Comparative Analysis of Machine Learning Models for Credit Card Fraud Detection

Makineedi Venkat Dinesh
Electronics and Communication Engineering,
National Institute of Technology Andhra Pradesh, Tadepalligudem, India

Abstract - **This paper presents a comprehensive study on credit card fraud detection utilizing machine learning models. Three distinct approaches were explored, each employing different preprocessing techniques and models. The performance of each approach was evaluated based on various classification metrics, including precision, recall, and F1-score. The experimental results indicate that the approach combining resampling and feature normalization, coupled with the lightGBM model, achieved the highest recall and area under the ROC curve.**

***Keywords*: credit card fraud detection, machine learning models, lightGBM, logistic regression, K-neighbors classification, resampling, feature normalization, Synthetic Minority Over-sampling Technique.**

1. INTRODUCTION

Credit card fraud remains a significant concern for financial institutions and consumers worldwide. Detecting fraudulent transactions in real-time is crucial to minimize financial losses and protect consumers' assets. Machine learning techniques offer promising solutions for automated fraud detection by leveraging historical transaction data. In this study, we explore the effectiveness of different machine learning models in detecting credit card fraud.

2. IMPLEMENTATION

Three distinct approaches were explored in the study: the first involved (approach 1) normalizing the 'Amount' feature while eliminating the 'time' feature; the second (approach 2) focused on normalizing all features; and the third (approach 3) entailed resampling all data to achieve a balanced dataset. Each of these approaches underwent rigorous evaluation through the training and assessment of three machine learning models: lightGBM, Logistic Regression, and K-Neighbors Classification.

2.1 Feature engineering

Feature engineering is a critical aspect of machine learning model development, serving to enhance the quality and effectiveness of predictive algorithms. In this study, feature engineering techniques were meticulously applied to optimize the performance of the credit card fault detection models. First and foremost, normalization was employed to standardize the range of features, ensuring that each attribute contributed proportionately to the model's predictive capabilities. This step not only mitigated the influence of varying scales within the dataset but also facilitated smoother convergence during model training. Additionally, resampling techniques were leveraged to address class imbalance issues inherent in the credit card transaction data. By augmenting the minority class through oversampling, the dataset was rebalanced, thereby preventing the model from exhibiting bias towards the majority class. Furthermore, the Synthetic Minority Over-sampling Technique (SMOTE) which is not used in this analysis but can also be used to generate synthetic samples of the minority class, thereby amplifying its representation in the dataset. These techniques played a pivotal role in alleviating the impact of class imbalance, ultimately enhancing the model's ability to discern fraudulent transactions amidst most legitimate ones.

Feature engineering constitutes a strategic cornerstone in the development of robust and reliable machine learning models, particularly in domains characterized by imbalanced datasets such as credit card fraud detection. In this research endeavor, normalization, resampling techniques were diligently applied to harness the predictive power of the underlying data. Through normalization, the features were rendered uniform in scale, circumventing potential biases that may arise from disparate attribute magnitudes. Furthermore, resampling methodologies were instrumental in rectifying class imbalance, ensuring equitable representation of both fraudulent and non-fraudulent transactions within the dataset. By judiciously employing these feature engineering techniques, the developed models were primed to deliver robust and reliable predictions, thereby advancing the efficacy of credit card fault detection systems in safeguarding against fraudulent transactions.

2.1.1 Normalization

Normalization is a crucial preprocessing step in feature engineering aimed at standardizing the scale of features within a dataset, thereby enhancing the performance of machine learning models. By rescaling the range of values to a common scale, normalization ensures that each feature contributes proportionately to the model's learning process, preventing attributes with larger magnitudes from dominating those with smaller scales. The normalization technique employed in this study is Min-Max scaling, which transforms the features to a predefined range, typically between 0 and 1, according to the formula:

$$X\text{normalized} = (X\text{-}X\text{min}) / (X\text{max}\text{-}X\text{min}) \qquad (1)$$

where X represents the original feature value, Xmin is the minimum value of the feature in the dataset, and Xmax is the maximum value. This transformation ensures that all features are constrained within the specified range, facilitating smoother convergence during model training, and preventing numerical instabilities.

2.1.2 Resampling

Resampling, particularly up sampling, is a pivotal technique in addressing class imbalance within datasets, a common challenge in machine learning tasks such as credit card fault detection. This method involves augmenting the minority class by randomly duplicating instances until a balanced distribution is achieved between classes. By synthesizing additional instances of the minority class, up sampling mitigates the bias towards the majority class, thus enabling machine learning algorithms to learn from the available data more effectively.

2.1.3 Synthetic minority over-sampling technique

One popular technique for up sampling is Synthetic Minority Over-sampling Technique (SMOTE), which generates synthetic samples by interpolating between existing minority class instances. The formula for SMOTE is as follows:

$$X_{new} = X_i + \lambda(X_{zi} - X_i) \qquad (2)$$

where X_i represents an instance from the minority class, X_{zi} denotes one of its k-nearest neighbors within the feature space, and λ is a random value between 0 and 1 determining the proportion of the synthetic instance to be generated. This resampling strategy not only alleviates the class imbalance but also enhances the model's ability to discern patterns in the data, ultimately leading to improved predictive performance.

3. MODEL EVALUATION RESULTS

Detailed classification reports were generated for each model under all the three approaches as shown in Figure's 1 to 9. Classification metrics like precision, recall, and F1-score for both training and test datasets are depicted in Table's 1 to 18 for all the three approaches. Additionally, ROC curves were analyzed to compare and assess all the three model's performance in each approach which are shown in Figure's 10 to 12. The results indicate that the approach 3 combining resampling and feature normalization, along with the lightGBM model, achieved the highest recall of 0.9091 and an area under the ROC curve of 0.972.

4. CONCLUSIONS

In conclusion, this study delved into the realm of credit card fraud detection through a thorough exploration of distinct approaches and preprocessing techniques within the domain of machine learning. By rigorously evaluating the performance of each approach using essential classification metrics like precision, recall, and F1-score

Table-1: llightGBM classification metrics for train data in approach 1

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.87	0.62	0.72
Accuracy	1.00		

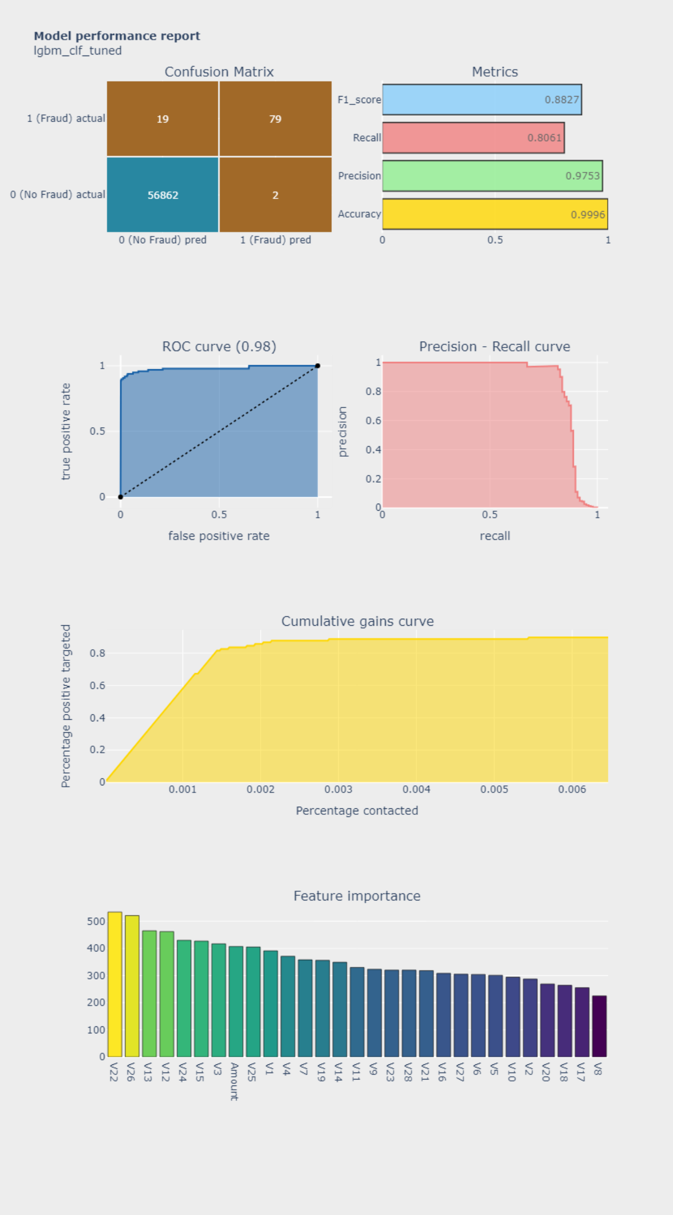

Fig -1: lightGBM classification report for approach 1

Table-2: llightGBM classification metrics for test data in approach 1

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.98	0.81	0.88
Accuracy	1.00		

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.87	0.62	0.72
Accuracy	1.00		

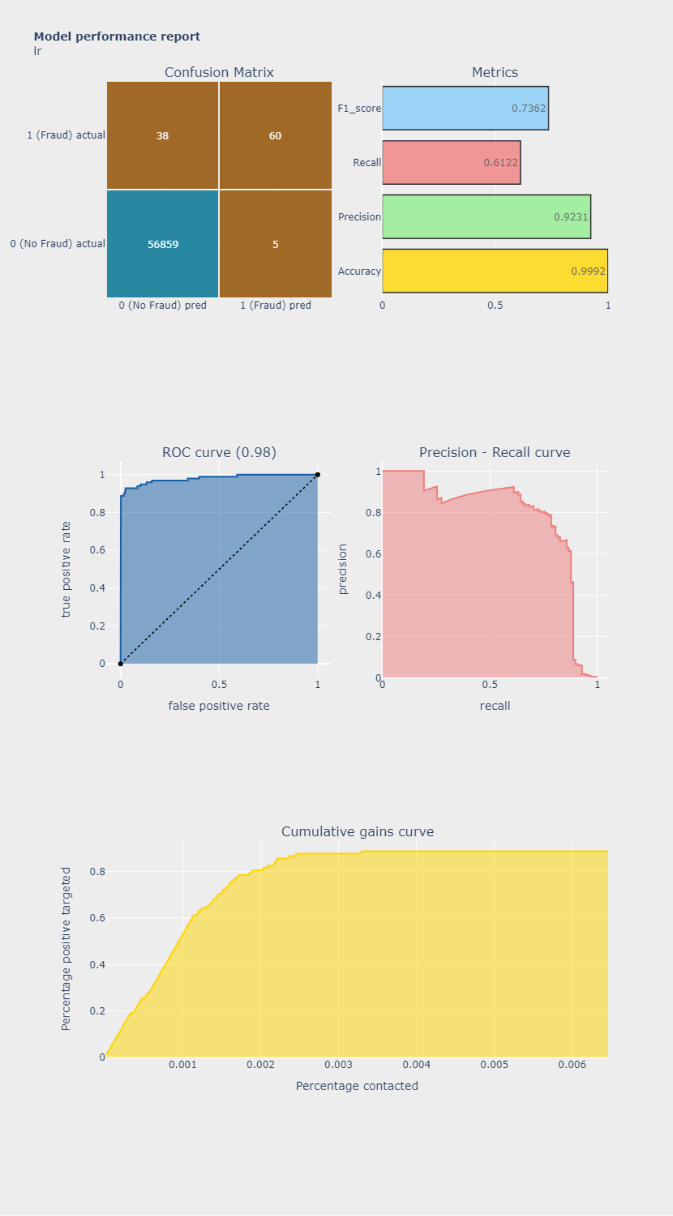

Fig -2: logistic regression classification report for approach 1

Table-3: logistic regression classification metrics for train data in approach 1

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.92	0.61	0.74
Accuracy	1.00		

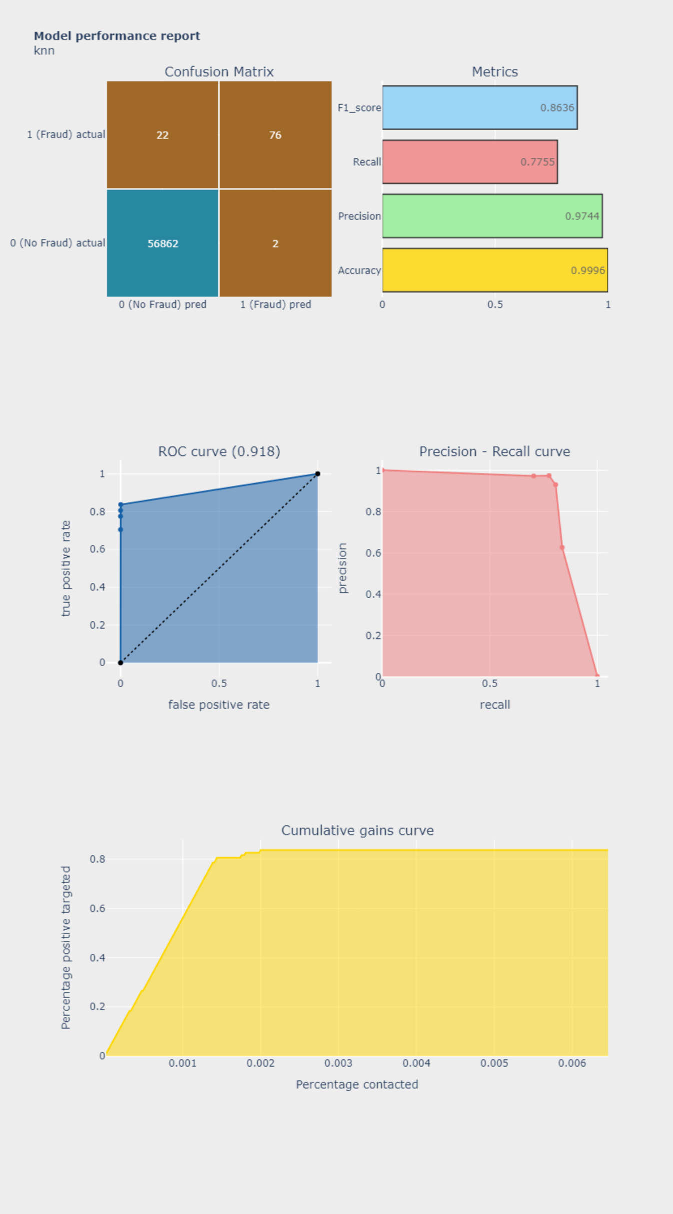

Fig -3: k nearest neighbor classification report for approach 1

Table-4: logistic regression classification metrics for test data in approach 1

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.98	0.79	0.87
Accuracy	1.00		

Table-5: k nearest neighbor classification metrics for train data in approach 1

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.97	0.78	0.86
Accuracy	1.00		

Table-6: k nearest neighbor classification metrics for test data in approach 1

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	1.00	1.00	1.00
Accuracy	1.00		

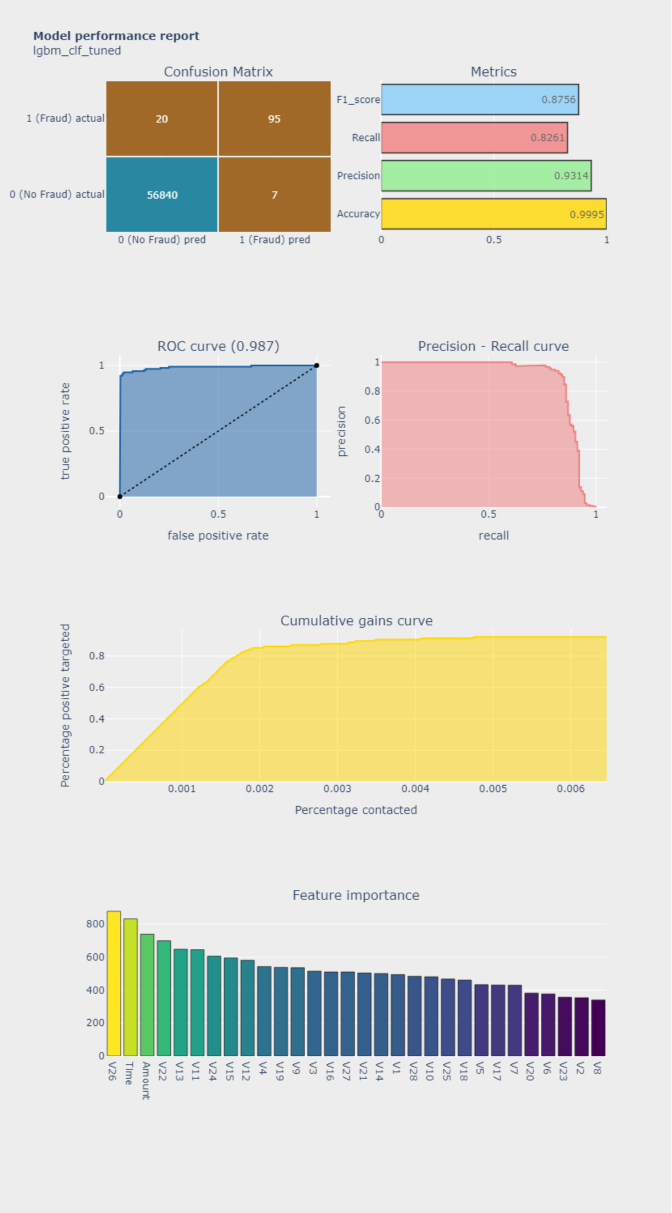

Fig -4: lightGBM classification report for approach 2

Table-7: llightGBM classification metrics for train data in approach 2

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.93	0.83	0.88
Accuracy	1.00		

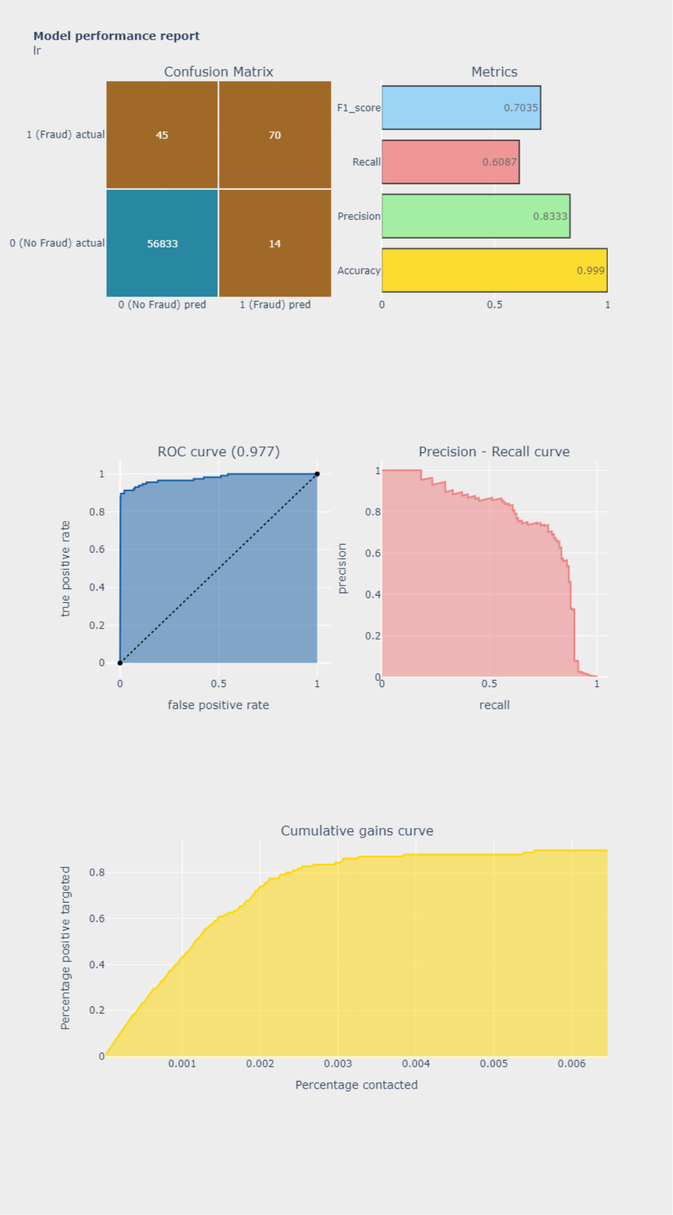

Fig -5: logistic regression classification report for approach 2

Table-8: llightGBM classification metrics for test data in approach 2

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.89	0.63	0.74
Accuracy	1.00		

Table-9: logistic regression classification metrics for train data in approach 2

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.83	0.61	0.70
Accuracy	1.00		

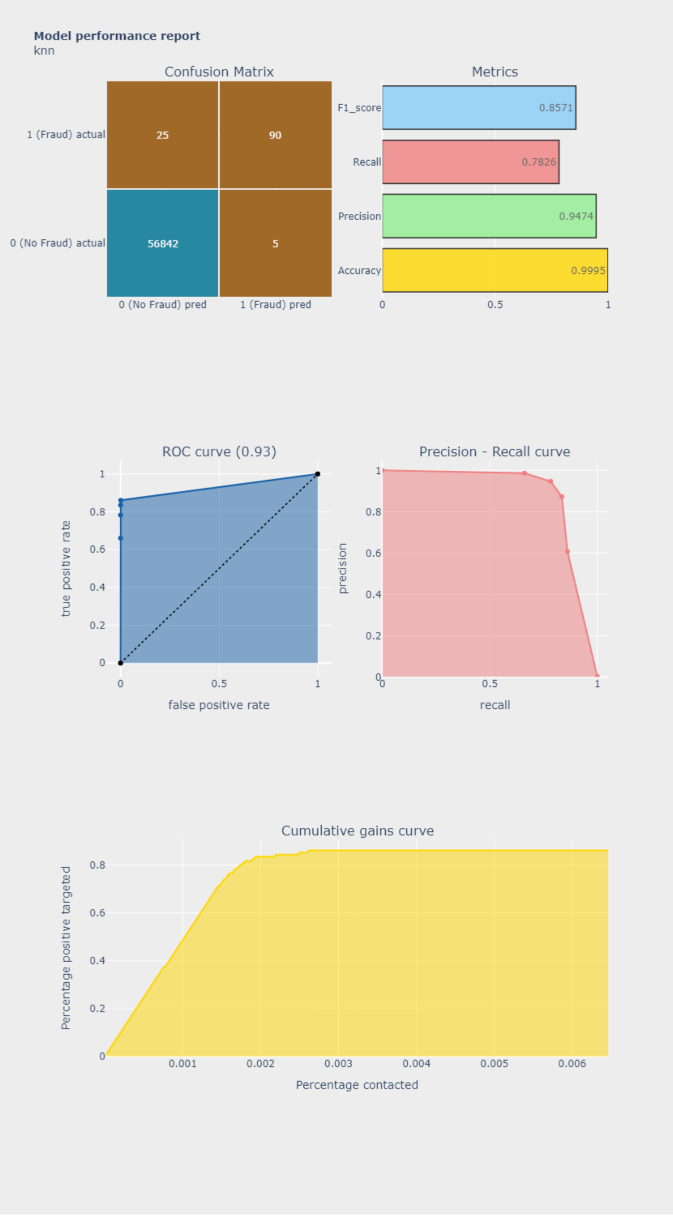

Fig -6: k nearest neighbor classification report for approach 2

Table-10: logistic regression classification metrics for test data in approach 2

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.97	0.79	0.87
Accuracy	1.00		

Table-11: k nearest neighbor classification metrics for train data in approach 2

	Precision	recall	F1-score
No Fraud	1.00	1.00	1.00
Fraud	0.95	0.78	0.86
Accuracy	1.00		

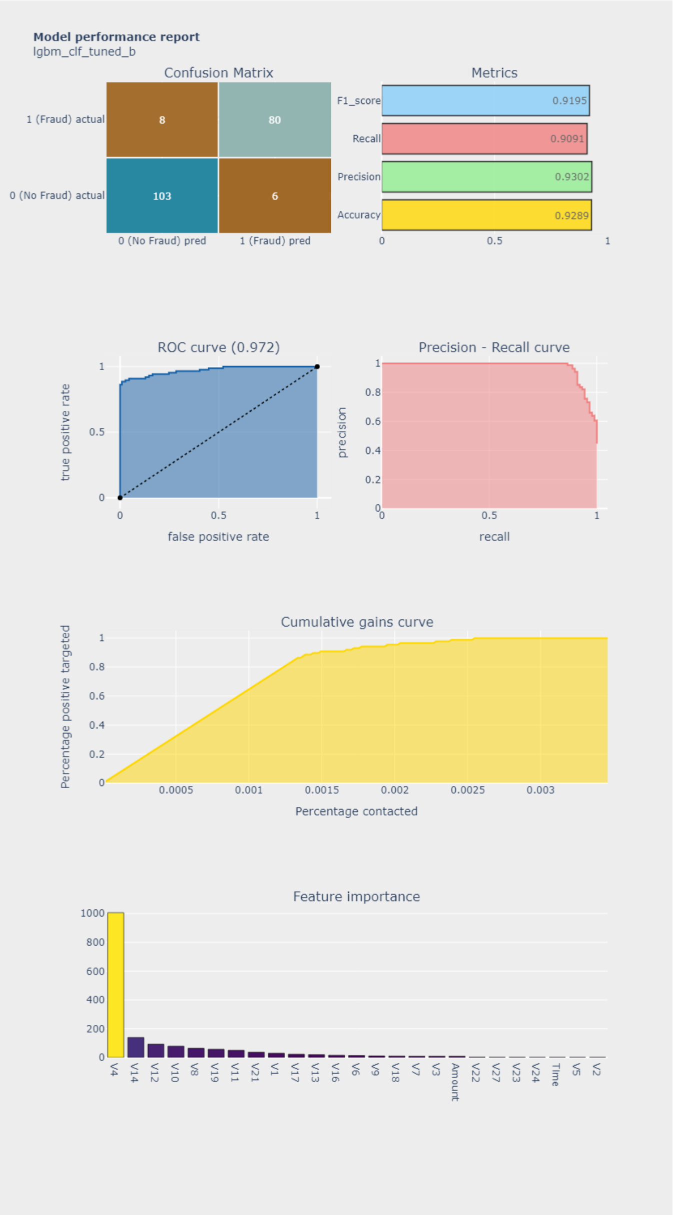

Fig -7: lightGBM classification report for approach 3

Table-12: k nearest neighbor classification metrics for test data in approach 2

	Precision	recall	F1-score
No Fraud	0.93	0.98	0.96
Fraud	0.98	0.93	0.96
Accuracy	0.96		

Table-13: llightGBM classification metrics for train data in approach 3

	Precision	recall	F1-score
No Fraud	0.93	0.94	0.94
Fraud	0.93	0.91	0.92
Accuracy	0.93		

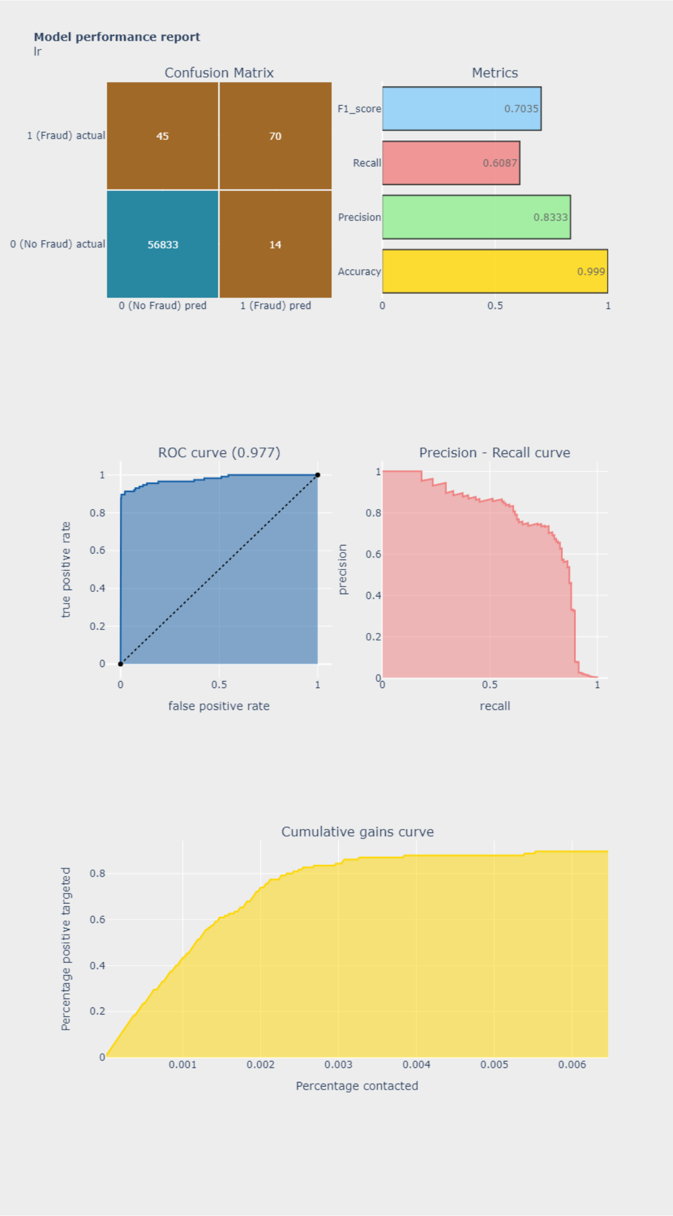

Fig -8: logistic regression classification report for approach 3

Table-14: llightGBM classification metrics for test data in approach 3

	Precision	Recall	F1-score
No Fraud	0.92	0.98	0.95
Fraud	0.98	0.92	0.95
Accuracy	0.95		

Table-15: logistic regression classification metrics for train data in approach 3

	Precision	recall	F1-score
No Fraud	0.94	0.97	0.95
Fraud	0.96	0.92	0.94
Accuracy	0.95		

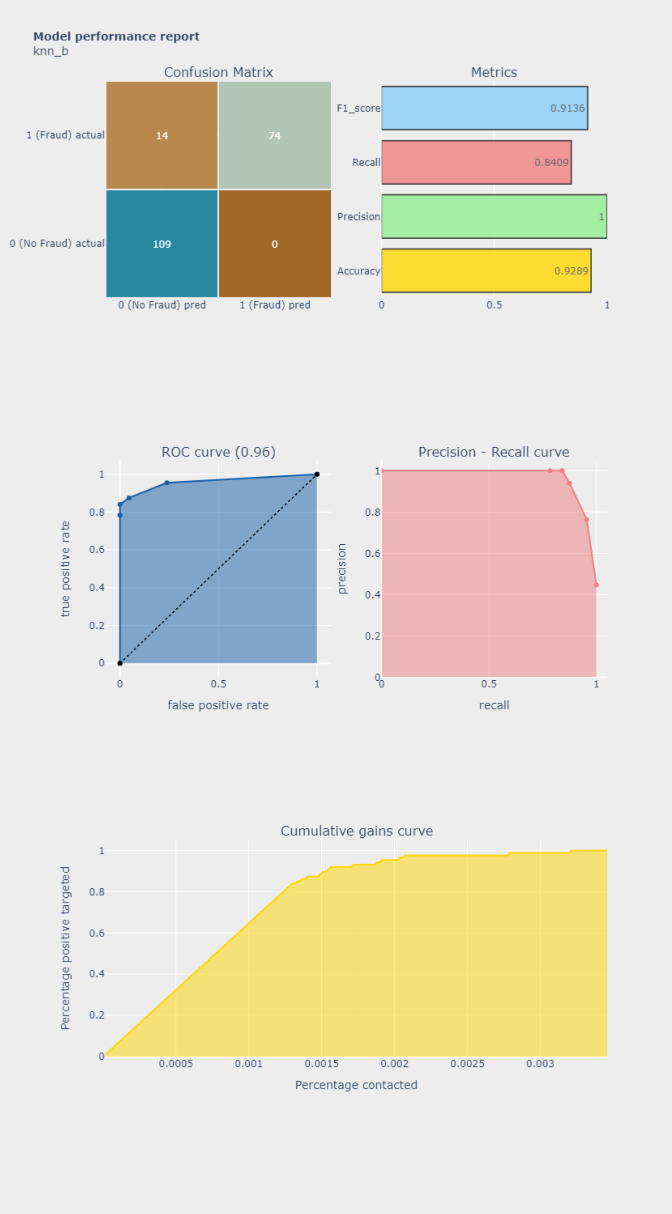

Fig -9: k nearest neighbor classification report for approach 3

Table-16: logistic regression classification metrics for test data in approach 3

	Precision	recall	F1-score
No Fraud	0.88	0.99	0.93
Fraud	0.99	0.87	0.93
Accuracy	0.93		

Table-17: k nearest neighbor classification metrics for train data in approach 3

	Precision	recall	F1-score
No Fraud	0.89	1.00	0.94
Fraud	1.00	0.84	0.91
Accuracy	0.93		

Table-18: k nearest neighbor classification metrics for test data in approach 3

	Precision	recall	F1-score
No Fraud	0.89	1.00	0.94
Fraud	1.00	0.84	0.91
Accuracy	0.93		

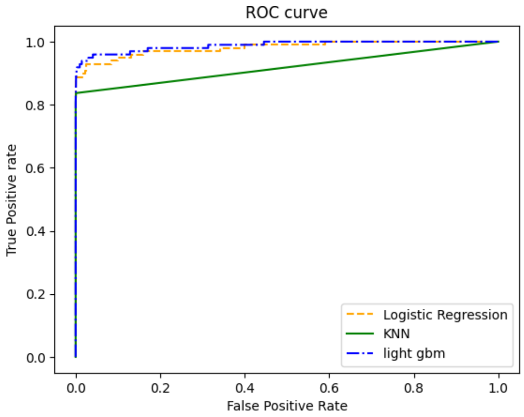

Fig-1: ROC curve for all three models in approach 1

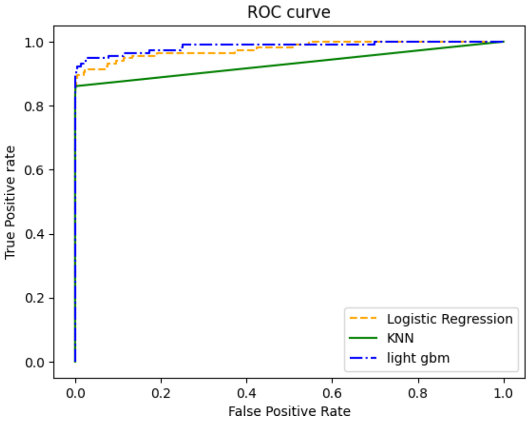

Fig-2: ROC curve for all three models in approach 2

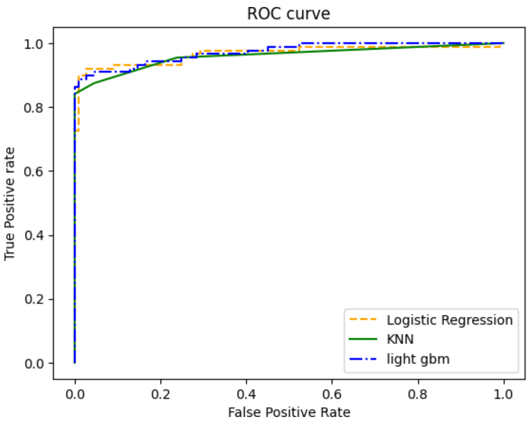

Fig-3: ROC curve for all three models in approach 3

valuable insights were garnered regarding the efficacy of various methodologies in mitigating fraud risks. The empirical findings underscored the significance of integrating resampling and feature normalization techniques, synergistically enhancing the predictive capabilities of the model. Particularly noteworthy was the exemplary performance exhibited by the lightGBM model in tandem with this approach, achieving a remarkable recall rate of 0.9091 and showcasing a robust area under the ROC curve of 0.972. These results not only affirm the effectiveness of the proposed methodology but also underscore the pivotal role of advanced machine learning techniques in bolstering fraud detection systems, thereby offering tangible solutions to combat financial malfeasance in the realm of credit card transactions.

ACKNOWLEDGEMENTS

I would like to express my gratitude to the various online resources, including websites like Kaggle and YouTube videos, that provided invaluable insights and knowledge during this research. Their content and guidance were instrumental in shaping my understanding and approach to the subject matter.

REFERENCES

[1] Gupta, A., Lohani, M. C., & Manchanda, M. (2021). Financial fraud detection using naive Bayes algorithm in highly imbalance data set. Journal of Discrete Mathematical Sciences and Cryptography, 24(5), 1559–1572.

[2] Itoo, F., Meenakshi, & Singh, S. (2020). Comparison and analysis of logistic regression, Naïve Bayes and Knn Machine Learning Algorithms for credit card fraud detection. International Journal of Information Technology, 13(4), 1503–1511.

[3] Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis. 2017 International Conference on Computing Networking and Informatics (ICCNI).

[4] Daly, L. (2021, October 27). Identity theft and credit card fraud statistics for 2021: The ascent. The Motley Fool.

[5] Malini, N., & Pushpa, M. (2017). Analysis on credit card fraud identification techniques based on KNN and outlier detection. 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics