Real-Time Credit Card Fraud Detection Using Ensemble and Supervised Learning Approaches

Ajay Kumar[1]; Subhash Chand Dambhiwal[2]; Dr. Avinash Panwar[3]

[1]Research Scholar, Department of Computer Science, MLSU, Udaipur
[2] Research Scholar, Department of Computer Science, MLSU, Udaipur
[3] Head of Department, Department of Computer Science, MLSU, Udaipur

Publication Date: 2025/09/02

Abstract:

- ***Background:***

Credit card fraud has been a growing concern with the expansion of digital payment systems. Traditional fraud detection methods face challenges in adapting to new fraudulent patterns and often result in high rates of false positives (FP) and false negatives FN). Machine learning (ML) offers a promising solution by learning from historical data to detect hidden patterns within transactions.

- ***Objectives:***

The goal of this project is to create a system for the real-time identification of fraudulent credit card transactions that is powered by machine learning., with a focus on reducing false negatives and false positives.

- ***Methods:***

Several ML methods were used in this study, for analyzing transaction data, including Random Forest, Voting Classifier, Logistic Regression, Decision Tree, and XGBoost. The dataset used for training and validation was obtained from publicly available credit card transaction data, focusing on recognizing key characteristics that indicate potential fraudulent behavior.

- ***Results:***

The machine learning model exhibited higher performance over traditional rule-based systems., achieving an accuracy rate of 98%, with a significant reduction in both false positives and false negatives. With respective area under the receiver operating characteristic (ROC) curves of 99.14% and 99.13%, the XGBoost and Voting Matrix models performed the best.

- ***Conclusion:***

This study shows that ML algorithms can significantly improve the identification of credit card fraud, offering a more flexible and precise system in contrast to conventional approaches.

Keywords: *Credit Card Fraud (CCF); Machine Learning (ML); Random Forest (RF); Voting Classifier; XGBoost; Support Vector Machines (SVM).*

How to Cite: Ajay Kumar; Subhash Chand Dambhiwal; Dr. Avinash Panwar (2025) Real-Time Credit Card Fraud Detection Using Ensemble and Supervised Learning Approaches. *International Journal of Innovative Science and Research Technology*, 10(8), 1893-1910. https://doi.org/10.38124/ijisrt/25aug1392

I. INTRODUCTION

Credit card fraud (CCF) has remained a persistent and growing challenge as the global adoption of digital payments increases. With the shift toward online shopping, mobile payments, and digital banking, the volume of electronic transactions has surged, creating new opportunities for fraudsters. The sophistication of cybercriminal tactics has risen in tandem, making it increasingly difficult to identify and avoid fraud. fraudulent activities using traditional methods. This rapid escalation of fraud activities has brought about serious concerns for consumers, financial institutions, and regulatory bodies alike, demanding more effective and adaptive fraud detection systems.

Traditional fraud detection systems predominantly rely on rule-based methods, where pre-defined patterns and heuristics are used to flag suspicious transactions. Despite their early efficacy, these methods have major limitations. Most notably, they struggle to adapt to new and emerging fraud tactics, are prone to high false-positive rates, and often fail to identify novel fraudulent behavior. These systems are rigid and unable to evolve in response to the dynamic nature of cybercrime.

Additionally, the reliance on manual intervention to resolve flagged transactions has led to inefficiencies and frustration for both financial institutions and customers. Consequently, the financial industry is under growing pressure to create more adaptable, efficient, and accurate systems capable of responding to the complexities of modern fraud [1].

The increasing demand for advanced and flexible fraud detection systems has prompted the investigation of Machine Learning (ML) as a possible solution [2]. Algo-rithms in machine learning, capable of learning from past data and consistently adjusting to new insights, present a valuable method for detecting fraud. Models like these can uncover complex patterns in transaction data that might otherwise go undetected by traditional systems. By utilizing extensive transaction data [3], [4]. ML models can detect suspicious behaviors with enhanced precision, decrease false positives, and enhance the overall efficiency of fraud prevention systems [5], [6].

In today’s financial market, there are obvious prerequisites for a successful fraud detection system.: high accuracy, low false positives, adaptability, and real-time performance. Machineˆ learning techniques meet these needs by offering several key advantages:

- *Dynamic Learning:* ML models can improve their effectiveness over time by examining new data, allowing them to detect fresh fraud patterns that static rule-based systems might miss.
- *Complex Pattern Recognition*: Unlike traditional models that rely on simple rules, ML models, for example Random Forest, Voting Classifier, NN and, are SVM capable of identifying intricate, nonlinear relationships in data, providing a more sophisticated approach to fraud detection.
- *Scalability:* ML techniques are adequate of handling large-scale datasets, making them appropriate for the growing volumes of transaction data generated by modern financial systems.

Several ML algorithms, such as Random Forest, Voting Classifier, Neural Networks, and SVM has been frequently used in the field of identifying credit card fraud [7]. Random Forest (RF) employs ensemble learning by aggregating numerous decision trees to improve accuracy and minimize overfitting. SVM excel in classifying data enabling them to detect complex patterns in transaction behavior that are indicative points in high-dimensional spaces, making them effective for fraud detection tasks where the data is complex and non-linear. Deep learning (DL) models, especially neural networks, can autonomously derive features from raw data [8].

The novelty of this study lies in the application of ML to fraud detection, focusing on identifying patterns that traditional rule-based systems have struggled to detect. Although previous studies have explored various ML algorithms, this research advances beyond merely contrasting methods to focus on improving detection precision and reducing false positives. This contribution is crucial for practical deployment, as financial institutions have major obstacles when distinguishing between legitimate transactions and fraud.

The novelty of this study lies in the application of ML to fraud detection, focusing on identifying patterns that traditional rule-based systems have struggled to detect. Although previous studies have explored various ML algorithms, this research advances beyond merely contrasting methods to focus on improving detection precision and reducing false positives. This contribution is crucial for practical deployment, as Financial institutions have major obstacles when distinguishing between legitimate transactions and fraud.

Furthermore, this study aims to address key limitations of existing fraud detection systems, particularly:

- *Reducing False Positives(FP):* One of the critical issues with conventional fraud detection systems frequently have a high false positive (FP) rate, which occurs when valid transactions are wrongly classified as fraudulent. This problem can be considerably lessened by applying machine learning, particularly ensemble approaches and deep learning, the suggested method aims to minimize false alerts while ensuring a strong level of accuracy in fraud detection.
- *Adaptability to Emerging Fraud Techniques:* ML models can adapt by learning from newly gathered data, which ensures that fraud detection systems can progress alongside evolving fraud strategies. This research contributes to the development of models that can quickly adapt to new types of fraud without requiring manual rule updates.
- *Real-Time Performance:* The research examines the potential use of machine learning in creating fraud detection systems that function in real-time, delivering instant insights and reactions to transactions that may be fraudulent. This is an essential feature for financial institutions that need to act quickly to prevent fraud.

The contribution of this work lies in improving the resilience and effectiveness of fraud detection systems, providing a solution that is more scalable, flexible, and precise compared to conventional approaches. This research also highlights the importance of integrating machine learning strategies into operational frameworks, enabling financial organizations to take proactive measures against the rising threat of credit card fraud.

The goal of this project is to develop a machine learning-based framework that can instantly identify fraudulent credit card transactions. By utilizing cutting-edge machine learning methods, our goal is to decrease false positives, enhance detection rates, and ultimately deliver a more reliable solution for identifying credit card fraud. How do various machine learning models, (including deep learning approaches), stack up against each other concerning accuracy, speed, and efficiency when applied to a large, imbalanced dataset of transactions for credit card fraud detection.

Through this comparative analysis, in addition to providing insights into the possibilities of deep learning approaches for real-time credit card fraud detection systems, the study seeks to determine the most successful fraud detection model.

II. LITERATURE REVIEW

The increasing sophistication of cybersecurity threats in the financial sector has led to a growing reliance on machine learning (ML) and artificial intelligence (AI) techniques to mitigate these challenges [1]. Emphasize the potential of AI in addressing cybersecurity issues, specifically in the financial business, by providing dynamic and efficient solutions to detect, predict, and prevent various types of cyberattacks, including credit card fraud. AI models, especially ML algorithms, have shown significant promise in identifying patterns within massive volumes of transaction data, which traditional methods often fail to uncover. The integration of AI into cybersecurity systems offers scalability, adaptability, and enhanced decision-making capabilities, allowing financial institutions to better protect sensitive data and prevent fraud [9].

Cyberwarfare is another area of concern, as highlighted by [2] who reports that cybercrime damages were predicted to exceed $6 trillion globally in 2021. This astronomical rise in cyber threats underscores the importance of robust cybersecurity measures. The financial sector, in particular, has been a major target due to the highly sensitive nature of financial transactions and personal data. ML approaches are being used in this context to defend against the ever-growing range of cyberattacks, including those targeting financial transaction [2] Furthermore, as reported by global cybersecurity spending is expected to exceed $1 trillion between 2017 and 2021, highlighting the crucial need for financial institutions to participate in advanced technologies such as AI to protect their systems and customers [2].

Credit card fraud detection is an essential concern for financial organizations, has benefited from the application of various ML methods. A comprehensive evaluation of fraud detection methods within the banking industry, providing insights into the benefits of employing ML models for the identification of fraud. They observed that tools like decision trees, (SVM), and neural networks have proven effective in recognizing fraudulent activity with high accuracy [4]. Different types of fraud detection systems were reviewed, a variety of fraud detection systems were examined, emphasizing the need for improved algorithms that can manage extensive datasets while preserving high levels of precision and recall. Their results also showed the need of using different approaches to increase detection performance [5].

Several studies have explored the use of deep learning models for fraud detection. Proposed a ML-based credit card fraud detection model that incorporated ensemble methods to improve accuracy and reduce false positives. Their model demonstrated better performance compared to traditional methods, emphasizing the effectiveness of ensemble models in fraud detection [6]. A similar approach using Long Short-Term Memory (LSTM) networks, a type of recur-rent neural network (RNN), Capturing temporal relationships in transaction data is crucial for discovering sequential fraud trends that may be ignored by other models [7].

Additionally, studies on ensemble classification methods for fraud detection have shown that combining multiple ML approaches can greatly enhance the model's effectiveness in identifying credit card fraud, particularly when user behavior information is included [8] ML algorithms such as Random Forest, which were also highlighted by [10] have been found to offer a balanced trade-off between detection rate and false positives, this implies them ideal for real-time fraud detection systems [10].

In addition to the traditional ML models, newer techniques involving deep learning architectures such as auto encoders and Restricted Boltzmann Machines (RBMs) have shown promise in detecting fraudulent activities with higher precision. Deep learning-based auto encoders combined with RBMs for fraud detection, which significantly increased detection accuracy when compared to the conventional methods [11]. This deep learning approach has gained traction as it allows models to automatically learn patterns from unstructured data without the need for manual feature extraction.

Despite the advances in fraud detection techniques, limitations remain in terms of real-time performance and adaptability. Many ML models still struggle with achieving a high balance between precision and recall, which is crucial in minimizing both false positives and false negatives. Since illegal transactions are much less common than valid ones, there is an inherent imbalance in the data that makes detecting credit card fraud difficult, leading to biases in model performance [12]. To address this, researchers have focused on developing novel methods such as real-time streaming analytics [13], which aim to reduce processing time and improve fraud detection in live environments.

III. DATA AND METHODOLOGY

A. Data

Evaluation was conducted using a pre-processed, publicly accessible real dataset from Kaggle. The dataset is extremely unbalanced because it includes 7,195 fraudulent transactions out of 100,000 total transactions. Transaction ID, Date, Weekday, Time, Card Type, Entry Mode, Amount, Transaction Type, Merchant Group, Transaction Country, Shipping Address, Country of Residence, Gender, Age, Bank, and Fraud are among the 16 variables in the dataset. The attribute is illustrated in Table 1.

The dataset used for training and validation was derived from publicly available credit card transaction data, which provided a rich source of information for our analysis. This dataset contained numerous transaction records, including both fraudulent and non-fraudulent instances, making it ideal for training and evaluating ML models. The data included key features such as transaction amounts, timestamps, card type, merchant group, and geo-graphical information, among others, which are indicative of fraud [14]. In the process of preparing the data for model training, we focused on extracting key features that could help in identifying patterns of fraudulent activity. Features such as transaction amount (with unusually high or low values), time of transaction (indicating purchases outside normal business hours), day of the week, and merchant group were all considered critical in distinguishing between normal and fraudulent behavior. Additionally, demographic information like age and gender of cardholders were used to create segments and detect any anomalies specific certain user groups [11], [15], [16].

Table 1 Illustration of the Variables Recovered from the Data.

Column Name	Description
Transaction ID	A unique identifier for each transaction. Used for tracking and referencing individual transactions.
Date	The calendar date on which the transaction occurred. Helps in analyzing seasonal trends, patterns, and potential fraud detection.
Day of Week	The day of the week (e.g., Monday, Tuesday) the transaction took place. Identifies trends or anomalies in transaction activity.
Time	The time the transaction occurred, typically recorded in 24- hour format. Helps identify peak transaction hours or suspicious activity outside business hours.
Type of Card	The category of the credit card used, such as MasterCard or Visa.
Entry Mode	The method used to enter the card information (e.g., Tap, PIN, CVC).
Amount	The monetary value of the transaction. Critical for financial analysis and fraud detection.
Type of Transaction	The nature of the transaction, such as purchase, refund, cash withdrawal, or recurring payment.
Merchant Group	The classification of merchants (e.g., retail, travel, dining). Useful for identifying industry-specific transaction patterns.
Country of Transaction	The location where the transaction was initiated. Used for detecting suspicious international transactions.
Shipping Address	The address where goods or services were delivered. Verifies legitimacy and identifies mismatches with the billing address.
Country of Residence	The country where the cardholder resides. Provides context for evaluating cross-border transaction risks.
Gender	The gender of the cardholder. Supports demographic analysis and personalization of services.
Age	The age of the cardholder. Facilitates segmentation and detection of anomalies (e.g., high-value transactions from very young cardholders).
Bank	The financial institution that issued the card. Analyzes card usage trends across different banks.
Fraud	Indicates whether the transaction was fraudulent (Yes/No). The key target variable for fraud detection.

B. *Data Pre-Processing*

The data was cleaned and structured during the pre-processing step to avoid missing numbers, as our analysis is based on complete data. By conducting feature scaling, we retained all numeric explanatory variables in the same domain by utilizing range transformation to calculate all numeric variables to be between 0 and 1 [17].

Before training the ML models, we conducted data pre-processing, which included:

- *Handling Missing Values:* Data points that were missing were either filled in or discarded depending on the pattern of messiness.
- *Feature Scaling:* Standardization of continuous variables was performed to ensure all features had comparable scales.
- *Feature Selection:* We employed correlation-based feature selection to identify the most important variables contributing to the model's performance.

C. *Feature Selection and Extraction*

Effective fraud detection relies heavily on identifying relevant features. The features extracted and used for model training were selected based on their ability to differentiate fraudulent transactions from legitimate ones. The key features included: Table 2 and Table 3 shows the summery statistics of the types of variables used in the study.

Table 2 Basic Statistics for the Character Variables.

Variable Name	Count	Unique	Top Value	Frequency
Transaction ID	100000	95680	#2547 017	5
Date	100000	4	14-Oct-20	50184
Day of Week	100000	4	Wednesday	50177

Type of Card	100000	2	Visa	53812
Entry Mode	100000	3	PIN	49976
Amount	99994	396	£17	2153
Type of Transaction	100000	3	Online	33481
Merchant Group	99990	10	Children	10679
Country of Transaction	100000	5	United Kingdom	71199
Shipping Address	99995	5	United Kingdom	60905
Country of Residence	100000	5	United Kingdom	81859
Gender	99996	2	M	50875
Bank	100000	8	Barclays	29936

- Time of Transaction: Transactions occurring at unusual hours may signal fraudulent activity.
- Day of the Week: Fraudulent activity may vary depending on the day (e.g., more activity on weekends).
- Merchant Group: Specific merchant categories (e.g., high-end retailers) may be more prone to fraud.
- Location Data: The country or region of the transaction was compared with the cardholder’s usual spending patterns to detect suspicious cross-border transactions.
- Demographic Features: Attributes like the cardholder’s age, gender, and bank were also considered to segment the data and identify abnormal behaviors in different demographic groups.
- Transaction Amount: Unusually high or low transaction amounts are often indicative of fraud.

Table 3 Basic Statistics for the Numeric Variables.

Statistic	**Time**	**Amount**	**Age**	**Fraud**
Count	100000	99994	100000	100000
Mean	14.56	112.58	44.99	0.072
Std	5.31	123.43	9.95	0.26
Min	0.00	5.00	15.00	0.00
25%	10.00	17.00	38.20	0.00
50%	15.00	30.00	44.90	0.00
75%	19.00	208.00	51.70	0.00
Max	24.00	400.00	86.10	1.00

D. Methodology

In order to classify fraudulent transactions, this section covers supervised machine learning models such as Random Forest, Voting Classifier, KNN, XGBoost, and Decision Tree.

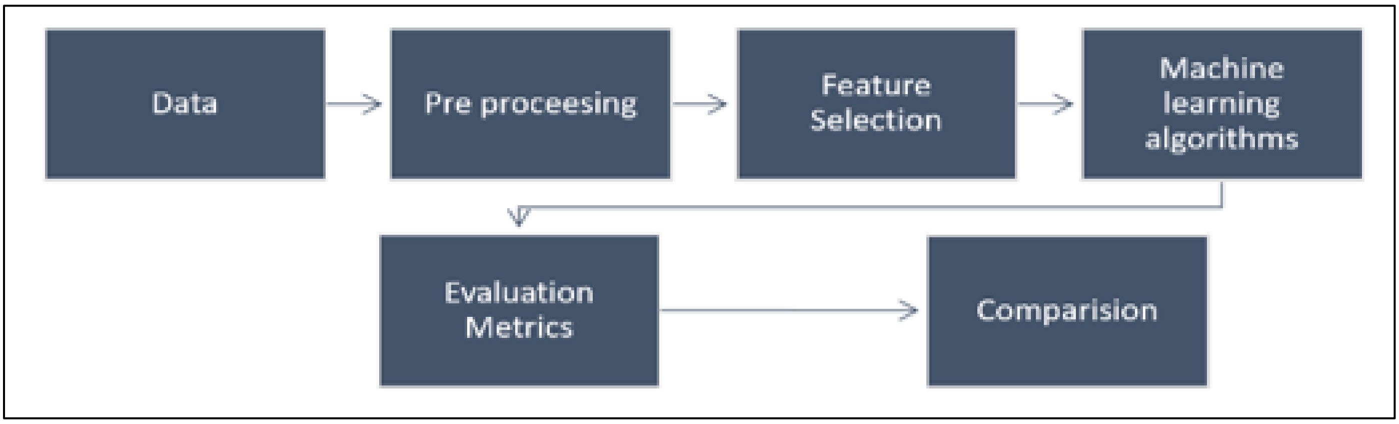

Fig 1 Flowchart of Methodology.

➢ *Random Forest*

An ensemble learning approach that integrates various decision trees to enhance classification precision and minimize overfitting. It effectively manages imbalanced datasets and offers insights into feature significance, making it well-suited for intricate fraud detection challenges. Random Forest typically achieves high accuracy, precision, and AUC-ROC [18]. The Random Forest algorithm creates a set of decision trees using the bagging technique. The procedure initially creates a vector of Ki random variables (i = 1, 2, 3, N) given a dataset (X, Y) of N observations, where X stands for the predictor variables and Y for the outcome variables. Following that, a decision tree is constructed using each K_i random vector, producing dk_i decision trees ($dK_1(X)$, $dK_2(X)$,…………,$dK_N(X)$). These decision trees are aggregated to determine the final classification [17].

➢ *Voting Classifier*

An ensemble learning technique called a voting classifier combines the predictions of several machine learning models to improve performance as a whole. A Voting Classifier is very useful in detecting credit card fraud since it combines the benefits of many algorithms to improve accuracy, precision, and recall. The Voting Classifier combines predictions from different models (e.g., Logistic Regression, Random Forest, XGBoost, Decision Tree, and KNN) to make a final classification decision[1], [2].

➢ *K-Nearest Neighbors (KNN)*

A straightforward, non-parametric machine learning method for classification and regression applications is K-Nearest Neighbors (KNN). Because it doesn't explicitly learn a model during training, it is regarded as a lazy learning algorithm. Rather, when a query is sent, it predicts based on the nearest data points. Instead, it memorizes the training dataset and predicts based on the similarity (distance) of data points [3].

➢ *XGBoost*

XGBoost (Extreme Gradient Boosting) is a sophisticated gradient-boosted ensemble algorithm that is particularly effective in detecting credit card fraud. It constructs a sequence of decision trees, each rectifying the flaws of the preceding ones, and using sophisticated approaches to enhance accuracy and processing efficiency [4].

➢ *Decision Tree*

A transparent model that splits data based on feature values, providing clear decision rules. While Decision Trees capture non-linear relationships, they are prone to overfitting, especially with deep trees. Pruning techniques are essential to control model complexity and avoid instability. It is a good choice when model interpretability is a priority. For credit card fraud detection, the goal is to classify transactions as either fraudulent (1) or legitimate (0) [5]. Below is a mathematical explanation of how a decision tree works in this context. The two most common splitting criteria are:

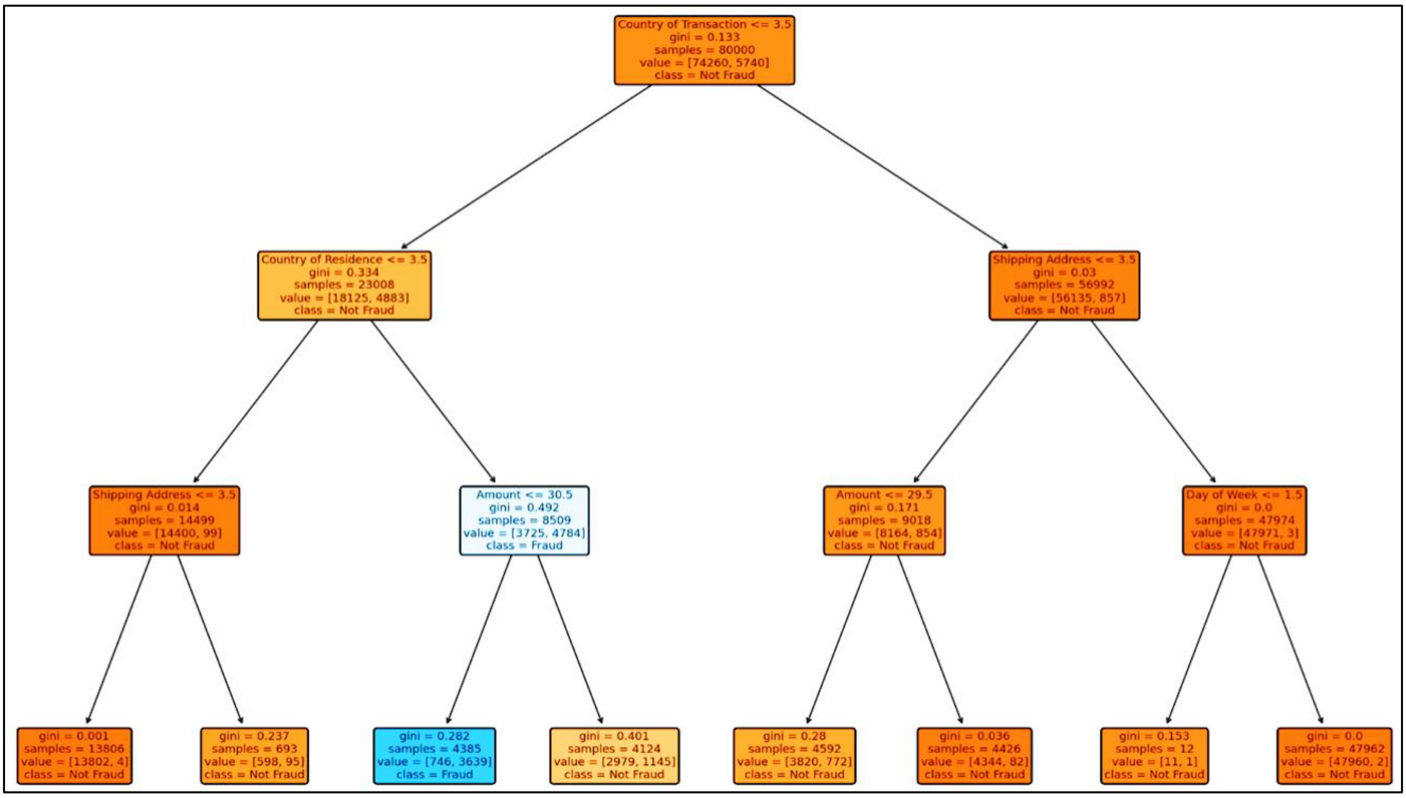

Fig 2 Decision Tree

- *Gini Impurity:*

If a randomly chosen element is randomly labeled according to the class distribution inside the subset, the Gini impurity measures the probability that it will be incorrectly classified. The value of the Gini index falls between 0 and 0.5 [6]. This It is calculated as:

$$Gini = \left[1 - \sum_{i=1}^{k} p_i^2\right] \tag{1}$$

Where:

p_i is the proportion of class *i* instances in the dataset.

k is the number classes (fraud or not fraud).

To calculate the proportion of each transaction ("fraud" and "not fraud") in the node.

$$p_{fraud} = \frac{Number\ of\ fraudulent\ transactions}{Total\ transactions\ at\ the\ node} \tag{2}$$

$$p_{fraud} = \frac{Number\ of\ fraudulent\ transaction}{Total\ transaction\ at\ the\ node} \tag{3}$$

The data set contains 7195 fraud cases out of a total of 100,000 transactions. Then theˆ Gini impurity of the data set is

- *The Probability of Fraud of the Data Set is:*

$$p_{fraud} = \frac{7195}{100000} = 0.07195 \qquad (4)$$

- *The Probability of Non-Fraud of the Data Set is:*

$$p_{not-fraud} = \frac{92805}{100000} = 0.92805 \qquad (5)$$

- *Gini Impurity of the Data Set is:*

$$G=1-(0.07195^2 + 0.92805^2) \qquad (6)$$

- *The Gini Impurity for this Dataset is Approximately 0.1335.*

- *Entropy:*

Entropy defines a dataset's uncertainty or disorder. In the domain of fraud detection, entropy assists in determining how mixed or" impure" a node is in terms of class distribution (for example," fraud" and" not fraud") [7].

$$Entropy(D) = -\sum_{i=1}^{k} (\mathcal{P}_i) \log_2 \mathcal{P}_i \qquad (7)$$

- *Entropy of the Data Set is:*

$$Entropy(D) = -(p_{fraud} \log_2 p_{fraud} + p_{not\ fraud} \log_2 p_{not\ fraud} \qquad (8)$$

✓ The Entropy of the Dataset is Approximately 0.3732.

- *Information Gain (IG):*

IG is a measure used in decision trees to determine how well a feature splits data in terms of reducing uncertainty. In the realm of credit card fraud detection, IG helps discover the most important features that contribute to identifying fraudulent transactions from authorized ones. The IG is determined as the projected reduction in entropy attributed to the information received [6].

The dataset contains 100,000 entries with 16 columns. The target variable for information gain calculation is" Fraud" (binary: 0 or 1). The IG for each feature with respect to" Fraud" using entropy. It appears that" Country of Transaction" has the highest impact on determining fraud, while" Day of Week" has the least impact.

The information gain values for each categorical feature concerning fraud detection:

✓ Country of Transaction: 0.0782 (Most influential)
✓ Country of Residence: 0.0151
✓ Entry Mode: 0.0096
✓ Merchant Group: 0.0051
✓ Type of Transaction: 0.0037
✓ Gender: 0.0016
✓ Type of Card: 0.0009
✓ Bank: 0.0003
✓ Day of Week: 0.0001 (Least influential)

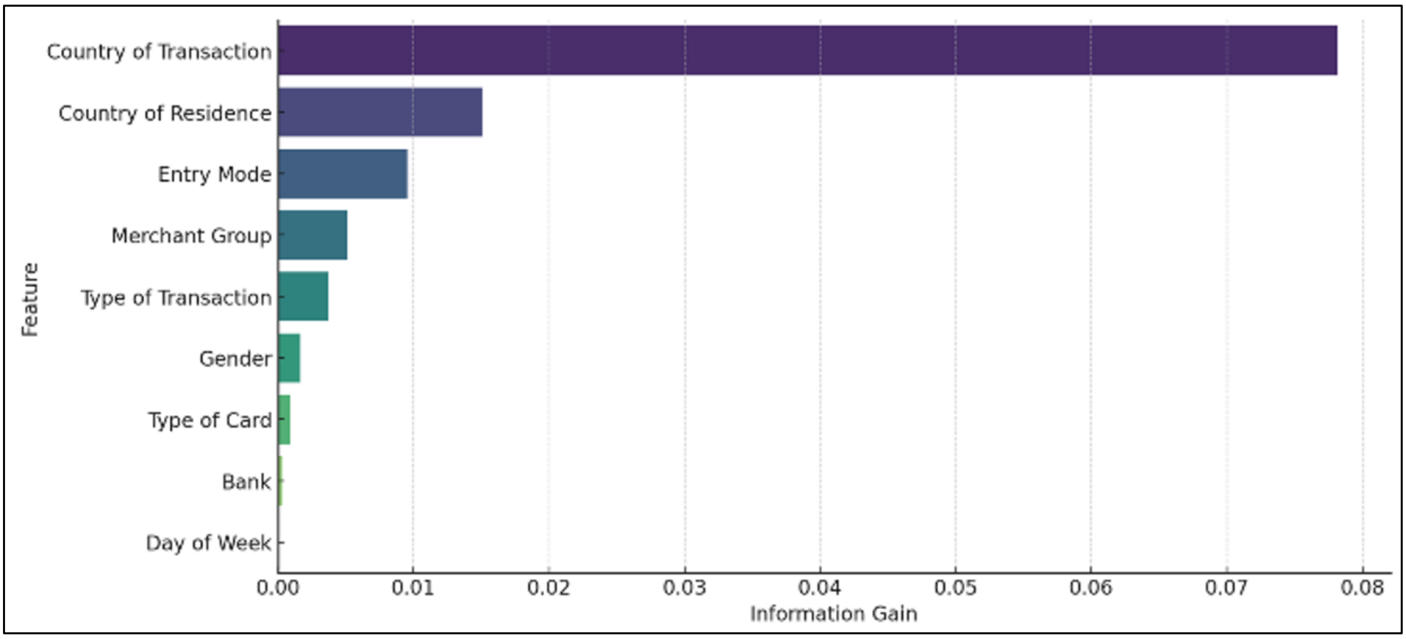

Fig 3 Information Gain of Features for Fraud Detection.

- *Logistic Regression*

A simple and interpretable model suitable for linearly separable data. While it provides probabilistic outputs that are useful for decision-making, Logistic Regression can struggle with highly imbalanced datasets unless special techniques like regularization or resampling are employed. It is highly interpretable and efficient for baseline models. In logistic regression, the core model is based on a linear function of input features, but the output is transformed by the sigmoid function to produce a probability [8]. The formula is to calculate a linear combination of input features:

$$z = w_0 + w_1 x_1 + w_2 x_2 + \cdots + w_n x_n = W^T X \qquad (9)$$

Where:

z is Linear predictor,

w_0 is the Intercept (bias),

$w = [w_1 , w_2 , \ldots\ldots , w_n]$ *are the* Coefficients (weights),

$x = [x_1 , x_2 , \ldots. , x_n]$ are the Input feature values.

w and x are the weight and feature vectors, respectively.

The linear combination z is transformed into a probability using the sigmoid function:

$$\sigma(z) = \frac{1}{1+e^{-z}} \qquad (10)$$

Where:

$\sigma(z)$ is the sigmoid function, which maps the real-valued z to a probability between 0 and 1.

z to a probability between 0 and 1.

$z \epsilon \mathbb{R}$ is the input (a real number),

e is the base of the natural logarithm ($e \approx 2.718$).

This function maps any real number z to a value in (0, 1) which represents a probability.

$$P(Y = 1|X) = \sigma(z) = \frac{1}{1+e-(w^T x)} \qquad (11)$$

$$P(Y = 0|X) = 1 - \sigma(z) \qquad (12)$$

The sigmoid function has an S-shaped curve, ensuring that the output probability is always between 0 and 1. This is important because we interpret the result as the probability of a given instance belonging to the positive class (e.g., fraud).

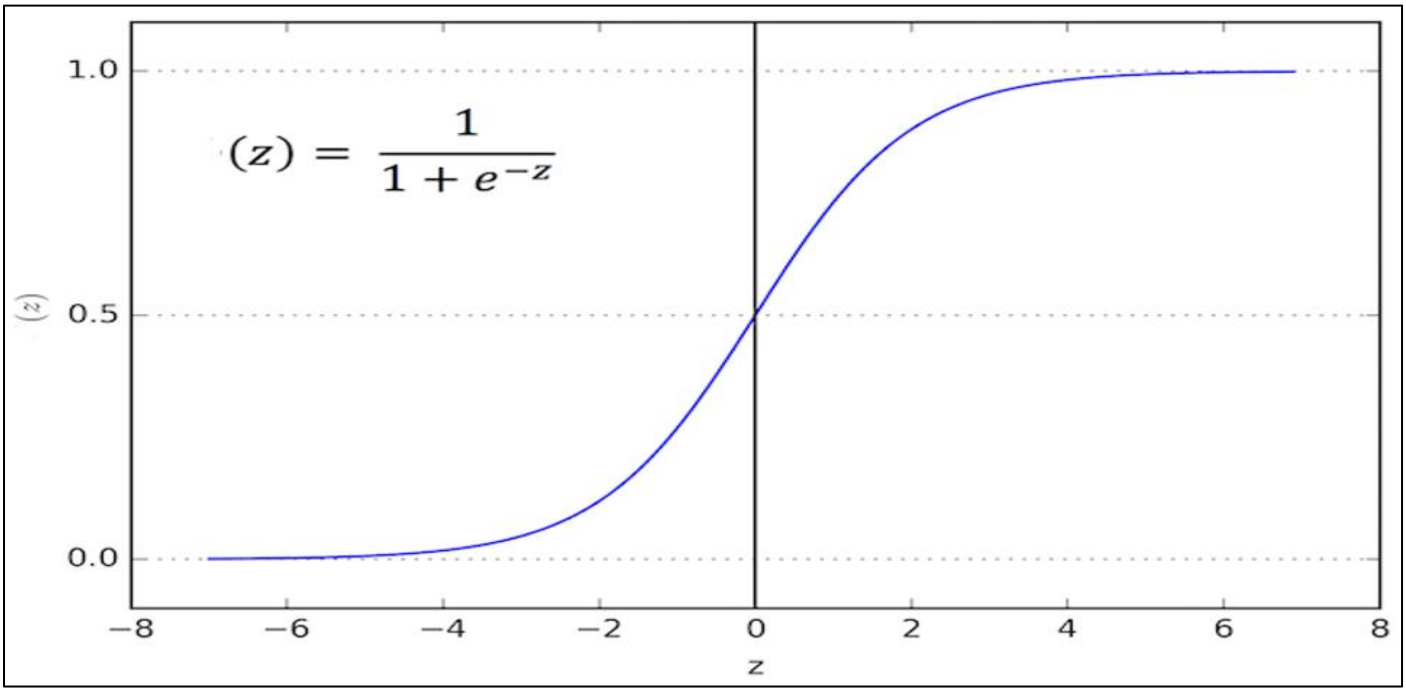

Fig 4 S-Shaped Curve.

After training, logistic regression makes predictions as:

$$\hat{y} = \begin{cases} 1 & if\ \sigma\ (z) \geq 0.5 \quad (Fraud) \\ 0 & if\ \sigma(z) < 0.5\ (Legitimate) \end{cases} \qquad (13)$$

Where:

When $z > 0, \sigma(z) > 0.5$ (Closer to 1, higher probability for class 1.)

When $z < 0, \sigma(z) < 0.5$ (Closer to 0, higher probability for class 0.)

When $z = 0, \sigma(z) = 0.5$ (Equal probability for both classes.)

- *Evaluation Metrics*

The performance of the models was evaluated using the following metrics:

- *Accuracy:*

The proportion of correctly identified cases (including true positives and true negatives) to all instances is known as accuracy [9].

$$Accuracy = \frac{T.N+T.P}{T.N+T.P+F.N+F.P} \qquad (14)$$

- *Precision:*

Precision evaluates the ratio of accurately identified positive instances (fraudulent transactions) out of all predicted positive cases [10].

$$Precision = \frac{T.P}{T.P+F.P} \quad (15)$$

- *Recall (Sensitivity):*

Recall (Sensitivity) It calculates the percentage of real positive cases-fraudulent transactions-that the model accurately detects [11].

$$Recall\ (Sensitivity) = \frac{T.P}{T.P+F.N} \quad (16)$$

- *Specificity:*

The percentage of real negative cases (non-fraudulent transactions) that the model accurately detects is known as specificity [2].

$$Specificity = \frac{T.N}{T.N+F.P} \quad (17)$$

- *F1-Score:*

It represents the harmonic mean of precision and recall, generating a single metric that balances both of these factors. The F1-Score is especially beneficial when you need to find a compromise between minimizing false positives (precision) and minimizing false negatives (recall) [12].

$$F1 - Score = 2 \times \frac{Precision\ x\ Recall}{Precision + Recall} \quad (18)$$

- *Area Under the ROC Curve (AUC-ROC):*

A measure of the model’s ability to distinguish between fraudulent and legitimate transactions. When a model's curve approaches the upper-left corner of the ROC space, it indicates a high true positive rate and a low false positive rate, which is indicative of greater performance. Conversely, its performance worsens as it approaches the 45-degree diagonal line, which represents a random classifier. In (Figure 5), This metric plots the true positive rate (TPR) on the y-axis and the false positive rate (FPR) on the x-axis to get the AUC for each threshold value between 0 and 1. The likelihood that a positive real class outcome will be predicted as a positive class by the model is shown by the Receiver Operating Characteristic (ROC) curve and the AUC [1], [6].

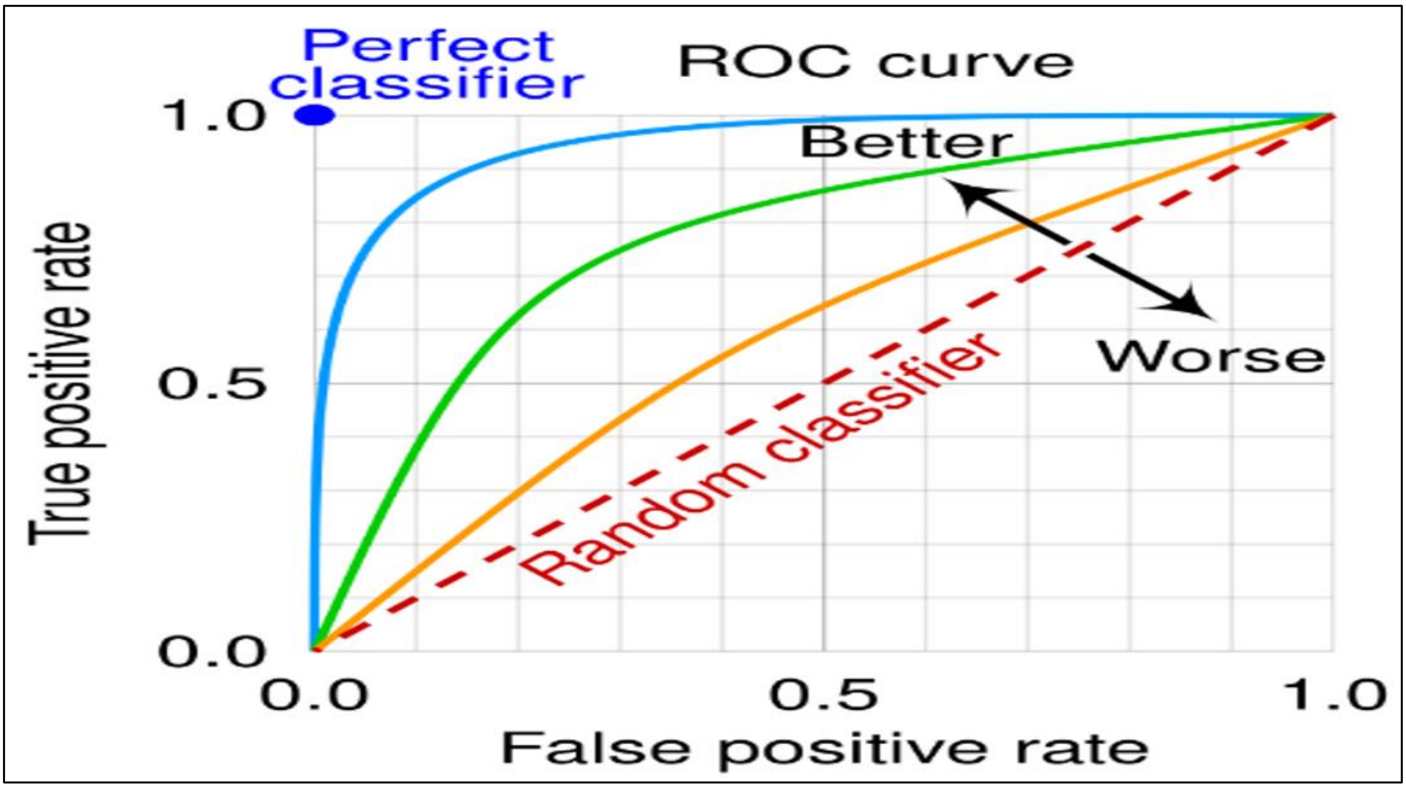

Fig 5 ROC Curve

IV. RESULTS AND DISCUSSION

A. Model Performance

The results of performance evaluation of selected ML algorithms over chosen metrics.

For the Logistic Regression model, the confusion matrix showed that the model correctly identified 18,133 fraudulent transactions as True Positives (TP), while it failed to detect 425 fraudulent transactions, resulting in False Negatives (FN). The model also mistakenly flagged 329 non-fraudulent transactions as fraudulent, which were recorded as False Positives (FP) (Figure 6 and Table 4). On the other hand, it correctly identified 1,109 legitimate transactions as True Negatives (TN) [29].

Table 4 Evaluation of Logistic Regression.

	Precision	**Recall**	**F1-score**
0	-0.98	-0.98	-0.98
1	-0.72	-0.77	-0.75
%Accuracy			-0.96
%Macro Avg.	-0.85	-0.87	-0.86
Weighted Avg.	-0.96	-0.96	-0.96

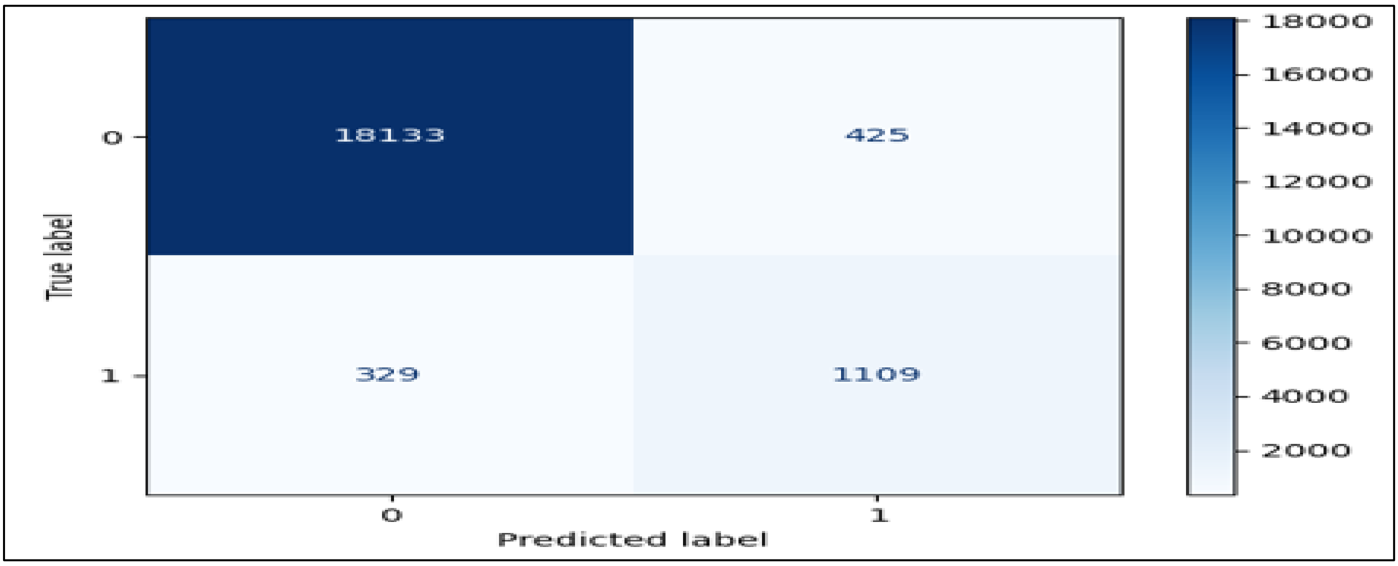

Fig 6 Confusion Matrix for Logistic Regression.

The Decision Tree model performed slightly differently, with 18,175 True Positives and 383 False Negatives. This model had a better performance in terms of True Negatives with 1,173 correctly identified legitimate transactions, but there were also fewer false positives. (FP) 265 compared to the Logistic Regression model. This suggests that the Decision Tree model may have been slightly more conservative in flagging fraudulent transactions (Figure 7 and Table 5).

Table 5 Evaluation of Decision Tree.

	Precision	**Recall**	**F1-score**
0	-0.99	-0.98	-0.98
1	-0.75	-0.82	-0.78
%Accuracy			-0.97
%Macro Avg.	-0.87	-0.90	-0.88
Weighted Avg.	-0.97	-0.97	-0.97

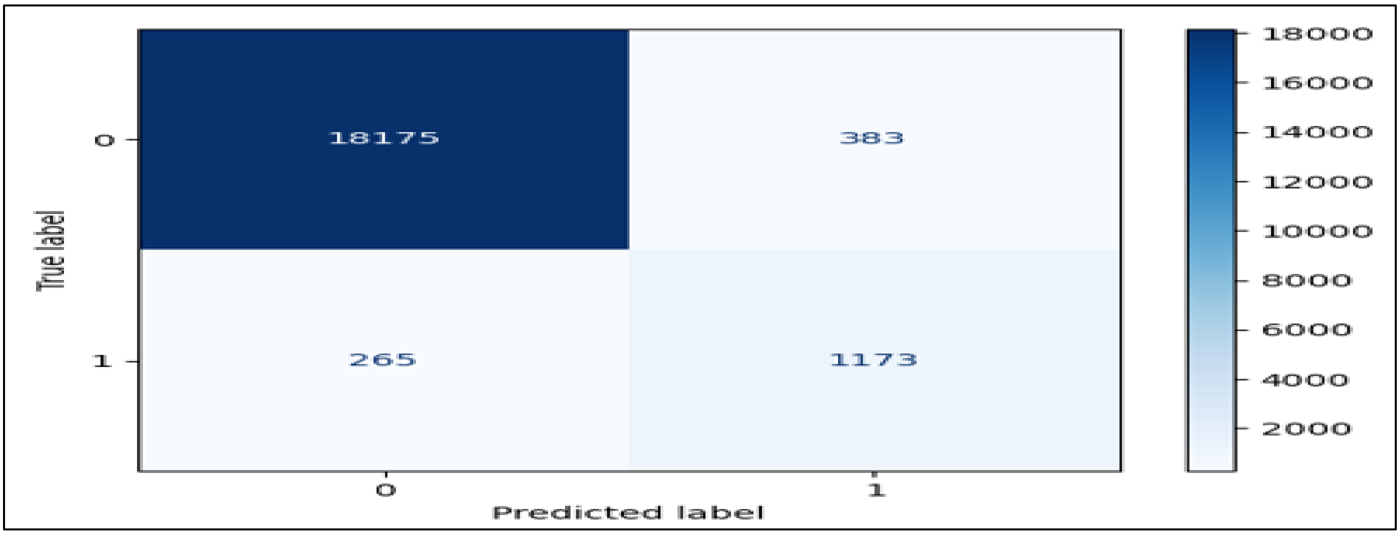

Fig 7 Confusion Matrix for Decision Tree.

The Random Forest model had the fewest false negatives (179) and the greatest number of true positives (18,379), indicating it was particularly effective at identifying fraudulent transactions. However, it did flag 285 legitimate transactions as fraudulent (False Positives) and correctly identified 1,153 True Negatives. The Random Forest model's ability to successfully detect fraudulent transactions while keeping an appropriately balanced False Positive rate suggests it could offer a better trade-off between detecting fraud and reducing the risk of false alarms compared to the other two models (Figure 8 and Table 6).

Table 6 Evaluation of Random Forest.

	Precision	**Recall**	**F1-score**
0	-0.98	-0.99	-0.99
1	-0.87	-0.80	-0.83
%Accuracy			-0.98
%Macro Avg.	-0.93	-0.90	-0.91
Weighted Avg.	-0.98	-0.98	-0.98

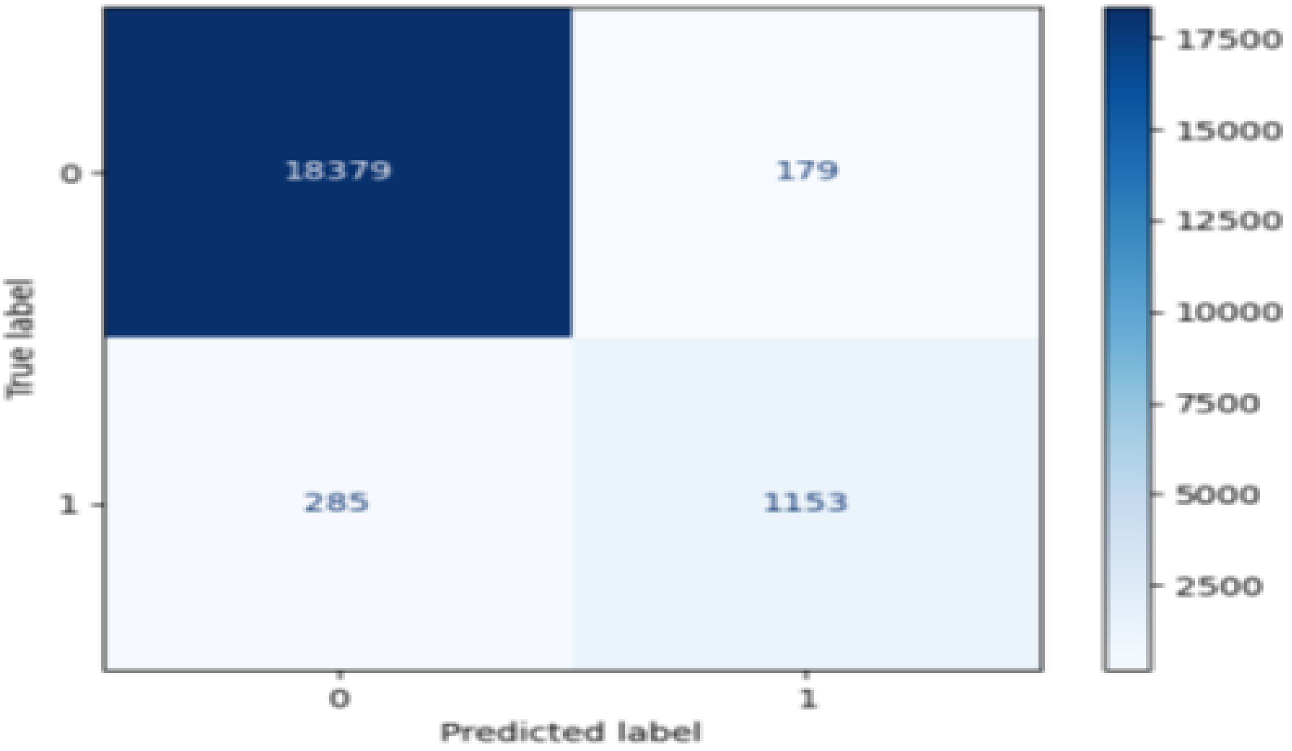

Fig 8 Confusion Matrix for Random Forest.

The XGBoost model exhibited the highest number of True Positives 18,369 and the lowest number of False Negatives 189, indicating it was particularly effective at identifying fraudulent transactions. However, it did flag 284 legitimate transactions as fraudulent (False Positives) and correctly identified 1,154 True Negatives (Figure 9 and Table 7).

Table 7 Evaluation of XGBoost.

	Precision	**Recall**	**F1-score**
0	-0.98	-0.99	-0.99
1	-0.86	-0.80	-0.83
%Accuracy			-0.98
%Macro Avg.	-0.92	-0.90	-0.91
Weighted Avg.	-0.98	-0.98	-0.98

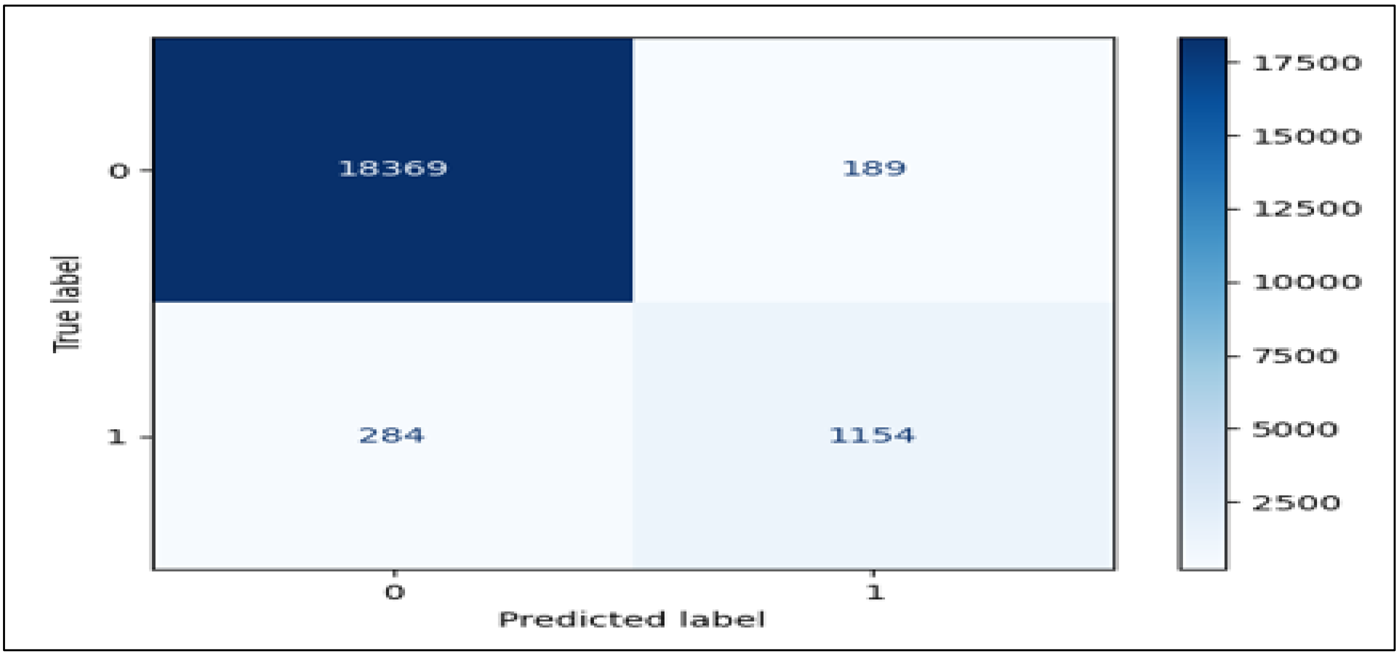

Fig 9 Confusion Matrix for XGBoost.

For the KNN model, the confusion matrix showed that the model correctly identified 18,343 fraudulent transactions as True Positives (TP), while it failed to detect 215 fraudulent transactions, resulting in False Negatives (FN). The model also mistakenly flagged 510 non-fraudulent transactions as fraudulent, which were recorded as False Positives (FP) (Figure 10 and Table 8). On the other hand, it correctly identified 928 legitimate transactions as True Negatives (TN)[29].

Table 8 Evaluation of KNN.

	Precision	Recall	F1-score
0	-0.97	-0.99	-0.98
1	-0.81	-0.65	-0.72
%Accuracy			-0.97
%Macro Avg.	-0.89	-0.82	-0.85
Weighted Avg.	-0.96	-0.96	-0.96

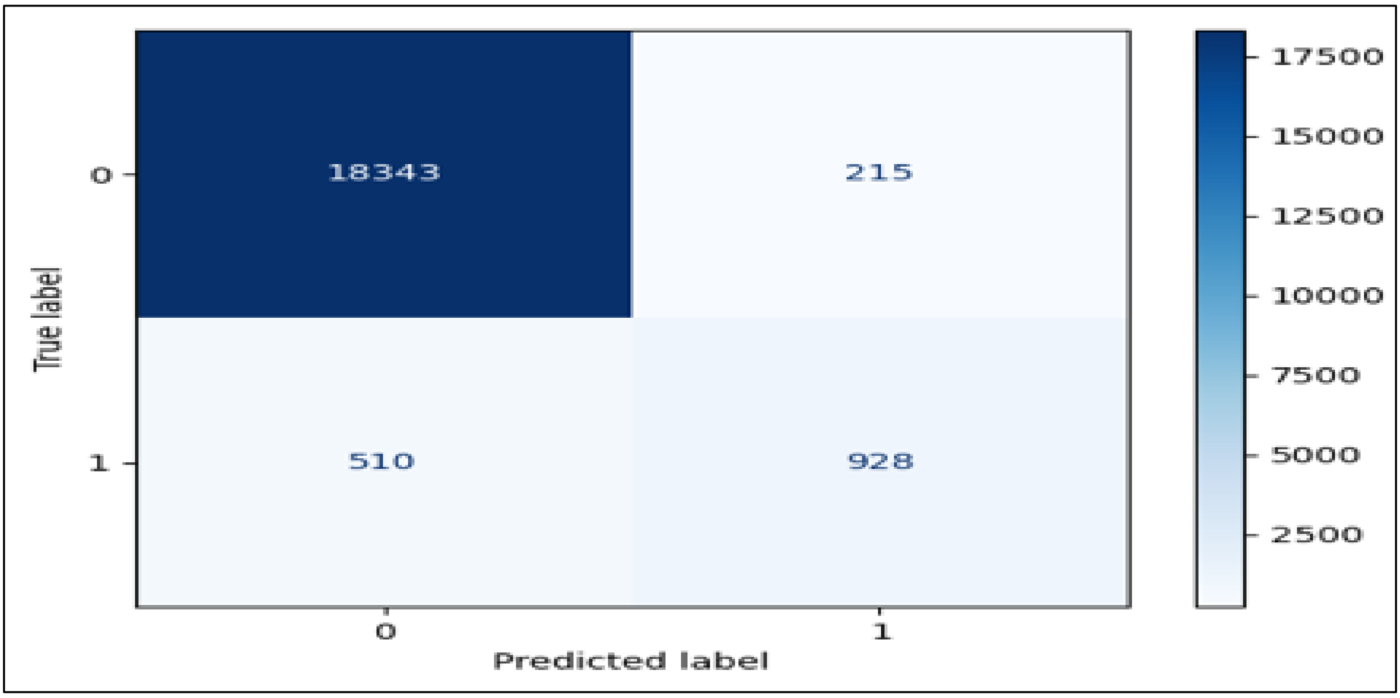

Fig 10 Confusion Matrix for KNN.

The Voting Classifier model exhibited the lowest number (Figure 9 and Table 9) of True Positives 18,372 and the lowest number of False Negatives 186, indicating it was particularly effective at identifying fraudulent transactions. However, it did flag 276 legitimate transactions as fraudulent (False Positives) and correctly identified 1,162 True Negatives. (Figure 11 and Table 9).

Table 9 Evaluation of Voting Classifier.

	Precision	Recall	F1-score
0	-0.99	-0.99	-0.99
1	-0.86	-0.81	-0.83
%Accuracy			-0.98
%Macro Avg.	-0.92	-0.90	-0.91
Weighted Avg.	-0.98	-0.98	-0.98

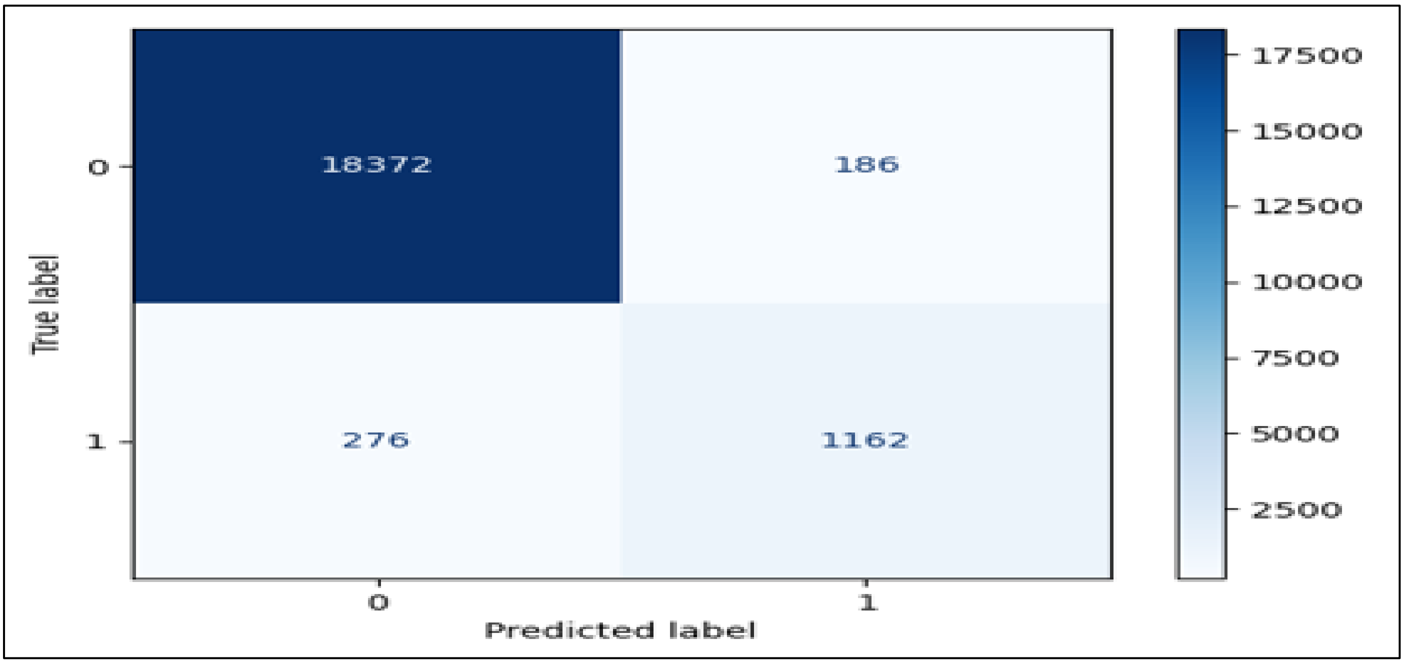

Fig 11 Confusion Matrix for Voting Classifier.

Table 10 Comparison of all machine learning algorithms.

Model	Accuracy	Precision(NF)	Precision(F)	Recall(NF)	Recall(F)
L.R.	97%	0.98	0.77	0.98	0.75
D.T.	97%	0.98	0.78	0.98	0.79
R.F.	98%	0.98	0.91	0.99	0.77
XGBoost	98%	0.98	0.91	0.99	0.78
KNN	97%	0.98	0.82	0.99	0.71
V.T.	98%	0.99	0.86	0.99	0.81

Based on the analysis of fraud cases, a total of 7,192 fraudulent transactions were identified, comprising 7.19% of all transactions. All the ML algorithms give the accuracy above then 97% (Table 10). (Figure 11) shows the majority (98.2%) of fraud cases originated from the United Kingdom, with Visa cards being the most commonly used (60.1%) in (Figure 12). The" Children" merchant group was the most targeted, representing 17.8% of fraud cases (Figure 13). Fraudulent transactions were mostly linked to the" CVC" entry mode (44.5%) and predominantly occurred in online transactions, showing a perfect correlation between fraud and online activity (Figure 14). The highest frequency of fraud occurred on Tuesdays and Wednesdays, with transactions peaking between 12 AM and 5 AM (Figure 15). Males accounted for 59.4% of fraudulent transactions (Figure 16). Most fraudulent transactions involved relatively small amounts, with an average of 63.89 and a median of 21.00 for fraudulent transaction and 32.00 for non-fraudulent transactions. Additionally, a discrepancy was noted between the country of transaction and the country of residence, indicating that many fraudsters likely operate from abroad to avoid detection. (Figure 17 shows the median age for individuals involved in fraudulent transactions being 44.9 provides an important demographic insight. According to the median age of 44.9, people in their mid-40s are most frequently linked to fraudulent transactions. (Figure 18) Shows the merchant group with the highest number of fraudulent transactions is 'Children'. The card type that is most commonly involved in fraudulent transactions is 'Visa.'

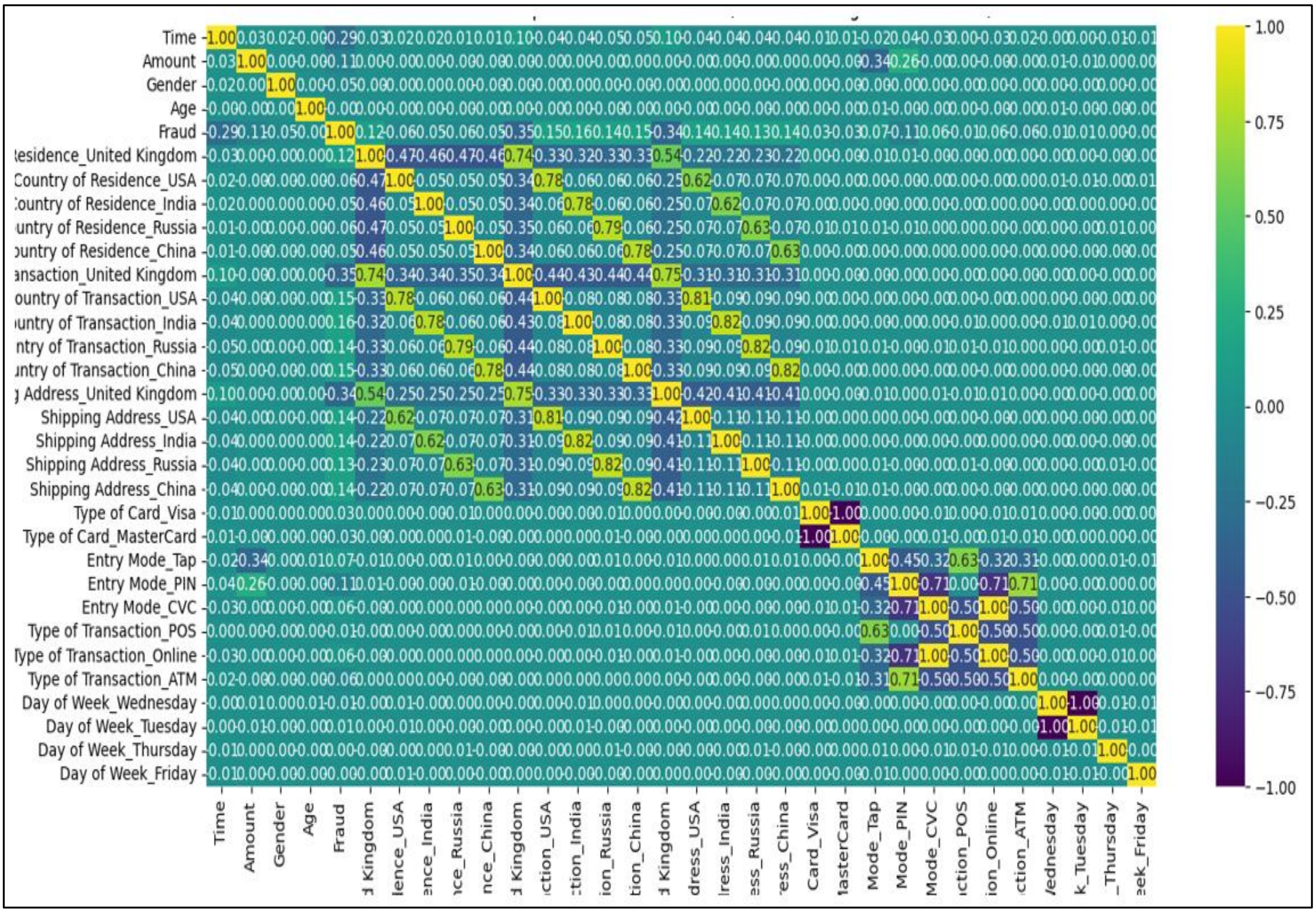

Fig 12 Correlation Heatmap for Numeric Columns (Encoded Categorical Variables).

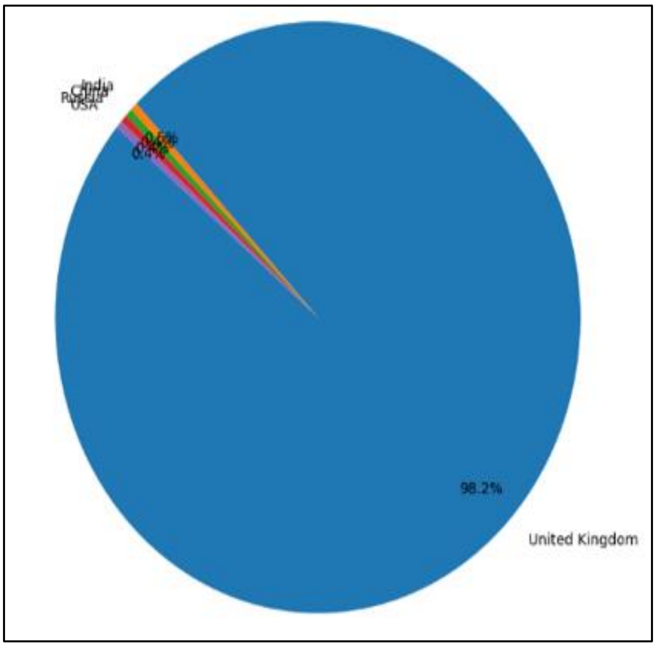

Fig 13 Fraudulent Transaction Country of Residence.

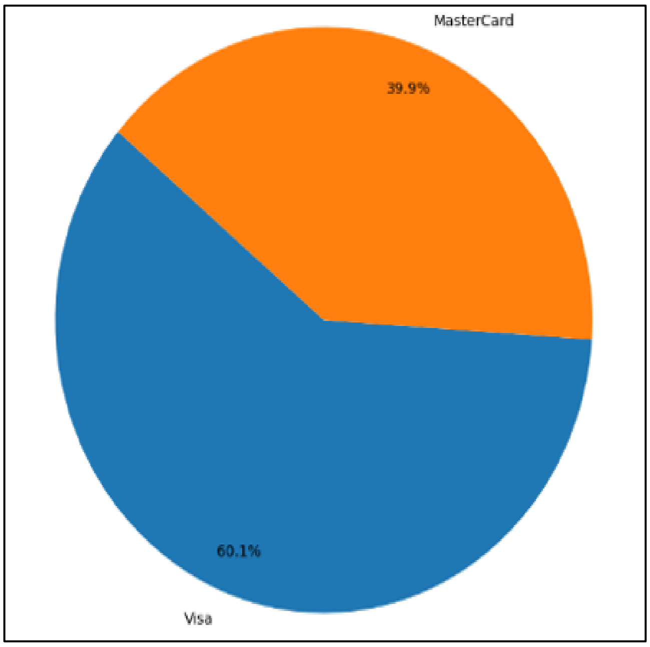

Fig 14 Fraudulent Transaction by Type of Card.

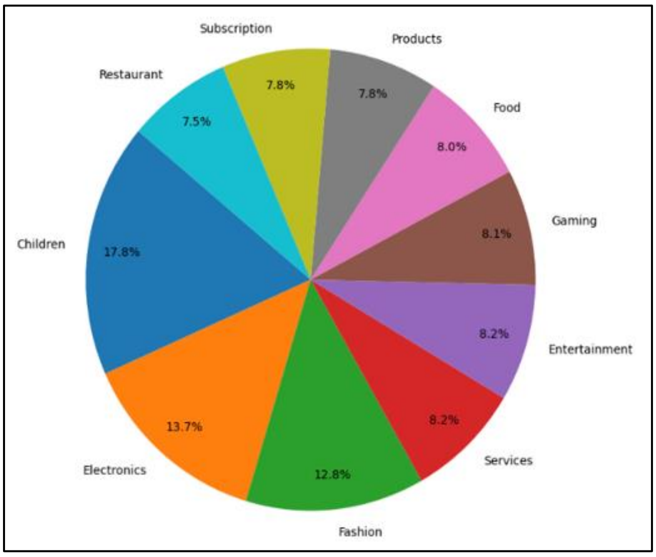

Fig 15 Fraudulent Transaction Across Merchant Categories.

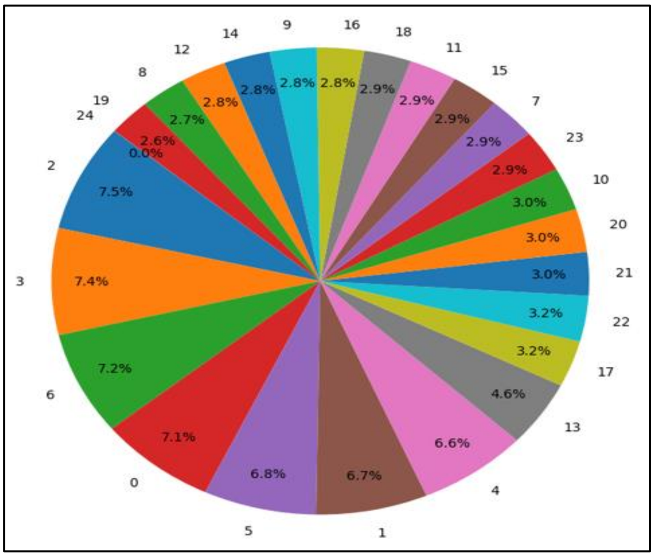

Fig 17 Fraudulent Transaction by Time in Hours.

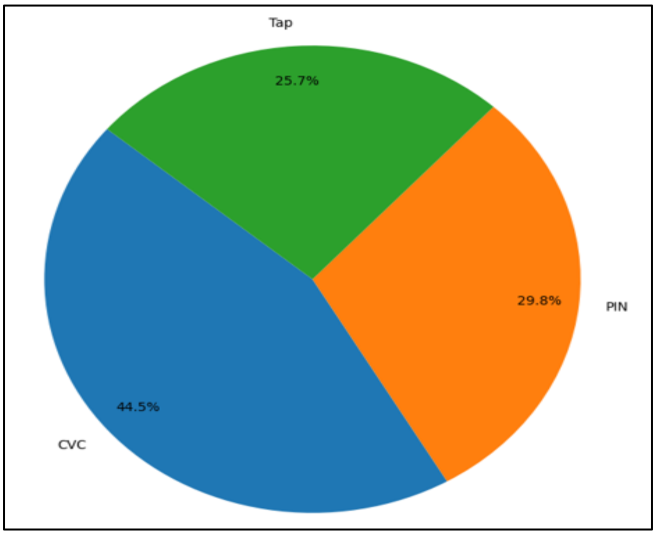

Fig 16 Fraudulent Transaction by Entry Mode.

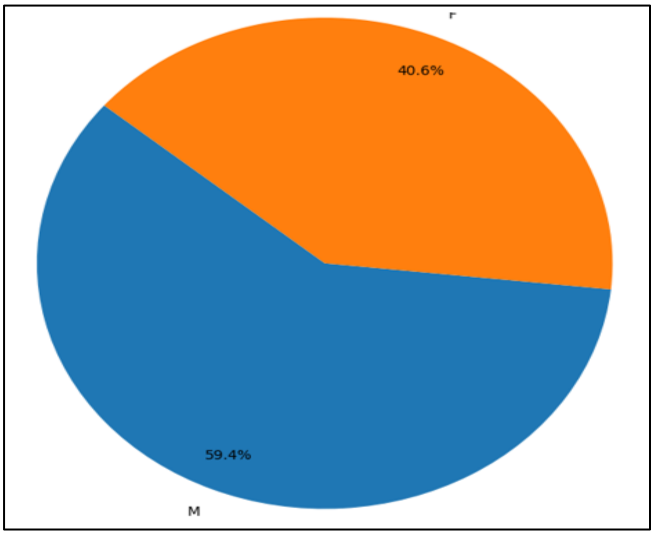

Fig 18 Fraud Status by Gender.

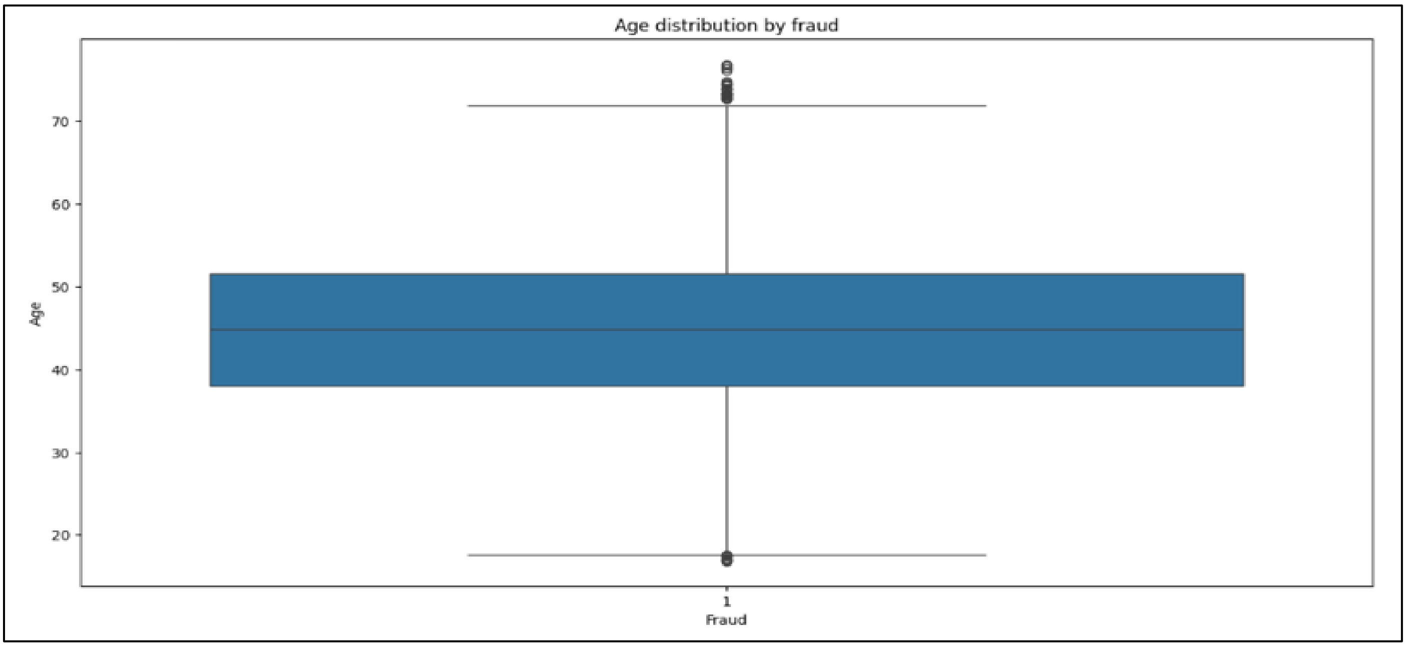

Fig 19 Distribution of Age Group and Fraud Status.

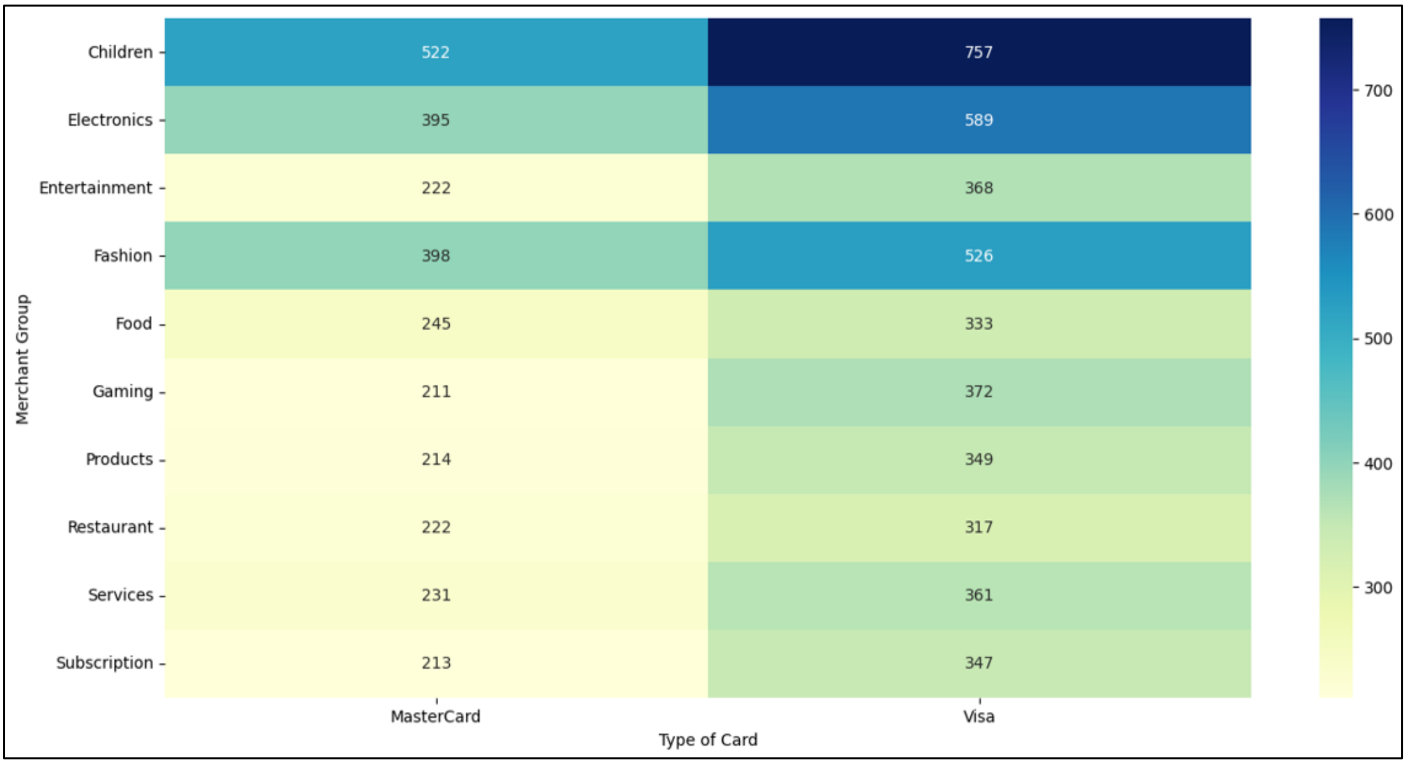

Fig 20 Heatmap of Fraud Merchant Group and Card Type.

The AUC and ROC curves for each model are shown in Figure 20. The Voting Classifier model, with an AUC of 99.14%, comes in second to the XGBoost model, which has the highest AUC at 99.18%. The AUC of the Random Forest model is 99.05%, whereas the AUC of the Logistic Regression model is 97.70%. The KNN and Decision Tree models shows the lower AUC scores value with 90.74% and 89.75%. This information shows that the XGBoost and Voting Classifier models is more useful in detect fraud transactions because the False Positive (FP) rate and True Positive (TP) rate were close to 1(100%).

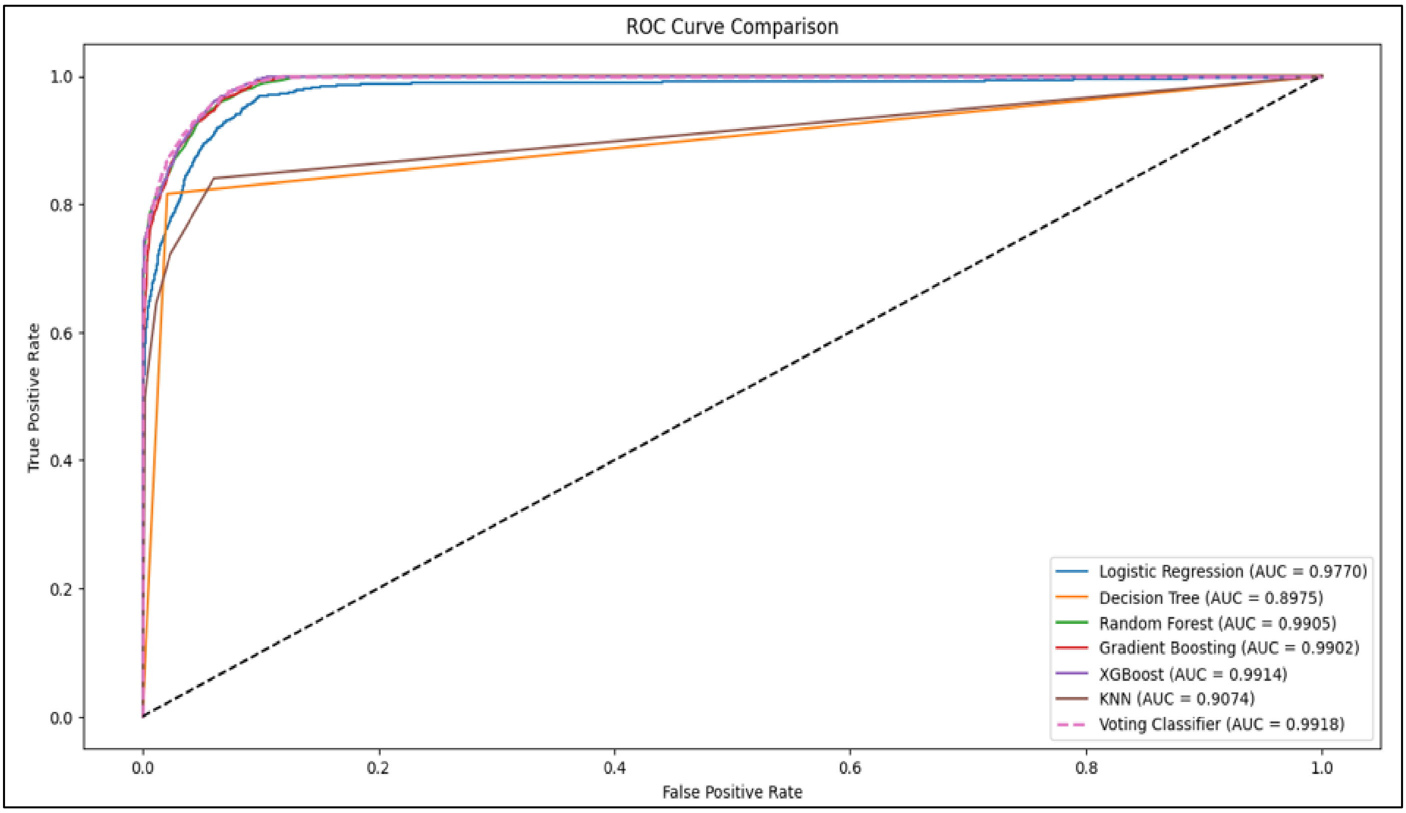

Fig 21 AUC and ROC for Comparison.

➢ *Discussion*

The assessment of the six ML models (Logistic Regression, Decision Tree, Voting Classifier, XGBoost, KNN and Random Forest) was conducted using a variety of metrics such as precision, accuracy, recall, and F1-score. These metrics provide a clear indication of how well the models performed in distinguishing fraudulent transactions from non-fraudulent ones. The results obtained from our models are similar in some respects to those found in previous studies, but some discrepancies may be attributed to differences in the datasets, features, and model configurations. Several studies, such as those by (Jiang and Broby, 2021) and (Al Smadi and Min, 2020), have also explored ML for fraud detection and reported comparable findings, though with some notable variations.

V. CONCLUSION

With a focus on real-time applications, this study presents a machine learning-based methodology for identifying fraudulent credit card transactions. The study results demonstrate that ML models, particularly XGBoost and Voting Classifier, significantly outperform traditional fraud detection methods. These models provide a flexible, responsive, and scalable approach to addressing the issues of credit card fraud detection. The models' limitations, such as high False Positive (FP) rates and issues with imbalanced data, point to the need for further improvements in data pre-processing, feature engineering, and model optimization.

ACKNOWLEDGEMENT

We acknowledge the creators of the publicly available credit card transaction dataset, which made this study possible. There is no funding available. Data information is shared and provided on request.

REFERENCES

[1]. C. Jiang and D. Broby, "Mitigating cybersecurity challenges in the financial sector with artificial intelligence," 2021, Accessed: Nov. 24, 2024. [Online]. Available: https://pure.ulster.ac.uk/files/98691946/Jiang_Broby_CeFRI_2021_Mitigating_cybersecurity_challenges_in_the_financial_sector_with_Artificial_Intelligence.pdf

[2]. S. Morgan, "2021 Report: Cyberwarfare In The C-Suite," Cybercrime Facts and Statistics, 2021. Accessed: Nov. 24, 2024. [Online]. Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[3]. S. Morgan, "Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021," Cybercrime Magazine, 2019, Accessed: Nov. 24, 2024. [Online]. Available: https://cybersecurityventures.com/cybersecurity-market-report/

[4]. E. Btoush, X. Zhou, R. Gururaian, K. C. Chan, and X. Tao, "A survey on credit card fraud detection techniques in banking industry for cyber security," in 2021 8th International Conference on Behavioral and Social Computing (BESC), IEEE, 2021, pp. 1–7.

[5]. B. Al Smadi and M. Min, "A critical review of credit card fraud detection techniques," in 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE, 2020, pp. 732–736.

[6]. N. K. Trivedi, S. Simaiya, U. K. Lilhore, and S. K. Sharma, "An efficient credit card fraud detection model based on machine learning methods," International Journal of Advanced Science and Technology, vol. 29, no. 5, 2020.

[7]. I. Benchaji, S. Douzi, and B. El Ouahidi, "Credit card fraud detection model based on LSTM recurrent neural networks," Journal of Advances in Information Technology, vol. 12, no. 2, 2021, doi: 10.12720/jait.12.2.113-118.

[8]. E. M. H. Al Rubaie, "Improvement in credit card fraud detection using ensemble classification technique and user data," International Journal of Nonlinear Analysis and Applications, vol. 12, no. 2, 2021, doi: 10.22075/IJNAA.2021.5228.

[9]. I. D. Mienye and N. Jere, "Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions," IEEE Access, 2024.

[10]. G. J. Priya and S. Saradha, "Fraud detection and prevention using machine learning algorithms: A review," in Proceedings of the 7th International Conference on Electrical Energy Systems, ICEES 2021, 2021. doi: 10.1109/ICEES51510.2021.9383631.

[11]. A. Pumsirirat and L. Yan, "Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine," International Journal of Advanced Computer Science and Applications, vol. 9, no. 1, 2018, doi: 10.14569/IJACSA.2018.090103.

[12]. M. Zareapoor, Seeja. K. R. Seeja.K.R, and M. Afshar Alam, "Analysis on Credit Card Fraud Detection Techniques: Based on Certain Design Criteria," Int J Comput Appl, vol. 52, no. 3, 2012, doi: 10.5120/8184-1538.

[13]. U. Rajeshwari and B. S. Babu, "Real-time credit card fraud detection using Streaming Analytics," in Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology, iCATccT 2016, 2017. doi: 10.1109/ICATCCT.2016.7912039.

[14]. N. Sethi and A. Gera, "A Revived Survey of Various Credit Card Fraud Detection Techniques," International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, 2014.

[15]. S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random forest for credit card fraud detection," in 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), IEEE, Mar. 2018, pp. 1–6. doi: 10.1109/ICNSC.2018.8361343.

[16]. R. Jain, B. Gour, and S. Dubey, "A Hybrid Approach for Credit Card Fraud Detection using Rough Set and Decision Tree Technique," Int J Comput Appl, vol. 139, no. 10, 2016, doi: 10.5120/ijca2016909325.

[17]. J. K. Afriyie et al., “A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions,” Decision Analytics Journal, vol. 6, p. 100163, 2023.

[18]. L. Theodorakopoulos, A. Theodoropoulou, F. Zakka, and C. Halkiopoulos, “Credit Card Fraud Detection with Machine Learning and Big Data Analytics: A PySpark Framework Implementation,” 2024.

[19]. S. E. Sorour, K. M. AlBarrak, A. A. Abohany, and A. A. Abd El-Mageed, “Credit card fraud detection using the brown bear optimization algorithm,” Alexandria Engineering Journal, vol. 104, pp. 171–192, 2024.

[20]. S. Tyagi and S. Mittal, “Sampling approaches for imbalanced data classification problem in machine learning,” in Proceedings of ICRIC 2019: Recent innovations in computing, Springer, 2019, pp. 209–221.

[21]. I. D. Mienye and N. Jere, “Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions,” IEEE Access, 2024.

[22]. K. K. Renganathan, J. Karuppiah, M. Pathinathan, and S. Raghuraman, “Credit card fraud detection with advanced graph based machine learning techniques,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 35, no. 3, p. 1963, 2024.

[23]. H. Sinha, “An examination of machine learning-based credit card fraud detection systems,” International Journal of Science and Research Archive, vol. 12, no. 2, pp. 2282–2294, 2024.

[24]. L. Theodorakopoulos, A. Theodoropoulou, F. Zakka, and C. Halkiopoulos, “Credit Card Fraud Detection with Machine Learning and Big Data Analytics: A PySpark Framework Implementation,” 2024.

[25]. S. Bagga, A. Goyal, N. Gupta, and A. Goyal, “Credit card fraud detection using pipeling and ensemble learning,” Procedia Comput Sci, vol. 173, pp. 104–112, 2020.

[26]. M.-Y. Chen, “Bankruptcy prediction in firms with statistical and intelligent techniques and a comparison of evolutionary computation approaches,” Computers & Mathematics with Applications, vol. 62, no. 12, pp. 4514–4524, 2011.

[27]. N. Rtayli and N. Enneya, “Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization,” Journal of Information Security and Applications, vol. 55, p. 102596, 2020.

[28]. T. C. Tran and T. K. Dang, “Machine learning for prediction of imbalanced data: Credit fraud detection,” in 2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM), IEEE, 2021, pp. 1–7.

[29]. J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, “Credit card fraud detection using machine learning techniques: A comparative analysis,” in Proceedings of the IEEE International Conference on Computing, Networking and Informatics, ICCNI 2017, 2017. doi: 10.1109/ICCNI.2017.8123782.