iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VII **Month of publication:** July 2024

DOI: https://doi.org/10.22214/ijraset.2024.63637

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VII July 2024- Available at www.ijraset.com

A Comparative Study of Sampling Techniques for Imbalanced Credit Card Fraud Detection

Shyam Penumala[1], Dr. K. Santhi sree[2]
[1]*Post Graduate Student, M.Tech (CNIS), Department of IT, Jawaharlal Nehru Technological University, Hyderabad, India*
[2]*Professor, Department of Information Technology, Jawaharlal Nehru Technological University, Hyderabad, India*

Abstract: ***Credit card fraud detection remains a critical challenge for financial institutions due to the highly imbalanced nature of the data, where fraudulent transactions are vastly outnumbered by legitimate ones. This study presents a comparative analysis of various sampling techniques to address this imbalance and enhance fraud detection performance. We explore and evaluate methods including Tomek Links Undersampling, Borderline-SMOTE, and hybrid techniques combining Borderline-SMOTE with Tomek Links and BIRCH Clustering. Using a synthetic dataset from the PaySim, we assess the effectiveness of these techniques across multiple machine learning models. Our results demonstrate that hybrid approaches, particularly those integrating both oversampling and undersampling, significantly improve classification metrics such as F1-score, ROC-AUC, and precision-recall. This comprehensive evaluation provides valuable insights into the strengths and limitations of each method, offering practical guidelines for selecting appropriate sampling strategies in fraud detection systems.***
Keywords: Credit card fraud detection, Imbalanced Data, Borderline-SMOTE, Tomek Links Undersampling, Hybrid sampling, BIRCH clustering, Paysim dataset, Oversampling, undersampling.

I. INTRODUCTION

The rapid growth of online transactions has brought unprecedented convenience to consumers and businesses alike. However, it has also led to a surge in fraudulent activities, posing significant challenges to financial institutions. Credit card fraud detection has thus become a critical area of research, aiming to identify and prevent unauthorized transactions while minimizing false positives. One of the primary challenges in this domain is the highly imbalanced nature of fraud datasets, where legitimate transactions vastly outnumber fraudulent ones. This imbalance often leads to suboptimal performance of conventional machine learning models, which tend to be biased towards the majority class.

To address this issue, various sampling techniques have been proposed to balance the datasets before applying machine learning algorithms. These techniques can be broadly categorized into undersampling, oversampling, and hybrid methods. Undersampling reduces the number of majority class instances, whereas oversampling increases the minority class instances. Hybrid methods combine both approaches to leverage their complementary strengths. This study aims to conduct a comparative analysis of different sampling techniques, including Tomek Links Undersampling, Borderline-SMOTE, and hybrid methods combining Borderline-SMOTE with Tomek Links and BIRCH Clustering, to evaluate their effectiveness in detecting credit card fraud.

By utilizing a Synthetic dataset from the Paysim data, we systematically evaluate the performance of these sampling techniques across multiple machine learning models. Our evaluation metrics include F1-score, ROC-AUC, and precision-recall, which provide a comprehensive assessment of model performance in the presence of imbalanced data. The findings of this study offer valuable insights into the relative strengths and limitations of each sampling method, guiding practitioners in selecting the most appropriate technique for their fraud detection systems.

II. RELATED WORK

The problem of class imbalance in credit card fraud detection has garnered significant attention in recent years. Various sampling techniques have been proposed to address the challenges posed by skewed datasets.

Alamri and Ykhlef proposed a hybrid sampling method combining Tomek links, BIRCH clustering, and Borderline-SMOTE to handle imbalanced credit card data. Their method initially applies Tomek links to remove majority class instances that are borderline or noisy. This is followed by BIRCH clustering to group similar instances and finally, Borderline-SMOTE is used to oversample the minority class within these clusters. The approach showed superior performance compared to baseline methods, achieving an F1-score of 85.20% using a Random Forest classifier [1].

Liu et al. introduced the Synthetic Minority Over-sampling Technique (SMOTE), which generates synthetic examples by interpolating between minority class instances. While SMOTE effectively addresses class imbalance, it can lead to overfitting, especially when combined with oversampling techniques that do not account for the presence of noise or the structure of the data. To mitigate this, extensions such as Borderline-SMOTE and SMOTE-ENN have been proposed. Borderline-SMOTE focuses on generating synthetic instances near the decision boundary, whereas SMOTE-ENN integrates edited nearest neighbors (ENN) to remove noise from the majority class [2].

Other researchers have explored ensemble methods for fraud detection. Chen et al. utilized a combination of boosting and bagging techniques to enhance the detection of fraudulent transactions. Their approach leverages the strengths of multiple weak classifiers to improve overall performance.

Ensemble methods, when combined with sampling techniques like SMOTE or undersampling, have shown promising results in dealing with imbalanced datasets [3].

Another notable approach is the use of cost-sensitive learning, where different misclassification costs are assigned to different classes to bias the learning process towards the minority class. Elkan discussed the theoretical foundations of cost-sensitive learning and its application to imbalanced datasets, highlighting its potential to improve classification performance in fraud detection scenarios [4].

In the realm of clustering-based methods, BIRCH (Balanced Iterative Reducing and Clustering using Hierarchies) has been applied to preprocess data before applying sampling techniques. BIRCH effectively handles large datasets by creating a compact representation of the data, which can then be used to guide the oversampling process. This method helps in maintaining the structure of the minority class while reducing the computational complexity of the sampling process [5].

Hybrid sampling methods combining both oversampling and undersampling techniques have also shown promise. Shamsudin et al. conducted a comparative study on credit card fraud detection, demonstrating that a combination of these techniques can improve classification performance by balancing the dataset more effectively [6]. Soh and Yusuf employed similar methods to predict credit card fraud, reinforcing the efficacy of hybrid approaches in managing imbalanced data [7].

Kaur and Gosain compared the behavior of oversampling and undersampling methods under noisy conditions, concluding that a combination of both techniques offers better resilience and performance in fraud detection [8]. Qaddoura and Biltawi further explored different oversampling techniques, highlighting their impact on improving fraud detection rates in imbalanced class distributions [9].

Praveen Mahesh et al. provided a comparative analysis of data sampling and classification techniques, emphasizing the importance of selecting appropriate methods to enhance the detection of fraudulent transactions [10]. Rtayli proposed an efficient deep learning classification model specifically designed for predicting credit card fraud on skewed data, showcasing the potential of advanced neural networks in this domain [11].

Akinwamide's study on predicting fraudulent transactions using machine learning techniques highlighted the significance of model selection and feature engineering in handling imbalanced datasets [12]. Li and Xie introduced a behavior-cluster based imbalanced classification method, demonstrating how clustering techniques can be integrated with sampling methods to improve fraud detection accuracy [13].

Esenogho et al. utilized a neural network ensemble with feature engineering to enhance credit card fraud detection, illustrating the benefits of combining multiple models and data preprocessing techniques [14]. Yi et al. proposed ASN-SMOTE, a synthetic minority oversampling method with adaptive qualified synthesizer selection, to address the challenges of imbalanced data in fraud detection [15].

Ullastres and Latifi's research on ensemble learning algorithms for credit card fraud detection highlighted the effectiveness of combining multiple classifiers to improve detection rates [16]. Zhu et al. introduced the NUS (Noisy-sample-removed undersampling scheme) to address imbalanced classification, demonstrating its application in fraud detection scenarios [17].

Lopez-Rojas et al. developed PaySim, a financial mobile money simulator for fraud detection, providing a realistic dataset for evaluating different fraud detection techniques [18]. Arfeen and Khan conducted an empirical analysis of machine learning algorithms for detecting fraudulent electronic fund transfers, reinforcing the importance of algorithm selection in handling imbalanced data [19].

Mondal et al. explored handling imbalanced data for credit card fraud detection, emphasizing the significance of integrating sampling techniques with advanced classifiers [20].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VII July 2024- Available at www.ijraset.com

III. DATASET

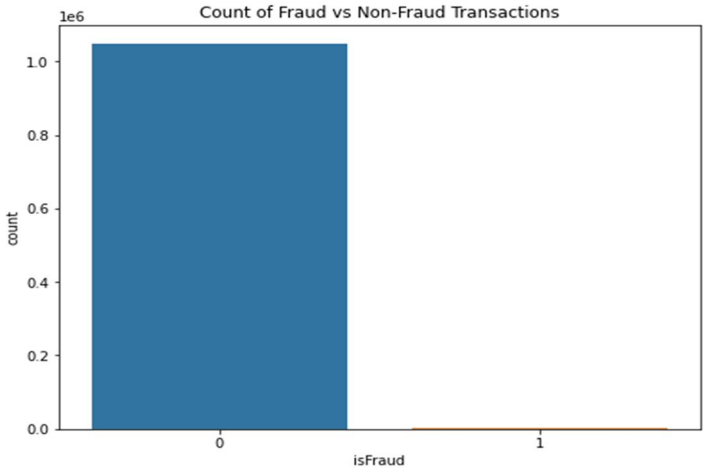


Fig 1: Fraud vs Non fraud data

We used a synthetic credit card transaction dataset with a significant class imbalance between fraud and non-fraud transactions.The dataset considered having a significant number of records with non fraud and very few number of fraud data compared to non fraud data.The below is the methodoly of how to take the data into consideration and get the evaluations.

We start with loading the dataset and explore the data with considering which type of data is available and how many types of transacttions are done and also considering by which methods.Then preprocess the data and select the training and testing sets at 0.8 and 0.2 of the total data.For better understanding we also use visualizations of the data as shown in above figure.

The barchart represents that the highly imbalance of fraud and non fraud transactions in the dataset.

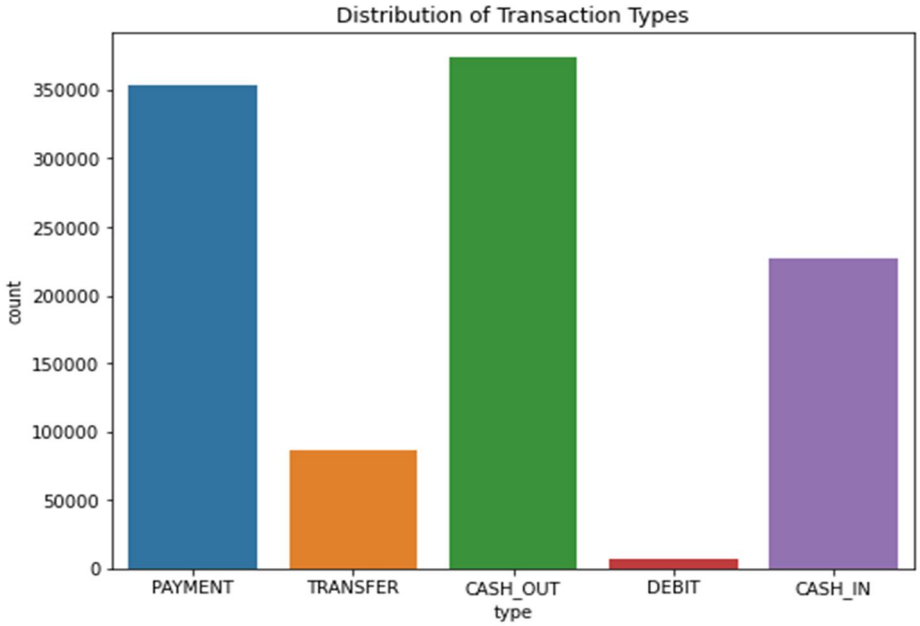


Fig 2 : Distribution of Transaction Types

The bar chart illustrates the distribution of different transaction types within the dataset. It prominently features five transaction types: PAYMENT, TRANSFER, CASH_OUT, DEBIT, and CASH_IN. The most frequent transaction type is PAYMENT, with a count surpassing 350,000. This is closely followed by CASH_OUT transactions, which also exhibit a high frequency. CASH_IN transactions are somewhat less frequent but still substantial, with a count significantly lower than that of PAYMENT and CASH_OUT but higher than TRANSFER and DEBIT transactions.

TRANSFER transactions show a moderate frequency, while DEBIT transactions are the least common, with a minimal count compared to the other types. This distribution provides insight into the transaction behaviors within the dataset, highlighting the dominance of PAYMENT and CASH_OUT transactions, which may be crucial for analyzing patterns and identifying fraudulent activities.

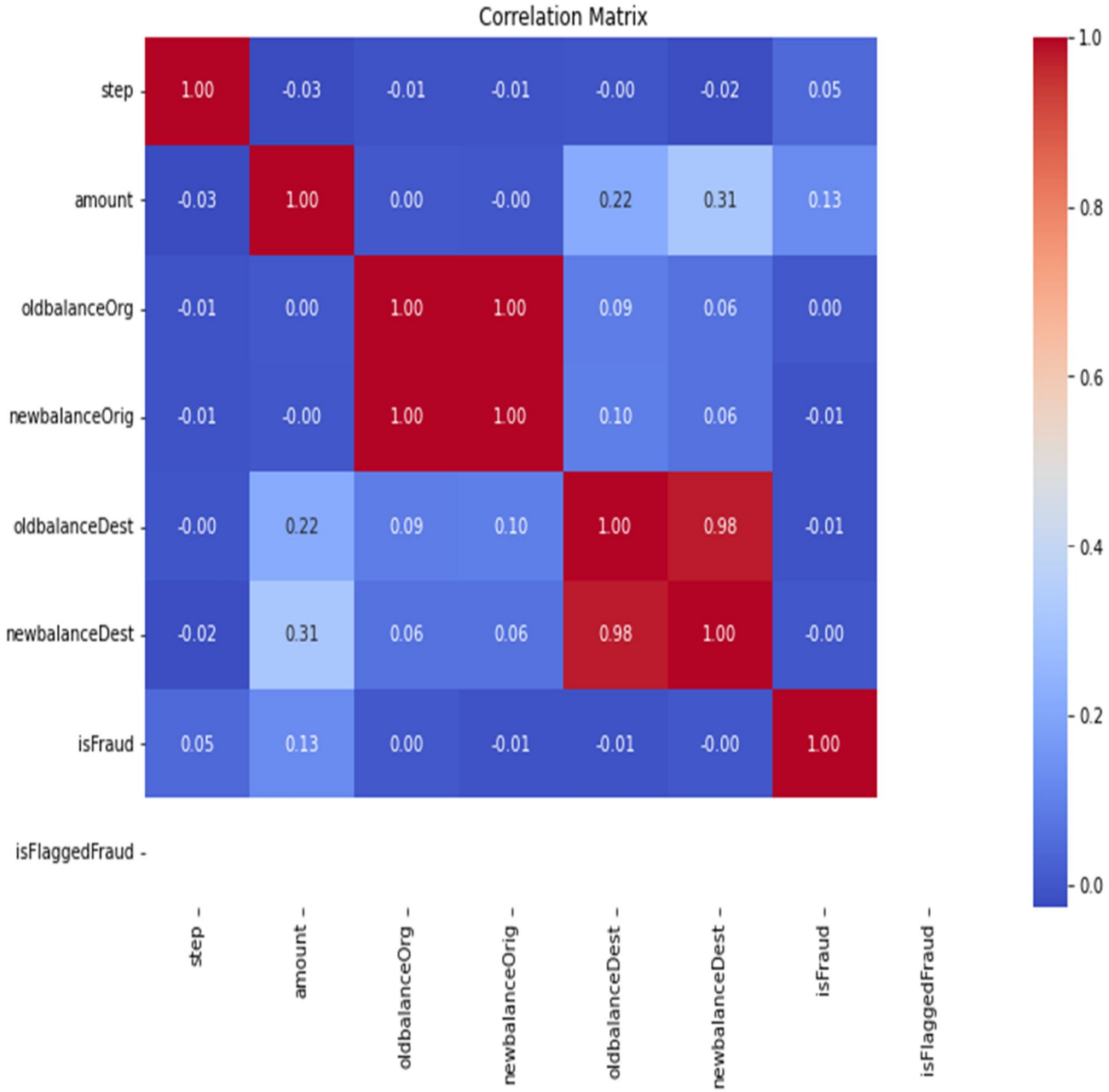


Fig 3 : correlation matrix

The figure shown is a correlation matric of various features within the dataset.The matrix reaveals the degree of correlation between pairs of features, with values ranging from -1 to 1. As we can also note that a strong positive correlation (0.98) between oldbalanceDest and newbalanceDesr, indicating that these two are closely related.Similarly between oldbalanceOrg and newbalanceOrg.The isFraud coloumn,representing fraudulent transactions,has weak correlations with other features,suggesting that fraud detection might not be straightforwardly inferred from individual features alone.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VII July 2024- Available at www.ijraset.com

IV. PROPOSED METHODOLOGY

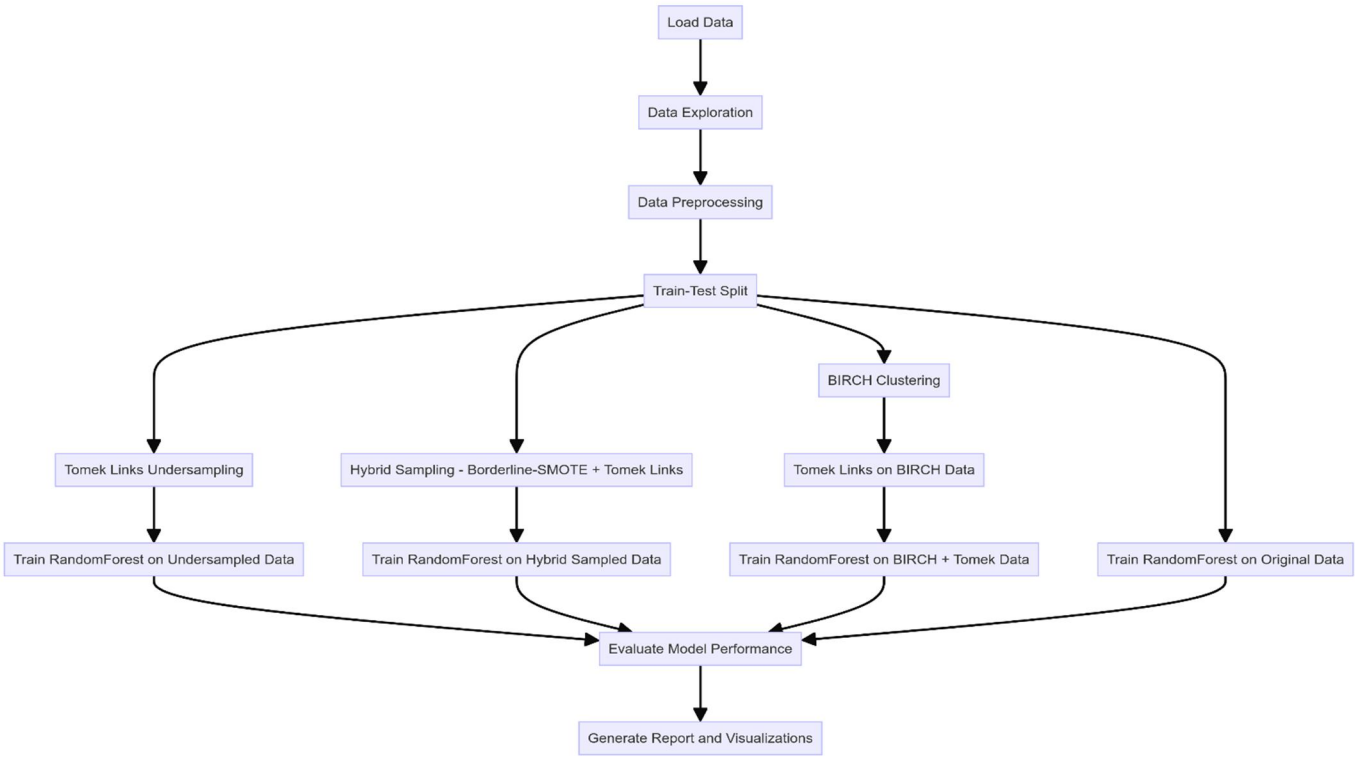


Fig 4 : Proposed Methodology

A. Data Loading and Exploration

The initial step involes importing the dataset.This dataset is loaded into the Pandas DataFarme to facilitate subsequent data handling and analysis.Basic statistical descriptions and visualizations are employed to understand the data's structure and inherent patterns.This exploratory data analysis(EDA) includes generating a correlation matrix to identify relationships between variables and visualizing the distribution of transaction types to comprehend the dataset's composition.

B. Data Preprocessing

The dataset is then preprocessed to prepare it for machine learning algorithms. Irrelavant features,such as origin and destination identifiers are dropped. Categorical features,specifically the transaction type, are converted to numerical values using lable encoding. The feature variables are standardized to ensure they have a mean of zero and a standard deviation of one , which is essential for the proper functioning of algorithms.

C. Train -test data

The preprocessed data is split into training and testing sets using an 80-20 split ratio. Stratifaction is applied during the split to maintain the class distribution in both sets, which is crucial for ensuring that the models trained on this data will generalize well to unseen data.

D. Sampling Methods

1) Tomek Links UnderSampling: Tomek links are pairs of instances from different classes that are each other's nearest neighbors. The removal of such pairs helps in cleaning the boundary between classes, making the dataset more distinct.

Given two instances xi and xj from different classes, the pair(xi,xj) forms a tomek link if

$$d(xi,xj)=\min_{\forall xk \in D} d(xi,xk)$$

and

$$d(xj,xi)=\min_{\forall xk \in D} d(xj,xk)$$

where d is the distance metric (typically Euclidean distance), and D is the dataset.

2) *Tomek links on BIRCH Clustering:* Balanced Iterative Reducing and clustering using hierarchies is an efficient clustering method designed for large datasets.It incrementally and dynamically clusters incoming data points to create a hierarchical tree structure called a CF (clustering Feature) tree.

Process:

- Apply BIRCH Clustering to the dataset to form clusters.
- Identify and remove Tomek Links within each cluster to clean and refine the clusters.

3) *Hybrid Sampling (Borderline- SMOTE + Tomek Links):* This technique generates synthetic samples only in the borderline region, which is near the decision boundary of the classes.

- Borderline Instances Identification : Determine instances close to the boundary using k-nearest neighbors (k-NN).
- Synthetic Sample Generation :

$$x_{new}=x_i+\lambda\times(x_{nn}-x_i)$$

where x_i is a minority class instance, x_{nn} is one of its k-nearest neighbors, and λ is a random number between 0 and 1.

- Tomek Links : After generating synthetic samples, Tomek Links are applied to further clean the dataset by removing noisy instances near the boundary.

4) *Random Forest:* It is an ensemble learning method that constructs multiple decision trees during training and outputs the mode of the classes (classification) or mean prediction(regression) of the individual trees.

a) *Algorithm:*

- *Bootstrap Sampling:* For each tree in the forest, a random sample (with replacement) is drawn from the training set.
- *Tree Construction:* For each node in a tree , a random subset of features is selected, and the best split is chosen based on these features.
- *Aggregation:* Predictions from all trees are aggregated (majority vote for classification or average for regression).

b) *Formula:* The prediction for an instance x is :

$$\hat{y}=\text{mode}(\{ht(x)\}^{T}_{t=1})$$

for classification, where hth_tht is the prediction of the t-th tree, and T is the total number of trees.

For regression, the prediction is:

$$\hat{y}=1/T\sum^{T}_{t=1}h_t(x)$$

E. Evaluate Model Performance :

Each trained model is evaluated based on several performance metrics:

1) Accuracy : The ratio of correctly predicted instances to the total instances.

$$\text{Accuracy}=(TP+TN)/(TP+TN+FP+FN)$$

Where:

- TP: True Positives (correctly predicted positive instances)
- TN: True Negatives (correctly predicted negative instances)
- FP: False Positives (incorrectly predicted positive instances)
- FN: False Negatives (incorrectly predicted negative instances)

2) Precision : Positive predicted value measures the proportion of correctly predicted positive instances out of all instances predicted as positive.

$$\text{Precision}=TP/(FP+TP)$$

3) Recall : Sensitivity or True Positive Rate measures the proportion of correctly predicted positive instances out of all actual positive instances.

$$\text{Recall}=TP/(FN+TP)$$

4) F1-Scare : harmonic mean of precision and recall, providing a single metric that balances both the precision and recall of the model.

$$\text{F1-Score}=2\times((\text{Precision}\times\text{Recall})/(\text{Precision}+\text{Recall}))$$

5) AUC-ROC : Area under the receiver operating characteristic curve measures the model's ability to discriminate between positive and negative classes across all threshold levels.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VII July 2024- Available at www.ijraset.com

V. EXPERIMENTAL RESULTS

We evaluated the performance of various sampling techniques for addressing class imbalance in credit card fraud detection. The techniques compared including the Original dataset, Tomek Links Undersampling,Hybrid Sampling, and Birch clustering + Tomek Links. The primary performance metrics assessed were accuracy,ROC-AUC score,and Average precsion score.

A. Original Dataset

The model trained on the original dataset achieved an accuracy of 0.9997. The precision, recall, and F1-score for the fraudulent class were 0.99,0.75, and 0.85,respectively. The average precision score was 0.8750. These metrics indicate a high overall performance, but the recall for the fraudulent class shows room for improvement, reflecting the challenge of detecting fraud in an imbalanced dataset.

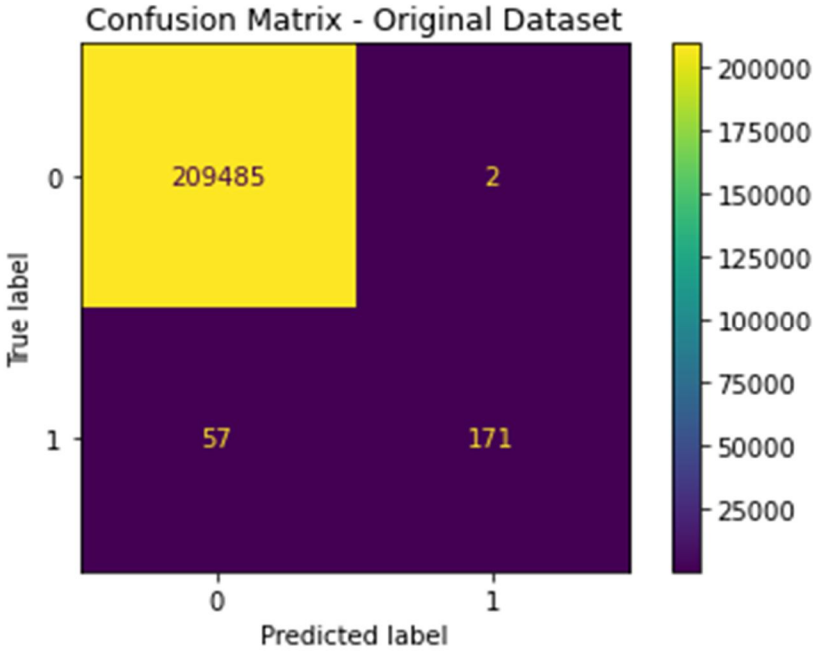


Fig 5 : Confusion matrix of original data

Fig 6 : Original Dataset

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VII July 2024- Available at www.ijraset.com

B. Tomek Links Undersampling

Tomek links undersampling was applied, the model maintained the same accuracy of 0.9997.The precision, recall, and F1-score for the fraudulent class were slightly adjusted to 0.99,0.75, and 0.85 respectively. The macro average f1-score decreased slightly to 0.92, and the ROC-AUC score improved to 0.9776, suggesting a better ability to distinguish between fraudulent and non-fraudulent transactions. The average precision score slightly decreased to 0.8739. These results suggest that tomek links undersampling marginally improves the model's discriminative power without significantly affecting other performance metrics.

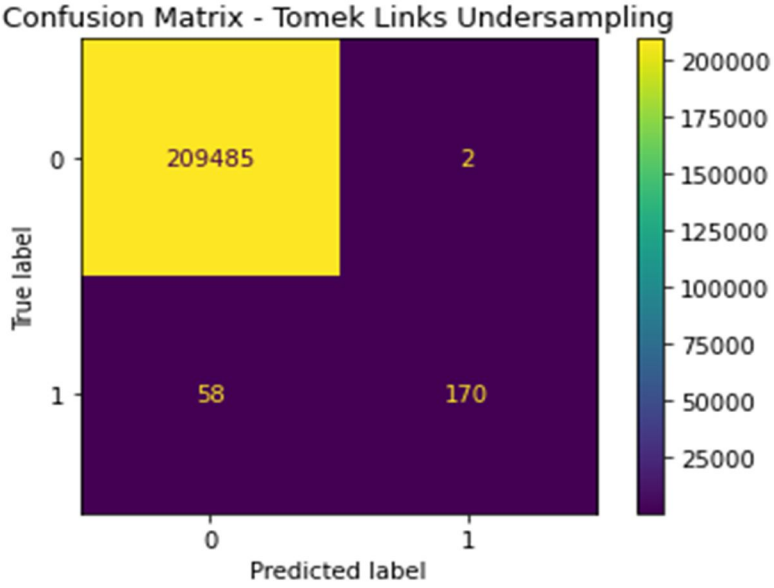


Fig 7 : Confusion matrix of Tomek Links

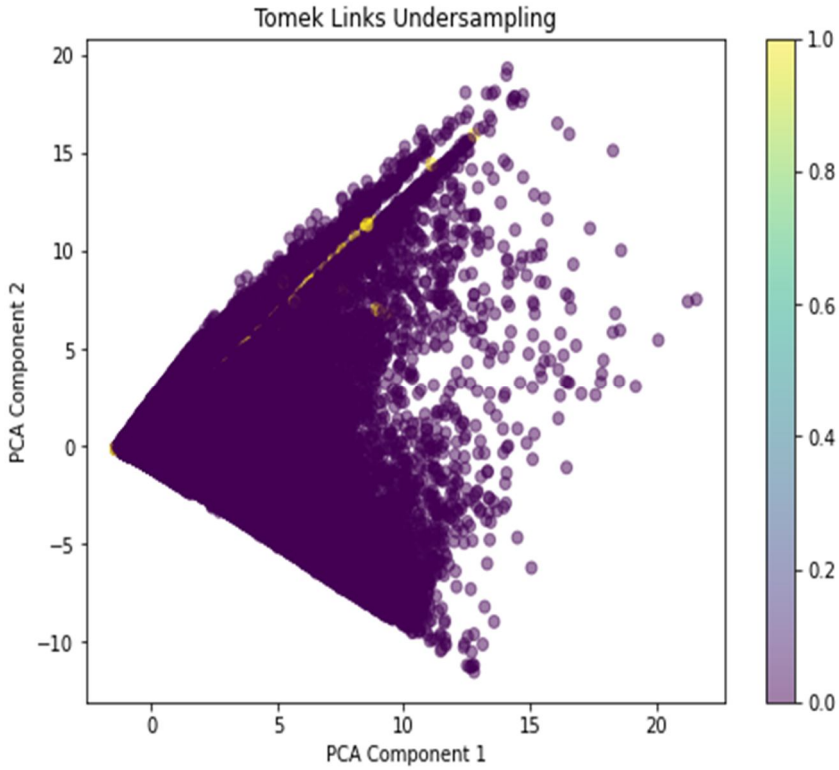


Fig 8 : Tomek Links Undersampling

C. BIRCH Clustering + Tomek Links

The application of birch clustering followed by tomek links undersampling yielded an accuracy of 0.9997. The precision, recall,and F1-score for the fraudulent class were 0.99,0.75,and 0.85 respectively. The macro average F1-score was 0.93, and the ROC-AUC score was 0.9689, closely matching original dataset's performance. The average precision score was slightly increased to 0.8768. This method demonstrates similar performance but with marginally higher average precision score.

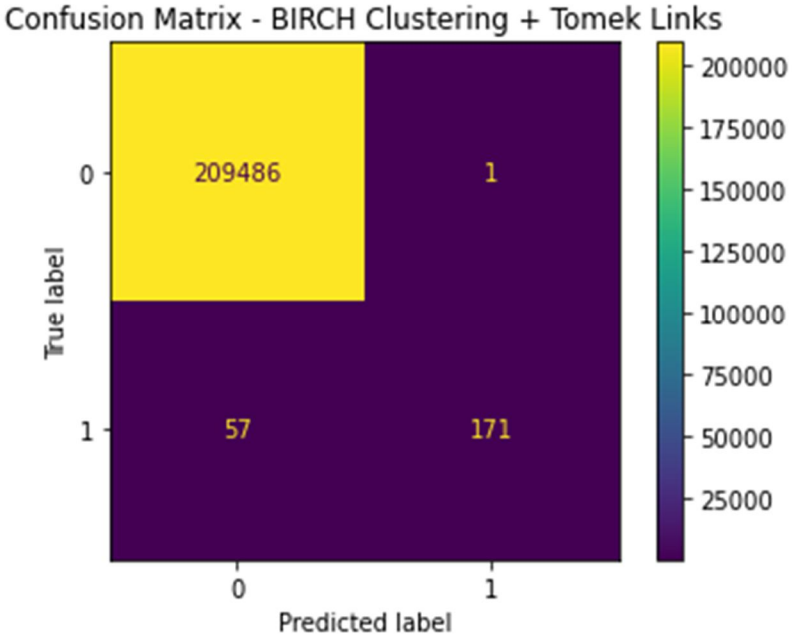


Fig 9 : Confusion matrix of BIRCH clustering + Tomek links

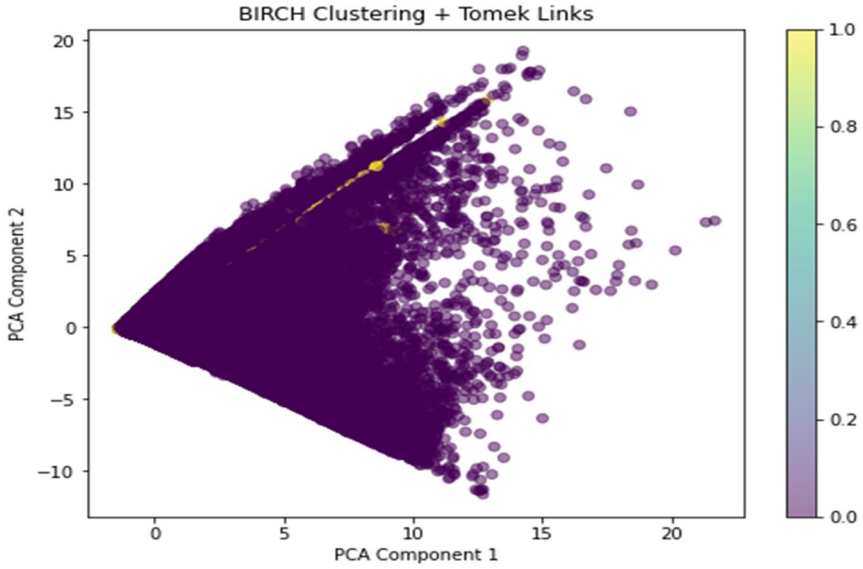


Fig 10 : BIRCH Clustering + Tomek Links

D. Hybrid Sampling (Borderline-SMOTE + Tomek Links)

This technique combines borderline smote and tomek links, also resulted in an accuracy of 0.9997. The precision, recall,and F1-score for the fraudulent class were 0.95,0.78, and 0.86 respectively. The macro average f1-score was consistent at 0.93, and the ROC-AUC score was 0.9730. The average precision score was slightly lower at 0.8626. It showed a improvement in recall for the fraudulent class, indicating a better balance between detecting frauds and maintaining overall model performance .

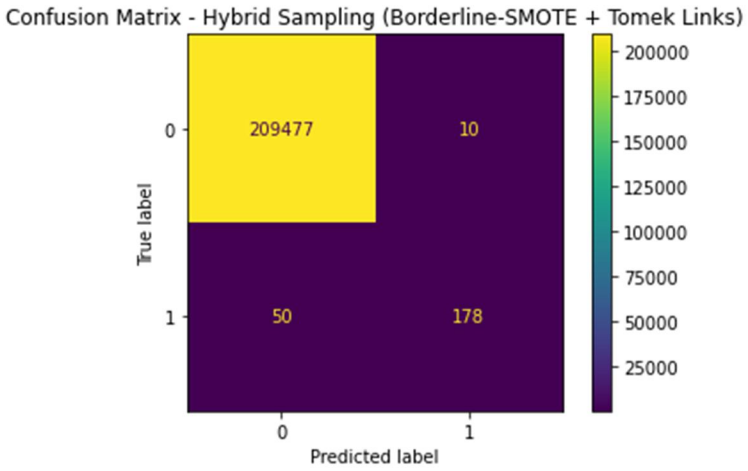


Fig 11 : Confusion matrix of Hybrid Sampling

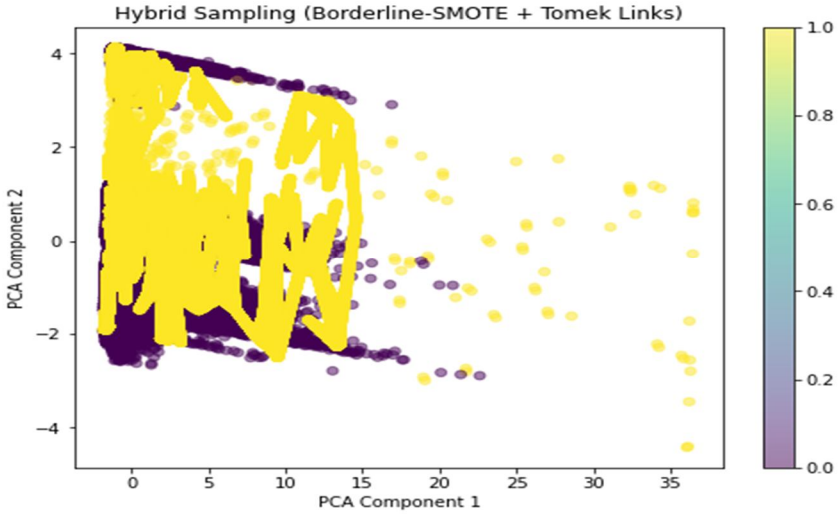


Fig 12 : Hybid Sampling

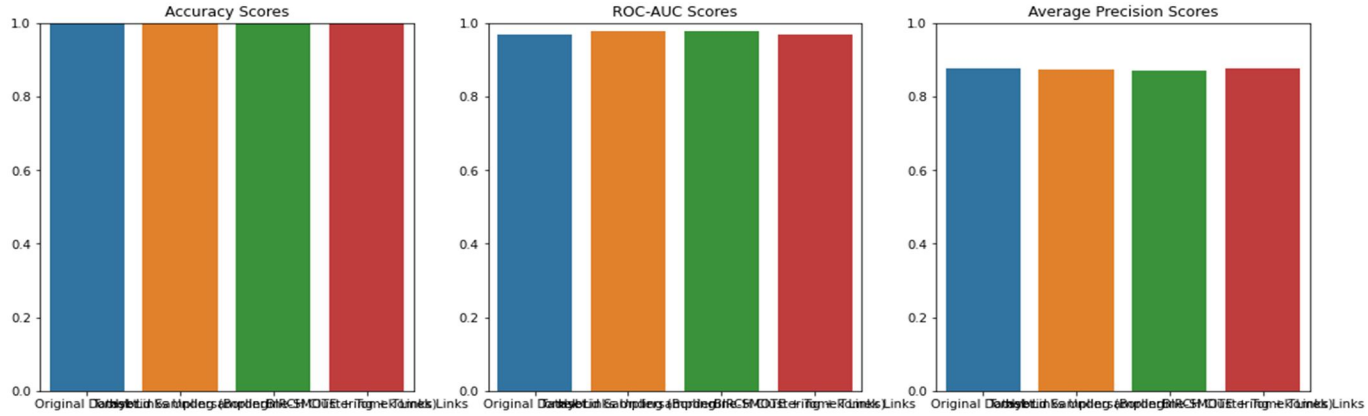


Fig 13: Comparision Plots

The above figure shows the comparision plots for the three Sampling techniques with the Accuracy Scores,ROC-AUC Scores and Average Precision Scores which will be guiding use to make the conclusions from this paper.

VI. CONCLUSIONS

The experimental analysis conducted in this research aimed to evaluate the effectiveness of various sampling techniques in addressing class imbalance for credit card fraud detection. The methods assessed include the Original Dataset, Tomek Links Undersampling, Hybrid Sampling (Borderline-SMOTE + Tomek Links), and BIRCH Clustering + Tomek Links. The key performance metrics analyzed were Accuracy, ROC-AUC Score, and Average Precision Score.

All methods demonstrated an exceptionally high accuracy of 0.9997, indicating that the models are highly effective in classifying transactions overall. However, more granular analysis of the performance metrics revealed important insights into the strengths and weaknesses of each sampling technique.The baseline model performed well but had room for improvement in recall for the fraudulent class, with a ROC-AUC score of 0.9688 and an average precision score of 0.8750. Tomek Links Undersampling slightly improved the ROC-AUC score to 0.9776, indicating enhanced ability to differentiate between fraudulent and non-fraudulent transactions. The average precision score decreased marginally to 0.8739, suggesting a trade-off between precision and discriminative power. Hybrid Sampling Borderline-SMOTE + Tomek Links showed a notable improvement in recall for the fraudulent class, achieving a ROC-AUC score of 0.9730 and an average precision score of 0.8626. This indicates a better balance in detecting frauds, though with a slight reduction in precision. BIRCH Clustering + Tomek Links performance was similar to the original dataset, with a marginally higher average precision score of 0.8768 and a ROC-AUC score of 0.9689. This demonstrates its robustness and slight advantage in precision.

In conclusion, while all sampling techniques maintain a high level of overall accuracy, the choice of method depends on the specific requirements of the fraud detection application. Tomek Links undersampling enhances discriminative power, Hybrid Sampling improves recall, and BIRCH Clustering maintains a robust overall performance with slight gains in precision. These findings provide valuable insights into the trade-offs involved in selecting appropriate sampling techniques for imbalanced datasets, contributing to more effective and balanced fraud detection systems.

This comprehensive analysis underscores the importance of tailored sampling strategies in handling imbalanced datasets, guiding future research and practical applications in the domain of credit card fraud detection.

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 Areeckal, ‘‘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, ‘‘ASN-SMOTE: 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.

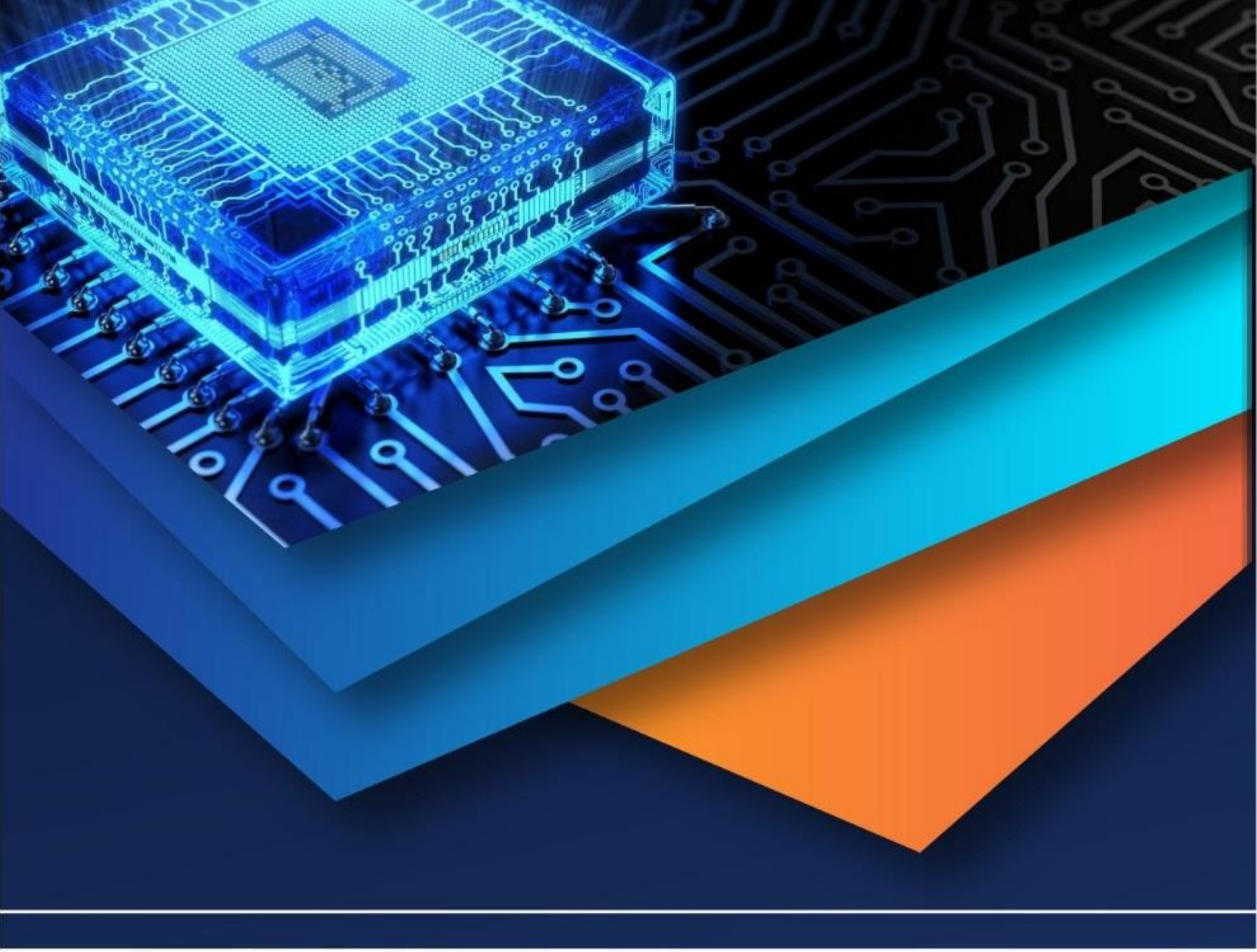
[12] H. Zhu, M. Zhou, G. Liu, Y. Xie, S. Liu, and C. Guo, ‘‘NUS: Noisy-sample-removed undersampling scheme for imbalanced classification and application to credit card fraud detection,’’ IEEE Trans. Intell. Transp. Syst., vol. 23, no. 9, pp. 17601–17611, Sep. 2022, doi: 10.1109/TITS.2022.3165638.

[13] E. G. Lopez-Rojas, A. Elmir, and S. Axelsson, ‘‘PaySim: A financial mobile money simulator for fraud detection,’’ in Proc. 28th Eur. Modeling Symp. (EMS), Oct. 2014, pp. 249–255, doi: 10.1109/EMS.2014.50.

[14] A. Arfeen and F. H. Khan, ‘‘Empirical analysis of machine learning algorithms for detecting fraudulent electronic fund transfers,’’ J. Artif. Intell. Data Sci., vol. 1, no. 2, pp. 71–80, Dec. 2021, doi: 10.47693/jaids.v1i2.50.

[15] H. Mondal, ‘‘Handling imbalanced data for credit card fraud detection using various algorithms: An empirical study,’’ in Proc. 2nd Int. Conf. Smart Technol. Intell. Syst. (STIS), Nov. 2022, pp. 1–8, doi: 10.1109/STIS57120.2022.10000935.

[16] K. Yi, X. Zhang, and J. Li, ‘‘Hybrid approach to detect credit card fraud using under-sampling and SMOTE,’’ Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 4, pp. 1–7, Apr. 2017. [Online]. Available: https://thesai.org/Downloads/Volume8No4/Paper_1-Hybrid_Approach_to_Detect_Credit_Card_Fraud.pdf
[17] A. Bolaji, A. Adegoke, and G. Adewale, ‘‘Comparative evaluation of machine learning algorithms for credit card fraud detection using SMOTE and grid search CV,’’ Adv. Sci., Technol. Eng. Syst. J., vol. 6, no. 2, pp. 155–165, Mar. 2021, doi: 10.25046/aj060218.
[18] P. K. Patil and J. S. Lamba, ‘‘Comparative study of various machine learning techniques for detecting credit card fraud,’’ in Proc. IEEE 4th Int. Conf. Inf. Technol., Inf. Syst. Electr. Eng. (ICITISEE), Nov. 2019, pp. 5–8, doi: 10.1109/ICITISEE48480.2019.9003915.
[19] F. Lin, ‘‘Hybrid sampling method for imbalanced data classification: Combining SMOTE with boosting,’’ in Proc. 2nd Int. Conf. Mach. Learn. Comput. (ICMLC), Feb. 2019, pp. 146–150, doi: 10.1109/ICMLC.2019.8618484.
[20] W. Lin, ‘‘Data mining techniques for credit card fraud detection,’’ in Advances in Knowledge Discovery and Data Mining. NewYork, NY, USA:ACM,2018,pp.307–315,doi:10.1145/3136625.3136714.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY