Safeguarding Finances: State-of-the-Art Fraud Detection Methods for Credit Cards

Vishnu Kant[1], Kanwarpartap Singh Gill[1], Mukesh Kumar[2], Ruchira Rawat[3]

Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India[1]

Computer Science & Engineering, Graphic Era Hill University, Dehradun, Uttarakhand, India[2]

Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India[3]

Corresponding author: Kanwarpartap Singh Gill, Email: kanwarpartap.gill@chitkara.edu.in

This research primarily aims to shed light on the serious issue of credit card fraud, which has become much worse with the advent of internet shopping and, more specifically, the present COVID-19 epidemic. Developing a machine learning system capable of distinguishing between legitimate and fraudulent credit card transactions is the primary objective of this project, which aims to decrease an annual loss of $24 billion. Using data such as transformed numerical characteristics after PCA analyses, transaction time and amount, and Logistic Regression, Decision Tree Classifier, and K-Nearest Neighbours approaches are employed in the research study. The accuracy rates of these algorithms are demonstrated by the cross-validation score, ROC AUC score, and F1 score within the context of fraud detection. Improving the models' accuracy and resilience is as simple as using statistical tests like ANOVA when selecting features. To improve the detection of fraudulent behaviour and to accurately compare the results of various algorithms, balanced datasets are essential, as this shows. There was a 91% F1 score, 92.35% ROC AUC, and 98.01% cross-validation accuracy rate for fraud detection in the logistic regression model. Alternatively, a decision tree classifier's fraud detection cross-validation score was 96.67%, ROC AUC was 91.36%, and F1 was 90%. When it came to detecting fraud, K-Nearest Neighbours performed exceptionally well with scores of 97.63% for ROC AUC, 99.34% for cross-validation, and 97% for F1.

Keywords: Credit card fraud, PCA transformation, Transaction amount, Fraud detection, Classification, Unbalanced dataset.

2024. In Mukesh Saraswat & Rajani Kumari (eds.), *Applied Intelligence and Computing*, 105–114. Computing & Intelligent Systems, SCRS, India. DOI: https://doi.org/10.56155/978-81-955020-9-7-12

1 Introduction

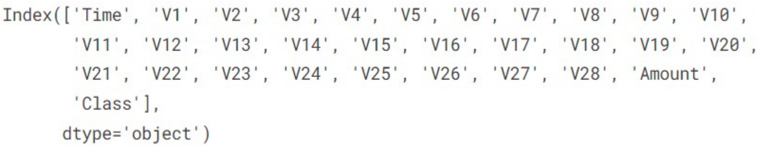
The COVID-19 pandemic has coincided with a rise in online shopping and transactions, making credit card theft an increasingly pressing concern for consumers' financial safety. More than $24 billion is lost annually due to unauthorised usage of credit cards, which hurts consumer trust and causes major economic problems. It is clear that a quicker resolution is required since several businesses have emerged inside the banking industry in response to this increasing threat. The credit card sector is worth $30 billion, which allows for the possibility of automatically developing models to reduce fraud using machine learning. This research aims to enhance current fraud detection efforts by classifying credit card transactions as either legitimate or fraudulent using machine learning approaches. The purpose of this research is to compare and contrast three popular machine learning algorithms: Logistic Regression, Decision Tree Classifier, and K-Nearest Neighbour. Multiple criteria, such as quantity, transaction time, and numerical attributes transformed by principal component analysis, are used to accomplish this evaluation. Examining three important metrics—the F1 Score, the ROC AUC Score, and the Cross Validation Score—for fraud detection, the study sought to illuminate how well these algorithms address the issues posed by credit card fraud. The study also looked at how to use statistical feature selection methods like ANOVA to increase model accuracy and robustness by expanding the feature space. More secure online financial transactions should be the result of this study on fraud detection systems, which is expected to be quite advanced. The COVID-19 pandemic has coincided with a rise in online shopping and transactions, making credit card theft an increasingly pressing concern for consumers' financial safety. More than $24 billion is lost annually due to unauthorised usage of credit cards, which hurts consumer trust and causes major economic problems. Numerous new entrants in the financial sector have emerged in reaction to this rising danger, clearly calling for an expedited settlement. The credit card sector is worth $30 billion, which allows for the possibility of automatically developing models to reduce fraud using machine learning. This project's overarching goal is to improve current efforts at fraud detection by developing a system to distinguish between legitimate and fraudulent credit card transactions using advanced machine learning techniques. Using data such as numerical characteristics processed by principal component analysis (PCA), transaction time, and quantity, this article attempts to evaluate the performance of three popular machine learning algorithms: K-Nearest Neighbour, Decision Tree Classifier, and Logistic Regression. Examining three important metrics—the F1 Score, the ROC AUC Score, and the Cross Validation Score—for fraud detection, the study sought to illuminate how well these algorithms address the issues posed by credit card fraud. The study also looked at how to use statistical feature selection methods like ANOVA to increase model accuracy and robustness by expanding the feature space. More secure online financial transactions should be the result of this study on fraud detection systems, which is expected to be quite advanced.

2 Literature

Research into methods to detect fraudulent credit card activity has grown in importance in recent years, both to both the enormous economic effect and the technical advances in the field. In their proposal for an intelligent system to identify fraudulent charges on payment cards, Seera et al. (2024) [1] highlight the need of employing sophisticated algorithms to combat such crimes. In one study, Chatterjee et al. (2024) [2] look at how digital twins may be used to identify fraud. They talk about the pros and cons of this measure's implementation. The importance of interpretable models in boosting confidence and compliance is highlighted by Hasan et al. (2024) [3], who conducted research on fraud detection and emphasised Explainable Artificial Intelligence (XAI). The effects of model variety and collaboration are the subject of investigation in the ensemble learning approaches conducted by Paldino et al. (2024) [4] and Khalid et al. (2024) [5]. In their discussion of unbalanced data, Kennedy et al. (2024) [6] propose techniques for producing class labels, whereas Huang et al. (2024) [7] offer a hybrid approach using undersampling and neural networks. The occurrence of catastrophic forgetting in continuous fraud detection systems is investigated in the work of Lebichot et al. (2024) [8]. Their findings underscore the need of keeping models stable and the ramifications of this need. In their causal temporal graph neural network (CaT-GNN), Duan et al. (2024) [10] offer a more sophisticated method for identifying fraudulent activities. Cherif et al. (2023) [11] and Alarfaj et al. (2022) [12] are only a couple of the previous research that thoroughly compare and evaluate several machine learning approaches. Researchers Bin Sulaiman et al. (2022) [13], Chen and Lai (2021) [14], and Asha and KR (2021) [15] have also made important contributions to the area of fraud detection approaches via their work on classical and deep learning methods. All things considered, the results show how many different parts there are to detecting credit card fraud and how hard people are trying to make better detection systems.

3 Input Dataset

This study's dataset contains a number of important factors for identifying credit card fraud. V1–V28, numerical characteristics derived from Principal Component Analysis (PCA) processing, make up the features. This transformation is designed to reduce dimensionality while keeping crucial information intact. A 'interval' feature that displays the amount of time (in seconds) that elapses between transactions is also included of the dataset. Using this characteristic, we may examine trends in the volume of transactions over time. The amount of a transaction, as shown by the characteristic "Amount," is critical for spotting questionable trends or behaviours. In this context, the 'Class' property serves as the dependent variable, with a value of 1 indicating a fraudulent transaction and a value of 0 indicating a legitimate one. The primary objective of this research is to create reliable machine learning models that can differentiate between legitimate and fraudulent credit card transactions as shown in Figure 1. Improving fraud detection methods and financial security are the goals of our study, which is why we are exploring such features as shown in Figure 2.



```
Index(['Time', 'V1', 'V2', 'V3', 'V4', 'V5', 'V6', 'V7', 'V8', 'V9', 'V10',
       'V11', 'V12', 'V13', 'V14', 'V15', 'V16', 'V17', 'V18', 'V19', 'V20',
       'V21', 'V22', 'V23', 'V24', 'V25', 'V26', 'V27', 'V28', 'Amount',
       'Class'],
      dtype='object')
```

Figure 1. Input Dataset Utilized in Study

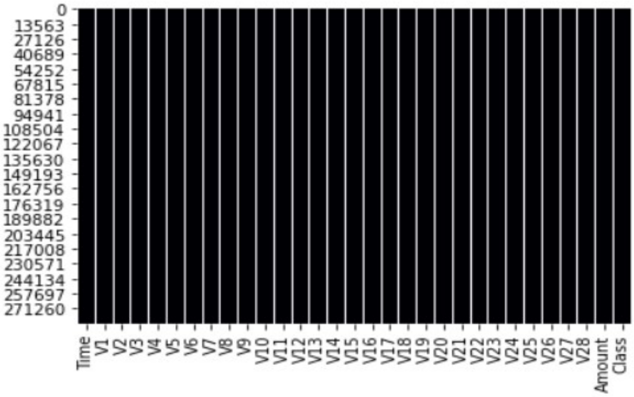


Figure 2. Heatmap of Input Dataset

4 Proposed Methodology

Like laying out a new metropolis, the suggested method for avoiding credit card theft starts with an exhaustive examination of our data to learn its ins and outs. Following this, we employ data visualisation to draw attention to key aspects of the transactions, much like a map would to prominent routes and landmarks, facilitating the discovery of hidden patterns. The next step in making a lean and effective model is to highlight efficiency by picking the most important fraud detection criteria. The Synthetic Minority Over-sampling Technique is one method that can fix imbalanced data. It levels out our dataset by adding weights to a scale that measure equivalently. Next, we train a number of ML models—including Logistic Regression, Decision Tree Classifier, and K-Nearest Neighbors—with the intention of testing their efficacy in detecting fraud using measures like F1, ROC AUC Score, and Cross-Validation Score. This method is analogous to judging dishes in a cooking competition using a variety of criteria. We are committed to continuously improving our fraud detection system through our rigorous evaluation and refining process. Our goal is to provide the highest level of digital financial security, as seen in Figure 3.

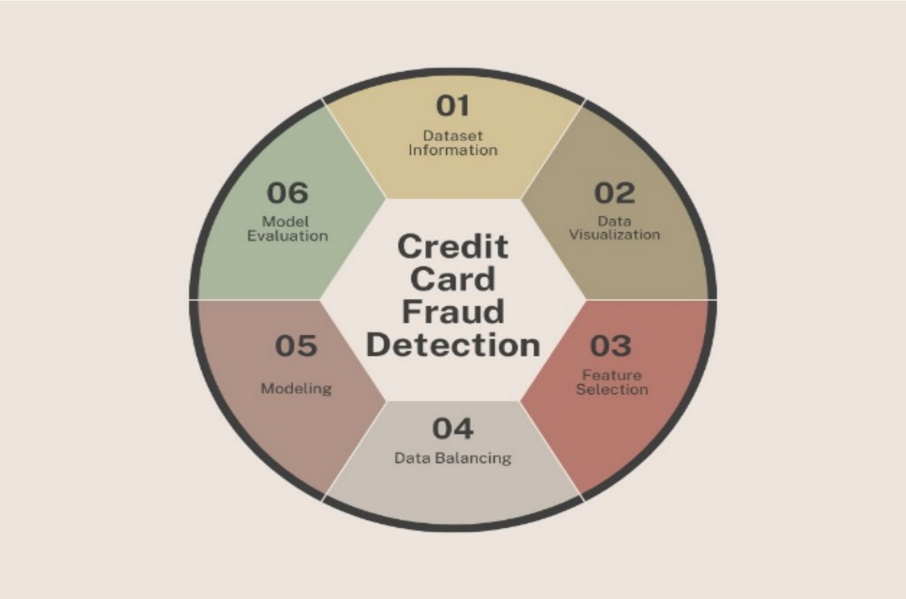


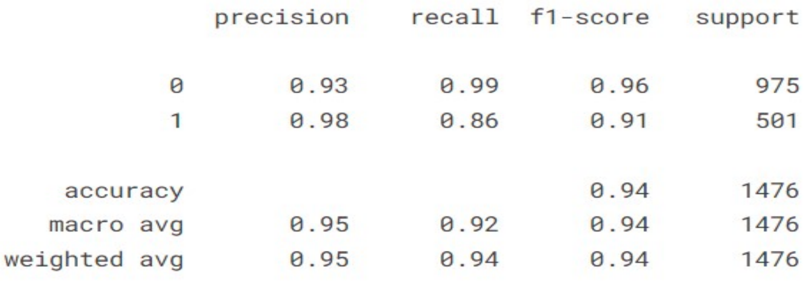
Figure 3. Proposed methodology for the proposed Approach

Data preparation is a crucial part of machine learning, particularly in cases when there are significant class imbalances in the dataset. In order for the model to accurately forecast both groups without bias, it is crucial to ensure that it does not favour the majority class. Undersampling and oversampling are two main approaches that are frequently employed to tackle this problem. In undersampling, the emphasis is on the dominant class, but in oversampling, the minority class is given more attention. Find a happy medium between the two methods, and you'll have a dataset that's more accurate for training models. Using the imbalanced-learn package simplifies implementing these techniques. For instance, the Synthetic Minority Over-sampling Technique, or SMOTE, is a popular method in the field for increasing the representation of underrepresented groups by the generation of synthetic samples. Therefore, the fallacy of conclusions might result from depending just on traditional measurements for correctness. Rather, the metrics for evaluating performance utilising ROC-AUC scores, graphs, and confusion matrices should take centre stage. These measures show how well the model handles class imbalance and discriminates between classes. To make sure that models learn from a broad and representative dataset, data scientists practise data balancing during training. It guarantees that predictions made in real-world settings will be accurate and reliable.

5 Results

5.1 Logistic Regression

Class 0 recall was 0.99 and class 1 recall was 0.86, both of which were strong results from the model. With accuracy rates of 0.98 for class 1 and 0.93 for class 0, it was similarly good in that regard. So, it seems the model did a decent job of picking out instances from both groups. The most effective model, derived from ANOVA scores, achieved 96% accuracy, 98.45% cross-validation, and an impressive 94.69% ROC AUC. Alternatively, the model that took ANOVA scores into account fared better than the others; it achieved an impressive ROC AUC score of 94.69%, a cross-validation score of 98.45%, and an accuracy of 96%. As evidence of its effectiveness for the job at hand and its capacity to decrease false positives and false negatives, the model displayed the greatest accuracy of 0.95 for class 0 and 0.97 for class 1, as well as a good recall of 0.99 for class 0 and 0.91 for class 1. The significance of selecting features correctly for increased classification accuracy was highlighted once again by the fact that the ANOVA score-based model outperformed the correlation-based model (Figure 4 & 5).



```
              precision    recall  f1-score   support

           0       0.93      0.99      0.96       975
           1       0.98      0.86      0.91       501

    accuracy                           0.94      1476
   macro avg       0.95      0.92      0.94      1476
weighted avg       0.95      0.94      0.94      1476
```

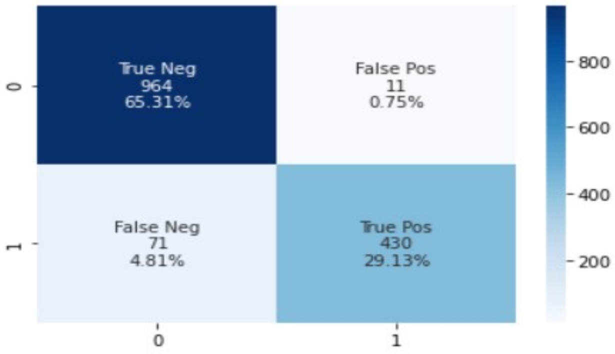
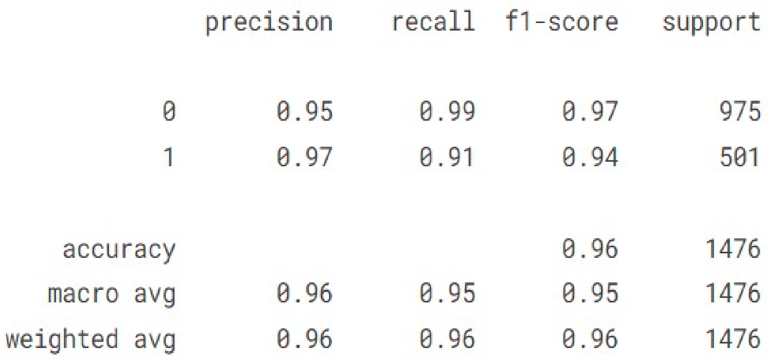


Figure 4. Model based on Correlation Plot



```
              precision    recall  f1-score   support

           0       0.95      0.99      0.97       975
           1       0.97      0.91      0.94       501

    accuracy                           0.96      1476
   macro avg       0.96      0.95      0.95      1476
weighted avg       0.96      0.96      0.96      1476
```

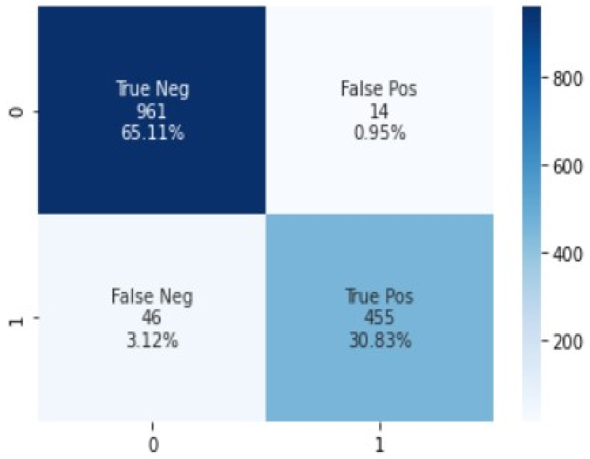


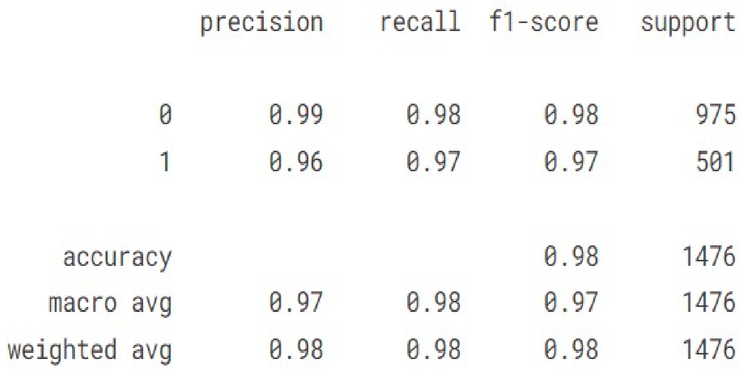
Figure 5. Model based on ANOVA score

5.2 Decision Tree Classifier

Utilising the Decision Tree Classifier module from scikit-learn, we trained the decision tree classifier with settings limiting the depth to 4 and requiring a minimum of 1 sample at each leaf. The feature selection approaches used to train the two models are analysis of correlation plots and analysis of variance (ANOVA). We used measures like ROC AUC and cross-validation score to assess how well each model performed. With a ROC AUC of 91.36% and a cross-validation score of 96.67%, the correlation plot-based model achieved impressive results. Furthermore, it calculated the F1-score, recall, and precision for both the 0 and 1 classes, demonstrating excellent accuracy and balanced performance. In contrast, the ANOVA-based model generated ROC AUC results of 93.69% and a cross-validation score of 97.13%. It states that performance is solid after computing recall, accuracy, and F1-score again.

5.3 K-Nearest Neighbour

Created a K-Nearest Neighbours (KNN) classifier using scikit-learn's KNeighborsClassifier module; used a leaf size of 1 and three nearest neighbours based on Manhattan distance with p=1. One model was trained using analysis of variance scores, and the other using correlation plot analysis, two distinct feature selection methods. Metrics like the ROC AUC and cross-validation scores were used to assess the performance of each model. A very high cross-validation score of 99.34% and a ROC AUC score of 97.63% were seen in the model that was developed from the correlation plot. This classifier had strong performance in differentiating between the 0 and 1 classes, as it evaluated accuracy, recall, and F1-score for both as shown in Figure 6.



```
              precision    recall  f1-score   support

           0       0.99      0.98      0.98       975
           1       0.96      0.97      0.97       501

    accuracy                           0.98      1476
   macro avg       0.97      0.98      0.97      1476
weighted avg       0.98      0.98      0.98      1476
```

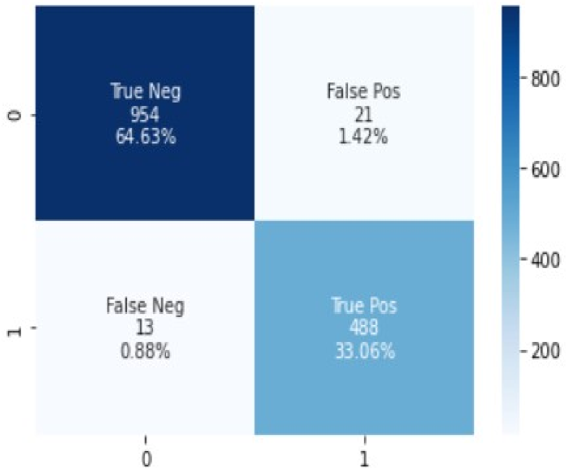
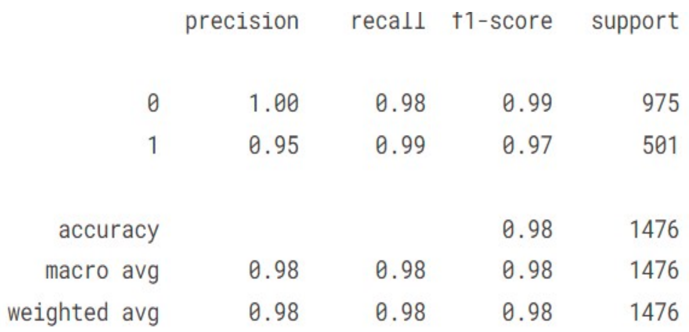


Figure 6. Model based on Correlation Plot



```
              precision    recall  f1-score   support

           0       1.00      0.98      0.99       975
           1       0.95      0.99      0.97       501

    accuracy                           0.98      1476
   macro avg       0.98      0.98      0.98      1476
weighted avg       0.98      0.98      0.98      1476
```

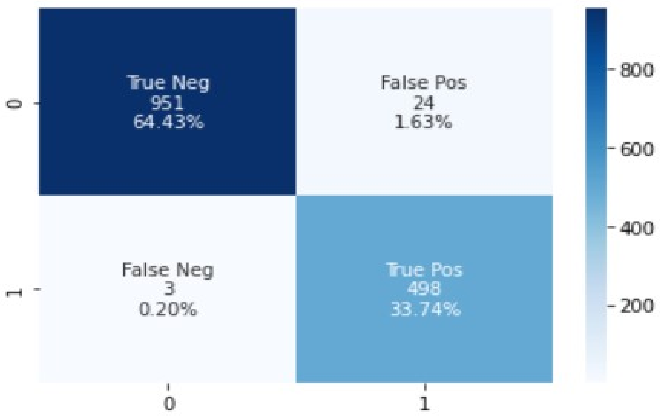


Figure 7. Model based on ANOVA score

5.4 Model Comparison

Table 1 and Table 2 shows the metrics for the performance of several machine learning algorithms used for fraud detection in the ML Algorithm Result table. For the purpose of fraud detection solely, it displays F1 Score Fraud, ROC AUC values, and cross-validation scores. In the first table, logistic regression achieved 98.01% for cross-validation, 92.35% for ROC AUC, and 91% for F1. Decision Tree is likewise quite close; it has an F1 score of 90%, a ROC AUC of 91.36%, and a cross-validation score of 96.67%. With a 99.34% cross-validation score, a 97.63% ROC AUC score, and a 97% F1 score for fraud, K Nearest Neighbours is the best. The findings that were obtained by selecting ANOVA scores are shown in the second table. Logistic regression continues to perform admirably in this case, with a 98.45% cross-validation score, a 94.69% ROC AUC, and a 94% F1 score for fraud detection. Equally impressive are Decision Tree's 97.13% cross-validation, 93.69% ROC AUC, and 93% F1 scores, all of which demonstrate great performance. Maintaining a high cross-validation score of 99.54%, ROC AUC score of 98.47%, and F1 score for fraud detection of 97%, K Nearest Neighbours continues to deliver strong results. When taken as a whole, these two tables give a thorough assessment of the different algorithms' ability to detect fraudulent actions, allowing for well-informed choices about fraud detection tactics as shown in Figure 7.

Table 1. ML Algorithm Result table

Sr. No	ML Algorithm	Cross Validation Score	ROC AUC Score	F1 Score(Fraud)
1.	Logistic Regression	98.01%	92.35%	91%
2.	Decision Tree	96.67%	91.36%	90%
3.	K Nearest Neighbour	99.34%	97.63%	97%

Table 2. Result Table for Models Based on Anova Score

Sr.No	ML Algorithm	Cross Validation Score	ROC AUC Score	F1 Score(Fraud)
1.	Logistic Regression	98.45%	94.69%	94%
2.	Decision Tree	97.13%	93.69%	93%
3.	K Nearest Neighbour	99.54%	98.47%	97%

6 Conclusion

In conclusion, the results of evaluating several machine learning algorithms for fraud detection are encouraging, demonstrating that the models can adequately detect fraudulent activity. The cross-validation scores, ROC AUC scores, and F1 ratings for fraud detection demonstrated that each of the offered algorithms—Decision Tree, Logistic Regression, and K Nearest Neighbours—provided robust performance and high accuracy outcomes. Based on these findings, machine learning algorithms have the potential to revolutionise fraud detection systems, equipping organisations and enterprises with cutting-edge methods to identify and prevent fraud. Applying more sophisticated methods, such as ANOVA score selection, further enhances their effectiveness, highlighting the significance of algorithm selection and feature engineering in creating efficient fraud detection solutions. In order to tackle the constantly changing problems of fraud, safeguard financial systems, and ensure the integrity of transactions, the study emphasises the significance of using machine learning techniques.

References

[1] Seera, M., Lim, C.P., Kumar, A., Dhamotharan, L. and Tan, K.H., 2024. An intelligent payment card fraud detection system. Annals of operations research, 334(1), pp.445-467.

[2] Chatterjee, P., Das, D. and Rawat, D.B., 2024. Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements. Future Generation Computer Systems.

[3] Hasan, M.R., Gazi, M.S. and Gurung, N., 2024. Explainable AI in Credit Card Fraud Detection: Interpretable Models and Transparent Decision-making for Enhanced Trust and Compliance in the USA. Journal of Computer Science and Technology Studies, 6(2), pp.01-12.

[4] Paldino, G.M., Lebichot, B., Le Borgne, Y.A., Siblini, W., Oblé, F., Boracchi, G. and Bontempi, G., 2024. The role of diversity and ensemble learning in credit card fraud detection. Advances in Data Analysis and Classification, 18(1), pp.193-217.

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

[6] Kennedy, R.K., Villanustre, F., Khoshgoftaar, T.M. and Salekshahrezaee, Z., 2024. Synthesizing class labels for highly imbalanced credit card fraud detection data. Journal of Big Data, 11(1), p.38.

[7] Sulaiman, S.S., Nadher, I. and Hameed, S.M., 2024. Credit Card Fraud Detection Challenges and Solutions: A Review. Iraqi Journal of Science, 65(4), pp.2287-2303.

[8] Lebichot, B., Siblini, W., Paldino, G.M., Le Borgne, Y.A., Oblé, F. and Bontempi, G., 2024. Assessment of catastrophic forgetting in continual credit card fraud detection. Expert Systems with Applications, p.123445.

[9] Huang, H., Liu, B., Xue, X., Cao, J. and Chen, X., 2024. Imbalanced Credit Card Fraud Detection Data: A Solution Based on Hybrid Neural Network and Clustering-based Undersampling Technique. Applied Soft Computing, p.111368.

[10] Duan, Y., Zhang, G., Wang, S., Peng, X., Ziqi, W., Mao, J., Wu, H., Jiang, X. and Wang, K., 2024. CaT-GNN: Enhancing Credit Card Fraud Detection via Causal Temporal Graph Neural Networks. arXiv preprint arXiv:2402.14708.

[11] Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M. and Imine, A., 2023. Credit card fraud detection in the era of disruptive technologies: A systematic review. Journal of King Saud University-Computer and Information Sciences, 35(1), pp.145-174.

[12] Alarfaj, F.K., Malik, I., Khan, H.U., Almusallam, N., Ramzan, M. and Ahmed, M., 2022. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access, 10, pp.39700-39715.

[13] Bin Sulaiman, R., Schetinin, V. and Sant, P., 2022. Review of machine learning approach on credit card fraud detection. Human-Centric Intelligent Systems, 2(1), pp.55-68.

[14] Chen, J.I.Z. and Lai, K.L., 2021. Deep convolution neural network model for credit-card fraud detection and alert. Journal of Artificial Intelligence, 3(02), pp.101-112.

[15] Gill, K.S., Anand, V., Gupta, R. and Pahwa, V., 2023, July. Insect Classification using Deep Convolutional Neural Networks and Transfer Learning On MobileNetV3 Model. In 2023 World Conference on Communication & Computing (WCONF) (pp. 1-5). IEEE.

[16] Trivedi, N.K., Simaiya, S., Lilhore, U.K. and Sharma, S.K., 2020. An efficient credit card fraud detection model based on machine learning methods. International Journal of Advanced Science and Technology, 29(5), pp.3414-3424.

[17] Asha, R.B. and KR, S.K., 2021. Credit card fraud detection using artificial neural network. Global Transitions Proceedings, 2(1), pp.35-41.

[18] Gill, K.S., Sharma, A., Anand, V. and Gupta, R., 2023, March. Flower Classification Utilisizing Tensor Processing Unit Mechanism. In 2023 2nd International Conference for Innovation in Technology (INOCON) (pp. 1-5). IEEE.

[19] Sailusha, R., Gnaneswar, V., Ramesh, R. and Rao, G.R., 2020, May. Credit card fraud detection using machine learning. In 2020 4th international conference on intelligent computing and control systems (ICICCS) (pp. 1264-1270). IEEE.

[20] Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J. and Singh, A.K., 2021. Credit card fraud detection using machine learning: a study. arXiv preprint arXiv:2108.10005.