Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.14, No.2, 2024

Fraud Guard: A Comprehensive Comparative Analysis of Machine Learning Approaches to Enhance Credit Card Fraud Detection

Omar Gheni Abdulateef
College Of Literature, University Of Samarra, Iraq
E-mail of the corresponding author: omar.ghani@uosamarra.edu.iq

Abstract
The COVID-19 pandemic has constrained people's mobility, prompting a surge in reliance on online services due to challenges in offline purchasing. Machine learning (ML) methods have played a crucial role in advancing classification and prediction techniques across various domains. In the realm of Credit Card Fraud Detection, the significance of ML is particularly pronounced. These methods harness the power of data-driven algorithms to distinguish between legitimate and fraudulent transactions, contributing significantly to the enhancement of security measures in financial transactions. The dynamic and adaptive nature of ML allows for the continuous evolution of fraud detection systems, ensuring a proactive approach to safeguarding against emerging threats in the credit card landscape. With this shift, credit card fraud has become a significant concern within the domain of internet-based transactions. Hence, there is a pressing demand to devise an optimal machine learning method for preventing fraudulent credit card transactions. The study employed four resampling techniques (CNN, AllKNN, SMOTE, and SVMSM) and three machine learning approaches (XGBoost , CatBoost, and RF) for analysing credit card fraud datasets with the aim of detection. These findings demonstrated that integrating AllKNN as an undersampling technique and CatBoost as a classifier are achieving superior results across the evaluated methods. The accuracy, precision, recall, and f1-score were 99.9%, 95.9%, 80%, and 87.4%, respectively.
Keywords: Unbalanced data, machine learning techniques, fraud detection, and credit card fraud.
DOI: 10.7176/JIEA/14-2-02
Publication date: March 31st 2024

1. Introduction.

The increasing trend of cashless society is causing a greater dependence on internet transactions. Contemporary fraud has evolved beyond the need for physical presence at crime scenes, allowing malevolent actors to operate discreetly from the confines of their homes. Various tactics for concealing identities further complicate the tracking process, encompassing methods like employing a VPN, directing victim traffic through the Tor network, and employing other sophisticated techniques. Tracing these perpetrators proves to be a formidable challenge.

The ramifications of online financial losses are profound and should not be underestimated. Once offenders gain access to card details, they have the option to exploit the cards directly or sell the pilfered information to others. In India, for instance, approximately 70 million individuals have fallen victim to this trend, with their card details circulating on the dark web [1]. The UK witnessed a particularly severe credit card fraud case, resulting in a staggering total about GBP 17 million in lost revenue. This incident unfolded when an international group of fraudsters collaborated to illicitly obtain detailed information from over 32,000 credit cards in the mid-2000s [2]. Regarded as the largest card fraud in history, it underscores the substantial financial repercussions arising from inadequate security measures [3]. Both cardholders, trusting in the integrity of their transactions, and card issuers, responsible for processing these transactions, often find themselves misled. Despite assurances of transactional security, fraudsters remain dedicated to duping financial institutions and cardholders, presenting a significant challenge to the prevailing belief in the benign nature of all transactions.

Furthermore, an ongoing concern involves surreptitious fraudulent transactions conducted for financial gain, evading detection by both card issuers and cardholders. The obscure nature of these unauthorized activities presents a significant challenge, as institutions and individuals may remain unaware of their occurrence within the realm of credit card transactions [4].

Various fraud detection techniques are employed in the financial industry to counteract such illicit activities. Predictive analytics and data mining are particularly important, and modelling algorithms that use anomaly detection and clustering approaches are used [5]. It is impossible to overestimate the importance of machine learning algorithms—supervised or unsupervised—in accurately identifying credit card fraud [6]. Despite their efficacy, these algorithms encounter numerous challenges in striving to identify all instances of fraudulent activity [7].

It becomes critical to optimise widely used evaluation criteria in the pursuit of the perfect machine learning model. To do this, the field must continue to advance, tackling issues with resampling strategies, cross-validation approaches, and machine learning algorithms. Understanding these elements is crucial to improving model

performance, as evidenced by the results' validation using reliable assessment measures.

In practical scenarios, attaining a balanced dataset is a rarity, leading to a prevailing challenge where classification algorithms tend to downplay the significance of the minority class. This issue becomes particularly pronounced in credit card fraud detection, where the minority class holds paramount importance. The proposed methodology in this study addresses the unbalanced distribution of classes by emphasizing the imbalance class challenge, employing diverse resampling techniques after identifying the most effective machine learning algorithms. This paper not only explores resampling techniques but also delves into enhanced cross-validation (CV) methods as integral components of the overall approach. Distinguished by its innovative perspective, this approach uniquely tackles the challenge of class imbalance within the dataset. The methodology stands out by not only comparing the efficacy of leading machine learning algorithms but also incorporating CV and diverse resampling techniques.

This paper introduces a sophisticated methodology for optimizing machine learning algorithms in conjunction with effective resampling techniques. The approach is structured in two stages, employing a meticulous analysis using performance evaluation metrics. In the initial stage, three algorithms — Extreme Gradient Boosting (XGBoost) [8], Random Forest (RF) [9], and Category Boosting (CatBoost) [12] undergo scrutiny. From this set, the most effective algorithm is selected for the second stage. The subsequent phase involves an in-depth examination of best resampling technique, each paired with the chosen algorithm from the first stage. The overarching objective of the second stage is to identify the optimal combination of ML approaches and resampling methods, thereby formulating the most effective model based on comprehensive performance evaluations.

The forthcoming sections of the paper are organized as follows: Commencing with the Related Work section, an in-depth exploration of prior studies unfolds, spotlighting their methodologies and addressing prevalent issues in the field. Proceeding from this, the proposed model section meticulously elaborates on the techniques employed to accomplish the paper's objectives. Subsequently, the results section provides a detailed description of the outcomes obtained through the application of the proposed model. Following this, a dedicated section conducts a comprehensive comparison of our proposed model with other published works utilizing the same dataset. The Conclusion section succinctly encapsulates the key findings and contributions of the study, while the Future Work section propounds potential directions for future research, pinpointing areas for continued exploration and development. This structured framework aims to provide a comprehensive understanding of the research process and outcomes.

2. Related work

Considering the significance of credit card fraud prevention, numerous effective methods have been established to thwart this nefarious activity. Financial institutions and banks play a crucial role not only in offering convenient financial services but also in serving as the primary defenders of cardholders against fraudulent activities. Furthermore, they actively invest in and advance a diverse range of strategies, incorporating cutting-edge technologies such as machine learning, which has become a cornerstone for many security systems.

One of the methodologies employed is Decision Trees (DT). Although it is straightforward to implement, it necessitates scrutinizing each transaction individually [16]. Khatri et al. [14] conducted an analysis using an imbalanced European credit card fraud detection (ECCFD) dataset, exploring various models without incorporating resampling techniques. Their findings revealed that DT generally outperformed other methods, displaying commendable Recall (79.21%), Precision (85.11%), and processing time (5 s). On the other hand, K-Nearest Neighbors (KNN) demonstrated superior Recall (81.19%) and Precision (91.11%) but lagged in processing time (463 s).

Taha and Malebary [15] employed LightGBM as a key strategy, conducting experiments on two datasets: ECCFD and the UCSD-FICO Data Mining Contest 2009 dataset. Their approach involved optimizing Light Gradient Boosting Machine (OLightGBM) by integrating hyper-parameter tuning with advanced techniques, utilizing a 5-fold version of K-Fold Cross-Validation. Across both datasets, OLightGBM consistently outperformed other methods. For instance, on the ECCFD dataset, OLightGBM achieved an AUC of 90.94%, accuracy of 98.40%, recall of 40.59%, precision of 97.34%, and F1-score of 56.95%. Similarly, on the UCSD-FICO dataset, OLightGBM demonstrated notable performance with an AUC of 92.88%, accuracy of 98.35%, recall of 28.33%, precision of 91.72%, and F1-score of 43.27%.

In pursuit of other options, scientists investigated the fields of K-Nearest Neighbours (KNN) and Logistic Regression (LR). Using the unbalanced ECCFD dataset, Vengatesan et al. [16] carefully examined the LR and KNN performances. KNN performed exceptionally well, as seen by its 95% Precision, 72% Recall, and 82% F1-Score. In a different study, Random Forest (RF), Support Vector Machine (SVM), and LR were the three algorithms that Puh and Brkić [17] tested using the European cardholder dataset. They used the Synthetic Minority Oversampling Technique (SMOTE) to correct the class imbalance. The two learning models that were used were incremental and static. LR was used in both cases, with specific parameter modifications (C set to 100, L2-Regulation). The AUC scores for incremental learning were 91.07%, and for static learning they were 91.14%.

The corresponding average precision scores were 73.37% and 84.13%.

Turning attention to Random Forest (RF), Hema [18] assessed the ECCFD dataset without addressing class imbalance, employing RF, LR, and Category Boosting (CatBoost). RF emerged as the top performer, achieving notable metrics such as 99.95% Accuracy, 91.95% Precision, 79.2% Recall, 85.1% F1-Score, 85.31% Matthews Correlation Coefficient (MCC), and 89% AUC. In a simpler exploration, Kumar et al. [19] conducted a basic study using RF on the ECCFD dataset, yielding a 90% accuracy rate.

Exploring the realm of Artificial Neural Networks (ANN), Asha and KR [20] conducted a comparative analysis of SVM, KNN, and ANN models using the ECCFD dataset. Notably, the ANN model exhibited superiority, achieving remarkable performance metrics with 99.92% Accuracy, 81.15% Precision, and 76.19% Recall. In a distinct study focusing on the Credit Card Customer dataset, Dubey et al. [1] implemented an ANN architecture comprising input, hidden (15 neurons with RELU activation function), and output layers (Sigmoid activation function). Impressively, their ANN model delivered exceptional results, attaining 99.92% Accuracy, 99.96% Recall, 99.96% Precision, and 99.96% F1-Score. Furthermore, Varmedja et al. [22] adopted a comprehensive approach, partitioning the ECCFD dataset in an 80:20 ratio and deploying LR, RF, Naive Bayes (NB), Multilayer Perceptron, and ANN models. Employing SMOTE to address imbalanced data, RF emerged as the leading performer, boasting outstanding metrics, including 99.96% Accuracy, 81.63% Recall, and 96.38% Precision. These studies collectively underscore the efficacy and versatility of ANN models in diverse domains, showcasing their potential to deliver robust and high-performing solutions.

Multiple research endeavors have delved into assessing the efficacy of Local Outlier Factor (LOF) and Isolation Forest (iForest) algorithms for anomaly detection. LOF operates by pinpointing outliers through local density analysis [23], whereas iForest employs a tree-based approach for outlier detection [24]. John and Naaz [25] undertook a comparative study utilizing both LOF and iForest algorithms on the ECCFD dataset, however, without addressing the imbalanced class problem inherent in the dataset. The findings indicated that LOF attained the highest accuracy rate, reaching 97%.

When examining related work, it becomes evident that multiple considerations are essential for effectively detecting fraudulent activity in credit card transactions. Each approach employs a distinct methodology to enhance model performance. However, the outcome of a machine learning algorithm can vary across approaches. To gain a comprehensive understanding of algorithm performance, increasing the diversity of algorithms in experiments is advisable. Addressing the common issue of imbalanced classes in datasets is crucial, and this can be accomplished through the application of stratified cross-validation and various resampling techniques. Numerous resampling techniques are available for experimentation. Additionally, the choice of evaluation metrics plays a vital role in assessing a model's performance comprehensively from different perspectives.

It is noteworthy that some prior works that omit one or more of these essential components. Thus, there is a need for an innovative approach that incorporates a broader range of algorithms, addresses class imbalance, and employs diverse evaluation metrics to provide a more comprehensive assessment of model performance.

3. The proposed model

The proposed model is devised through a meticulous voting process, selecting the most effective classifier among three contenders, each assessed for optimal performance on the same Credit Card Fraud Detection dataset. Subsequently, this selected classifier is seamlessly integrated with the most efficient resampling methods. The holistic outcome encapsulates the synergy of the best classifier and resampling approaches, as illustrated in Figure 1. This approach ensures a robust and tailored solution for Credit Card Fraud Detection based on the specific demands of the dataset.

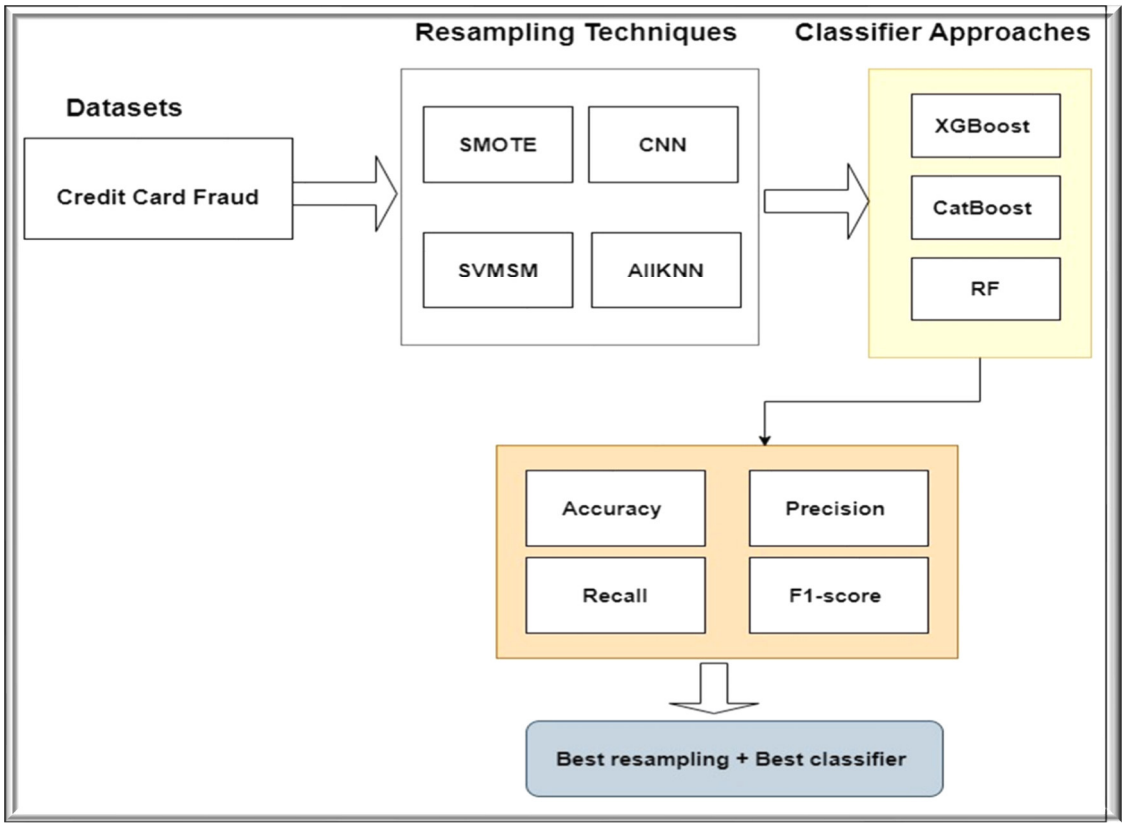

Figure 1: The proposed model flowchart.

3.1 Experimental Framework

3.1.1 Software

The investigation is carried out on a 64-bit Windows 10 machine in a virtual environment. Python 3.8, Jupyter Notebook 6.1.4, and Anaconda Navigator 1.10.0 are set up on the server. Essential libraries like as Scikit-Learn, Pandas, Numpy, Seaborn, Matplotlib, and Imbalanced-Learn are included in the Anaconda Navigator environment along with a number of machine learning classifiers.

3.1.2 Hardware

The developed model is implemented using the Intel core i7-8565U processor and 32 GB RAM.

3.2 Dataset

This dataset contains transaction records spanning a two-day period, with 492 identified as fraudulent out of a total of 284,807 transactions. It's important to note that the dataset exhibits a significant class imbalance, as the positive class (fraudulent transactions) represents only 0.172% of the entire transaction dataset [26].

Preprocessing may not always be necessary, especially when specific criteria are met. One crucial criterion involves checking for missing values that could impact predictions. Upon inspecting the dataset, it is observed that each feature contains 284,807 values, indicating the absence of missing values. Consequently, preprocessing is deemed unnecessary. Figure 2 presents the correlation matrix accompanied by a heat map. The correlation matrix serves as a valuable tool for assessing the necessity of feature removal. The matrix reveals that all features are correlated with the 'Class' feature, irrespective of the strength of the correlation. This leads to the determination that no feature removal is required, and therefore, preprocessing is not warranted. Additionally, features 'V1' through 'V28' result from a PCA dimensionality reduction transformation, performed to safeguard sensitive information in the original data. Since the dataset has already undergone this processing, deliberately avoiding further preprocessing is opted for, ensuring a more realistic approach.

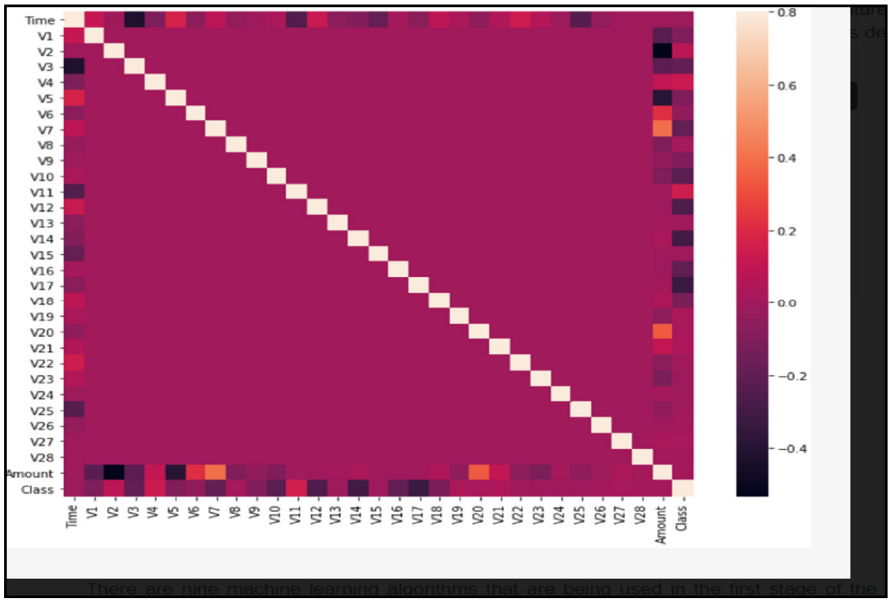

Figure 2: correlation matrix.

3.3 Classifier Approaches

In this study, three classifier approaches were employed to identify the most effective classifier with superior performance compared to others. The classifiers are outlined as follows:

3.3.1 CatBoost

Within the family of decision tree (DT) classifiers, one notable example is CatBoost. Researchers and engineers at Yandex have created this sophisticated, open-source gradient boosting library for decision trees [27]. CatBoost stands out for its versatility, offering applicability across a diverse range of tasks and problem domains.

3.3.2 XGBoost

XGBoost is a well-known decision tree-based ensemble machine learning classifier and another member of the decision tree (DT) family. Utilising a collection of classification and regression trees (CART) to improve its prediction power, XGBoost functions within a gradient boosting framework [28].

3.3.3 Random Forest

Random Forest (RF) operates as a supervised learning method, forming an ensemble of multiple decision trees (DTs). It involves a three-step process [29]: 1) The input data is partitioned into various subsets, and decision trees are constructed using random sets of features. 2) Determining two crucial hyperparameters, namely the number of trees and the count of randomly selected features at each tree node. 3) For predicting new unknown data classes, RF leverages the collective insights from decision trees to identify the most accurate prediction. As described in Figure 3.

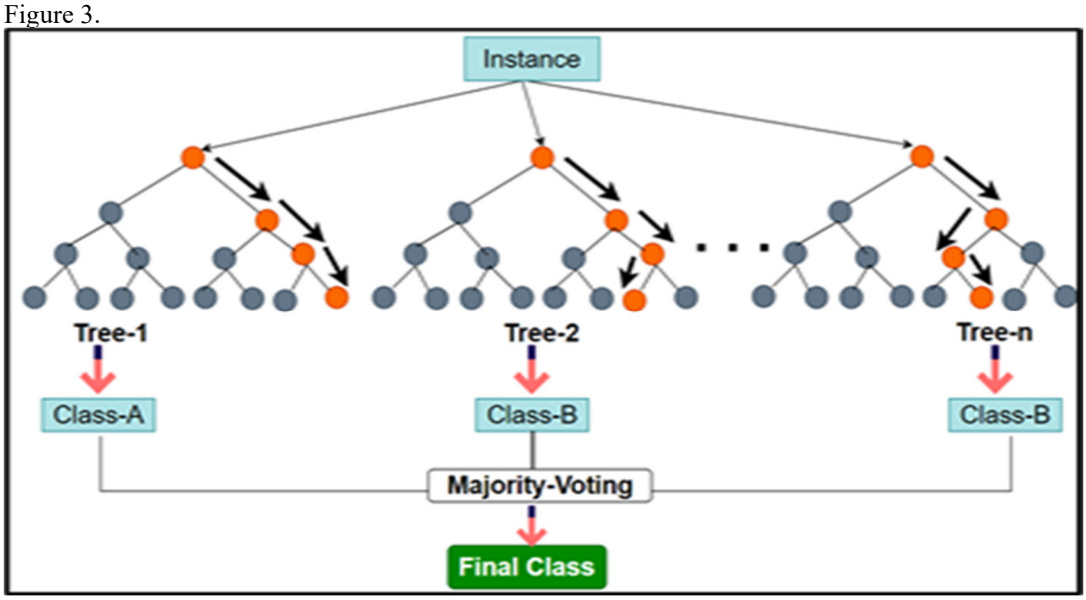

Figure 3: Random Forest Process

3.4 Resampling Methods

To address the class imbalance in a dataset [30], resampling techniques are commonly employed. In the current dataset, there are 284,315 valid cases and 492 fraud cases, with valid cases constituting 99.827% and fraud cases representing only 0.173% of the total instances. Clearly, the dataset is highly unbalanced, highlighting the need for resampling techniques. The effectiveness of algorithms is closely tied to how the imbalance class issue is handled [31].

3.4.1 Undersampling.

Undersampling methods are recognized for creating a concise and balanced training set, offering the advantage of reducing the computational costs during the learning phase [32]. However, a drawback associated with undersampling techniques is the substantial removal of instances from the majority class in situations where it is significantly larger. This removal can result in the loss of critical cases, posing challenges for accurate classification and prediction.

3.4.2 Oversampling.

In contrast to undersampling, oversampling methods are designed to retain instances from the majority class while duplicating instances from the minority class to address imbalanced training sets. However, a drawback of this approach is the potential for poor model performance, as generating accurate representations of the minority class data in the training set can be challenging [33,34].

3.5 Cross-Validation (CV).

CV is a statistical technique employed in machine learning (ML) to mitigate or eliminate overfitting issues across various classifier paradigms. The k-fold cross-validation approach involves training a model on multiple training datasets, not just one. By partitioning the dataset into k-folds and training the model on each fold, the model achieves better generalization, indicating robustness [35]. This approach also provides a more accurate assessment of the algorithmic prediction performance. Illustrated in Figure 4, the dataset is divided into k-folds, typically with k set to 5.

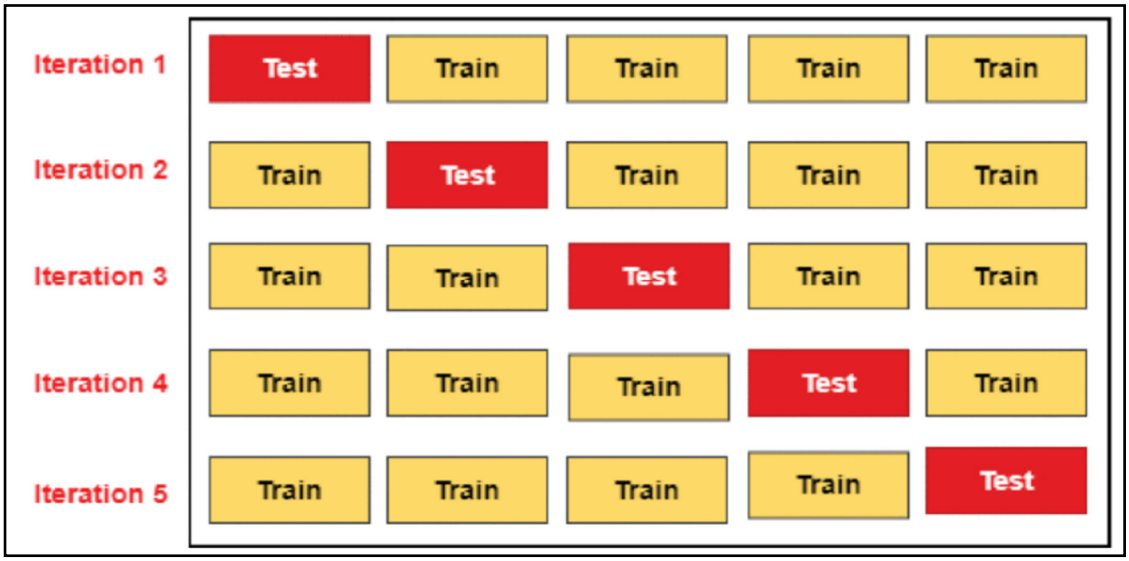

Figure 4: Cross validation with K=5 [35]

3.6 Evaluation Performance

3.6.1 Accuracy (Acc) [36]

Accuracy, synonymous with the error rate, serves as a metric to determine the classifier's effectiveness in correctly classifying data points . Equation (1) outlines the calculation of accuracy, expressed as the ratio of correctly classified cases (true positives for fraud (TP) and true negatives for non-fraud (TN)) to the total number of cases in the dataset.

$$\text{Acc} = \frac{TP+TN}{TP+FN+TN+FP} \qquad (1)$$

3.6.2 Precision (Pre) [37]

Precision and Recall are two separate assessment criteria that function differently to achieve goals. Precision and recall frequently have to be traded off; a rise in precision might cause a fall in recall, and vice versa. Equation (2) shows that precision, sometimes referred to as positive predictive value, evaluates how well positive cases were predicted relative to all positive cases.

$$\text{Pre} = \frac{TP}{TP+FP} \quad (2)$$

3.6.3 Recall (Rec) [36]

Recall, also referred to as sensitivity, is defined as the average probability of complete retrieval. The recall formula is expressed as Equation (3) :

$$\text{Rec} = \frac{TP}{TP+FN} \quad (3)$$

3.6.4 F1-score [37]

A perfect F1 score is equal to 1, while the lowest score is equal to 0. The F1 score is a weighted average of precision and recall.

$$\text{F1} = 2 * \frac{Precision*Recall}{Precision+Recall} \quad (4)$$

4. Results

4.1 Experiment results.

After analysing the results from three tables (Table 1, Table 2, and Table 3) comparing three classifiers (CatBoost, XGBoost, and RF) alongside four resampling techniques two undersampling methods (CNN and AllKNN) and two oversampling methods (SMOTE and SVMSM)—it is evident that AllKNN and CatBoost consistently outperformed the other approaches. These findings highlight the effectiveness of AllKNN as an undersampling technique and CatBoost as a classifier in achieving superior results across the evaluated methods. The results were 99.9%, 95.9%, 80%, 87.4% for accuracy, precision, recall , and f1-score respectively.

Table 1: CatBoost with Resampling Methods.

Classifier approach	Accuracy%	Precision%	Recall%	F1-score%
SMOTE	99.9	72.56	84.76	78
CNN	99.8	49.9	85.9	63
SVMSM	99.9	85.8	82	84
AllKNN	99.9	95.9	80	87.4

Table 2: XGBoost with Resampling Methods.

Classifier approaches	Accuracy%	Precision%	Recall%	F1-score%
SMOTE	99.95	86	83.94	85
CNN	99.76	41	86.38	55.58
SVMSM	99.96	93	80.89	86.52
AllKNN	99.96	94.53	80	86.7

Table 3: RF with Resampling Method.

Classifier approaches	Accuracy%	Precision%	Recall%	F1-score%
SMOTE	99.95	89.94	83	86.39
CNN	99.87	58	85.77	69
SVMSM	99.96	95	79	86.57
AllKNN	99.96	95	79	86

4.2 Comparing to prior studies.

In ensuring a comprehensive and equitable comparison, the proposed model has been meticulously evaluated against 8 previously published works that utilized the same datasets. This rigorous comparative analysis aims to provide a thorough understanding of the proposed model's performance within the broader context of existing research efforts. As discussed in Table 4.

Table 4 : Comparing the proposed model against other published work.

Ref.	Approach	Accuracy %	Precision %	Recall %	F1-score %
[43]	RF	99.95	79	91.95	85
[15]	LGBM+Hyper-Parameter	98.4	0.4059	97.34	56.95
[16]	KNN	None	72	95	82
[14]	KNN	None	81	91	None
[20]	ANN	99.92	76	81	None
[21]	RF+SMOTE	99.96	0.8163	0.9638	None
[25]	LOF	97	None	None	None
[19]	RF	90	None	None	None
The proposed	AllKNN-CatBoost	99.96	95.9	80	87.4

5. Conclusion and Future direction

As reliance on online transactions and credit cards grows, criminals and fraudsters continually evolve their methods to exploit financial vulnerabilities. However, it is imperative to adopt a proactive strategy by ML approaches to effectively combat this issue, irrespective of the evolving sophistication of countermeasures.

The suggested methodology unfolds in two phases. The first phase focuses on selecting an optimal ML algorithm among three candidates. In the second stage, the chosen algorithm is integrated with four resampling techniques. The evaluation criteria encompass evaluation metrics for each model. The three initial algorithms are RF, XGBoost , and CatBoost . Subsequently, the four resampling techniques are categorized into two undersampling and two oversampling methods. The model that emerges as the most effective is the combination of AllKNN with CatBoost (AllKNN-CatBoost). These findings highlight the effectiveness of AllKNN as an undersampling technique and CatBoost as a classifier in achieving superior results across the evaluated methods. The results were 99.9%, 95.9%, 80%, 87.4% for accuracy, precision, recall , and f1-score respectively. To gauge its performance, AllKNN-CatBoost is benchmarked against prior studies using the same dataset and employing similar methodologies.

Prospective research avenues could involve exploring alternative datasets and employing different optimization algorithms. Some noteworthy algorithms for consideration include Monarch Butterfly Optimization (MBO) [38], Earthworm Optimization Algorithm (EWA) [39], Elephant Herding Optimization (EHO) [40], Moth Search (MS) algorithm [41], Slime Mold Algorithm (SMA), and Harris Hawks Optimization (HHO) [42].

References

[1] Dubey, S.C.; Mundhe, K.S.; Kadam, A.A. Credit Card Fraud Detection using Artificial Neural Network and BackPropagation. In Proceedings of the 2020 4th International
[2] Conference on Intelligent Computing and Control Systems (ICICCS), Rasayani, India, 13–15 May 2020; pp. 268–273.
[3] Alfaiz, N.S.; Fati, S.M. Enhanced Credit Card Fraud Detection Model Using Machine Learning. Electronics 2022, 11, 662. https://doi.org/10.3390/electronics11040662.
[4] Zhang, X.; Han, Y.; Xu, W.; Wang, Q. HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Inf. Sci. 2019, 557, 302–316.
[5] McCue, C. Advanced Topics. Data Mining and Predictive Analysis; Butterworth-Heinemann: Oxford, UK, 2015; pp. 349–365.
[6] Berad, P.; Parihar, S.; Lakhani, Z.; Kshirsagar, A.; Chaudhari, A. A Comparative Study: Credit Card Fraud Detection Using Machine Learning. J. Crit. Rev. 2020, 7, 1005. [Google Scholar]
[7] Jain, Y.; Namrata, T.; Shripriya, D.; Jain, S. A comparative analysis of various credit card fraud detection techniques. Int. J. Recent Technol. Eng. 2019, 7, 402–403. [Google Scholar]
[8] Shirodkar, N.; Mandrekar, P.; Mandrekar, R.S.; Sakhalkar, R.; Kumar, K.C.; Aswale, S. Credit card fraud detection techniques–A survey. In Proceedings of the 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Shiroda, India, 13–15 May 2020; pp. 1–7.
[9] Shirodkar, N.; Mandrekar, P.; Mandrekar, R.S.; Sakhalkar, R.; Kumar, K.C.; Aswale, S. Credit card fraud detection techniques–A survey. In Proceedings of the 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Shiroda, India, 13–15 May 2020; pp. 1–7.
[10] Zareapoor, M.; Seeja, K.; Alam, M.A. Analysis on credit card fraud detection techniques: Based on certain design criteria. Int. J. Comput. Appl. 2012, 52, 35–42
[11] Q. Wang, "Support Vector Machine Algorithm in Machine Learning," 2022 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Dalian, China, 2022, pp. 750-756.
[12] YandexTechnologies. CatBoost. Available online: https://yandex.com/dev/catboost/ (accessed on 22 January 2022).
[13] Delamaire, Linda, H. A. H. Abdou, and John Pointon. "â€ œCredit card fraud and detection techniques: are view." (2009).
[14] Khatri, Samidha, Aishwarya Arora, and Arun Prakash Agrawal. "Supervised machine learning algorithms for credit card fraud detection: a comparison." 2020 10th international conference on cloud computing, data science & engineering (confluence). IEEE, 2020.
[15] Taha, Altyeb Altaher, and Sharaf Jameel Malebary. "An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine." IEEE Access 8 (2020): 25579-25587.
[16] Vengatesan, K., et al. "Credit card fraud detection using data analytic techniques." Advances in Mathematics: Scientific Journal 9.3 (2020): 1185-1196.
[17] Puh, Maja, and Ljiljana Brkić. "Detecting credit card fraud using selected machine learning algorithms." 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2019.
[18] Hema, Appala. "Machine Learning methods for Discovering Credit Card Fraud. IRJCS:: International

Research Journal of Computer Science, Volume VIII, 01-06." (2020).
[19] Kumar, M.S.; Soundarya, V.; Kavitha, S.; Keerthika, E.; Aswini, E. Credit card fraud detection using random forest algorithm. In Proceedings of the 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 21–22 February 2019; pp. 149–153.
[20] Asha, R.; KR, S.K. Credit card fraud detection using artificial neural network. Glob. Trans. Proc. 2021, 2, 35–41.
[22] Varmedja, D.; Karanovic, M.; Sladojevic, S.; Arsenovic, M.; Anderla, A. Credit card fraud detection-machine learning methods. In Proceedings of the 2019 18th International Symposium Infoteh-Jahorina (Infoteh), Novi Sad, Serbia, 20–22 March 2019; pp. 1–5.
[23] Breunig, M.M.; Kriegel, H.P.; Ng, R.T.; Sander, J. LOF: Identifying density-based local outliers. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, Dallas, TX, USA, 15–18 May 2000; pp. 93–104.
[24] Liu, F.T.; Ting, K.M.; Zhou, Z.H. Isolation Forest. In Proceedings of the 2008 Eighth IEEE International Conference on Data Mining, Ballarat, VIC, Australia, 15–19 December 2008; pp. 413–422.
[25] John, H.; Naaz, S. Credit card fraud detection using local outlier factor and isolation forest. Int. J. Comput. Sci. Eng 2019, 7, 1060–1064.
[26] Dal Pozzolo, A.; Caelen, O.; Johnson, R.A.; Bontempi, G. Calibrating probability with undersampling for unbalanced classification. In Proceedings of the 2015 IEEE Symposium Series on Computational Intelligence, Cape Town, South Africa, 7–10 December 2015; pp. 159–166.
[27] Yandex Technologies. CatBoost. Available online: https://yandex.com/dev/catboost/ (accessed on 22 January 2022).
[28] XGBoost Developers. Introduction to Boosted Trees. Available online: https://xgboost.readthedocs.io/en/latest/tutorials/model.html (accessed on 22 January 2022).
[29] M. Khalsan, M. Mu, E. S. Al-Shamery, L. Machado, M. O. Agyeman and S. Ajit, "Intersection Three Feature Selection and Machine Learning Approaches for Cancer Classification," 2023 International Conference on System Science and Engineering (ICSSE), Ho Chi Minh, Vietnam, 2023, pp. 427-433, doi: 10.1109/ICSSE58758.2023.10227163.
[30] Scikit-Learn-Contrib. Imbalanced-Learn. Available online: https://github.com/scikit-learn-contrib/imbalanced-learn (accessed on 22 January 2022).
[31] He, H.; Garcia, E.A. Learning from imbalanced data. IEEE Trans. Knowl. Data Eng. 2009, 21, 1263–1284.
[32] Dal Pozzolo, A.; Caelen, O.; Bontempi, G. When is undersampling effective in unbalanced classification tasks? In Proceedings of the Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Porto, Portugal, 7–11 September 2015; pp. 200–215.
[33] García, V.; Mollineda, R.A.; Sánchez, J.S. On the k-NN performance in a challenging scenario of imbalance and overlapping. Pattern Anal. Appl. 2008, 11, 269–280.
[34] Cieslak, D.A.; Chawla, N.V. Start globally, optimize locally, predict globally: Improving performance on imbalanced data. In Proceedings of the 2008 Eighth IEEE International Conference on Data Mining, Notre Dame, IN, USA, 15–19 December 2008; pp. 143–152.
[35] M. Khalsan, M. Mu, E. S. Al-Shamery, S. Ajit, L. R. Machado and M. Opoku Agyeman, "A Novel Fuzzy Classifier Model for Cancer Classification Using Gene Expression Data," in IEEE Access, vol. 11, pp. 115161-115178, 2023.
[36] M. Khalsan, M. Mu, E. S. Al-shamery, L. Machado, M. O. Agyeman and S. Ajit, "Enhancing Cancer Classification Through the Development of a Fuzzy Gene Selection-Wrapper Plus Method," 2023 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET), Kota Kinabalu, Malaysia, 2023, pp. 39-44.
[37] M. Khalsan et al., "A Survey of Machine Learning Approaches Applied to Gene Expression Analysis for Cancer Prediction," in IEEE Access, vol. 10, pp. 27522-27534, 2022, doi: 10.1109/ACCESS.2022.3146312.
[38] Wang, G.-G.; Deb, S.; Cui, Z. Monarch butterfly optimization. Neural Comput. Appl. 2019, 31, 1995–2014.
[39] Ghosh, I.; Roy, P.K. Application of earthworm optimization algorithm for solution of optimal power flow. In Proceedings of the 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, India, 18–20 March 2019; pp. 1–6.
[40]Wang, G.-G.; Deb, S.; Coelho, L.d.S. Elephant herding optimization. In Proceedings of the 2015 3rd International Symposium on Computational and Business Intelligence (ISCBI), Xuzhou, China, 7–9 December 2015; pp. 1–5.
[41]Wang, G.-G. Moth search algorithm: A bio-inspired metaheuristic algorithm for global optimization problems. Memetic Comput. 2018, 10, 151–164.
[42] Heidari, A.A.; Mirjalili, S.; Faris, H.; Aljarah, I.; Mafarja, M.; Chen, H. Harris hawks optimization: Algorithm and applications. Future Gener. Comput. Syst. 2019, 97, 849–872.
[43] Hema, A. Machine Learning methods for Discovering Credit Card Fraud. Int. Res.J. Comput. Sci. 2020, 8, 1–6.