersampling methods. Oversampling techniques such as SMOTE, SMOTE ENN, SAFE SMOTE, ROS, and SMOTE TL are employed to augment the minority class instances. At the same time, undersampling strategies like RUS, CNN, CNN TL, and TL aim to reduce the dominance of majority class instances.

Supervised machine learning techniques have traditionally been the cornerstone of fraud detection systems. However, Lakshika Sammani Chandradeva and others(2019) highlight a critical limitation of such approaches[4]: their reliance on labeled datasets for training, often scarce in real-world environments. Chandradeva propose an innovative solution leveraging unsupervised machine learning, particularly autoencoders, for fraud detection to address these challenges. By eschewing the need for labeled data, autoencoders offer a promising avenue for detecting fraudulent transactions accurately using raw transactional data—a ubiquitous resource in financial systems. The authors report impressive results, with the autoencoder achieving an AUC score of 83

III. Methodology

The methodology section outlines the process and techniques used to address the problem of credit card fraud detection. The approach integrates various steps, including data preprocessing, model selection, training, and evaluation.

A. Data Preprocessing

The credit card transaction dataset is loaded and contains features such as transaction amount, time, and other relevant parameters. Features and labels are separated, with features denoted as X and labels as y. The available data has been segregated into two subsets, namely training, and testing, maintaining an 80:20 ratio, which guarantees that the model has enough data for training while keeping a separate part for assessment.

In our dataset preprocessing phase, we employed robust scaling for the 'Amount' feature and normalized the 'Time' feature to enhance model performance and stability. Robust scaling, utilizing the formula:

This normalization brings the temporal data within a uniform range of 0 to 1, facilitating consistent representation across the dataset.

B. Model Selection and Training

Two primary models for fraud detection are logistic regression and a supervised autoencoder neural network. Logistic regression is a baseline model due to its simplicity and interpretability, making it suitable for initial comparisons. A supervised autoencoder neural network is selected as the primary model for its ability to capture nonlinear relationships and intricate patterns in the data, which is especially beneficial for detecting complex fraud patterns.

C. Training and Evaluation

Logistic regression involves training the model on the rebalanced training dataset and post-SMOTE application and assessing its performance using the designated testing set. Evaluation metrics, including accuracy, precision, recall, and F1-score, were calculated to gauge the model's effectiveness. Similarly, the supervised autoencoder neural network is trained on the resampled training dataset and evaluated using the testing set. The model's performance is evaluated using binary cross-entropy loss, and predictions are compared with ground truth labels to compute classification metrics. Confusion matrices are generated for both models to provide a detailed understanding of true positives, false positives, true negatives, and false negatives, facilitating a comprehensive evaluation of model performance.

D. Implementation

The logistic regression model and supervised autoencoder neural network are implemented using appropriate libraries such as sci-kit-learn and TensorFlow/Keras. The training process includes setting up the model architecture, compiling suitable loss functions and optimizers, and training for a specified number of epochs. Checkpoints are used to save the best-performing models during training, ensuring reproducibility and facilitating model deployment in real-world scenarios.

E. Performance Comparison

Finally, the performance of both models is compared in terms of various metrics, highlighting the strengths and weaknesses of each approach. Insights derived from the evaluation process are used to select the most effective model for credit card fraud detection, considering detection accuracy, computational efficiency, and interpretability.

Overall, the methodology provides a systematic framework for addressing the credit card fraud detection problem, leveraging traditional machine learning techniques like logistic regression and advanced deep learning approaches such as supervised autoencoder neural networks. The methodology aims to identify the most suitable model for detecting fraudulent transactions effectively and efficiently through rigorous training, evaluation, and comparison.

F. Figures and Tables

a) Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation "Fig. 1", even at the beginning of a sentence.

TABLE I
TABLE TYPE STYLES

Table Head	**Table Column Head**		
	Table column subhead	***Subhead***	***Subhead***
copy	More table copy[a]		

[a]Sample of a Table footnote.

Fig. 1. Example of a figure caption.

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity "Magnetization", or "Magnetization, M", not just "M". If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write "Magnetization (A/m)" or "Magnetization {A[m(1)]}", not just "A/m". Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

CONCLUSION

In conclusion, our investigation presents notable advancements in fraudulent transaction detection methodologies, particularly within credit card transactions. By employing innovative techniques such as autoencoder-based clustering, logistic regression, and supervised autoencoders, discernible enhancements in model efficacy have been realized. These improvements are distinctly evident in the substantial reduction of false positives and negatives, affirming our proposed methodologies' efficacy in accurately discerning fraudulent activities within transactional datasets. The rigorous evaluation encompassing a diverse array of performance metrics, including accuracy, precision, recall, and F1-score, corroborates our approaches' effectiveness. Our empirical findings underscore the pivotal role of robust preprocessing methodologies, notably exemplified by utilizing SMOTE resampling, in ameliorating the challenges posed by class imbalance inherent in transaction datasets. Furthermore, incorporating deep learning techniques demonstrates promising potential in augmenting the detection capabilities of fraudulent transactions, thereby fostering the development of more dependable and resilient fraud detection systems. Our study contributes meaningfully to the evolution of fraudulent transaction detection methodologies, providing valuable insights for deploying advanced machine learning algorithms in practical financial contexts. Looking ahead, continued exploration and refinement of these techniques and their integration into real-time transaction monitoring systems hold considerable promise for bolstering the security and integrity of financial transactions, thus mitigating the perils associated with fraudulent activities.

ACKNOWLEDGMENT

I would like to express my sincere appreciation to Professor Kanika Sood for her invaluable guidance and support throughout the duration of this research project. Additionally, I extend my gratitude to my institution, California State University Fullerton, for providing access to necessary resources.

REFERENCES

Please number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use "Ref. [3]" or "reference [3]" except at the beginning of a sentence: "Reference [3] was the first ..."

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [4]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

REFERENCES

[1] A. Singh, A. Singh, A. Aggarwal and A. Chauhan, "Design and Implementation of Different Machine Learning Algorithms for Credit Card Fraud Detection," 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Maldives, Maldives, 2022, pp. 1-6, doi: 10.1109/ICECCME55909.2022.9988588.

[2] Kanika and J. Singla, "Class Balancing Methods for Fraud Detection using Deep Learning," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 395-400, doi: 10.1109/ICAIS53314.2022.9742836.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.