International Journal of Safety and Security Engineering
Vol. 15, No. 6, June, 2025, pp. 1243-1250
Journal homepage: http://iieta.org/journals/ijsse

A Hybrid Oversampling Approach for Fraud Detection: Integrating SMOTE-ENN and ADASYN

Ammar Ali Mustafa[1*], Haneen Mohammed Hussein[1], Mohammed Mundher Kadhim[2], Marwan J. Hussein[1]

[1] Division of Construction and Projects, Mustansiriyah University, Baghdad 10064, Iraq
[2] Center of Continuing Education, University of Information and Communication Technology (UoITC), Baghdad 10067, Iraq

Corresponding Author Email: ammar.ali@uomustansiriyah.edu.iq

https://doi.org/10.18280/ijsse.150614

Received: 2 May 2025
Revised: 11 June 2025
Accepted: 22 June 2025
Available online: 30 June 2025

Keywords:
machine learning, fraud detection systems, class imbalance, hybrid resampling, ADASYN, SMOTE-ENN, credit card fraud, credit card transactions

ABSTRACT

Detecting financial fraud is challenging due to class imbalance in transactional datasets, where legitimate transactions vastly outnumber fraudulent ones. This imbalance biases traditional machine learning models toward the majority class, leading to high false negative rates despite high overall accuracy. To address this, the study proposes a hybrid oversampling method combining SMOTE-ENN and ADASYN to enhance detection performance. Initially, seven machine learning models were evaluated using SMOTE, with Random Forest, KNN, and XGBoost achieving the highest scores in accuracy, recall, and F1-score. These models were further tested using the proposed hybrid method, which integrates noise removal (via SMOTE-ENN) with adaptive minority sampling (via ADASYN). The hybrid approach significantly improved recall and F1-score, especially for Random Forest and XGBoost, achieving up to 99.99% accuracy. Results confirm that combining hybrid oversampling with robust classifiers reduces false negatives and improves generalization in fraud detection systems.

1. INTRODUCTION

The speedy digitization of the financial services sector has, on the one hand, made a quantum leap in online transactions; on the other hand, it has also exponentially increased various types of financial crimes, particularly credit card fraud. The damages dealt with by these malpractices are enormous to consumers, institutions, and governments. A top priority that needs to be timely manner is effective and efficient banking and financial fraud. Machine learning is being increasingly adopted as a powerful approach since it can discern complicated regularities plus anomalies within large volumes of data concerning transactions.

A big problem in fraud spotting is the natural class skew of the data, where the count of real transactions greatly outnumbers the fake ones. This skew can badly limit how well normal machine learning models work since they often get biased towards the larger class [1]. To fix this, data-level rebalancing techniques like the Synthetic Minority Over-Sampling Technique (SMOTE) have been used a lot to artificially balance datasets before training.

In this work, we start by assessing the accuracy of seven popular machine learning classifiers—Random Forest, Logistic Regression, XGBoost, Stochastic Gradient Descent Classifier (SGD-SVM), K-Nearest Neighbors (KNN), Naïve Bayes, and Multi-Layer Perceptron (MLP)—with the application of the conventional SMOTE technique. After setting this baseline assessment, we pick out the best-performing models among them (Random Forest, XGBoost, and KNN) and expose them to even more advanced resampling techniques namely SMOTE-ENN which combines SMOTE with Edited Nearest Neighbors for noise reduction as well as ADASYN that adaptively focuses on hard-to-classify minority examples.

In the end, to make the model even stronger and better at finding smaller groups, we use a mix of methods that bring together SMOTE-ENN and ADASYN. This mixed approach is made to use the good points of both ways—SMOTE-ENN's skill in tidying up where decisions are made and ADASYN's focused way of creating examples—to make the classifier work better when there is a big difference. The results show that using hybrid resampling not only improves recall and the F1-score but also keeps things stable across different ways of measuring, making it a very good method for fraud detection systems in the real world [2].

This paper's key contribution lies in its experimental comparison of individual and hybrid resampling techniques, and the introduction of a novel hybrid method that combines SMOTE-ENN and ADASYN. This approach aims to address both class imbalance and noise reduction more effectively than traditional methods, ultimately enhancing fraud detection system performance in real-world applications.

2. CONTRIBUTION

2.1 Comprehensive evaluation of multiple classifiers

The output of widely used machine learning models was initially tested—Random Forest, Logistic Regression,

XGBoost, Stochastic Gradient Descent Classifier (SGD-SVM), K-Nearest Neighbors (KNN), Naïve Bayes, and Multi-Layer Perceptron (MLP)—on a big and unbalanced credit card action data set. This first check gives a benchmark compare under normal oversampling rules.

2.2 Analysis of traditional SMOTE oversampling

This study first applies the widely-used Synthetic Minority Oversampling Technique (SMOTE) to deal with class imbalance and its effects on different classifiers. This step will find out how standard oversampling impacts the sensitivity and generalization of various models.

2.3 Advanced resampling with SMOTE-ENN and ADASYN

The best classifiers (Random Forest, XGBoost, and KNN) from the first round are tested again using fancier methods.

2.4 Development and evaluation of a hybrid resampling strategy

A mixed oversampling approach, combining SMOTE-ENN and ADASYN, was proposed and evaluated. This new combination tries to reduce noise at the same time as improving minority class representation. The mixture technique demonstrates much better performance especially in increasing recall and F1-score without sacrificing precision and also without causing overfitting.

2.5 Real-world relevance and model robustness

The combined approach's steady results across both training and test data prove its strength and possible fit for use in real-life fraud spotting systems, where lowering missed cases is very important.

3. RELATED WORK

Recent studies explored different machine learning techniques toward fraud detection in financial transactions. In one study, the authors highlighted how neural network methods are being applied for classification [3]. A number of machine learning algorithms for credit card fraud detection have been reviewed and made diverse predictions and conclusions [4-8]. Both classification and ensemble learning approaches were employed by these studies to effectively detect fraudulent transactions.

Zhu et al. [9] combined Neural Nets and the Synthetic Minority Over-sampling Technique (SMOTE) to deal with data imbalance in detecting fraud on credit cards. This improved precision and recall. Just like that, Alshameri and Xia [10] looks at the effect of the Synthetic Minority Oversampling Technique (SMOTE) on how well different machine learning methods work at finding fraud in credit cards. Zhao and Bai [11] applied SMOTE and machine learning algorithms to predict financial fraud in listed companies. They commented on the importance of class imbalance being addressed. Ileberi et al. [12] studied presents a machine learning framework for credit card fraud detection imbalanced datasets challenge Synthetic Minority Over-samplingTechnique (SMOTE) theirs benchmarking several machine learning algorithms Support Vector Machine (SVM), Logistic Regression (LR), Random Forest (RF), Extreme Gradient Boosting (XGBoost), Decision Tree (DT), Extra Tree (ET) with Adaptive Boosting (AdaBoost).

Another contribution is by Ghaleb et al. [13] who proposed a new model to credit card fraud detection using Ensemble Synthesized Minority Oversampling techniques along with Generative Adversarial Networks (ESMOTE-GAN) and Random Forest algorithm giving solution to class imbalance issue. Khalid et al. [14] proposed a new ensemble machine learning model that integrates Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Random Forest (RF), Bagging and Boosting classifiers. Du et al. [15] proposed a novel method called AutoEncoder with probabilistic LightGBM (AED-LGB) for detecting credit card frauds.

Bonde and Bichanga [16] proposed a novel ensemble deep learning-based approach that combines Convolutional Neural Networks (CNN), Gated Recurrent Units (GRU), and Multilayer Perceptron (MLP) with the Synthetic Minority Oversampling Technique and Edited Nearest Neighbors (SMOTE-ENN) to address class imbalance and improve detection accuracy. Mienye and Sun [17] Suggested a strong deep-learning way that combines Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) neural networks as base learners inside a stacking ensemble framework, with a Multilayer Perceptron (MLP) acting as the meta-learner. About ADASYN, the research by He et al. [18] proposed ADASYN, an adaptive approach to generate synthetic data focusing more on minority samples that are harder to learn. Ahmed et al. [19] proposed an ensemble machine-learning model for detecting fraudulent credit card transactions. It incorporates the Synthetic Minority Oversampling Technique (SMOTE) with Edited Nearest Neighbor (ENN) to address the problem of the imbalanced datasets.

Another study explored combining SMOTE and GANs and showed that hybrid techniques like SMOTified-GANs outperform standalone methods in detecting fraudulent activities.

In summary, class imbalance handling has improved with SMOTE and its variations, including Borderline-SMOTE and ADASYN; yet, many of these methods handle noisy data arbitrarily. While methods such as SMOTE-ENN are useful for removing noise from data, they might not be as effective at producing varied minority occurrences. By improving minority class representation and data quality, the hybrid strategy suggested in this study, on the other hand, makes use of both ADASYN's adaptive sampling and SMOTE-ENN's noise reduction capabilities to provide a more reliable solution. Our results demonstrate that this dual mechanism leads to greater recall and F1-scores, especially for high-stakes classifiers like Random Forest and XGBoost.

4. METHODOLOGY

4.1 Dataset

This study employs a real-world credit card transaction dataset obtained from a Kaggle repository, which contains 1,000,000 anonymized records and 8 characteristics. The binary target variable in the eighth column indicates whether a transaction is legitimate (0.0) or fraudulent (1.0), with 912,597 non-fraudulent and 87,403 fraudulent cases, demonstrating a substantial class imbalance common in fraud

detection tasks [20]. The dataset, which has no missing values, only comprises numerical characteristics that have previously been standardized using PCA transformation, removing the need for additional normalization. Because of their predictive relevance, all PCA-transformed variables (V1 through V28) and the transaction Amount were automatically retained. To ensure the quality of the input for model training and evaluation, the data was pre-processed by separating predictors and target features, followed by a stratified train-test split to preserve class distribution. Standardizing procedures was also used where applicable to guarantee that all features contributed uniformly. Figure 1 shows a sample of the dataset and its important features.

To address class imbalance and enhance the models' ability to detect fraud, multiple data balancing techniques were explored, including SMOTE, ADASYN, and SMOTE-ENN. These techniques were integrated into the training pipeline to improve the detection of fraudulent transactions, particularly by increasing sensitivity (recall) on the minority class. Figure 2 is a representation of no. of Fraudulent and non-Fraudulent transactions in our dataset.

The dataset's extreme class imbalance is depicted in the above Figure, which might lead to misleadingly high accuracy while failing to detect fraudulent transactions, a minority class.

```
w=pd.read_csv('card_transdata.csv')
w
```

	distance_from_home	distance_from_last_transaction	ratio_to_median_purchase_price	repeat_retailer	used_chip	used_pin_number	online_order	fraud
0	57.877857	0.311140	1.945940	1.0	1.0	0.0	0.0	0.0
1	10.829943	0.175592	1.294219	1.0	0.0	0.0	0.0	0.0
2	5.091079	0.805153	0.427715	1.0	0.0	0.0	1.0	0.0
3	2.247564	5.600044	0.362663	1.0	1.0	0.0	1.0	0.0
4	44.190936	0.566486	2.222767	1.0	1.0	0.0	1.0	0.0

Figure 1. Features of fraud detection dataset

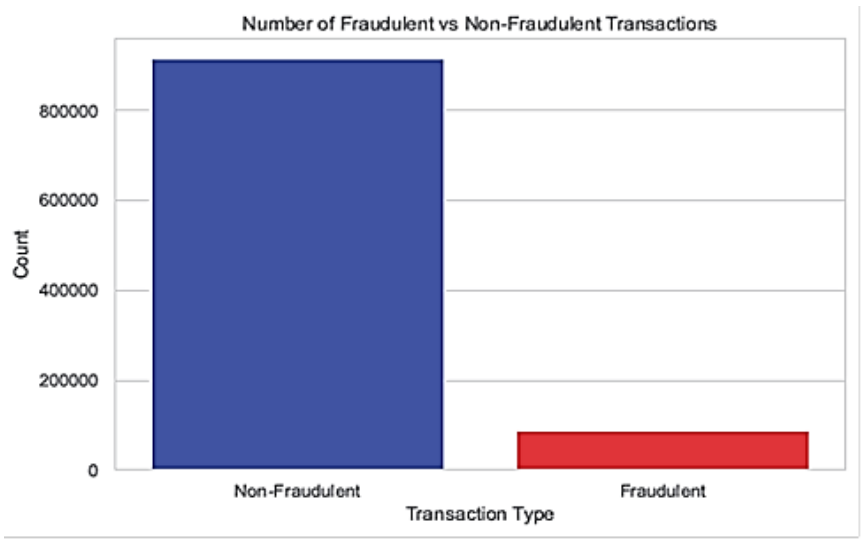

Figure 2. Number of fraudulent vs non-fraudulent transactions

4.2 Machine learning models

The following models were tested:

- Random Forest Classifier – Ensemble-based decision trees
- Logistic Regression – Statistical binary classifier
- XGBoost Classifier – Gradient boosting decision trees
- Stochastic Gradient Descent Classifier (SGDClassifier) – Linear classifier using stochastic gradient descent
- K-Nearest Neighbors (KNN) – Distance-based classification
- Naïve Bayes – Probabilistic classification
- Multi-Layer Perceptron (MLP) – Neural network-based model

4.3 Balancing data

4.3.1 SMOTE (Synthetic Minority Over-Sampling Technique)

It is a technique used to handle imbalanced datasets by generating synthetic samples for the minority class. In fraud detection (or any classification task with imbalanced data), the minority class (fraudulent transactions) has much fewer samples than the majority class (non-fraudulent transactions). This causes machine learning models to favour the majority class, leading to poor recall for fraud detection. SMOTE helps by balancing the dataset [21]. Figure 3 shows how SMOTE generates synthetic minority samples.

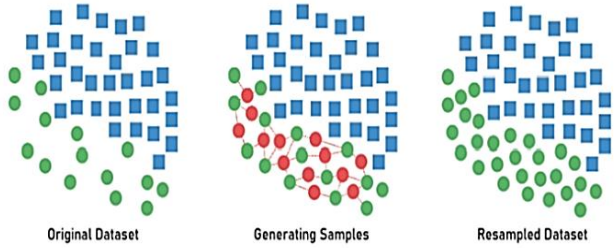

Figure 3. SMOTE technique

4.3.2 SMOTE-ENN (SMOTE + Edited Nearest Neighbours)

This technique uses Edited Nearest Neighbours (ENN) for data cleansing and SMOTE for oversampling. While ENN eliminates unclear or noisy cases (both majority and minority) by determining if a sample's label deviates from the majority of its three nearest neighbours, SMOTE creates synthetic samples for the minority class. The sample is eliminated if it does. By reducing noise and class overlap, this combination method improves decision boundaries for model training and produces cleaner data [22]. Figure 4 shows the process of SMOTE-ENN balancing data.

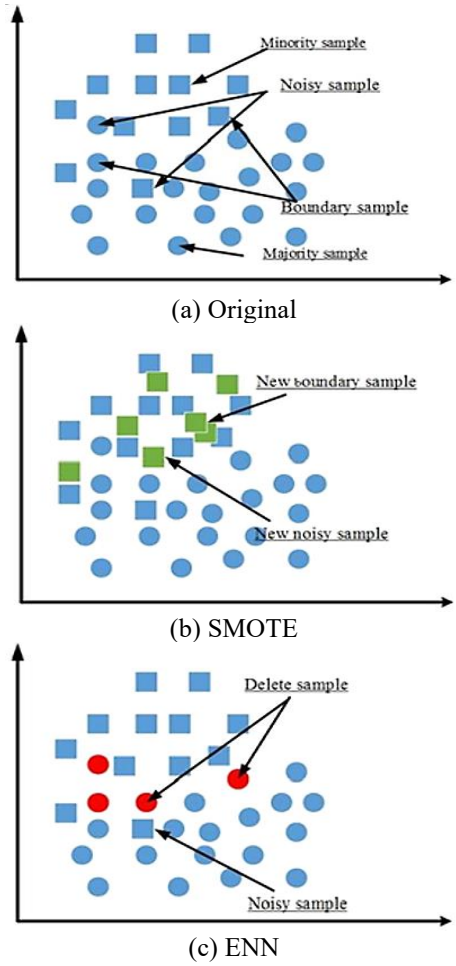

Figure 4. Illustration for SMOTE-ENN

4.3.3 ADASYN (Adaptive Synthetic Sampling Approach for Imbalanced Learning)

This advanced oversampling method creates synthetic samples for the minority class, concentrating on harder-to-learn examples, in order to enhance classification performance on unbalanced datasets. Finding minority class samples and assessing their local learning difficulty by looking at their k nearest neighbours are the first steps in the process. A minority instance is considered more difficult to learn and is given more synthetic examples if it is surrounded by a large number of majority class neighbours. Samples in simpler areas get little to no synthetic points. ADASYN adaptively distributes the generation of synthetic data according to this difficulty, as contrast to SMOTE, which handles all minority instances identically. This targeted approach allows ADASYN to emphasize complex regions near class boundaries, ultimately enhancing the model's ability to learn from challenging patterns and improving overall classification performance [23]. As shown in Figure 5 which illustrates ADASYN balancing technique.

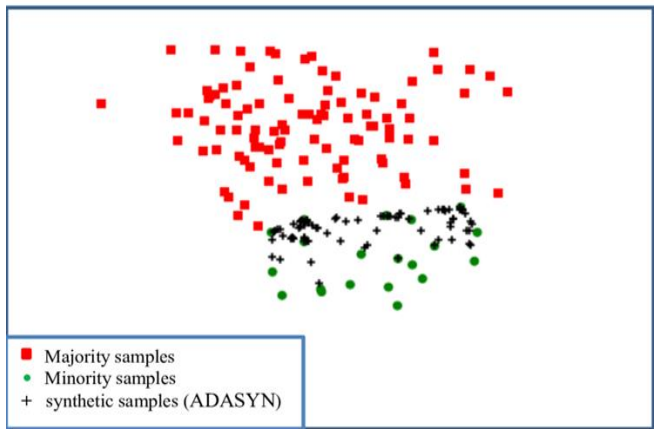

Figure 5. Illustration for ADASYN

Figure 6 presents a flowchart that summarizes the entire classification process, including data collection, feature selection, balancing and dataset splitting, classification, and evaluation.

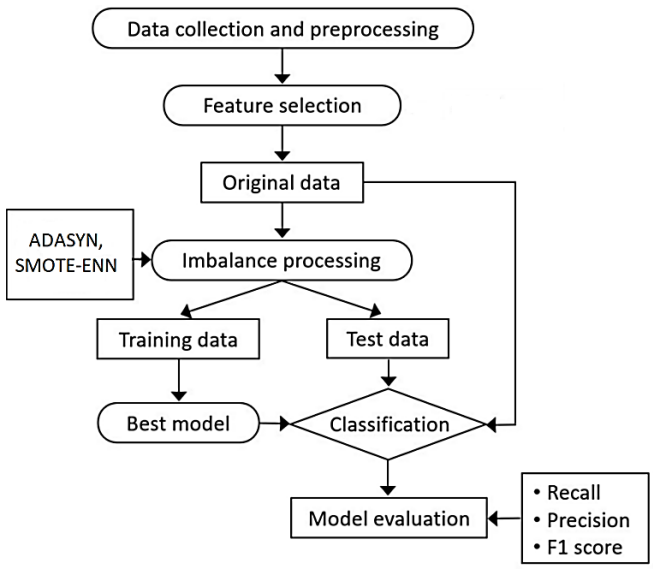

Figure 6. Workflow for fraud detection using techniques (ADASYN & SMOTE-ENN)

4.4 Evaluation metrics

To assess the output of every machine learning model, a confusion matrix was employed. The confusion matrix gives four major elements: True Positives (TP), False Positives (FP),

True Negatives (TN), and False Negatives (FN). These values are obtained based on the comparison between the model's predictions and the actual labels of the dataset.

Using these components, accuracy, precision, recall, specificity, and the F1-score were computed. Metrics — what they mean to the model: How well it detects fraud without setting off too many false alarms. High recall is important in fraud detection so as not to miss fraudulent transactions; precision helps to reduce false positives — it sets off a disruption for legitimate users [24].

$$Accuracy = \frac{TF + TN}{TP + FP + TN + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

(How many predicted frauds were actually fraud)

$$Recall\ (Sensitivity) = \frac{TP}{TP + FN}$$

(How many actual frauds were detected)

$$F1 - Score = \frac{2 * Precision * Recall}{Precision + Recall}$$

(Balances Precision & Recall)

5. RESULTS AND DISCUSSION

5.1 Model performance comparison

The performance of each model before and after SMOTE balancing is summarized in Table 1 and Figure 7.

The early-stage results, highlighted in Table 1 and represented in Figure 7 after over-sampling balancing (SMOTE) reveal that ensemble-based models such as Random Forest, Balanced Random Forest, and XGBoost demonstrate exceptional performance, achieving near-perfect metrics in accuracy, precision, recall, and F1-score. (KNN) also reached perfect scores, though such results should be interpreted cautiously due to possible overfitting. Balanced variants of models (e.g., Logistic Regression, XGBoost) generally improve recall, indicating enhanced detection of minority (fraudulent) instances.

Table 1. Initial test for models before and after SMOTE balancing

Model	Accuracy	Precision	Recall	Specificity	F1-Score
Random Forest	99.99%	100%	99.98%	100%	99.99%
Balanced Random Forest	99.99%	100%	99.98%	100%	99.99%
Logistic Regression	95.90%	89.50%	60.20%	99.30%	71.60%
Balanced Logistic Regression	93.50%	57.80%	94.70%	93.40%	71.70%
XGBoost	99.83%	98.99%	99.14%	99.90%	99.06%
Balanced XGBoost	99.77%	97.75%	99.64%	99.78%	98.69%
SGDClassifier	96.23%	81.99%	72.92%	98.47%	77.21%
Balanced SGD	85.3%	94.74%	88.35%	61.76%	91.42%
KNN	100%	100%	100%	100%	100%
Balanced KNN	100%	100%	100%	100%	100%
Naïve Bayes	95.01%	79.59%	59.26%	98.55%	67.97%
Balanced Naïve Bayes	63.76%	18.95%	96.15%	60.6%	31.45%
MLP	99.78%	99.93%	98.02%	99.96%	98.97%
Balanced MLP	94%	94.96%	98.33%	58.82%	96.63%

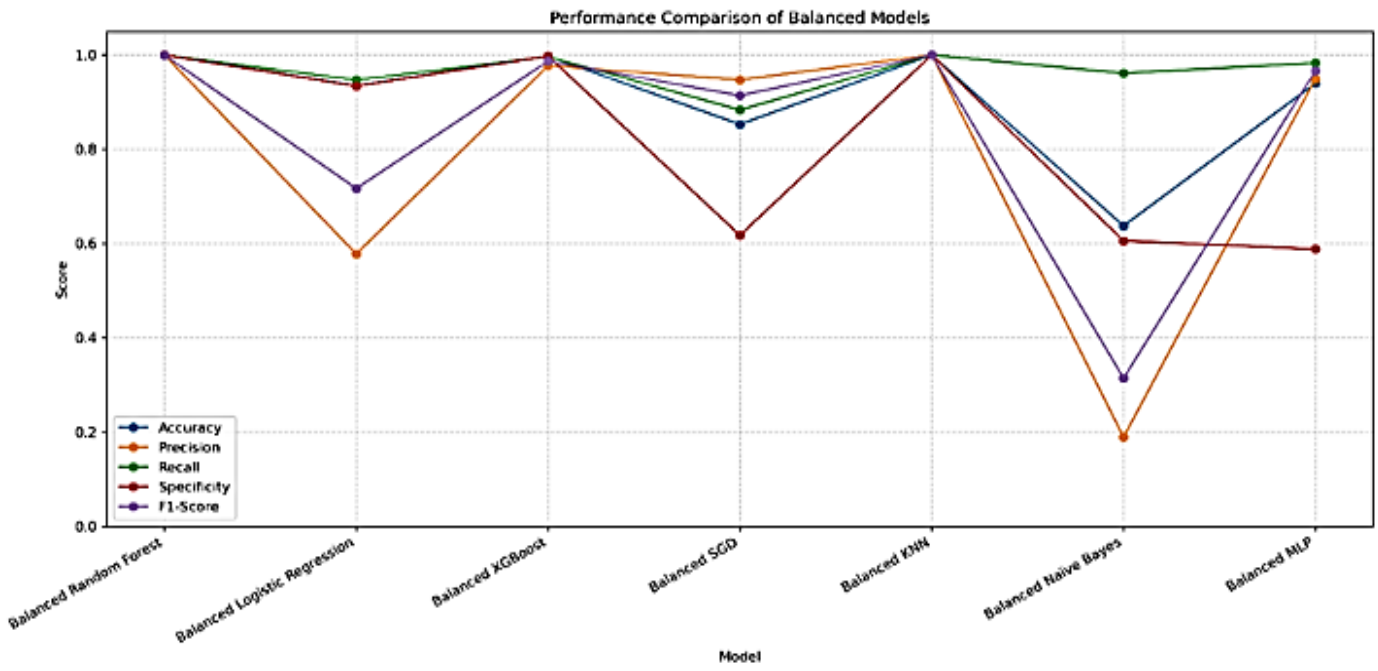

Figure 7. Illustration for initial results

Table 2. Performance after applying SMOTE-ENN and ADASYN

Balancing Technique	Model	Accuracy	Precision	Recall	Specificity	F1-Score
SMOTE-ENN	Random Forest	99.99%	99.85%	99.99%	99.98%	99.92%
	XGBoost	99.89%	98.76%	99.94%	99.88%	99.35%
	KNN	99.64%	95.98%	99.93%	99.80%	97.91%
ADASYN	Random Forest	99.99%	99.99%	99.98%	99.99%	99.98%
	XGBoost	99.93%	99.35%	99.81%	99.94%	99.58%
	KNN	99.86%	98.79%	99.59%	99.88%	99.19%

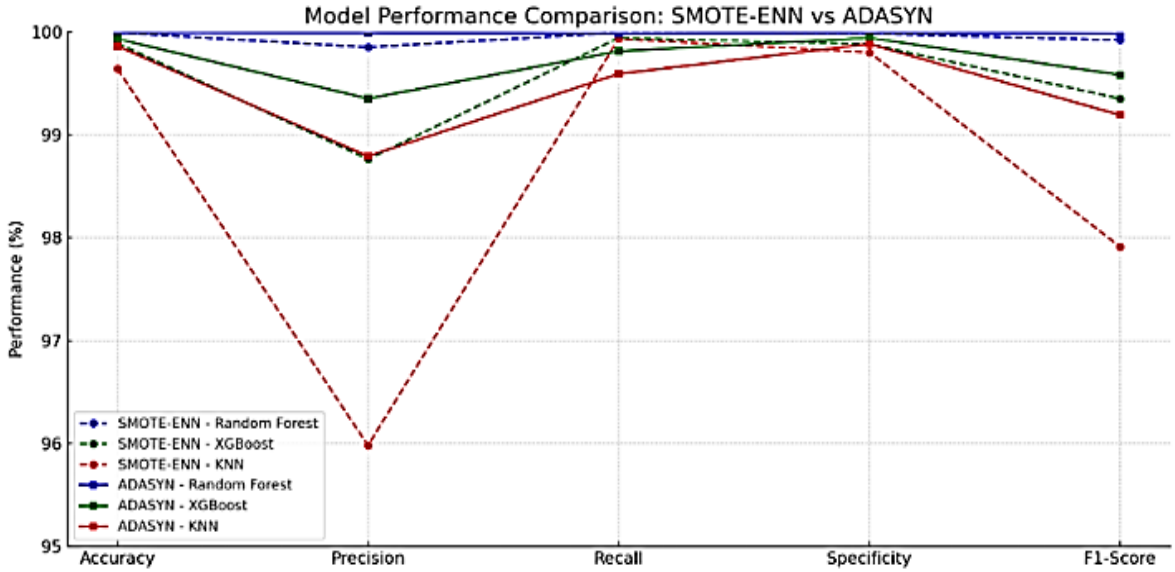

Figure 8. Illustration for models' performance after SMOTE-ENN and ADASYN balancing

Table 3. Performance after applying hybrid balancing SMOTE-ENN and ADASYN

Balancing Technique	Model	Accuracy	Precision	Recall	Specificity	F1-Score
Hybrid (SMOTE-ENN & ADASYN)	Random Forest	99.99%	99.84%	100%	99.99%	99.99%
	XGBoost	99.34%	96.63%	99.77%	99.67%	98.17%
	KNN	97.39%	77.56%	98.73%	97.26%	86.99%

Random Forest, XGBoost, and KNN have been selected based on their superior performance in the initial evaluation. To further validate the robustness of these models, Additional balancing techniques such as SMOTE-ENN and ADASYN were applied and tested. The results listed in Table 2 and graphically represented in Figure 8.

Table 2 and Figure 8 shows the performance of the selected models—Random Forest, XGBoost, and KNN—remained consistently high across both the initial and rebalanced evaluations using techniques SMOTE-ENN and ADASYN. Random Forest maintained near-perfect accuracy, precision, recall, and F1-score, demonstrating exceptional reliability. XGBoost also showed excellent results, particularly in recall and F1-score, making it effective for identifying fraudulent cases. KNN achieved slightly lower precision than the others but still performed very well overall. These outcomes confirm the robustness and effectiveness of the chosen models in handling imbalanced fraud detection datasets.

Table 3 compares the performance of three machine learning models—Random Forest, XGBoost, and K-Nearest Neighbors (KNN)—following a hybrid balancing strategy that combines SMOTE-ENN and ADASYN.

The application of the hybrid balancing technique combining SMOTE-ENN and ADASYN significantly enhanced model performance across all classifiers. Random Forest achieved near-perfect results, with 99.99% accuracy and an F1-score of 99.99%, demonstrating its exceptional ability to generalize while detecting all fraudulent cases without compromising specificity. XGBoost also performed remarkably well, particularly in recall (99.77%) and F1-score (98.17%), confirming its strength in minimizing false negatives—an essential factor in fraud detection. KNN, It proved to be slightly less precise (77.56%) but achieved an astounding recall of 98.73%. This implies that its effectiveness in identifying fraudulent instances comes at some trade-off with precision. These findings further validate the worth of hybrid resampling approaches in handling class imbalance more robustly than standalone methods as they enhance model generalization, reduce overfitting, and improve minority (fraudulent) class detection without significantly increasing false positives.

Figures 9-11 showing the results in confusion metrics after applying hybrid balancing for Random Forest-XGBoost-KNN) classifiers.

The confusion matrix heatmaps for the three models provide a clear comparison of performance in fraud detection using the hybrid balancing technique.

Random Forest performs exceptionally well, with nearly flawless categorization. It properly identifies nearly all fraudulent and non-fraudulent transactions, with only one false negative and 41 false positives, demonstrating its great precision and recall. XGBoost, while slightly less accurate

than Random Forest, remains highly effective. It misclassifies 59 fraudulent and 914 non-fraudulent transactions, which is very low given the big dataset. This signifies strong generalization at the expense of slightly less precision. K-Nearest Neighbors (KNN) has a greater rate of misclassification, namely 332 false negatives and 7,498 false positives. Although its recall stays high, showing good sensitivity, its precision declines, implying more false alarms in fraud detection.

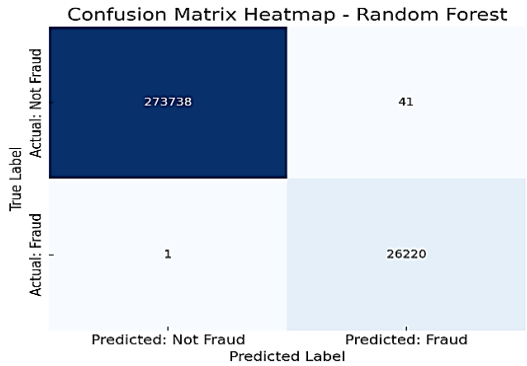

Figure 9. Confusion matrix for Random Forest classifier after hybrid balancing

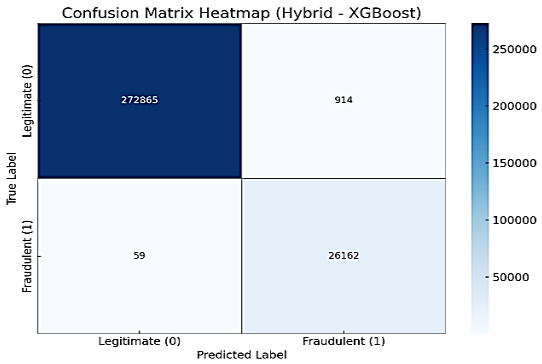

Figure 10. Confusion matrix for XGboost classifier after hybrid balancing

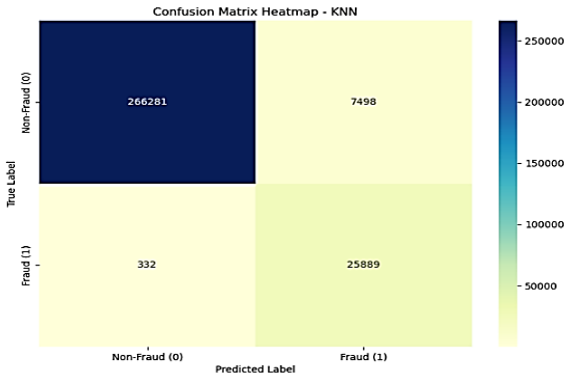

Figure 11. Confusion matrix for KNN classifier after Hybrid balancing

5.2 Discussion

The evaluation results confirm that K-Nearest Neighbors (KNN), Random Forest, and XGBoost are very strong in imbalanced datasets for fraudulent transaction predictions. Within all of these, Random Forest delivered near-perfect scores on accuracy, precision, recall, specificity, and F1-score. This highlights not only its robustness but also its suitability when a high-stakes fraud detection task is at hand. XGBoost performed extremely well with respect to recall and F1-score which probably means it is better in terms of false negative minimization. KNN also delivered very good results, particularly in recall which is the most important attribute for fraud to go unrecognized; however, its precision was slightly lower than available in some other cases. Results using resampling methods SMOTE-ENN and ADASYN advanced the findings by keeping per model performance at a very high level and equally ensuring reliability under different class balancing conditions. To improve minority class recognition further still, hybrid oversampling combined SMOTE-ENN with ADASYN. This results in a merging of the best attributes of both methods—SMOTE-ENN's noise removal and ADASYN's adaptive generation of harder-to-learn instances—which should result in even more outstanding classification performance. The models, especially XGBoost and Random Forest, trained via this hybrid method have achieved F1 scores of 0.999 and 0.981 respectively; therefore, they possess an implied superior capability to capture subtle patterns in imbalanced data without incurring unnecessary false positives or false negatives. Results such as these underline the concept that, for real-world applications involving fraud detection systems, effective classifiers need to be combined with resampling strategies that are both strong and complementary to improve not only accuracy but also generalizability. Moreover, converting these models into real-time fraud detection systems has practical issues such as latency constraints, the need for continuous learning from streaming data, and ensuring quick response to developing fraud trends while maintaining detection accuracy.

6. CONCLUSION AND FUTURE WORK

This work carried out an assessment of machine learning models—Random Forest, XGBoost, K-Nearest Neighbors, Logistic Regression, SGD-SVM, Naïve Bayes, and MLP—using imbalanced data for credit card fraud detection. First, class imbalance was taken care of by applying SMOTE wherein Random Forest, XGBoost, and KNN performed quite well with F1-scores above 0.97. However, Naïve Bayes and SGD-SVM proved to be weak after oversampling which indicates their limitations. To further improve minority class instance detection output from more advanced techniques like SMOTE-ENN and ADASYN was tried separately wherein XGBoost and Random Forest achieved F1 scores of 0.995 and 0.987 respectively. More importantly the results show that little improvements were realized when using hybrid resampling strategies involving both SMOTE-ENN & ADASYN in comparison to the standard versions alone where the best reached F1-score values are reported here: XGBoost with 0.999; Random Forest-0.998; KNN-0.996 reflecting an extraordinary trade-off between sensitivity and precision measures.

Future research will look into optimizing the deployment of fraud detection models in real-time systems, with a focus on minimizing latency and resource usage. Furthermore, the incorporation of explainable AI techniques such as SHAP and LIME will be investigated to improve model transparency and decision-making in operational environments. The study will also look into cost-sensitive learning mechanisms to better

manage the financial impact of false positives and negatives. Furthermore, the approach will be expanded and evaluated on datasets from other high-risk domains, such as healthcare insurance fraud and cybersecurity intrusion detection, to determine its generalizability and adaptability across sectors.

REFERENCES

[1] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., Bontempi, G. (2017). Credit card fraud detection: A realistic modeling and a novel learning strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8): 3784-3797. https://doi.org/10.1109/TNNLS.2017.2736643

[2] Dey, I., Pratap, V. (2023). A comparative study of SMOTE, borderline-SMOTE, and ADASYN oversampling techniques using different classifiers. In 2023 3rd International Conference on Smart Data Intelligence (ICSMDI), Trichy, India, pp. 294-302. https://doi: 10.1109/ICSMDI57622.2023.00060

[3] Bahnsen, A.C., Aouada, D., Ottersten, B. (2015). Example-dependent cost-sensitive decision trees. Expert Systems with Applications, 42(19): 6609-6619. https://doi.org/10.1016/j.eswa.2015.04.042

[4] Bolton, R.J., Hand, D.J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3): 235-255. https://doi.org/10.1214/ss/1042727940

[5] Chan, P.K., Fan, W., Prodromidis, A.L., Stolfo, S.J. (2002). Distributed data mining in credit card fraud detection. IEEE Intelligent Systems and Their Applications, 14(6): 67-74. https://doi.org/10.1109/5254.809570

[6] Srivastava, A., Kundu, A., Sural, S., Majumdar, A. (2008). Credit card fraud detection using hidden Markov model. IEEE Transactions on Dependable and Secure Computing, 5(1): 37-48. https://doi.org/10.1109/TDSC.2007.70228

[7] West, J., Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57: 47-66. https://doi.org/10.1016/j.cose.2015.09.005

[8] Sahin, Y., Duman, E. (2011). Detecting credit card fraud by ANN and logistic regression. In 2011 International Symposium on Innovations in Intelligent Systems and Applications, Istanbul, Turkey, pp. 315-319. https://doi.org/10.1109/INISTA.2011.5946108

[9] Zhu, M., Zhang, Y., Gong, Y., Xu, C., Xiang, Y. (2024). Enhancing credit card fraud detection a neural network and smote integrated approach. arXiv preprint arXiv:2405.00026. https://doi.org/10.48550/arXiv.2405.00026

[10] Alshameri, F., Xia, R. (2023). Credit card fraud detection: An evaluation of SMOTE resampling and machine learning model performance. International Journal of Business Intelligence and Data Mining, 23(1): 1-13. https://doi.org/10.1504/IJBIDM.2023.131791

[11] Zhao, Z., Bai, T. (2022). Financial fraud detection and prediction in listed companies using SMOTE and machine learning algorithms. Entropy, 24(8): 1157. https://doi.org/10.3390/e24081157

[12] Ileberi, E., Sun, Y., Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. IEEE Access, 9: 165286-165294. https://doi.org/10.1109/ACCESS.2021.3134330

[13] Ghaleb, F.A., Saeed, F., Al-Sarem, M., Qasem, S.N., Al-Hadhrami, T. (2023). Ensemble synthesized minority oversampling-based generative adversarial networks and random forest algorithm for credit card fraud detection. IEEE Access, 11: 89694-89710. https://doi.org/10.1109/ACCESS.2023.3306621

[14] Khalid, A.R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., Adejoh, J. (2024). Enhancing credit card fraud detection: an ensemble machine learning approach. Big Data and Cognitive Computing, 8(1): 6. https://doi.org/10.3390/bdcc8010006

[15] Du, H., Lv, L., Guo, A., Wang, H. (2023). AutoEncoder and LightGBM for credit card fraud detection problems. Symmetry, 15(4): 870. https://doi.org/10.3390/sym15040870

[16] Bonde, L., Bichanga, A.K. (2025). Improving credit card fraud detection with ensemble deep learning-based models: A hybrid approach using smote-ENN. Journal of Computing Theories and Applications, 2(3): 383-394. https://doi.org/10.62411/jcta.12021

[17] Mienye, I.D., Sun, Y. (2023). A deep learning ensemble with data resampling for credit card fraud detection. IEEE Access, 11, 30628-30638. https://doi.org/10.1109/access.2023.3262020

[18] He, H., Bai, Y., Garcia, E.A., Li, S. (2008). ADASYN: Adaptive synthetic sampling approach for imbalanced learning. In 2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence), pp. 1322-1328. https://doi.org/10.1109/IJCNN.2008.4633969

[19] Ahmed, K.H., Axelsson, S., Li, Y., Sagheer, A.M. (2025). A credit card fraud detection approach based on ensemble machine learning classifier with hybrid data sampling. Machine Learning with Applications, 20: 100675. https://doi.org/10.1016/j.mlwa.2025.100675

[20] Fraud, E. (2009). Credit card fraud. https://www.kaggle.com/datasets/dhanushnarayananr/credit-card-fraud.

[21] Chawla, N.V., Bowyer, K.W., Hall, L.O., Kegelmeyer, W.P. (2002). SMOTE: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research, 16: 321-357. https://doi.org/10.1613/jair.953

[22] Hairani, H., Priyanto, D. (2023). A new approach of hybrid sampling SMOTE and ENN to the accuracy of machine learning methods on unbalanced diabetes disease data. International Journal of Advanced Computer Science and Applications, 14(8): 585-591.

[23] Taskeen, A., Khan, S.U.R., Mashkoor, A. (2024). An adaptive synthetic sampling and batch generation-oriented hybrid approach for addressing class imbalance problem in software defect prediction. Soft Computing, 28(23): 13595-13614. https://doi.org/10.1007/s00500-024-10378-x

[24] Sathyanarayanan, S., Tantri, B.R. (2024). Confusion matrix-based performance evaluation metrics. African Journal of Biomedical Research, 27(4S): 4023-4031. https://doi.org/10.53555/AJBR.v27i4S.4345