Caliphate Journal of Science & Technology (CaJoST)

ISSN: 2705-313X (PRINT); 2705-3121 (ONLINE) Research Article

Open Access Journal available at: https://cajost.com.ng/index.php/files and https://www.ajol.info/index.php/cajost/index



DOI: https://dx.doi.org/10.4314/cajost.v8i1.4

**Article Info**

Received: 7th October 2025

Revised: 12th November 2025

Accepted: 22nd November 2025

# Machine Learning Approaches for Credit Card Fraud Detection: A Comparative Study of Logistic Regression and K-Nearest Neighbors KNN

Abdulrashid Sani*, Zahriya L. Hassan, Anas T. Balarabe, Jamilu M. Muhammad and Bashar A. Yauri

Department of Computer Science, Faculty of Computing, Sokoto State University, Sokoto State, Nigeria.

***Corresponding author's email:**

abdulrashid.sani@ssu.edu.ng

**Cite this:** *CaJoST*, 2026, 1, 24-34

The rapid expansion of online banking and digital transactions has revolutionized financial services, enhancing convenience and accessibility. However, this transformation has also led to an increase in fraudulent activities, posing significant risks to both consumers and financial institutions. Credit card fraud, in particular, has emerged as a prevalent threat, with fraudsters employing sophisticated techniques to exploit vulnerabilities in digital payment systems. Traditional fraud detection methods often fall short in identifying complex fraudulent patterns in real-time, necessitating the development of more robust and intelligent detection mechanisms. This study investigates the application of machine learning (ML) techniques, specifically Logistic Regression and K-Nearest Neighbors (KNN), to detect fraudulent credit card transactions. Using a dataset sourced from Kaggle, consisting of 568,630 transactions, the research evaluates the performance of these algorithms in accurately classifying transactions as fraudulent or legitimate. The results indicate that the KNN algorithm achieved higher accuracy on the evaluated dataset (0.999) compared to Logistic Regression (0.791). Similarly, KNN demonstrated superior classification performance across all evaluation metrics, including precision, recall, and F1-score. This study highlights the potential of machine learning in enhancing credit card fraud detection. The findings contribute to the ongoing efforts in financial cybersecurity, providing insights into the development of more effective and adaptive fraud prevention systems.

**Keywords:** Fraud Detection, Machine Learning (ML), Logistic Regression, K-Nearest Neighbors (KNN), Digital Transactions.

## 1. Introduction

The rapid expansion of online banking and digital payment systems has transformed the financial landscape, making transactions such as money transfers, bill payments, and e-commerce more convenient and accessible [1], [2]. While these advancements have enhanced efficiency in financial services, they have also given rise to significant security challenges, particularly in the form of financial fraud [3], [4], [5]. Fraud occurs when malicious actors exploit vulnerabilities within banking systems to gain unauthorized access to financial assets, often by impersonating legitimate customers [6]. As digital financial services continue to grow, so too has the prevalence and sophistication of fraudulent activities, posing substantial risks to individuals and financial institutions alike [7].

The scale of financial fraud has become increasingly alarming in recent years. For instance, between January and September 2020, financial institutions in Nigeria reported losses amounting to ₦5.2 billion due to fraudulent activities. The third quarter of 2020 alone accounted for ₦3.36 billion in losses, marking a staggering 510% increase compared to the ₦550 million lost in 2019. These figures underscore the growing severity of fraud and the urgent need for effective fraud detection mechanisms [8].

One of the most prevalent forms of financial fraud in digital transactions is credit card fraud, where unauthorized individuals exploit stolen credit card details to conduct illicit transactions [9]. As online and mobile-based payment methods become increasingly dominant, fraudsters continue to develop more sophisticated techniques, such as phishing, data breaches, and card cloning, to compromise financial security [10]. The ease of making remote purchases exacerbates this issue, as once a fraudster gains access to credit card information, the potential for financial losses is significant. This rising threat has led to an increased demand for advanced fraud detection systems that

  

can proactively identify and mitigate fraudulent activities [11].

In response to this challenge, machine learning (ML) techniques have emerged as powerful tools for detecting fraudulent transactions [12], [13]. Unlike traditional fraud detection methods, which often rely on predefined rules and manual analysis, ML algorithms can process large volumes of transaction data to uncover hidden patterns indicative of fraudulent behavior. These models excel at identifying subtle anomalies such as transactions occurring at unusual times, locations, or involving atypical amounts that may go unnoticed using conventional approaches [14], [15].

This study explores the application of machine learning algorithms, specifically Logistic Regression and K-Nearest Neighbors (KNN), in credit card fraud detection. By employing Python-based data analysis tools, including Pandas, NumPy, and Matplotlib, we evaluate the effectiveness of these models in distinguishing between legitimate and fraudulent transactions. The findings of this research aim to contribute to the development of more efficient, accurate, and scalable fraud detection systems, ultimately enhancing financial security in the digital banking ecosystem.

### 1.1 Logistic Regression Algorithm

Logistic Regression is a statistical method used for binary classification problems, where the output is a binary outcome (fraudulent or non-fraudulent in this context). It predicts the probability of a class based on the input features using the logistic function [16].

Mathematical Notation & Formula: In logistic regression, the predicted probability $P(y=1|X)$ (where y is the target variable, indicating fraud or not, and X represents the input features) is modeled using the logistic function:

$$P(y=1|X) = \frac{1}{1+e^{-(\beta 0+\beta 1X1+\beta 2X2+\cdots+\beta nXn)}} \quad (1)$$

β0 is the intercept term,

β1,β2,…,βn are the coefficients for the features X1,X2,…,Xn,

e is the base of the natural logarithm.

The decision rule for logistic regression is that if $P(y=1|X)$ is greater than a chosen threshold (commonly 0.5), the prediction is classified as fraudulent (class 1), otherwise, it is non-fraudulent (class 0).

Training the Model: The model parameters β0, β1,…,βn are estimated using maximum likelihood estimation (MLE), which maximizes the likelihood of observing the given data.

### 1.2 K-Nearest Neighbors (KNN) Algorithm

K-Nearest Neighbors (KNN) is a non-parametric, instance-based learning algorithm used for classification tasks. It works by comparing a test data point to its nearest neighbors (in terms of distance metrics) from the training data and assigns a class based on the majority vote among the neighbors [17].

Mathematical Notation & Formula: Let {(Xi,yi)} be the set of training data points, where Xi represents the input features and yi is the corresponding class label (fraud or non-fraud). For a new data point Xnew the KNN algorithm performs the following steps:

Distance Metric: Calculate the distance between the new point Xnew and each training data point Xi. Common distance metrics include Euclidean distance:

$$d(Xnew, Xi) = \sqrt{\sum_{j-1}^{n}(Xnew, j, -Xi, j)^2} \quad (2)$$

Where Xnew,j and Xi,j are the j-th features of the new point and training data point, respectively.

Neighbor Selection: Identify the K nearest training points based on the calculated distance.

Voting: The class label ypred for the new point is assigned by majority voting among the K nearest neighbors:

$$ypred = \arg max \sum_{i=1}^{K} |yi - c| \quad (3)$$

Where |yi=c| is an indicator function that equals 1 if the class label yi is c and 0 otherwise. The class with the highest number of votes is assigned to Xnew.

Choosing K: The choice of K (the number of nearest neighbors) is critical to the model's performance. If K is too small, the model may be sensitive to noise, while if K is too large, the model may become overly smooth and fail to capture local patterns.

## 2. Problem Definition

The widespread use of credit cards for online transactions has led to an alarming rise in credit card fraud, driven by advances in e-commerce systems and communication technologies. Fraudsters continuously exploit these technological advancements to perpetrate unauthorized transactions, resulting in significant financial losses for both consumers and businesses.

The detection of fraudulent credit card activity remains a critical challenge, as traditional detection methods, such as rule-based systems, statistical thresholds, and manual reviews, often fail to identify fraud in real-time, and fraud tactics continue to evolve rapidly. The financial impact of such fraud is severe, with losses mounting annually as more consumers and businesses rely on digital payment systems.

  

To address this escalating problem, there is a compelling need for more accurate and efficient fraud detection systems. This study proposes to exploit machine learning algorithms, specifically Logistic Regression and K-Nearest Neighbors (KNN), to develop a robust fraud detection model capable of identifying suspicious credit card transactions. By enhancing the precision and timeliness of fraud detection, this research aims to minimize financial losses, protect sensitive data, and restore trust in digital payment systems.

## 3. Literature Review

### 3.1 History and Overview of Credit Card Fraud Detection

Credit card fraud detection has evolved significantly over the years, transitioning from traditional rule-based systems to advanced machine learning techniques [18], [19], [20]. Initially, fraud detection relied heavily on rule-based systems that used pre-defined thresholds to identify suspicious transactions [21]. These systems flagged activities based on attributes such as transaction location, frequency, and amount. However, their static nature made them ineffective against evolving fraud tactics, which often exploited loopholes in rigid rules [22].

As fraud strategies became more sophisticated, the limitations of rule-based systems became increasingly evident [23]. Traditional models struggled to detect complex fraud patterns, particularly in cases involving identity theft, account takeover, or card-not-present transactions [24]. To address these challenges, financial institutions adopted statistical models such as decision trees, linear regression, and neural networks [25]. While these models offered improvements, they still faced challenges related to scalability, interpretability, and the detection of previously unseen fraudulent behaviors [26].

### 3.2 Machine Learning in Credit Card Fraud Detection

The advent of machine learning (ML) marked a revolutionary shift in credit card fraud detection, providing more adaptive, flexible, and accurate solutions [27]. Among the ML models that have shown significant promise are Logistic Regression and K-Nearest Neighbors (KNN) [28]. Logistic Regression, a widely used statistical technique for binary classification, is favored for its simplicity, interpretability, and efficiency in handling large datasets. It calculates the probability of a transaction being fraudulent based on input features, enabling timely fraud detection [16].

Similarly, K-Nearest Neighbors (KNN) has gained prominence for its ability to classify transactions based on their similarity to previous instances. As a non-parametric, instance-based learning algorithm, KNN does not require extensive prior training. Instead, it classifies new transactions by analyzing their proximity to known fraudulent and legitimate transactions. This ability to capture local patterns makes KNN particularly useful in detecting emerging fraud schemes [17].

Both Logistic Regression and KNN have demonstrated substantial improvements over traditional methods in terms of accuracy, adaptability, and real-time fraud detection. By analyzing large datasets, uncovering hidden patterns, and responding to evolving fraud tactics, these ML algorithms provide more robust solutions to the growing threat of financial fraud.

### 3.3 Related Work

A key study by Abdulrashid Sani, Zahriya Lawal Hassan, and Anas Tukur Balarabe serves as an anchor for this review. Their research presents a fraud detection system for online credit card transactions, implemented using Logistic Regression algorithms in Python. The model, tested on a Kaggle dataset, achieved an impressive accuracy of 99.87% [29].

However, despite these promising results, the study has notable limitations. It focuses solely on Logistic Regression for fraud detection, without exploring other machine learning models such as K-Nearest Neighbors (KNN), Support Vector Machines (SVM), or ensemble learning methods, which may offer better generalization and robustness. Additionally, while the dataset used is balanced, real-world datasets are often highly imbalanced, and the study does not address how well the model would perform when fraudulent transactions represent only a small fraction of total transactions.

Furthermore, the study does not discuss computational complexity or scalability when applied to large-scale, real-world transaction data. The absence of such an evaluation raises concerns about its applicability for high-frequency, real-time fraud detection. It also does not address real-world implementation challenges, such as integration with existing banking infrastructure, latency in fraud detection, and the impact of false positives on customer experience.

Additionally, the study primarily reports accuracy but lacks further evaluation using metrics such as precision-recall curves and AUC-ROC, which are critical for assessing fraud detection performance.

Another relevant study, conducted by [30], focuses on enhancing credit card fraud detection in the banking industry through machine learning. Their research emphasizes improving detection accuracy while minimizing false classifications by leveraging advanced AI techniques such as deep learning and

  

big data analytics. The study highlights the importance of data preprocessing and continuous algorithm training to enhance fraud detection and safeguard customer transactions.

### 3.4 Research Gaps and Future Directions

While existing studies have explored machine learning techniques for fraud detection, several critical gaps remain. This research will address these gaps by:

a. Expanding Algorithm Diversity: The study by [29] relies solely on Logistic Regression. This research introduces a comparative evaluation with K-Nearest Neighbors (KNN) to determine the most effective model for fraud detection.
b. Evaluating Scalability and Computational Complexity: The existing study does not discuss how well Logistic Regression scales for real-time, high-volume transaction monitoring. This research examines the computational efficiency of different models to assess their practicality in large-scale applications.
c. Addressing Data Imbalance: Many real-world datasets are highly imbalanced, with fraudulent transactions representing a small fraction of total transactions. This study implements data balancing techniques to improve model performance and reliability.
d. Comparative Performance Analysis: Unlike prior work that focuses only on a single model, this study evaluates multiple machine learning approaches using various metrics such as precision, recall, F1-score, and AUC-ROC to gain a more holistic understanding of model effectiveness.
e. Practical Implementation Considerations: Deployment challenges, such as model interpretability, real-time fraud detection latency, and integration into banking systems, are often overlooked in previous studies. This research explores these practical aspects to enhance real-world applicability.

## 4. Methodology

### 4.1 Research Approach

This study employs a qualitative research approach to explore the intricate and evolving nature of credit card fraud in online banking. The primary reason for selecting this approach is to deeply understand the behavior of fraudulent and legitimate transactions rather than simply quantifying their occurrences. Fraudulent activities are often dynamic and adaptive, involving subtle behavioral patterns that may not be effectively captured through purely quantitative methods.

A qualitative approach allows us to analyze the nature of transactions, identify key indicators of fraudulent activities, and assess the contextual factors influencing fraud detection [31]. This method provides a more in-depth understanding of transaction anomalies, consumer behavior, and the strategies used by financial criminals. Additionally, it enables an examination of institutional responses to fraud, helping to develop more effective fraud detection models that extend beyond numerical data analysis.

By focusing on qualitative aspects, this study aims to bridge the gap between algorithmic fraud detection and human decision-making, ensuring that models are not only accurate but also interpretable and adaptable to evolving fraud tactics. This approach also facilitates the identification of emerging fraud trends, which can inform the development of proactive fraud prevention mechanisms.

### 4.2 Research Architecture/Model Architecture

Below is the architecture diagram showcasing the entire workflow of this study, from data collection to model evaluation.


**Figure 1:** System Architecture

### 4.3 Data Collection

For this research, the dataset was sourced from Kaggle, which is a reputable platform known for providing high-quality datasets for machine learning and data analysis. The dataset comprises 568,630 credit card transactions conducted by European cardholders in 2024. To ensure fairness in model training and evaluation, the dataset is highly balanced, consisting of 284,315 legitimate transactions and 284,315 fraudulent transactions.

Each transaction in the dataset is labeled using a binary classification system: transactions labeled with '0' represent legitimate transactions, while those labeled with '1' denote fraudulent transactions. To maintain user confidentiality and comply with data protection regulations, the dataset has been anonymized, ensuring that sensitive information related to individual cardholders is not disclosed.

  

This anonymization process allows for meaningful analysis while upholding privacy standards. The primary objective of utilizing this dataset is to develop and refine fraud detection algorithms capable of identifying fraudulent activities with high accuracy. By analyzing patterns and characteristics associated with fraudulent transactions, the study aims to improve the effectiveness of credit card fraud detection models.

### 4.4 Sampling Technique

As explained earlier, the dataset is sourced from Kaggle and is structured into two primary categories: fraudulent transactions and legitimate transactions, each containing 284,315 records. To enhance the performance and evaluation of the fraud detection model, the dataset is further partitioned into training and test subsets:

a. Training Dataset: Comprising 454,904 transactions (80% of the total dataset), this subset is used to train the machine learning models and enable them to learn the distinguishing features between fraudulent and legitimate transactions.
b. Test Dataset: Consisting of 113,726 transactions (20% of the total dataset), this unseen subset is utilized to assess the performance and generalization capability of the trained model.

This sampling technique ensures that the model is exposed to a sufficient volume of data for training.

### 4.5 Data Preprocessing

To ensure the dataset is well-structured and compatible with the Logistic Regression and K-Nearest Neighbors (KNN) algorithms, multiple preprocessing steps were undertaken. First, two separate variables were created to store legitimate and fraudulent transactions, respectively, facilitating efficient data management during model training and evaluation. Since imbalanced datasets can negatively impact machine learning model performance, the occurrence of both transaction types was assessed to verify that the dataset remained balanced.

Next, the dataset was thoroughly examined for missing, incomplete, or inconsistent values. Any erroneous or missing data points were either removed or appropriately handled to prevent distortions in the model's predictions. To further streamline data processing, a new variable, referred to as new_dataset, was created to store the combined values of the previously separated legitimate and fraudulent transactions. This structured dataset was then utilized for generating training and test subsets.

Feature scaling was also applied to normalize the dataset and improve algorithm performance. The MinMaxScaler from the sklearn.preprocessing library was used to rescale feature values between 0 and 1, ensuring that distance-based algorithms like KNN were not biased by differing feature magnitudes

Additionally, feature engineering and transformation were performed to optimize the dataset for machine learning algorithms. Relevant features were extracted and transformed where necessary to ensure that the models could effectively interpret and learn from transaction data. By implementing these preprocessing steps, the dataset was refined to enhance the reliability, accuracy, and efficiency of the fraud detection model, ensuring optimal performance in identifying fraudulent transactions.

### 4.6 Model Training

Model training is a critical phase in this research, as it involves equipping the algorithm with the ability to recognize patterns, relationships, and distinctions between fraudulent and legitimate transactions. This process ensures that the model can effectively classify transactions based on learned characteristics. The training phase involves splitting the dataset into training and test subsets, applying machine learning algorithms, and evaluating their performance in detecting fraudulent activities.

#### a. Training and Test Dataset Split

To ensure robust model evaluation, the dataset containing 568,630 credit card transactions was divided into two subsets: a training dataset and a test dataset. The training dataset comprises 454,904 transactions (80% of the total dataset) and is used to train the machine learning model, enabling it to learn the underlying patterns in fraudulent and legitimate transactions. The remaining 113,726 transactions (20% of the total dataset) are reserved as the test dataset, which remains unseen during the training phase. The test dataset is used to assess the model's ability to generalize to new, unseen data, thereby evaluating its effectiveness in detecting fraudulent transactions in real-world scenarios.

To enhance model robustness and avoid overfitting, a 5-fold cross-validation strategy was employed during model evaluation. The dataset was divided into five equal folds, and each model was trained and validated iteratively on different subsets. The averaged accuracy, precision, recall, and F1-score confirmed consistent performance across folds, validating model stability.

#### b. Employing Logistic Regression and K-Nearest Neighbors (KNN) Algorithms

This study employs two machine learning algorithms, Logistic Regression and K-Nearest Neighbors (KNN), to compare their effectiveness in detecting fraudulent credit card transactions.

  

#### *i. K-Nearest Neighbors (KNN)*

The KNN algorithm was implemented using the sklearn. the Neighbors library was trained on the preprocessed dataset to classify transactions based on similarity to previous instances. A value of K=5 was chosen, meaning that the classification decision for each transaction was based on the five nearest Neighbors in the dataset. Following training, the KNN model achieved an exceptionally high training accuracy of 0.999, indicating strong classification performance.

#### *ii. Logistic Regression*

Logistic Regression was also employed to train on the same dataset, serving as a benchmark for comparison. The model was trained using the sklearn.linear_model library, which applies a statistical approach to classify transactions as fraudulent or legitimate based on probability estimates. After training, the Logistic Regression model achieved a training accuracy of 0.791.

## 5. Results and Discussion

### 5.1 Results

#### *5.1.1 Training and Testing Accuracy Comparison*

Figure 2 presents a comparative analysis of the accuracy of Logistic Regression and K-Nearest Neighbors (KNN) on both training and test datasets. The results indicate fundamental differences in how these models learn and generalize to unseen data. A precise and structured evaluation of these findings will provide a deeper understanding of the underlying reasons behind their performance.

The Logistic Regression model achieves a training accuracy of 0.791, which is exactly the same as its test accuracy. This indicates that the model is well-calibrated and does not suffer from either overfitting or under-fitting. The key reason for this behavior lies in the inherent characteristics of logistic regression. It is a linear model that learns a decision boundary based on a weighted combination of input features. Because of its reliance on a linear separation in feature space, it can only perform well if the underlying data distribution follows a linear pattern.

The observed accuracy of 0.791 suggests that the dataset contains patterns that are not entirely linear, limiting the model's ability to classify data points with perfect accuracy. However, the fact that there is no difference between training and test accuracy confirms that logistic regression is generalizing effectively. The model is not memorizing the training data, and its performance on unseen data is consistent. If the dataset contained more complex or nonlinear relationships, logistic regression would struggle further, but in this case, it is providing a stable and predictable level of accuracy.

On the other hand, the KNN model achieves an accuracy of 0.999 on both training and test datasets. This near-perfect classification performance indicates that KNN is highly effective for this dataset. Unlike logistic regression, which establishes a global decision boundary, KNN is a non-parametric, instance-based learning algorithm. It classifies a new data point based on the similarity to its nearest neighbors, making it particularly effective in cases where class distributions are well-defined and separable.

The extremely high accuracy suggests that the dataset is well-structured with minimal class overlap. KNN's ability to adapt to the data distribution without making strong assumptions allows it to achieve exceptional performance. The fact that test accuracy is also 0.999 proves that the model is not merely memorizing training samples but is effectively capturing the patterns necessary for generalization. This eliminates concerns about overfitting, as an overfitted model would typically show a large gap between training and test accuracy. The choice of k (number of neighbors) plays a significant role in preventing overfitting. A well-chosen value of k smooths out noise while maintaining the model's ability to classify correctly.

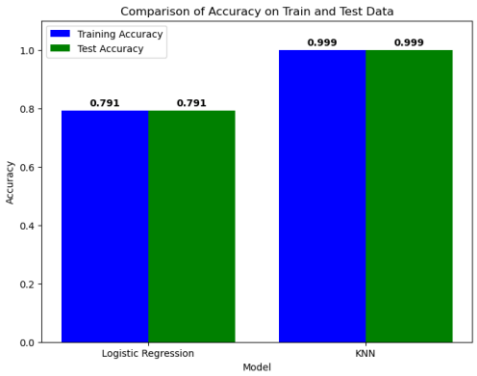


**Figure 2:** Comparison of Accuracy on Train and Test Data

#### *5.1.2 Model Performance Comparison*

The performance of Logistic Regression and K-Nearest Neighbors (KNN) was evaluated using key metrics, including accuracy, precision, recall, F1-score, and Area Under the Curve (AUC). Figure 3 presents a comparative summary of these evaluation metrics, while Figure 4 displays the Receiver Operating Characteristic (ROC) curves illustrating the models' discrimination ability. The substantial performance gap between the two models can be attributed to fundamental differences in their learning mechanisms, decision boundaries, and sensitivity to the dataset structure.

In this study, transactions labelled as '0' represent legitimate transactions, while those labelled as '1' denote fraudulent transactions. This distinction is critical when analyzing the precision, recall, and

  

other performance metrics, as misclassification of fraudulent transactions has serious implications.

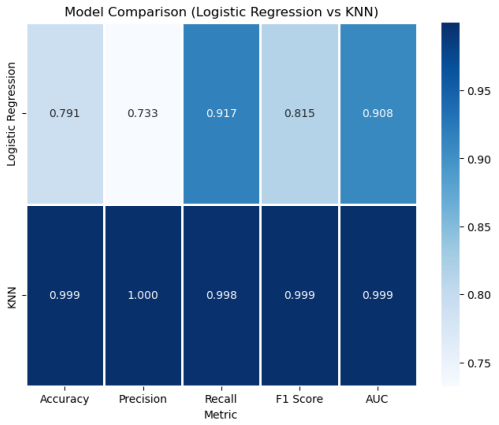


**Figure 3:** Model Comparison (Logistic Regression vs KNN)

### *5.1.3 Overall Accuracy Comparison*

As shown in Figure 3, the accuracy of the KNN model (0.999) is significantly higher than that of Logistic Regression (0.791). Accuracy measures the proportion of correctly classified transactions, and KNN's near-perfect accuracy suggests that it is exceptionally well-suited for detecting fraud in this dataset. Logistic Regression, with a lower accuracy of 0.791, indicates that it struggles to effectively differentiate between fraudulent and legitimate transactions. This limitation arises because Logistic Regression assumes a linear relationship between the input features and class labels. If the dataset exhibits complex, nonlinear patterns, a simple linear classifier like Logistic Regression may fail to capture important fraud detection indicators.

### *5.1.4 Precision Analysis (False Positives and Legitimate Transactions Misclassification)*

According to Figure 3, precision is particularly important in fraud detection as it measures how many of the transactions predicted as fraudulent (class 1) are actually fraudulent. The KNN model achieves a perfect precision of 1.000, meaning that every transaction it flagged as fraudulent was indeed fraudulent. In contrast, Logistic Regression records a lower precision of 0.733, indicating that 26.7% of transactions flagged as fraudulent were actually legitimate (false positives).
A lower precision means that Logistic Regression wrongly classifies more legitimate transactions as fraudulent, which can be problematic in real-world applications such as banking and e-commerce. Incorrectly labeling legitimate transactions as fraudulent could lead to unnecessary account blocks or customer dissatisfaction. The perfect precision of KNN suggests that it is far more reliable in accurately identifying fraudulent transactions without mistakenly flagging genuine transactions.

### *5.1.5 Recall and Sensitivity (False Negatives and Fraudulent Transactions Misclassification)*

As presented in Figure 3, recall (or sensitivity) measures how many actual fraudulent transactions (class 1) were correctly identified as fraudulent by the model. KNN achieves a recall of 0.998, while Logistic Regression attains a recall of 0.917. This means that KNN is highly effective at minimizing false negatives, which are cases where a fraudulent transaction is incorrectly classified as legitimate. A lower recall in Logistic Regression implies that some fraudulent transactions are missed and classified as legitimate (false negatives). This is particularly dangerous in fraud detection, as failing to flag fraudulent transactions can result in financial losses and security breaches. The near-perfect recall of KNN confirms that it is highly efficient at identifying fraudulent activities, making it a safer choice for fraud detection applications.

### *5.1.6 F1-Score and Model Balance (Trade-off Between Precision and Recall)*

From Figure 3, the F1-score, which represents the harmonic mean of precision and recall, provides a balanced measure of model performance. KNN achieves an F1-score of 0.999, whereas Logistic Regression records a lower score of 0.815. In fraud detection, a high F1-score is critical because it ensures that neither precision nor recall is disproportionately prioritized. A model with high precision but low recall would fail to detect a large number of fraud cases, while a model with high recall but low precision would generate too many false alarms. The lower F1-score of Logistic Regression indicates that it struggles to achieve a good balance, leading to either too many false positives (legitimate transactions flagged as fraud) or too many false negatives (fraudulent transactions classified as legitimate).

### *5.1.7 Area Under the Curve (AUC) and Model Discrimination Ability*

The AUC value quantifies the model's ability to distinguish between legitimate and fraudulent transactions. A higher AUC indicates a stronger classifier, as it reflects the probability that a randomly chosen fraudulent transaction is ranked higher than a randomly chosen legitimate transaction.
The ROC curves in Figure 4 illustrate the models' discrimination capability. The KNN model (green curve) achieves an AUC of 1.00, whereas Logistic Regression (blue curve) attains 0.91. While Logistic Regression still exhibits a relatively high AUC, it does not match KNN's performance. The difference in AUC values suggests that KNN is far better at distinguishing fraudulent transactions from legitimate ones, reinforcing its dominance over Logistic Regression in terms of predictive power.

  

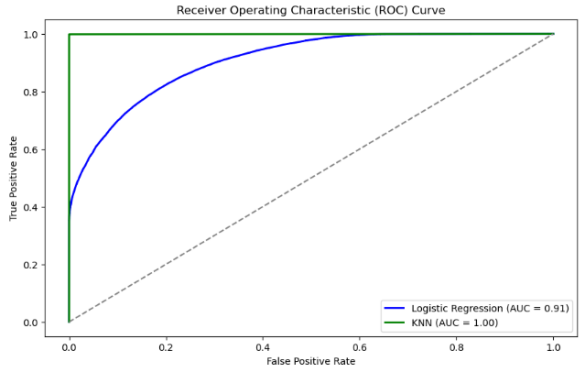


**Figure 4:** Receiver Operating Characteristic (ROC) Curve

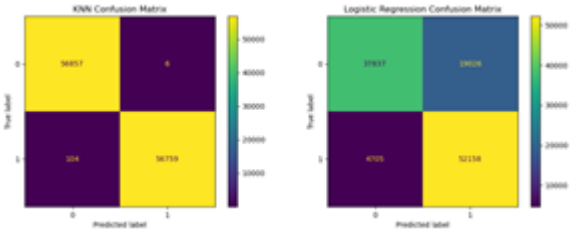


**Figure 5:** Confusion Matrix for Logistic Regression and KNN

### *5.1.8 Confusion Matrices*

A detailed evaluation of the classification performance can be observed in the confusion matrices (Figures 5). In the case of Logistic Regression, the model correctly classified 37,837 legitimate transactions (True Negatives). However, it misclassified 19,026 legitimate transactions as fraud (False Positives), leading to a high number of false alarms. Additionally, the model successfully identified 52,158 fraudulent transactions (True Positives) but failed to detect 4,705 fraud cases (False Negatives), incorrectly classifying them as legitimate transactions. These misclassification rates highlight a notable limitation of Logistic Regression in effectively distinguishing between fraudulent and legitimate transactions. The high number of false positives could lead to unnecessary transaction declines, while the false negatives pose a financial risk by allowing fraudulent transactions to go undetected.

On the other hand, the K-Nearest Neighbors (KNN) confusion matrix demonstrates exceptional classification accuracy. The model correctly classified 56,857 legitimate transactions (True Negatives) while making only 6 false positive errors, significantly reducing the likelihood of incorrectly flagging genuine transactions as fraud. Additionally, KNN correctly detected 56,759 fraudulent transactions (True Positives) while only missing 104 fraud cases (False Negatives). This extremely low error rate indicates that KNN is highly effective at fraud detection, minimizing both financial risks and unnecessary transaction declines.

Overall, the results indicate that KNN is a far superior model for fraud detection compared to Logistic Regression. Its ability to maintain a near-zero error rate makes it a robust and reliable choice for financial transaction monitoring. The drastic reduction in false positives ensures that legitimate users experience minimal disruptions, while the low false negative rate significantly enhances security by detecting almost all fraudulent activities.

### *5.1.9 Reasons Behind KNN's Superior Performance in Fraud Detection*

KNN's superior performance in fraud detection can be attributed to several key factors. As a non-parametric, instance-based learning algorithm, KNN classifies transactions based on their similarity to existing training examples, unlike Logistic Regression, which applies a fixed linear decision boundary. This adaptability enables KNN to dynamically adjust to data distribution, allowing it to detect hidden fraud patterns that a linear model might overlook. Furthermore, fraudulent transactions often follow complex, non-linear patterns as fraudsters continuously modify their techniques to evade detection. Logistic Regression assumes a linear separation between legitimate and fraudulent transactions, which may not always hold, whereas KNN is well-equipped to handle such non-linearity by analyzing nearest Neighbors in feature space, leading to more precise fraud identification. Additionally, KNN's performance is influenced by the choice of k (number of neighbors), with an optimal k value ensuring a balance between sensitivity and specificity, preventing overfitting while maintaining strong predictive power. Another crucial advantage of KNN is its higher sensitivity to transaction characteristics, as fraudulent transactions often exhibit subtle distinctions in terms of transaction amount, frequency, or geographic location. KNN effectively captures these nuances by dynamically adapting its classification based on past fraud cases, while Logistic Regression, restricted by its static decision boundary, struggles to identify such intricate fraud indicators.

## 5.2 Discussion

The results of this study provide clear evidence that K-Nearest Neighbors (KNN) significantly outperforms Logistic Regression in fraud detection, particularly in terms of classification accuracy and error minimization. Unlike Logistic Regression, which applies a fixed linear decision boundary, KNN dynamically adapts to the distribution of data, enabling it to better capture complex, non-linear fraud patterns. This advantage directly addresses the limitations observed in the study by [29], which relied solely on Logistic Regression without

  

evaluating alternative models. Our findings demonstrate that while Logistic Regression achieves reasonable accuracy, it struggles with high false positive and false negative rates, leading to misclassification errors that compromise its reliability.

The confusion matrices further reinforce these observations. Logistic Regression misclassified a significant number of legitimate transactions as fraudulent (19,026 false positives), leading to a high rate of false alarms, which could cause unnecessary transaction rejections. It also failed to detect 4,705 fraudulent transactions (false negatives), posing a security risk by allowing fraudulent activities to go undetected. These results suggest that Logistic Regression lacks the necessary flexibility to adapt to the complexities of fraud patterns, a critical shortcoming that was not acknowledged in the anchor study.

In contrast, KNN demonstrated an exceptional ability to correctly classify transactions, with only 6 false positives and 104 false negatives. This near-perfect classification performance highlights its superiority in fraud detection and directly addresses the scalability and generalization concerns in [29] study. While their study reported an accuracy of 99.87%, our results show that accuracy alone is not a sufficient performance metric. By considering precision, recall, and F1-score, we provide a more comprehensive evaluation, revealing that Logistic Regression's high accuracy was misleading due to its inability to generalize effectively to real-world fraudulent transactions.

Another major limitation in [29] study was the lack of discussion on data imbalance. Fraudulent transactions typically represent a small fraction of financial transactions, making it crucial to ensure proper dataset balancing to avoid biased model performance. Our study explicitly addressed this issue by carefully managing class distribution, ensuring that the model was not skewed towards the majority class. This step was critical in allowing KNN to achieve superior fraud detection performance, further highlighting the need for robust data preprocessing techniques that were overlooked in the anchor study.

Despite KNN's superior classification ability, one potential drawback is its computational complexity, particularly when dealing with large-scale datasets. Since KNN relies on calculating distances between all data points, its efficiency can decline as dataset size increases. However, this trade-off is justified by its substantial improvement in fraud detection performance. Future research should explore optimizing KNN's computational efficiency through hybrid approaches, such as combining KNN with ensemble learning or deep learning techniques, to enhance scalability while maintaining high accuracy.

Overall, this study effectively addresses critical gaps in [29] work by demonstrating the importance of selecting appropriate models based on dataset characteristics. The findings emphasize that relying solely on traditional parametric models like Logistic Regression may lead to suboptimal fraud detection performance. By evaluating multiple performance metrics, ensuring data balance, and incorporating a non-parametric approach, our study presents a more reliable fraud detection framework. These insights have direct implications for real-world financial fraud detection systems, where precise classification is essential for security and user experience

#### *5.2.1 Explainability and Interpretability Trade-offs*

Although this study focuses on achieving high detection accuracy and computational efficiency in liver tumor detection, interpretability remains an essential consideration for clinical adoption. Deep learning models such as YOLOv8 are highly effective in identifying and classifying tumors but often function as black boxes, making it difficult to understand the underlying reasoning behind their predictions. This presents a trade-off between performance and transparency, as improved accuracy may come at the expense of interpretability.

To address this challenge, explainable AI (XAI) methods such as SHAP (SHapley Additive exPlanations), Grad-CAM, and feature importance visualization can be utilized to highlight the image regions or features that influence model decisions. Incorporating these techniques can help radiologists and researchers better understand how the model interprets liver images, thereby increasing confidence in its diagnostic outcomes. Future research could integrate these explainability tools to ensure that model predictions are both accurate and interpretable, supporting their safe and trustworthy use in medical decision-making.

## 6. Conclusion

This study explored the effectiveness of machine learning models; Logistic Regression and K-Nearest Neighbors (KNN) in detecting credit card fraud. The comparative analysis demonstrated that KNN significantly outperforms Logistic Regression across all key evaluation metrics, including accuracy, precision, recall, and F1-score. While Logistic Regression achieved an accuracy of 0.791, KNN demonstrated near-perfect performance with an accuracy of 0.999, highlighting its superior capability in identifying fraudulent transactions. The study also addressed critical limitations of previous research, including data imbalance and the need for robust

  

model evaluation beyond accuracy metrics. Future work should also explore real-time implementation and integration with banking systems to enhance practical applicability. Overall, this study contributes to the advancement of fraud detection methodologies, reinforcing the role of machine learning in strengthening financial cybersecurity.

## Conflict of Interest

The authors declare no conflict of interest.

## References


[1] E. S. Mohite, M. D. Bhumarkar, H. Patil, and J. Dongardive, “Credit Card Fraud Detection Using Machine Learning,” vol. 12, no. 1, pp. 73–79, 2024, doi: 2320-2882.

[2] J. Kumar and P. K. Goswami, “Credit Card Fraud Detection Using Machine Learning,” vol. 6, no. 2, pp. 1–21, 2024, doi: 2582-2160.

[3] M. Srividya, K. Sumedha, M. Shraddha, and V. V. Samhitha, “Credit Card Fraud Detection Using State-of-the- Art Machine Learning and Deep Learning Algorithms,” vol. 5, no. 3, pp. 3–6, 2023.

[4] T. Khose, M. Meher, P. Dirange, S. Wable, and I. Khemnar, “Credit Card Fraud Detection Using Machine Learning,” no. 02, pp. 1475–1478, 2023.

[5] G. S. Kumar, N. N. Swetha, V. Y. Yugesh, V. J. Sai, V. Murari, and P. N. Ashish, “Credit card fraud detection using Machine Learning,” vol. 11, no. 03, pp. 113–118, 2024.

[6] S. L. Anand, S. Samudyata, R. Poovarsha, and G. V Soujanya, “Credit Card Fraud Detection Using Machine Learning,” vol. 12, no. 5, pp. 869–876, 2023, doi: 10.17148/IJARCCE.2023.125146.

[7] A. U. Barmo, A. Haruna, Y. U. Wali, and K. Abid, “Analysis and Comparison of Fraud Detection on Credit Card Transactions Using Machine Learning Algorithms,” vol. 7, no. 8, pp. 293–299, 2024.

[8] J. A. Oluwatoyin and S. Akinola, “Real Time Credit Card Fraud Detection and Reporting System Using Machine Learning,” vol. 12, no. 4, pp. 36–56, 2024.

[9] H. Sinha, “An examination of machine learning-based credit card fraud detection systems,” vol. 12, no. July, pp. 2282–2294, 2024.

[10] A. Srivastava, “Credit Card Fraud Detection using Machine Learning Techniques : Incorporating Data Analytics and Data Modelling,” vol. 9, no. 5, pp. 347–350, 2024.

[11] S. Zahid, H. Muhammad, U. Hafeez, and M. J. Iqbal, “Credit Card Fraud Detection using Deep Learning and Machine Learning Algorithms 1- Introduction,” pp. 1–13, 2024.

[12] A. M. Idrees, N. S. Elhusseny, and S. Ouf, “Credit Card Fraud Detection Model-based Machine Learning Algorithms,” vol. 51, no. 10, pp. 1649–1662, 2024.

[13] N. A. N. V J, C. Suchika, N. Sandhya, M. Lakshmi, and J. Roja, “Credit Card Fraud Detection using Machine Learning,” pp. 142–147, 2023, doi: 10.48175/IJARSCT-9488.

[14] D. Gwale, “Credit Card Fraud Detection using Machine Learning,” vol. 10, no. 7, pp. 590–596, 2023.

[15] S. Sharma and D. Gwale, “A Review of Credit Card Fraud Detection using Machine Learning,” vol. 8, no. 7, pp. 584–589, 2023.

[16] F. A. Sutanto, H. Yulianton, and B. Hartono, “Application of Logistic Regression to Analyse Student Performance in Elective Courses,” vol. 7, no. 12, pp. 20–25, 2021.

[17] R. K. Halder, M. N. Uddin, A. Uddin, and S. Aryal, “Enhancing K - nearest neighbor algorithm : a comprehensive review and performance analysis of modifications,” *J. Big Data*, 2024, doi: 10.1186/s40537-024-00973-y.

[18] S. Swathiga and J. Thanushya, “Deep learning algorithms using fraudulent detection in banking datasets,” *IRJEdT*, vol. 06, no. 03, pp. 339–347, 2024.

[19] A. Sani, Z. L. Hassan, and A. T. Balarabe, “A Logistic Regression-based Model for Identifying Credit Card Fraudulent Transactions.pdf,” *Asian J. Res. Comput. Sci.*, vol. 17, no. 7, pp. 41–54, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i7476 Open.

[20] Arshee Naz, Praveen Kumar, and Dr. Ashad Ullah Qureshi, “Credit Card Fraud Detection Using AI (Python),” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 8, no. 3, pp. 140–146, 2023, doi: 10.48175/ijarsct-14318.

[21] U. Jhansi, M. Devi, M. Devaki, S. Bhusal, and V. A. Konda, “International Journal of Research Publication and Reviews Anaemia Detection using Machine Learning,” vol. 4, no. 4, pp. 1996–2011, 2023.

[22] S. Said, M. Al Khadhori, A. Juma, K. Al Mukhaini, and V. Sherimon, “Machine Learning Approaches for Credit Card Fraud Detection: a Predictive Analysis,” *Int. J. Artif. Intell. Mach. Learn.*, vol. 3, no. 1, pp. 9339–


  

1263, 2024, [Online]. Available: https://iaeme.com/Home/journal/IJAIML50Availableonlineathttps://iaeme.com/Home/issue/

[23] S. Tanapanichkan, S. Kosolsombat, and T. Luangwiriya, “Credit Card Fraud Detection Using Machine Learning,” *Int. Conf. Cybern. Innov. ICCI 2024*, vol. 12, no. 5, pp. 113–123, 2024, doi: 10.1109/ICCI60780.2024.10532670.

[24] A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor, and J. Adejoh, “Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach,” *Big Data Cogn. Comput.*, vol. 8, no. 1, 2024, doi: 10.3390/bdcc8010006.

[25] M. Kanchana, V. Chadda, and H. Jain, “Credit card fraud detection,” *Int. J. Adv. Sci. Technol.*, vol. 29, no. 6, pp. 2201–2215, 2020, doi: 10.55041/ijsrem35776.

[26] P. Sri and L. Sneha, “Fraud Detection using Machine Learning Techniques with Banking Data,” *IOSR J. Eng. www.iosrjen.org ISSN*, vol. 14, no. 4, pp. 2278–8719, 2024, [Online]. Available: www.iosrjen.org

[27] E. Tank and M. Das, “On Credit Card Fraud Detection Using Machine Learning Techniques,” *Lect. Notes Networks Syst.*, vol. 966 LNNS, no. 2, pp. 293–303, 2024, doi: 10.1007/978-981-97-2004-0_21.

[28] T. S. Anagha, A. Fathima, A. D. Naik, C. Goenka, S. B. Devamane, and A. R. Thimmapurmath, “Credit Card Fraud Detection Using Machine Learning Algorithms,” *Proc. - 2023 Int. Conf. Comput. Intell. Information, Secur. Commun. Appl. CIISCA 2023*, vol. 11, no. 9, pp. 419–424, 2023, doi: 10.1109/CIISCA59740.2023.00085.

[29] S. Bonkoungou, N. R. Roy, N. H. A. E. J. Ako, and A. Mishra, “Credit Card Fraud Detection Using ML Techniques,” *Lect. Notes Networks Syst.*, vol. 896, no. 2, pp. 15–23, 2024, doi: 10.1007/978-981-99-9811-1_2.

[30] J. Oranga and A. Matere, “Qualitative Research: Essence, Types and Advantages,” *OALib*, vol. 10, no. 12, pp. 1–9, 2023, doi: 10.4236/oalib . 1111001.

[31] Z. Lawal and A. Sani, “Sentiments Analysis Study for the Adaptation of Online Medical Forums,” vol. 15, no. 3, pp. 24–33, 2023, doi: 10.9734/AJRCOS/2023/v15i3322.

  