A Comparative Analysis of Synthetic Minority Over-Sampling Technique (Smote) In Enhancing Credit Card Fraud Detection System

Ashish Ravindra Mewal[1], Dr. Syed Sumera Ali[2], A.G. Gaikwad[3], A.T. Jadhav[4], Dr. D.L. Bhuyar[5], Dr. G. B. Dongre[6]

[1]*MTech Student Dept. Of Electronics & Communication (Advanced Communication Technology), CSMSS Chh.Shahu College of Engineering, Chhatrapati Sambhajinagar (Aurangabad), MH, India*

[2]*Associate Professor & Head, Dept. Of Electronics & Communication (Advanced Communication Technology), CSMSS Chh.Shahu College of Engineering, Chhatrapati Sambhajinagar (Aurangabad), MH, India*

[3,4] *Assistant Professor, Dept. Of Electronics & Communication (Advanced Communication Technology), CSMSS Chh.Shahu College of Engineering, Chhatrapati Sambhajinagar (Aurangabad), MH, India*

[5]*Professor & Head, Dept. Of Electronics & Computer Engg., CSMSS Chh.Shahu College of Engineering, Chhatrapati Sambhajinagar (Aurangabad), MH, India*

[6]*Principal Of CSMSS Chh.Shahu College of Engineering, Chhatrapati Sambhajinagar (Aurangabad), MH, India*

***Abstract*—The explosive proliferation of digital payment networks has compounded the credit card fraud threat, and it has been a big challenge to both financial institutions and consumers. The highly skewed nature of transaction data is among the greatest challenges in fraud detection since fraudulent cases are a minority within the total data. This paper will offer comparative research of ML-based credit card fraud detection models with a specific focus on how SMOTE can help deal with the issue of class imbalance. The performance of several common classifiers such as, Logistic Regression, Decision Tree, Random Forest and SVM were tested on the initial imbalanced dataset and a new SMOTE-balanced dataset was tested. Standard evaluation metrics (accuracy, precision, recall, F1-score and area under the ROC curve (AUC)) were used to evaluate model performance. The findings indicate that models that were trained with imbalanced data were both accurate but their detection rate of fraudulent transactions was low. Conversely, SMOTE application enhanced minority classes detection considerably, which resulted in considerable improvements of recall and F1-score of all classifiers.**

***Index Terms*—Credit card Fraud Detection, SMOTE, ML, Random Forest, Data Mining;**

I. INTRODUCTION

The fast development of online payment apps and online shopping platforms have greatly altered the financial environment across the globe since the use of credit cards is now one of the significant components of the daily economic processes. Although this online transformation has brought about convenience and efficiency, it has equally contributed to making the financial systems more susceptible to fraudulent operations. One of the most important issues arising by financial institutions is credit card fraud that results in massive loss of money, customer confidence, and increase in the cost of operations. This has led to the establishment of effective and precise fraud detection systems becoming a major priority in the banking and financial services industry.

The problem of credit card fraud detection is inherently quite complex because the data on the transactions is highly imbalanced, and the cases of fraudulent transactions is a very small proportion of the total dataset. Conventional ML classifiers are not always able to have satisfactory results when they are operating in such conditions, as they are usually biased towards the majority (legitimate) class, which leads to poor detection of fraudulent cases. This asymmetry has a dire impact on the performance measures of recall, precision, and F1-score of the minority class, which is very important in detecting the fraud.

The SMOTE is one such technique that has been found to be an effective way of improving the representation of minorities in the form of synthetic samples and not through duplication. SMOTE through balancing the dataset will allow ML models to learn the underlying pattern of fraudulent transactions more appropriately, and thus detect fraudulent transactions with higher accuracy and fewer false negatives.

The research will compare existing models with and without SMOTE to prove the effect that the methods of oversampling had on the classification results and the creation of more trustful and efficient fraud detection software. It is believed that the results of this paper will be significant to scholars and practitioners interested in developing data-oriented fraud prevention strategies in practice in the field of finances.

1.1. OBJECTIVES OF THE STUDY

1. To analyze the class imbalance problem in credit card transaction datasets and its impact on fraud detection performance.
2. To apply the SMOTE for balancing the dataset and improving minority class representation.
3. To compare the performance of selected ML classifiers with and without the application of SMOTE using standard evaluation metrics such as accuracy, precision, recall, F1-score, and AUC.
4. To assess the effectiveness of SMOTE-based models in enhancing fraud detection capability and reducing misclassification of fraudulent transactions.

II. REVIEW OF LITERATURE

MOUSA, ÖZYURT, AND AVCI (2024) performed an in-depth investigation of improving the credit card fraud detection with the SMOTE combined with deep neural network models. In their study, they overcome the issue of extreme imbalance in the sample of financial transactions between different classes through the creation of synthetic minority class samples before the training of a model. The research found out that deep learning models, which were used in combination with proper oversampling methods, worked to be effective at detecting complex patterns of fraud and minimizing the number of false negatives.

AGHWARE ET AL. (2024) assessed the model at the start and end of the oversampling and indicated that there was a significant improvement in the minority classes detection when the dataset was balanced. The authors found out that there had been great improvement in recall, as well as in the overall classification reliability, but they did not lose acceptable levels of accuracy. The results highlighted that the combination of SMOTE and ensemble learning methods like the Random Forest enhanced the effectiveness of a fraud detector system in highly skewed settings.

MUAZ, JAYABALAN, AND THIRUCHELVAM (2020) carried out a comparative analysis of different data sampling methods that have been applied in detecting credit card fraud. They compared the performance of oversampling, under sampling, and hybrid sampling in relation to their effects on the performance of the classifier. The analysis was found to indicate that the oversampling methods, such as SMOTE, performed better as compared to under sampling methods as they maintained good information in the majority classes and increased the minority class representation. The authors concluded that the relevant sampling strategies were instrumental in improving the accuracy of the fraud detection and the misclassification rates.

ELMANGOUSH ET AL. (2024) examined the use of SMOTE in a combination with deep learning methods to detect credit card frauds. Their task was to balance the dataset with the help of SMOTE before

the deep neural network models were trained. The findings showed that the metrics of fraud detection, especially recall and AUC, improved significantly as compared to those of the models trained on the initial imbalanced data. The paper emphasized that the hybrid of SMOTE and deep learning algorithms offered a beneficial system of addressing the problem of imbalanced financial information and enhancing the detection rate in a non-controlled environment
Submit your manuscript electronically for review. prepare it in two-column format, including figures and tables (until it doesn't fit properly and data is not visible).

III. METHODOLOGY

Here, it defines the systematic nature of the approach that will be taken in the development and evaluation of a credit card fraud detector system based on the ML techniques. The aspects of the methodology are a description of datasets, data preprocessing, class imbalance management with the help of SMOTE, the choice of the model, training, and performance assessment criteria.

3.1 DATASET DESCRIPTION

Here, it defines the systematic nature of the approach that will be taken in the development and evaluation of a credit card fraud detector system based on the ML techniques. The aspects of the methodology are a description of datasets, data preprocessing, class imbalance management with the help of SMOTE, the choice of the model, training, and performance assessment criteria.

3.2 DATA PREPROCESSING

Prior to model development, essential preprocessing steps were carried out to ensure data quality and compatibility. The dataset was first examined for missing values and inconsistencies, and since none were found, no imputation was required. Numerical features were then standardized using z-score normalization to maintain a uniform scale across all attributes, which is particularly important for distance- and margin-based classifiers. Finally, the dataset was split into training and testing sets in an 80:20 ratio to enable unbiased evaluation of model performance.

3.3 HANDLING CLASS IMBALANCE USING SMOTE

Due to the imbalance between the legitimate and the fraudulent transactions being extremely high, the SMOTE was only applied on the training dataset. SMOTE creates artificial samples of minorities by interpolating between the existing minority samples and their closest features. It does not directly copy the minority samples and minimizes the possibility of overfitting.
Application of SMOTE has achieved a balanced training data that equally represents both classes which makes classifiers to learn discriminative patterns of fraud much better.

3.4 ML MODELS

Using four well-known ML classifiers with supervision, we tested how SMOTE affected the efficiency of fraud detection:

- LOGISTIC REGRESSION (LR): A baseline linear classification model suitable for probabilistic interpretation.
- DECISION TREE (DT): A rule-based model capable of capturing nonlinear relationships.
- RANDOM FOREST (RF): An ensemble learning approach that uses a number of DT to boost prediction accuracy.
- SUPPORT VECTOR MACHINE (SVM): In high-dimensional feature spaces, a margin-based classifier is useful.

So that we could compare the models, we trained them twice: once with the original imbalanced dataset and once with the SMOTE-balanced dataset.

3.5 MODEL TRAINING AND VALIDATION

The training of the models was done using default hyperparameters on the respective training datasets to ensure consistency and comparability. Training was done on two platforms of cross-validation so as to reduce bias and generalizability. The trained models were reviewed on the unknown test set to gauge the predictive ability in reality

IV. DATA ANALYSIS AND RESULTS

Here we present a comprehensive review of the results from our experiments using ML classifiers on the credit card fraud detection dataset. The analysis is

aimed at backing up the insight into what the imbalance in the data means and examining the performance enhancement on the utilization of the SMOTE. The models are measured based on conventional performance measures that are especially applicable to imbalanced classification problems.

4.1 DATASET CHARACTERISTICS AND CLASS DISTRIBUTION

The credit card transaction dataset used in this study is highly imbalanced, with fraudulent transactions forming a very small proportion of the total observations. Table 1 presents the original class distribution before applying SMOTE.

TABLE 1: ORIGINAL CLASS DISTRIBUTION OF THE DATASET

Class Label	Description	Number of Instances	Percentage (%)
0	Legitimate Transactions	284,315	99.83
1	Fraudulent Transactions	492	0.17
Total	—	284,807	100

According to the table, it is evident that the credit card transaction data is highly imbalanced. The majority of the data includes legitimate transactions (Class 0) that comprise 284,315 cases, which is 99.83 percent of the entire dataset. On the contrary, there are only 492 cases of fraudulent transactions (Class 1), which constitute only 0.17 percent of data. This extreme imbalance of the classes is highly problematic to ML models where the classifier learnt on such data would be biased to the majority class and would not always detect fraudulent transactions.

4.2 DATASET DISTRIBUTION AFTER APPLYING SMOTE

Synthetically generating fresh samples of the minority (fraud) class was done using SMOTE to solve the imbalance issue. Following oversampling, Table 2 displays the distribution of classes.

TABLE 2: RESULTS OF THE SMOTE TEST ON CLASS DISTRIBUTION

Class Label	Description	Number of Instances	Percentage (%)
0	Legitimate Transactions	284,315	50.0
1	Fraudulent Transactions	284,315	50.0
Total	—	568,630	100

The table illustrates the distribution of the classes following the use of the SMOTE on the training set. The legitimate and fraudulent transactions have the same number of entries and 284,315 entries of both have been obtained, making the dataset perfectly balanced. SMOTE addresses the problem of class imbalance that is present in the raw data by increasing the number of the minority (fraudulent) class to 50 percent. Such a balance distribution can help ML models more easily learn distinguishing patterns of fraudulent transactions, minimize bias to the majority, and dramatically increase minority class performance metrics, including recall and F1-score, which are vital to effective credit card fraud detection.

4.3 PERFORMANCE OF CLASSIFIERS WITHOUT SMOTE

Table 3 presents the performance of selected ML models trained on the original imbalanced dataset.

TABLE 3: MODEL PERFORMANCE WITHOUT SMOTE

Classifier	Accuracy (%)	Precision	Recall	F1-Score	AUC
LR	99.2	0.71	0.42	0.53	0.89
DT	99.4	0.76	0.48	0.59	0.91
RF	99.6	0.83	0.55	0.66	0.94
SVM	99.1	0.69	0.39	0.50	0.87

The table tabulates the execution of assorted ML classifiers prepared using the initial imbalanced dataset. Despite the high accuracy values of 99 and above when all of the classifiers were used, it is misleading because there were more legitimate transactions in the dataset. The recall values, a measure of the capability to properly detect fraudulent transactions, are relatively low in all the models, which means there were a high amount of

false negative. The Random Forest model was relatively the highest performance classifier with the highest precision (0.83), recall (0.55), F1-score (0.66), and AUC (0.94), indicating that it is a better discriminator than the other models.

4.4 PERFORMANCE OF CLASSIFIERS WITH SMOTE

Table 4 shows the performance of the same classifiers trained on the SMOTE-balanced dataset.

TABLE 4: MODEL PERFORMANCE WITH SMOTE

Classifier	Accuracy (%)	Precision	Recall	F1-Score	AUC
Logistic Regression	97.8	0.92	0.89	0.90	0.97
Decision Tree	98.1	0.93	0.91	0.92	0.98
Random Forest	98.6	0.96	0.94	0.95	0.99
Support Vector Machine	97.5	0.90	0.88	0.89	0.96

The table shows the performance of different ML classifiers trained on the SMOTE-balanced dataset. All classifiers show a significant increase in accuracy, recall, F1-score, and AUC relative to the models trained on the original imbalanced data, which means that they are more effective in detecting fraudulent transactions. In spite of the fact that the overall accuracy is decreased slightly, this trade-off is not significant because the models attain much higher minority classes detection. The best classifier according to the assessment of the classifiers is the Random Forest classifier, which has the best accuracy (0.96), recall (0.94), F1-score (0.95), and AUC (0.99), indicating its high discriminative ability and power.

4.5 COMPARATIVE IMPROVEMENT ANALYSIS

To clearly illustrate the impact of SMOTE, Table 5 compares recall and F1-score values before and after oversampling.

TABLE 5: COMPARATIVE IMPROVEMENT IN MINORITY CLASS DETECTION

Classifier	Recall (Before)	Recall (After)	F1-Score (Before)	F1-Score (After)
Logistic Regression	0.42	0.89	0.53	0.90
Decision Tree	0.48	0.91	0.59	0.92
Random Forest	0.55	0.94	0.66	0.95
Support Vector Machine	0.39	0.88	0.50	0.89

The table compares the results of recall and F1-score of various classifiers with and without the use of SMOTE. There is a great enhancement in all models after oversampling, which demonstrates the usefulness of SMOTE in the process of improving the minority classes. The recall values were also significantly higher in all classifiers, which means that the number of false negatives decreased significantly and more fraud cases were identified. Likewise, the F1-scores indicate a significant improvement on the basis of an increased precision and recall following the management of the issue of class imbalance. The Recall (0.94) and F1-score (0.95) of the Random Forest model are highest after the SMOTE, indicating that it had the highest overall improvement.

V. CONCLUSION

This paper has provided a comparative analysis of ML-based credit card fraud detection models with a narrow concentration on the mitigation of the issue of class imbalance through the SMOTE. As shown in the experimental results, the models that were trained using the original imbalanced dataset were able to achieve high accuracy but with limited ability to detect fraudulent transactions as shown by low values of recall and F1-score. Application of SMOTE has greatly increased the representation of minority classes resulting in great increases in recall, precision, F1-score, and AUC of all the classifiers evaluated. The model that was selected has demonstrated the best consistency, the best robustness among the other models, and this is the

Random Forest classifier with SMOTE, which implies its applicability in real-life fraud detection systems. Altogether, the results indicate that the data-level imbalance management methods like SMOTE are important to create efficient and reliable credit card fraud detection systems and the suggested system has valuable lessons to offer in the future research and in the practice of financial security applications.

REFERENCES

[1] Aghware, F. O., Ojugo, A. A., Adigwe, W., Odiakaose, C. C., Ojei, E. O., Ashioba, N. C., ... & Geteloma, V. O. (2024). Enhancing the random forest model via synthetic minority oversampling technique for credit-card fraud detection. Journal of Computing Theories and Applications, 1(4), 407-420.

[2] Ahmed, F., & Shamsuddin, R. (2021, January). A comparative study of credit card fraud detection using the combination of ML techniques with data imbalance solution. In 2021 2nd International Conference on Computing and Data Science (CDS) (pp. 112-118). IEEE.

[3] Andrade-Arenas, L., & Yactayo-Arias, C. (2025). Comparative Analysis of Machine Learning Models for Credit Card Fraud Detection Using SMOTE for Class Imbalance. International Journal of Safety & Security Engineering, 15(5).

[4] da Silva, R. Á. (2025). A Comparative Analysis of Imbalanced Learning Techniques for Optimizing Credit Card Fraud Detection (Master's thesis, Universidade NOVA de Lisboa (Portugal)).

[5] El Hajjami, S., & Diallo, G. (2025). SMOTE-OSBNR: An Effective Approach for Imbalanced Credit Card Fraud Detection. IEEE Access.

[6] Elmangoush, A. M., Hassan, H. O., Fadhl, A. A., & Alshrif, M. A. (2024, July). Credit Card Fraud Detection Using Synthetic Minority Oversampling Technique and Deep Learning Technique. In 2024 IEEE 7th International Conference on Advanced Technologies, Signal and Image Processing (ATSIP) (Vol. 1, pp. 455-458). IEEE.

[7] 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.

[8] 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.

[9] Mahesh, K. P., Afrouz, S. A., & Areeckal, A. S. (2022). Detection of fraudulent credit card transactions: A comparative analysis of data sampling and classification techniques. In Journal of Physics: Conference Series (Vol. 2161, No. 1, p. 012072). IOP Publishing.

[10] Mousa, A., Özyurt, F., & Avcı, E. (2024). Enhancing Credit Card Fraud Detection Using SMOTE and Deep Neural Networks: A Comprehensive Analysis. Int. J. Advanced Networking and Applications, 16(03), 6390-6401.

[11] Muaz, A., Jayabalan, M., & Thiruchelvam, V. (2020). A comparison of data sampling techniques for credit card fraud detection. International Journal of Advanced Computer Science and Applications, 11(6).

[12] Parkinson de Castro, E. (2020). An examination of the smote and other smote-based techniques that use synthetic data to oversample the minority class in the context of credit-card fraud classification.

[13] Salaudeen, L. G., Gabi, D., Garba, M., & Suru, H. U. (2024). Deep convolutional neural network based synthetic minority over sampling technique: a forfending model for fraudulent credit card transactions in financial institution. Journal of the Nigerian Society of Physical Sciences, 2037-2037.

[14] Singh, A., Ranjan, R. K., & Tiwari, A. (2022). Credit card fraud detection under extreme imbalanced data: a comparative study of data-level algorithms. Journal of Experimental & Theoretical Artificial Intelligence, 34(4), 571-598.

[15] Veigas, K. C., Regulagadda, D. S., & Kokatnoor, S. A. (2021). Optimized stacking ensemble (OSE) for credit card fraud detection using synthetic minority oversampling model. Indian

Journal of Science and Technology, 14(32), 2607-2615.
[16] S. S. Ali *et al.*, "An Efficient Quality Inspection of Food Products Using Neural Network Classification," *International Journal of Engineering Research & Technology*, 2017.
[17] S. S. Ali *et al.*, "A Review on Neural Network Based Quality Inspection of Food Products," *IJERT*, 2019
[18] S. S. Ali *et al.*, "Whale Optimized MLP Neural Network and Enhanced Region Growing for Food Product Inspection," 2025.
[19] S. S. Ali *et al.*, "MLP-WOA Neural Network-Based Automated Grading of Fruits and Vegetable Quality Detection," 2025.
[20] S. S. Ali *et al.*, "Investigating Blockchain Security Mechanisms for Tamper-Proof Data Storage," 2025
[21] S. S. Ali *et al.*, "Homomorphism Encryption Techniques Leveraging AI and Advanced Algebraic Structures," 2025.
[22] S. S. Ali *et al.*, "Quantum Cryptography in Secure Communication: Opportunities and Challenges," 2024