



## A Smart Approach to Credit Card Fraud Mitigation with Hybrid Sampling Using ML and AI

<sup>1</sup> Narender Kunta, [kuntanarender55@gmail.com](mailto:kuntanarender55@gmail.com)

**Abstract:** Credit card fraud has emerged as a significant concern with the rapid increase in online transactions, resulting in considerable financial losses for individuals and institutions. Fraud detection presents a challenge due to the highly imbalanced nature of datasets, where fraudulent transactions constitute a small fraction of legitimate ones. Addressing this imbalance is critical for building reliable and accurate fraud detection systems. To tackle this challenge, this study explores advanced hybrid undersampling and oversampling techniques to improve the detection of fraudulent transactions while maintaining high performance across various evaluation metrics. Sampling methods such as SMOTE, B-SMOTE, ADASYN, SMOTE-Tomek, SMOTE-EEN, and Hybrid BIRCH Borderline SMOTE were employed to balance the dataset and mitigate the challenges posed by skewed data. Among the models tested, the Voting Classifier, combining Boosted Decision Trees and ExtraTree, consistently outperformed others in terms of accuracy, precision, recall, and F1-score across all sampling techniques. This demonstrates its robustness and effectiveness in handling imbalanced credit card fraud datasets. The results highlight the potential of hybrid sampling methods combined with ensemble learning to significantly enhance fraud detection systems.

**Index Terms -** *Borderline SMOTE, class imbalance, credit card, fraud detection, sampling techniques, Tomek links.*

prevent fraudulent activities, safeguard customers' privacy, and build trust in their services.

### 1. INTRODUCTION

The rapid expansion of e-commerce has revolutionized shopping, enabling customers to make purchases online using credit cards or mobile wallets. As credit cards have become the primary payment method in the digital world, the volume of daily transactions has surged. However, this convenience has also created opportunities for criminals to devise sophisticated methods to steal credit card information. Consequently, credit card fraud has become a significant concern for businesses, leading to substantial financial and personal losses. The increasing prevalence of fraud has driven organizations to prioritize the development of innovative methods to detect and

Developing an accurate credit card fraud detection model requires analyzing transactions based on attributes, features, and values. These models aim to classify new transactions as either legitimate or fraudulent by learning patterns from historical data. However, the underlying challenge in this domain is the highly imbalanced nature of credit card datasets, where legitimate transactions vastly outnumber fraudulent ones. This imbalance poses a critical issue for classification models, as they can achieve high overall accuracy by predominantly predicting the majority class while failing to detect fraudulent transactions. Addressing class imbalance is therefore a crucial aspect of building reliable fraud detection systems [1].



Class inequality in datasets has garnered considerable attention in recent years due to its profound impact on the learning and classification process. When one class is significantly underrepresented, as in the case of fraudulent transactions, identifying rare patterns and abnormal behavior becomes challenging. This issue is exacerbated by the rarity and irregularity of instances in the minority class, which hinders effective classification [1]. To mitigate this challenge, data balancing techniques have emerged as a key solution.

Three primary approaches to balancing data include data-level techniques, algorithm-level techniques, and hybrid methods [2]. Data-level techniques are further divided into oversampling, undersampling, and hybrid sampling, with oversampling being the most commonly adopted strategy. By balancing the dataset prior to classification, oversampling ensures that the influence of the majority class is reduced, enabling models to focus more effectively on the minority class [3]. Algorithm-level approaches, on the other hand, aim to address sensitivity to class imbalance by modifying the internal structure of classification algorithms [3].

Recent advancements in credit card fraud detection have combined these two approaches into hybrid methods, achieving more robust and accurate results. Hybrid techniques balance the dataset while simultaneously improving algorithm performance, offering a promising solution to the persistent challenge of fraud detection in imbalanced datasets [3].

## 2. RELATED WORK

Credit card fraud detection is a significant challenge in the modern digital economy, as fraudulent activities pose substantial risks to businesses and consumers alike. The increasing reliance on credit cards for online transactions has amplified the urgency of developing robust and accurate fraud detection models. Several studies have addressed this challenge by employing various data sampling techniques, classification algorithms, and hybrid approaches to mitigate class imbalance and enhance model performance.

Mahesh et al. [5] conducted a comparative analysis of data sampling and classification techniques to detect fraudulent credit card transactions. Their study highlighted the importance of balancing imbalanced datasets to improve model performance. By experimenting with multiple sampling methods such as Synthetic Minority Oversampling Technique (SMOTE) and undersampling, they demonstrated that balanced datasets yield superior classification results. Their work underscored the necessity of aligning sampling strategies with classification models to achieve optimal outcomes.

Rtayli [6] proposed an efficient deep learning classification model tailored to skewed datasets. The study utilized advanced neural network architectures to address the challenges posed by imbalanced data. The model incorporated feature engineering to enhance the discriminative power of attributes and leveraged data augmentation techniques to improve minority class representation. This approach resulted in improved accuracy and recall, particularly in



identifying fraudulent transactions. The findings of this study illustrate the potential of deep learning methods for fraud detection when coupled with effective data preprocessing techniques.

Akinwamide [7] explored the application of machine learning algorithms to predict fraudulent transactions. By analyzing a publicly available credit card fraud detection dataset, the study compared several classification algorithms, including Decision Trees, Random Forest, and Support Vector Machines. Akinwamide emphasized the critical role of algorithm selection in addressing class imbalance and achieving high detection rates. The research further demonstrated the effectiveness of ensemble methods, particularly when combined with sampling strategies, in enhancing fraud detection capabilities.

Li and Xie [8] proposed a behavior-cluster-based imbalanced classification method for credit card fraud detection. Their method involved clustering transaction behaviors to create balanced subsets of data, which were then used for training classification models. By reducing the impact of majority class dominance, the approach improved the identification of fraudulent transactions. This study emphasized the value of domain-specific clustering techniques in addressing class imbalance and enhancing the interpretability of fraud detection models.

Esenogho et al. [9] introduced a neural network ensemble framework with feature engineering for improved credit card fraud detection. Their approach combined multiple neural network models to capture diverse patterns in transaction data. Feature

engineering played a crucial role in extracting meaningful attributes from raw data, thereby enhancing model performance. The study demonstrated that ensemble methods, when combined with robust feature selection techniques, significantly outperform single models in terms of precision and recall.

Ullastres and Latifi [11] focused on the application of ensemble learning algorithms for credit card fraud detection. Their research, conducted as part of a master's project, examined the effectiveness of ensemble techniques such as bagging and boosting. By leveraging multiple base classifiers, the ensemble models achieved higher accuracy and robustness compared to individual classifiers. The study highlighted the scalability and adaptability of ensemble methods in real-world fraud detection scenarios.

Zhu et al. [12] proposed the Noisy-SampleRemoved Undersampling Scheme (NUS) to address the challenges of imbalanced classification in credit card fraud detection. The method involved removing noisy and borderline samples from the majority class before training classifiers. This approach improved the overall quality of the dataset and reduced the risk of overfitting. The study demonstrated that targeted undersampling techniques, when applied judiciously, can enhance the performance of classification models.

Mondal et al. [15] investigated various strategies for handling imbalanced data in credit card fraud detection. Their research compared traditional oversampling techniques, such as SMOTE, with

novel hybrid approaches that combined undersampling and oversampling. The study found that hybrid methods yielded the best results by leveraging the strengths of both strategies. The authors also highlighted the importance of evaluating model performance using multiple metrics, including precision, recall, and F1-score, to ensure a comprehensive assessment.

### 3. MATERIALS AND METHODS

The proposed system addresses the challenge of detecting credit card fraud in highly imbalanced datasets by combining advanced sampling techniques with robust machine learning algorithms. To balance the dataset and improve the detection of fraudulent transactions, various sampling methods such as SMOTE, B-SMOTE, ADASYN, SMOTETomek, SMOTE-EEN, and Hybrid BIRCH Borderline SMOTE are utilized. These techniques effectively mitigate the imbalance between legitimate and fraudulent transactions, ensuring better model performance. Four machine learning algorithms are employed to analyze the resampled datasets: Random Forest, Boosted Decision Tree, ExtraTree, and a Voting Classifier combining Boosted Decision Tree and ExtraTree. The Voting Classifier leverages the strengths of its components to enhance prediction accuracy. This hybrid approach integrates effective sampling methods with ensemble learning models, aiming to provide a scalable, efficient, and reliable solution for realworld credit card fraud detection challenges. The system is designed to achieve high performance across key evaluation metrics.



Fig.1 Proposed Architecture

The image illustrates a machine learning pipeline for credit card fraud detection. It begins with raw credit card data, which undergoes preprocessing (data visualization, label encoding, and train-test split). Feature selection is performed to identify relevant attributes. The data is then fed into various machine learning models (Random Forest, Boosted Decision Tree, ExtraTree, and Voting Classifier). These models are trained on the training data and evaluated on the testing data using metrics like accuracy, precision, recall, and F1-score. Additionally, oversampling techniques (SMOTE, B-SMOTE, ADASYN, SMOTE-TOMEK, SMOTE-EEN, HYBRID BIRCH BORDERLINE SMOTE) are employed to address imbalanced data.

#### i) Dataset Collection:

The dataset used for fraud detection [13] was generated using the PaySim simulator, which produces synthetic credit card transaction data based on real-world patterns. Derived from aggregated financial logs of mobile money services, the dataset mimics typical transaction behaviors while injecting malicious activities to assess fraud detection techniques. It consists of over six million records



and includes 11 attributes: “step (transaction time), type (transaction type), amount, nameOrig (origin account), oldbalanceOrg and newbalanceOrig (account balances before and after the transaction), nameDest (destination account), oldbalanceDest and newbalanceDest (destination account balances), isFraud (fraud indicator), and isFlaggedFraud (illegal transaction flag)”. The dataset enables a detailed behavioral analysis of fraudulent transactions, offering a comprehensive testbed for fraud detection algorithms.

	step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrg	nameDest
0	1	PAYMENT	9838.84	C1231009815	170136.0	160296.36	M1979787155
1	1	PAYMENT	1864.28	C1699544295	21249.0	19384.72	M0044282225
2	1	TRANSFER	181.00	C1305480145	181.0	0.00	C593264095
3	1	CASH_OUT	181.00	C840083671	181.0	0.00	C38907010
4	1	PAYMENT	1568.14	C2048537720	41554.0	39865.86	M1230701703

Fig.2 Dataset Collection Table ii)

### Pre-Processing:

The pre-processing phase involves detailed steps, including data processing, visualization, label encoding, feature selection, and applying sampling techniques. These steps are crucial for preparing the dataset to enhance the accuracy and efficiency of the fraud detection model.

**a) Data Processing:** Data processing begins with loading the dataset into a pandas DataFrame, providing an efficient structure for data manipulation and analysis. During this phase, unwanted columns, such as those irrelevant to the fraud detection process, are dropped to streamline the dataset. This helps reduce noise and ensures the model focuses on meaningful features. Additionally, missing or null values may be handled through

imputation or removal, ensuring data consistency and preparing it for subsequent analysis and modeling.

**b) Data Visualization:** Data visualization is essential for understanding the distribution and relationships within the dataset. Seaborn and Matplotlib are used to create various plots, such as histograms, box plots, and heatmaps. These visualizations help identify trends, patterns, and potential outliers in the data. For instance, visualizing class distribution highlights the imbalance between fraudulent and legitimate transactions, while heatmaps can show correlations between different features. This step aids in making informed decisions during the feature selection and model-building phases.

**c) Label Encoding:** Label encoding is a technique used to convert categorical variables into numerical values, enabling them to be processed by machine learning algorithms. In this project, the LabelEncoder class from the scikit-learn library is used to transform categorical features, such as transaction types or names, into integers. This is essential because machine learning models typically require numerical input to perform computations. Label encoding ensures that categorical variables are appropriately handled without losing any inherent information during the transformation.

**d) Feature Selection:** Feature selection is a critical step in identifying the most important variables for fraud detection. This process involves evaluating the relevance and importance of different features in predicting fraudulent transactions.



Techniques like correlation analysis and univariate selection are used to eliminate redundant or irrelevant features, which can improve model performance and reduce overfitting. By focusing on the most informative features, feature selection enhances the model's ability to generalize to unseen data, making it more efficient and accurate.

**e) Sampling:** Sampling techniques are applied to address the class imbalance in the dataset. Methods like SMOTE (Synthetic Minority Over-sampling Technique) and its variations, including B-SMOTE and ADASYN, generate synthetic examples of the minority class (fraudulent transactions) to balance the data. SMOTE-Tomek and SMOTE-EEN further refine this by removing noisy or borderline samples, improving model generalization. The Hybrid BIRCH Borderline SMOTE technique combines clustering with over-sampling, ensuring that synthetic instances are generated in the most informative regions of the feature space. These techniques ensure a more balanced and reliable training dataset. **iii) Training & Testing:**

To split the data into training and testing sets, we use the `train_test_split` function from the scikit-learn library. Typically, the dataset is divided into a training set (80%) and a testing set (20%), though the split ratio can be adjusted based on the project's needs. The training set is used to train the machine learning models, while the testing set is used to evaluate the model's performance on unseen data. By ensuring a proper split, the model can generalize better, and we can assess its effectiveness in

detecting fraudulent transactions effectively. The `random_state` parameter ensures reproducibility. **iv)**

### Algorithms:

**Random Forest** enhances classification accuracy by aggregating multiple decision trees. It utilizes various sampling techniques, including SMOTE [4], B-SMOTE, ADASYN, SMOTE-Tomek, SMOTEEEN, and Hybrid BIRCH Borderline SMOTE, to effectively address class imbalance and improve fraud detection by accurately distinguishing between legitimate and fraudulent transactions.

**Boosted Decision Tree [10]** improves predictive performance by combining weak learners. It leverages sampling techniques like SMOTE, BSMOTE, ADASYN, SMOTE-Tomek, SMOTEEEN, and Hybrid BIRCH Borderline SMOTE to generate synthetic data, enhancing model sensitivity and ensuring better identification of fraudulent activities while reducing false negatives.

**ExtraTree [14]** accelerates training and enhances model diversity by creating multiple trees with random splits. Using sampling techniques such as SMOTE, B-SMOTE, ADASYN, SMOTE-Tomek, SMOTE-EEN, and Hybrid BIRCH Borderline SMOTE, it effectively addresses class imbalance, improving the accuracy of fraud detection in various transaction scenarios.

The **Voting Classifier** aggregates predictions from Boosted Decision Tree and ExtraTree to improve overall accuracy. By utilizing sampling techniques like SMOTE, B-SMOTE, ADASYN, SMOTETomek, SMOTE-EEN, and Hybrid BIRCH



Borderline SMOTE, it enhances the detection of fraudulent transactions while ensuring robustness against false positives and negatives.

#### 4. RESULTS & DISCUSSION

**Accuracy:** The accuracy of a test is its ability to differentiate the patient and healthy cases correctly.

To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (1)$$

**Precision:** Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

$$Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \quad (2)$$

**Recall:** Recall is a metric in machine learning that measures the ability of a model to identify all

relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

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

**F1-Score:** F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

$$F1\ Score = 2 * \frac{Recall * Precision}{Recall + Precision} * 100 \quad (1)$$

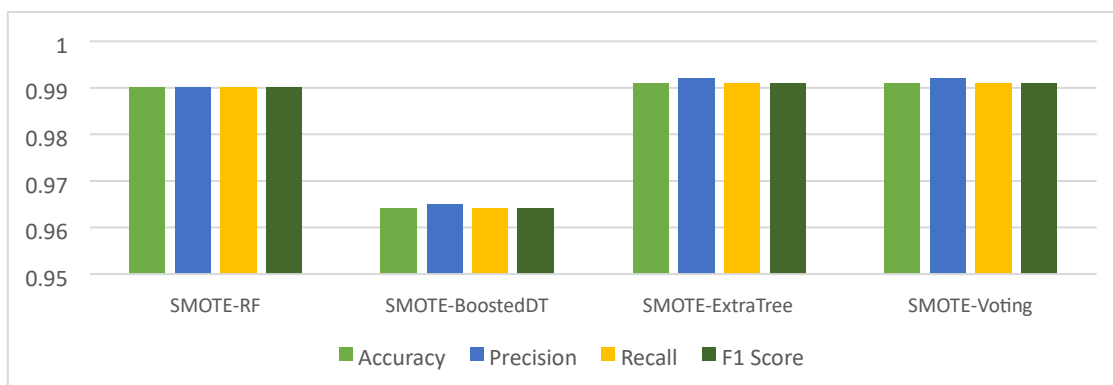
In Table 1, the Voting Classifier (Boosted DT + ExtraTree) achieved the highest accuracy and performance across all sampling techniques—SMOTE, B-SMOTE, ADASYN, SMOTE-Tomek, SMOTE-EEN, and Hybrid BIRCH Borderline SMOTE. It consistently outperformed other algorithms on all metrics, including accuracy, precision, recall, and F1 score.

Table.1 Performance Evaluation Metrics

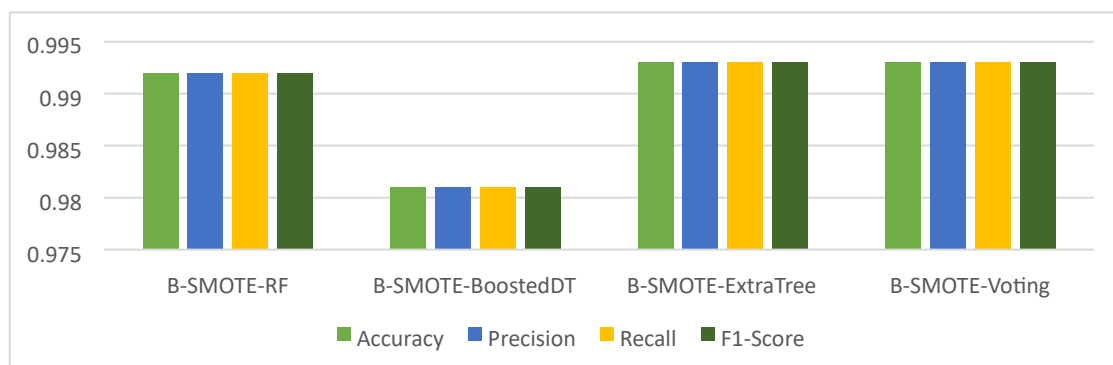
ML Model	Accuracy	Precision	Recall	F1 Score
SMOTE-RF	0.990	0.990	0.990	0.990
SMOTE-BoostedDT	0.964	0.965	0.964	0.964
SMOTE-ExtraTree	0.991	0.992	0.991	0.991
SMOTE-Voting	0.991	0.992	0.991	0.991
B-SMOTE-RF	0.992	0.992	0.992	0.992
B-SMOTE-BoostedDT	0.981	0.981	0.981	0.981
B-SMOTE-ExtraTree	0.993	0.993	0.993	0.993
B-SMOTE-Voting	0.993	0.993	0.993	0.993
Adasyn-RF	0.990	0.990	0.990	0.990

SMOTEEEN-BoostedDT	0.978	0.978	0.978	0.978
SMOTEEEN-ExtraTree	0.998	0.998	0.998	0.998
SMOTEEEN-Voting	0.997	0.997	0.997	0.997
Hybrid-RF	0.993	0.993	0.993	0.993
Hybrid-BoostedDT	0.975	0.976	0.975	0.975
Hybrid-ExtraTree	0.995	0.995	0.995	0.995
Hybrid-Voting	1.000	1.000	1.000	1.000
Adasyn-BoostedDT	0.956	0.959	0.956	0.956
Adasyn-ExtraTree	0.989	0.990	0.989	0.989
Adasyn-Voting	0.989	0.990	0.989	0.989
SMOTETomek-RF	0.990	0.990	0.990	0.990
SMOTETomek-BoostedDT	0.967	0.968	0.967	0.967
SMOTETomek-Extra Tree	0.992	0.992	0.992	0.992
SMOTETomek-Voting	0.992	0.992	0.992	0.992
SMOTEEEN-RF	0.996	0.996	0.996	0.996

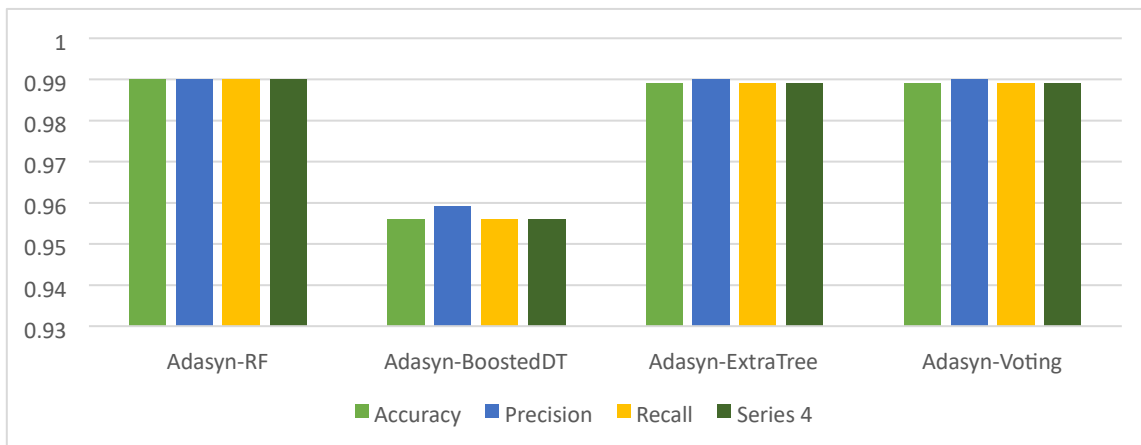
Graph.1 Comparison Graphs – SMOTE Sampling



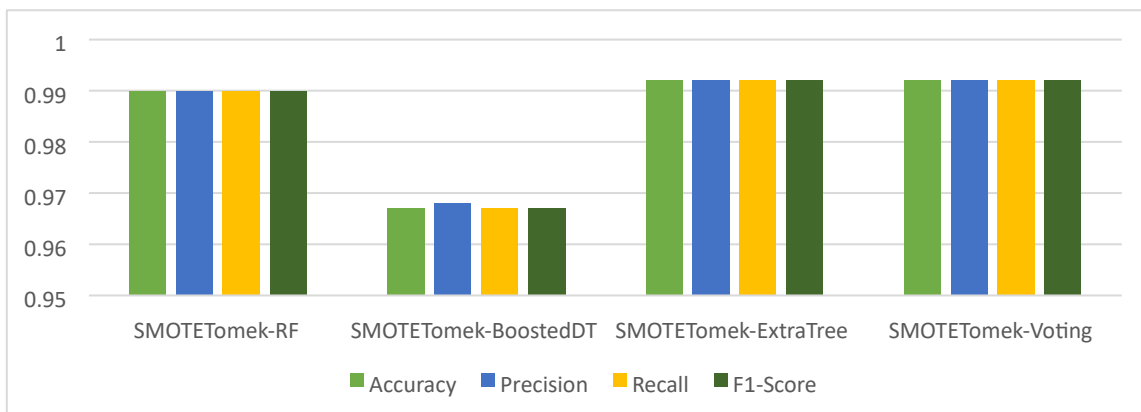
Graph.2 Comparison Graphs – B-SMOTE Sampling



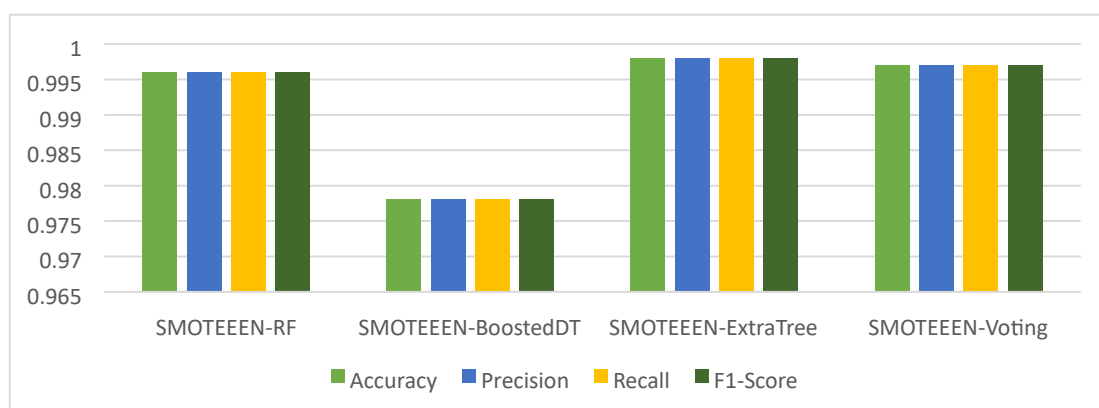
Graph.3 Comparison Graphs - Adasyn Sampling



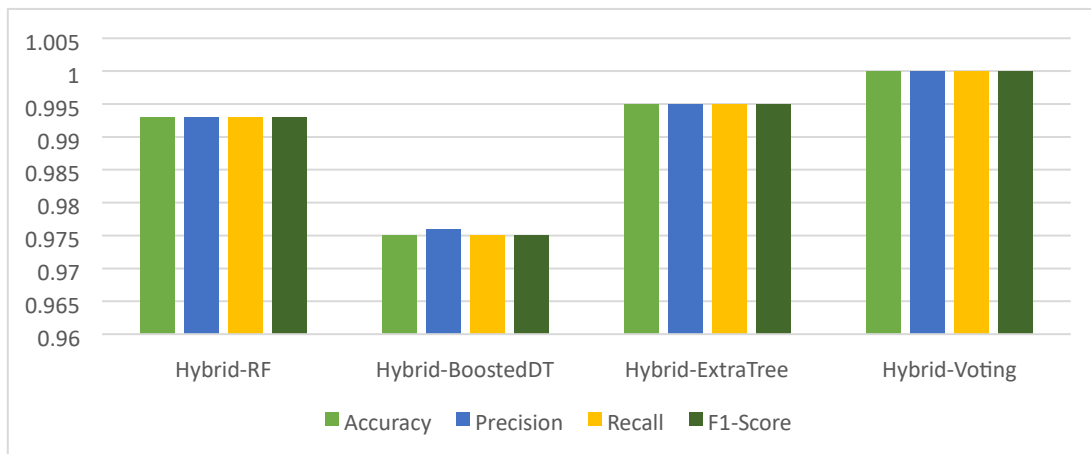
Graph.4 Comparison Graphs - SMOTE- Tomek Sampling



Graph.5 Comparison Graphs - SMOTE-EEN Sampling



Graph.6 Comparison Graphs - Hybrid BIRCH Borderline Smote Sampling



In Graphs (1,2,3,4,5&6) accuracy is represented in light green, precision in blue, recall in light yellow, and F1-score in green. The Voting Classifier outperforms the other algorithms in all metrics, with the highest values compared to the remaining models. These details are visually represented in the above graph.

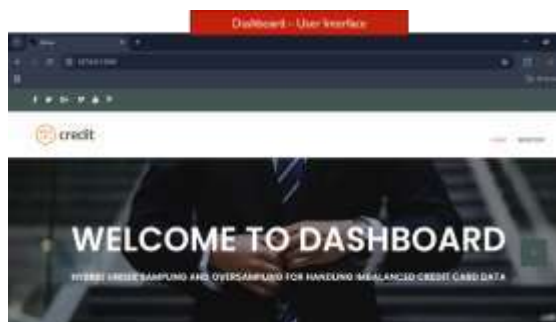


Fig. 3 Dash Board

The Fig. 3 shows a web page titled "Dashboard - User Interface." It has a "credit" logo and a welcome message with the tagline "Hybrid Under Sampling and Oversampling for Handling Imbalanced Credit Card Data."

## Step - 6

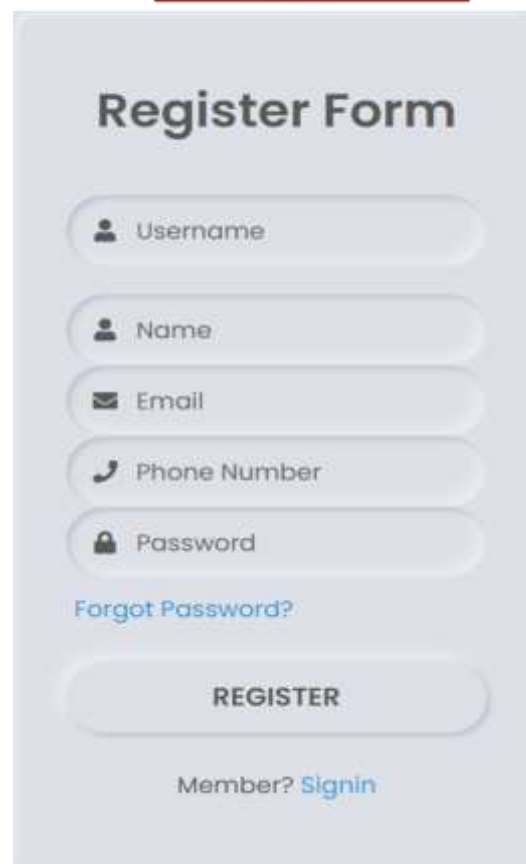
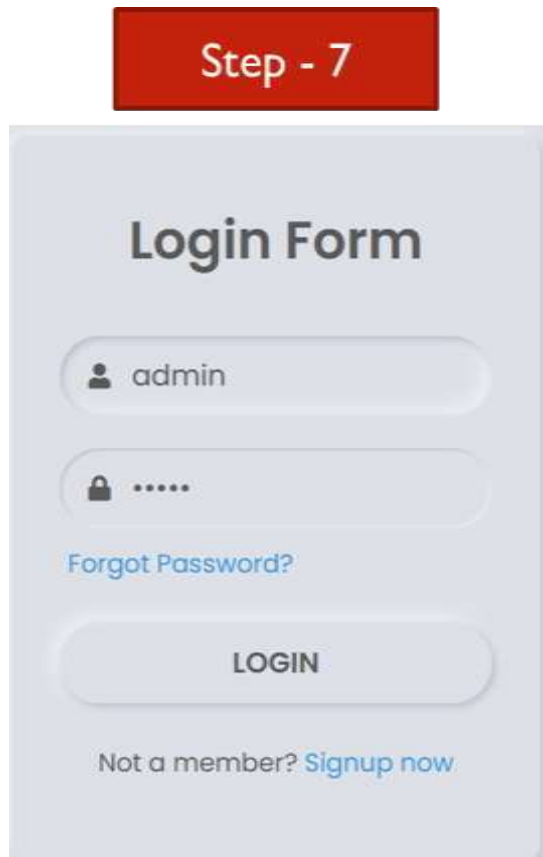


Fig. 4 Registration page

password. It also includes a "Forgot Password?" link and a "REGISTER" button.



**Step - 7**

## Login Form

admin

.....

[Forgot Password?](#)

**LOGIN**

Not a member? [Signup now](#)

Fig. 5 Login Page

The Fig. 5 shows a login form. The username field is pre-filled with "admin." It also has a password field, a "Forgot Password?" link, and a "LOGIN" button. There is also an option for new users to "Signup now."

The Fig. 4 shows a user registration form. It requires a username, name, email, phone number, and



Fig. 6 Home page

The Fig. 6 shows the homepage of a web application related to credit card data. It has a title "Welcome to Dashboard" and a tagline "Hybrid Under Sampling and Oversampling for Handling Imbalanced Credit Card Data."



**Step - 9**  
Test case - 1

### FORM

TYPE:

AMOUNT:

OLD BALANCE DRO:

NEW BALANCE CRED:

OUTCOME: **CREDIT CARD TRANSACTION HAPPENED IS FRAUD!**

Fig. 7 Test case – 1

The Fig. 7 shows a form for fraud detection in credit card transactions. It collects data like transaction

type, amount, and balances. After inputting data, the form predicts the transaction as "FRAUD."



Fig. 8 Test case - 2

The Fig. 8 shows a form for fraud detection in credit card transactions. It collects data like transaction type, amount, and balances. After inputting data, the form predicts the transaction as "NOT FRAUD."

## 5. CONCLUSION

This study demonstrates the effectiveness of combining advanced sampling techniques with robust machine learning models to address the challenge of detecting credit card fraud in imbalanced datasets. Among the evaluated algorithms, the Voting Classifier, which integrates Boosted Decision Tree and ExtraTree, consistently delivered superior performance across all sampling methods. With SMOTE, the Voting Classifier achieved an accuracy of 99.1%, demonstrating its

ability to handle the inherent imbalance in the dataset. Using B-SMOTE sampling, its performance improved further, reaching 99.3%. Similarly, with ADASYN sampling, it maintained a high accuracy of 98.9%, while SMOTE-Tomek sampling resulted in an accuracy of 99.2%. Notably, with SMOTEEN sampling, the Voting Classifier achieved one of its highest accuracies at 99.7%. Finally, the Hybrid BIRCH Borderline SMOTE sampling technique led the Voting Classifier to attain a perfect accuracy of 100%. These results highlight the robustness and reliability of the Voting Classifier in detecting fraudulent transactions, making it a powerful solution for credit card fraud detection.

The *future scope* of this research includes exploring advanced deep learning techniques, such as neural networks, to further enhance fraud detection accuracy. Additionally, integrating real-time monitoring capabilities can provide immediate alerts for suspicious transactions. Expanding the dataset to include diverse transaction types and leveraging more sophisticated sampling methods may also improve model performance. Furthermore, collaborations with financial institutions could facilitate the deployment of this system in live environments, contributing to ongoing efforts to combat credit card fraud effectively.

## REFERENCES

- [1] H. Shamsudin, U. K. Yusof, A. Jayalakshmi, and M. N. A. Khalid, "Combining oversampling and undersampling techniques for imbalanced classification: A comparative study using credit card fraudulent transaction dataset," in



Proc. IEEE 16th Int. Conf. Control Autom. (ICCA), Oct. 2020, pp. 803–808, doi: 10.1109/ICCA51439.2020.9264517.

[2] W. W. Soh and R. Yusuf, “Predicting credit card fraud on a imbalanced data,” *Int. J. Data Sci. Adv. Anal.*, vol. 1, no. 1, pp. 12–17, Apr. 2019. [Online].

Available:

<http://ijdsaa.com/index.php/welcome/article/view/3>

[3] P. Kaur and A. Gosain, “Comparing the behavior of oversampling and undersampling approach of class imbalance learning by combining class imbalance problem with noise,” in *Advances in Intelligent Systems and Computing*. Singapore: Springer, 2017, pp. 23–30, doi: 10.1007/978-981-10-6602-3\_3.

[4] R. Qaddoura and M. M. Biltawi, “Improving fraud detection in an imbalanced class distribution using different oversampling techniques,” in *Proc. Int. Eng. Conf. Electr., Energy, Artif. Intell. (EICEEAI)*, Nov. 2022, pp. 1–5, doi: 10.1109/EICEEAI56378.2022.10050500.

[5] K. Praveen Mahesh, S. Ashar Afrouz, and A. Shaju Areckal, “Detection of fraudulent credit card transactions: A comparative analysis of data sampling and classification techniques,” in *Proc. J. Phys., Conf.*, Jan. 2022, vol. 2161, no. 1, Art. no. 012072, doi: 10.1088/1742-6596/2161/1/012072.

[6] N. Rtayli, “An efficient deep learning classification model for predicting credit card

fraud on skewed data,” *J. Inf. Secur. Cybercrimes Res.*, vol. 5, no. 1, pp. 57–71, Jun. 2022, doi: 10.26735/tlyg7256.

[7] S. O. Akinwamide, “Prediction of fraudulent or genuine transactions on credit card fraud detection dataset using machine learning techniques,” *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 6, pp. 5061–5071, Jun. 2022, doi: 10.22214/ijraset.2022.44962.

[8] Q. Li and Y. Xie, “A behavior-cluster based imbalanced classification method for credit card fraud detection,” in *Proc. 2nd Int. Conf. Data Sci. Inf. Technol.* New York, NY, USA: ACM, Jul. 2019, pp. 134–139, doi: 10.1145/3352411.3352433.

[9] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, “A neural network ensemble with feature engineering for improved credit card fraud detection,” *IEEE Access*, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.

[10] X. Yi, Y. Xu, Q. Hu, S. Krishnamoorthy, W. Li, and Z. Tang, “ASNSMOTE: A synthetic minority oversampling method with adaptive qualified synthesizer selection,” *Complex Intell. Syst.*, vol. 8, no. 3, pp. 2247–2272, Jun. 2022, doi: 10.1007/s40747-021-00638-w.

[11] E. F. Ullastres and M. Latifi, “Credit card fraud detection using ensemble learning algorithms MSc research project MSc data analytics,”



M.S. thesis, Nat. College Ireland, Dublin,  
Ireland, May 2022.

[12] H. Zhu, M. Zhou, G. Liu, Y. Xie, S. Liu, and C. Guo, “NUS: Noisy-sample-removed undersampling scheme for imbalanced classification and application to credit card fraud detection,” *IEEE Trans. Computat. Social Syst.*, pp. 1–12, Mar. 2023, doi: 10.1109/TCSS.2023.3243925.

[13] E. A. Lopez-Rojas, A. Elmir, and S. Axelsson, “PaySim: A financial mobile money simulator for fraud detection,” in *Proc. 28th Eur. Modeling Simulation Symp. (EMSS)*, Sep. 2016, pp. 249–255.

[14] A. A. Arfeen and B. M. A. Khan, “Empirical analysis of machine learning algorithms on detection of fraudulent electronic fund transfer transactions,”

*IETE J. Res.*, pp. 1–13, Mar. 2022, doi: 10.1080/03772063.2022.2048700.

[15] I. A. Mondal, Md. E. Haque, A.-M. Hassan, and S. Shatabda, “Handling imbalanced data for credit card fraud detection,” in *Proc. 24th Int. Conf. Comput. Inf. Technol. (ICCIT)*, Dec. 2021, pp. 1–6, doi: 10.1109/ICCIT54785.2021.9689866.