# Harnessing Machine Learning to Detect and Prevent Credit Card Fraud

1st Hariom Singh
*School of computer science and engineering,*
*Sandip University*
Nashik, India
hariomvimal33333@gmail.com or https://orcid.org/0009-0000-5649-8459

2nd Mritunjay Kr Ranjan
*School of computer science and engineering,*
*Sandip University*
Nashik, India
mritunjaykranjan@gmail.com or https://orcid.org/0000-0003-0240-4909

3rd Pritam Soni
*Anishk Sustanable Development Foundation,*
*Korba, Chhatishgarh.*
Korba, India
pritamsoni3317@gmail.com or https://orcid.org/0009-0000-2905-8300

4th Vivek Shriwas
*Chemistry department, Shri Rawatpura Sarkar University*
Raipur, India
vivekshriwas14@gmail.com or https://orcid.org/0009-0001-6054-8823

5th Prasad Gadekar
*School of computer science and engineering, Sandip University*
Nashik, India
prasad01198@gmail.com or https://orcid.org/0009-0004-2628-482X

6th Sushil Panthi
*School of computer science and engineering, Sandip University*
Nashik, India
npanthi718@gmail.com or https://orcid.org/0009-0005-1259-8518

***Abstract*—This study investigates the utilization of machine learning algorithms to detect fraudulent credit card transactions in real-time with a dataset that includes transaction amounts, timestamps and other anonymized features. This research compares different models in terms of performance to catch fraud transactions, such as logistic regression, random forest. Looking ahead, it is observed in the analysis that some specific anonymized features, especially 'V17', 'V14', and 'V10', become important to predict fraudulent activity. Random Forest was the top-performing model, with better accuracy and precision and a sharp decrease in false positives. The study highlights the necessity of feature selection and data preprocessing that can improve model performance on such problems. This research is able to shed light on different ways that fraud detection systems can be made more effective in the financial sector. Implementing machine learning models with these systems is also capable of making a huge improvement in fraud prevention, which could provide more secure transactions and reduce financial loss significantly. Furthermore, the increased accuracy and speed of these models help increase customer confidence and satisfaction in financial institutions, strengthening them against advancing fraud methods. We are demonstrating that our system can enable the next generation of more accurate and much larger-scale AV fraud detection tools to be implemented based on current real-time data provided by the Multi-ETL cluster. Previously, OMV machines were known for their high scalability.**

***Keywords*—*Machine Learning, Credit Card, Detect, Prevent, Fraud***

## I. Introduction

This Credit card fraud is a major issue for the financial world, costing billions of dollars in annual losses. In an era of increasing online transactions, the sophistication level of fraudulent activity continues to rise [1]. The age-old manual reviews and rule-based systems are now obsolete for detecting fraud and cannot endure through traditional methods any longer [2]. These approaches are typically unable to identify novel kinds of fraud patterns and do not scale well against the huge volumes of data that modern, highly wired financial systems produce. Instead, machine learning allows us to automate the detection of complex patterns in large datasets. Using historical data, they can be trained to detect fraudulent transactions with good results (<95%) and adjust themselves for new fraud tactics. The aim of this study is to use several sophisticated machine learning classifiers to solve the problem of credit card fraud detection and assess their performance at detecting fraudulent activities while debating what it means for the financial sector. This histogram is useful as a broad look into the data and shows us that fraud cases represent less than 1 % of all transactions in our dataset. Understanding more about this distribution allows us to properly decide which statistical approach we can use, such as whether local outliers will be used for anomaly detection.

If we know how the transactions are distributed over time, we can see a sense of magnitude and why it is important to develop good fraud detection systems [3]. It (Fig.1) a sequence of histograms that convey the distribution of some attributes in a credit card fraud detection dataset. The 'Time' feature shows a wide spread of transaction times, which presents activity levels across periods in detail. The general features, 'V1' to 'V28', exhibit a bell-shaped distribution. Certain features, such as V17, V14, and feature '10', appear to be good predictors of fraudulent activity. The variable amount is right-skewed as there are fewer outliners and most of the transactions lie beneath lower values. We also consider these distributions when fitting machine learning models (random forests or support vector machines) to detect fraudulent transactions, as they reveal valuable information about the data. The variability and particular patterns in those attributes make it important to choose the right features and do processing on them, which will eventually increase our model's capability for the true detection of fraudulent transactions.

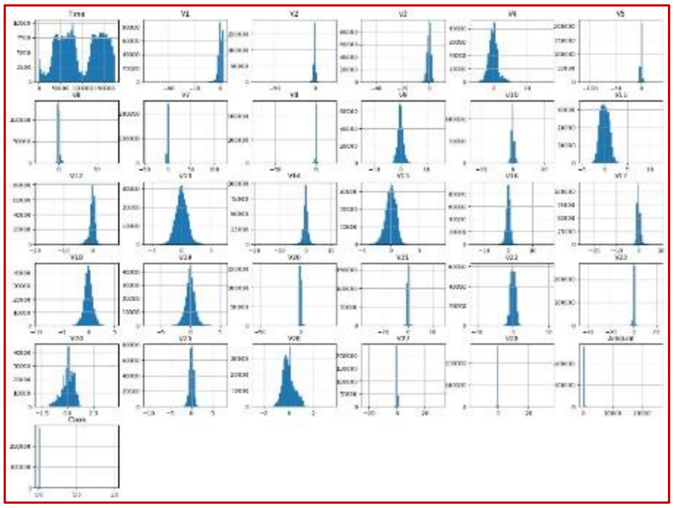

Fig. 1. Histogram of the dataset as per the transaction history

Objective:

- To evaluate the performance of machine learning models in detecting credit card fraud.
- To analyze the impact of feature selection and data preprocessing on fraud detection accuracy.
- To develop a robust machine learning framework to enhance fraud detection and reduce false positives in financial systems.

## II. Related Study

TABLE I. Comparative study based on Objective, Methods, Findings & Research Gap

| Objective | Methods | Findings | Research Gap |
|---|---|---|---|
| To create a neural network-based credit card fraud detection system. [4] | Neural Networks | Demonstrated the potential of neural networks in identifying fraudulent patterns in credit card transactions. | Limited to early-stage neural network capabilities with less focus on feature engineering. |
| To compare credit card fraud detection data mining methods. [5] | Decision Trees, Random Forest, Logistic Regression, and Bayesian Networks | Found Random Forest to be more effective compared to other methods in detecting fraud. | Relatively small dataset; lacked focus on feature selection's impact. |
| To create a scalable real-time credit card transaction fraud detection system. [6] | Spark, Random Forest, Streaming Algorithms | Successfully implemented a scalable, real-time fraud detection framework with high accuracy. | Focused mainly on Spark; limited exploration of other potential scalable solutions. |
| To test decision trees and SVM for credit card fraud detection. [7] | Decision Trees, Support Vector Machines (SVM) | Both models performed well, with SVM slightly outperforming decision trees in accuracy. | No consideration of deep learning models; feature importance not deeply analyzed. |
| To examine fraud detection methods, including credit card fraud. [8] | Literature Review, Comparative Analysis | Provided a comprehensive overview of fraud detection techniques and their application in credit card fraud. | Primarily a survey without empirical evaluation; older methods focused on traditional techniques. |
| Use delayed supervised information to address credit card fraud concept drift. [9] | Concept Drift Algorithms, Random Forest | Developed methods to adapt fraud detection models to evolving fraudulent behaviour, improving long-term detection rates. | Focused on concept drift; limited exploration of other evolving factors affecting fraud detection. |
| To examine how transaction aggregation affects fraud detection. [10] | Logistic Regression, Aggregated Features | Showed that aggregating transactions over time can significantly enhance detection accuracy. | Aggregation may lead to data loss; limited evaluation of other machine learning techniques. |

## III. Problem Statement

Credit card fraud is a rising financial problem and causes significant losses to consumers, businesses and financial institutions. Traditional rule-based fraud detection systems are inadequate at identifying new patterns perpetrated by sophisticated fraudsters. These approaches have a high level of false positives due to their inability to adapt to new fraud patterns. We are in dire need of better tools for an adaptative real-time solution that can properly identify credit card fraud and, at the same time, decrease false positives. A surge in computation will be needed to analyze millions of transactions, detect the patterns behind frauds, and learn from new data continuously so that next time there is an attack, we are prepared. This paper presents a data science initiative to create an elastic, online machine learning engine that natively prevents credit card fraud using prediction. To guide decisions about what data is processed and needs to be done quickly in milliseconds so that legitimate transactions are not rejected, and fraud gets through. The system works to enhance credit card security with the hopes of providing better fraud prevention, stopping losses from financial institutions, and keeping consumers trusting those organizations.

## IV. Purposed Methodology

It works by gathering anonymized credit card transaction data and then cleaning the dataset to remove typical challenges of class imbalance or feature engineering. We then train and evaluate these models in a methodical manner to detect fraud. After training various models, the best-performing model is deployed for real-time fraud detection and overtime monitored to be updated with new data in order to keep up against evolving patterns of fraudulent activities.

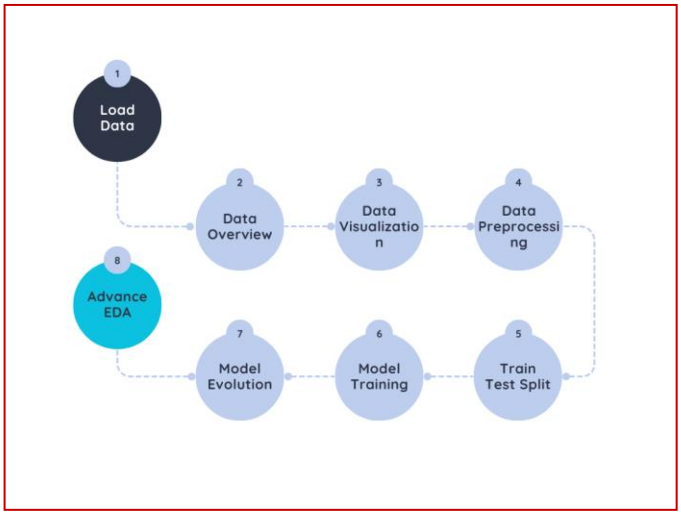

Fig. 2. Work Flow

Algorithm

TABLE II. ALGORITHMIC APPROACH

| | |
|---|---|
| S1. Data Collection<br>S2. Data Preprocessing<br>S3. Model Development | S4. Model Evaluation<br>S5. Deployment<br>S6. Monitoring and Continuous Improvement |

### A. Model Development

A logistic regression model was then built on transaction features to predict the probability that a transaction is fraudulent [11]. This model is also neat and simple, which will help us understand relatively well how each feature affects the chances of fraud. This works best when we have features that are related linearly to our target variable, but it could face difficulty with non-linear and more advanced patterns, which is where things like random forests come into play.

Formalized Mathematically

$$P(Y = 1) = \frac{1}{1 + e^{-(\beta_0+\beta_1 x_1+\beta_2 x_2+\cdots+\beta_n x_n)}} \ldots\ldots\ldots\ldots\ldots\ldots (i)$$

Where:

- $P(Y = 1)$ is the probability that the transaction is fraudlent.
- $x_i$ are the independent variables (transaction features).
- $\beta_i$ are the coefficient that represents the relationship between each independent variable and probability of fraud.

In the case of fraud detection, Random Forest, which is a method based on ensemble learning, was used to create highly accurate models by combining predictions from multiple decision trees [12]. So it was quite useful for us to understand which features were the most relevant and important in order to predict fraud. Random forests are especially good at dealing with high-dimensional data and non-linear relationships between input features and the target variable. Misclassified data points are selected from the training set; they were already fitted for quantitative evaluation and may remedy high-variance issues with individual decision trees since many prediction trees are combined. Having feature importance scores from the model is very useful to know how many features would be labeled as fraud.

$$\hat{y} = \frac{1}{N}\sum_{i=1}^{N} T_i\,(x) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (ii)$$

Where

- $N$ is the number of trees
- $T_i(x)$ is the prediction of the $i$-th tree.

## V. Exploratory Data Analysis (EDA)

The correlation (Fig.3) heatmap below. It can be observed that most of them do not correlate highly among themselves or with respect to the 'Class' feature (which denotes fraud). For one, the 'class' variable maintains quite a low relationship with most features, usually as small as 0.00 to 0. The statement says: “a correlation close to 1.0 at the diagonal with every feature perfectly correlating with itself. [13]” The low correlations are a testament to the challenge of fraud detection; they demonstrate that no single feature is strong enough by itself, meaning it would require quite complex machine learning techniques in order to sufficiently aggregate these weak signals into high-quality predictions of fraudulent transactions.

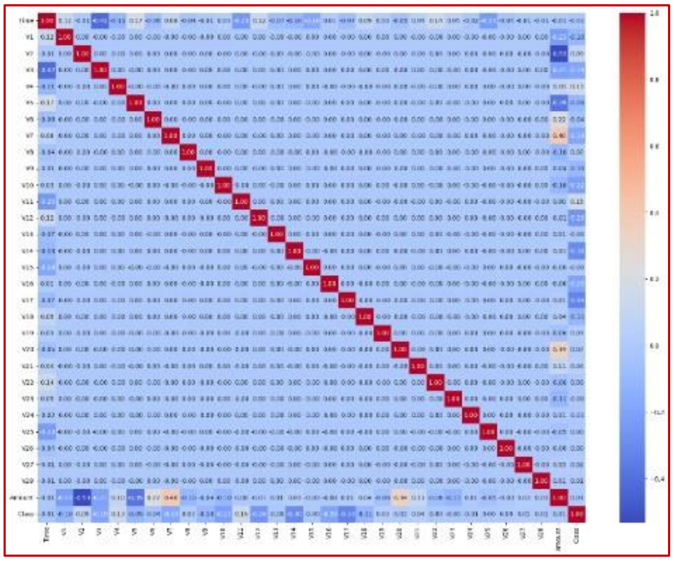

Fig. 3. Co-relational Heatmap

The (Fig.4) shows a comparison of transaction amount distribution and how this can differentiate between legitimate transactions (Class 0) and fraudulent ones (Class 1) for detecting credit card fraud. As per the plot, most fraudulent cases are getting done for well below $2k—ooutliers more than that. Legit transactions, on the other hand, have a wider spread; still, most are under $10,000, but as we can see, they have quite a left and right tail, with outliers up to $25,000. This large deviation from the transaction amount suggests a possibly significant feature for distinguishing fraudulent from legitimate transactions in practical machine learning models. This graph underscores the general pattern of smaller transaction values for fraudulent transactions, which allows machine learning models to more confidently predict whether a novel example is fraud or not [14].

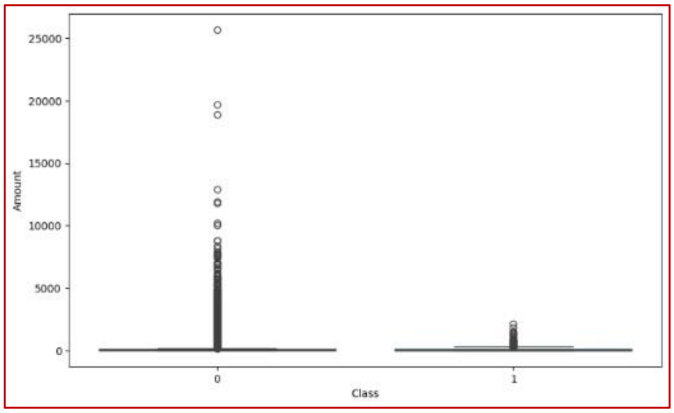

Fig. 4. Box plot Distribution of Transaction

A (Fig.5) correlation heatmap shows how the features within the C redit card fraud detection dataset are related to one another, with the correlation coefficient lying in between -1 and 1. The diagonal of the heatmap shows the correlation between each feature anditself, which is obviously 1.0. The majority of off-diagonal values are near 0, which means that V1 to V28 have a small correlation with each other since the Pearson coefficient varies between -1 (perfect inverse relationship) and +15 (perfect positive relationship). Independence Feature: This feature decreases the multicollinearity in machine learning models. The '0' corresponds to a normal transaction, and '1' means that the transaction was fraudulent. The Class variable is highly unbalanced, with 492 cases of fraud +ve (positive class) and 284315 cases of fraud -ve (negative class), which insha out attempts seem like wrong. The Class variable, V17, exhibits the highest correlation, indicating its significance. The fact that the one-to-one correlations are low suggests dealing with a lot of complexity in coming up with a fraud detection process; there is no single significant feature to help predict if something would be fraudulent or not. Therefore, the machine learning models need to work with combinations of features rather than individual attributes in order to catch fraud. This heatmap shows the gradient class activation maps that advanced models utilize to catch even mild data patterns detectable in fraud transactions [15].

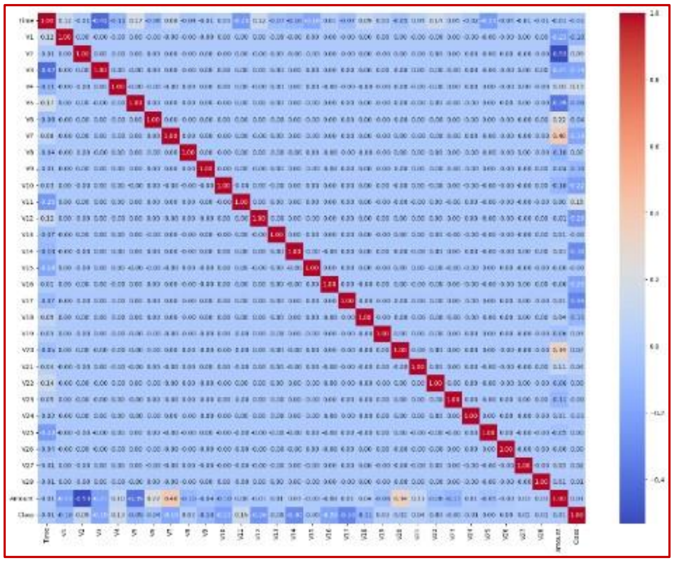

Fig. 5.Correlation Heatmap: Features

The (Fig.6) importance of features in detecting and preventing credit card fraud to building a machine learning model. Visualizing Feature Importance Positive and Negative Contributions In this bar chart, we visually illustrate the importance of each feature (V1 to V28, time, amount) and whether these features contribute positively or negatively to predicting fraudulent transactions. The most important ones are V4, V11 and V2, by far, with a positive importance around the range of 0.3 to 0.25 for them. In contrast, V14 has the lowest value of almost -0.45 and it will also be less influent in the positive sense to auto-conversion class-targeted analysis compared with features like V14, V12, and so on. The feature importance scores tell us how much each of the features contributed to the model predictions, with higher abs values indicating a greater contribution. This chart just helps to underline that different features have diverse importance, and some of them were absolutely necessary for fraud detection on this data (and there was no imbalanced

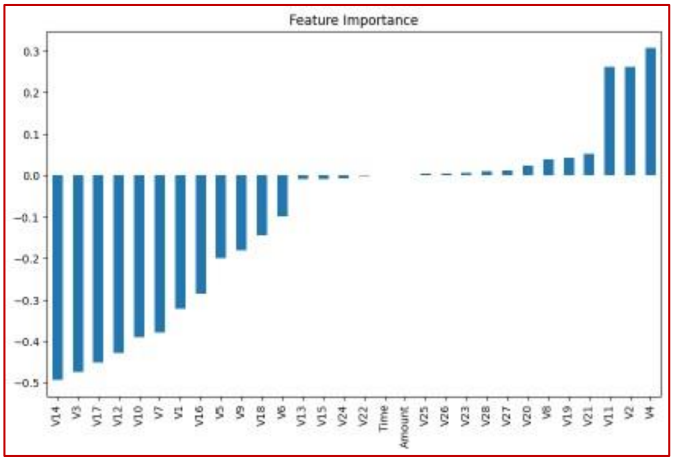

Fig. 6.Bar Chart Features Importance

## VI. Results and Discussion

The (Fig.7) ROC curve that we can see in the picture is from a logistic regression model for credit card fraud detection. The curve shows the true positive rate (TPR) against false positive rates (FPRs) at different thresholds. Our model has an Area Under the Curve (AUC) score of 0.97 and a very high accuracy rate. An AUC of 0.97 means this model is highly capable of identifying fraudulent transactions from legitimate transactions with few false negatives while keeping the rate optimally low. The sharp upward curve heading towards the top left corner points to a high-performing model: being able to sustain an elevated TPR while keeping FPR low—oone of the advantages when applied in fraud detection environments [17].

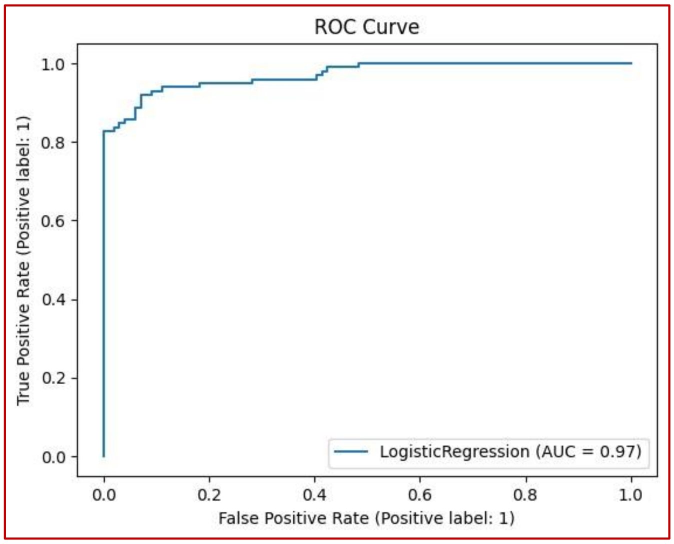

Fig. 7.ROC Curve

### A. Simulation Parameter

TABLE III. Simulation Parameter

| Metric | Value |
|---|---|
| Accuracy | 0.9137056 |
| Precision | 0.9764706 |
| Recall | 0.8469388 |
| F1 Score | 0.9071038 |
| ROC-AUC | 0.9577407 |
| PR-AUC | 0.9685902 |
| Log Loss | 0.2154891 |
| Matthews Correlation Coefficient | 0.834602 |
| Kappa Score | 0.827291 |

Model performance metrics show how well it predicts and prevents credit card fraud. The model accurately classified 91% of transactions as frauds or not frauds with a 0.9137 accuracy. This precision, 97.65%, means that 97.6% of the time, a transaction is fraudulent. With a recall of 0.8469, the model successfully detects ~84.7% of genuine fraud cases. The standard F1 score of 0.907097 balances precision and recall and shows how well our model detects fraud transactions in a sample set or data space. ROC-AUC score 0.9577 shows that the model can distinguish fraudulent and normal transactions, while PR AUC 0.9686 shows how well it handles imbalanced data since fraud detection problems are usually severe class imbalance problems at rates greater than (1:10000). A log loss of 0.2155 indicates that the model's predictions are somewhat uncertain, with lower values being better. The high Matthews Correlation Coefficient (MCC) of 0.8346 and Kappa Score of 0.8273 indicate strong agreement between predicted and actual classes, making it reliable for identifying willing fraud or future false-positive samples. Overall, these metrics suggest that our model can detect credit card fraud well and stop fraudulent charges.

The feature importance scores provided by the Random Forest model highlighted the most critical predictors of fraud. The Fig feature importance values from a machine learning model to build credit card fraud detection and prevention. It is a simple bar chart that ranks the features ( V1 to V28, time, and amount) on the basis of their importance for model prediction. For instance, features like V4, V11 and previous-V2 have high positive importance values around +/- 0.3 for the highest value, which is that of feature-ID number_V4. On the other hand, features V14, V3 to a lesser extent, and finally feature 17 show very negative importance, for example, -0.5. Contribution for the least contributing of them: feature v12. The values represent the strength of influence features have in implementing a decision, where a stronger positive or negative value indicates a higher impact. It illustrates how some features highly contribute to the fraud detection model, while others drive down its predictive powers—cclearly a sign of advanced sophistication when it comes to separating activities that are 'right' from those that are dubious [18].

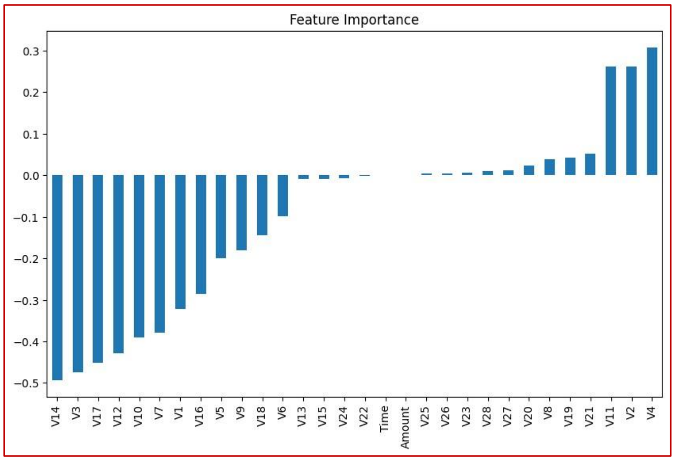

Fig. 8.Bar- Chart Features Importance

### B. Interpretation of Results

The precision-recall curve in the (Fig.9) assesses a logistics regression model in part with regards to recognition as well as prevention of credit card fraud. Here the curve plots precision, which is a ratio of true positive among all predictions that were labeled as positives (true sum),vs. recall or Sensitivity where now we care about not missing actual ones out of all truly existing (positive hang around). It is a high precision and recall curve with an AP (average percentile) score of 0.97, which means that the model effectively captures fraudulent transactions. It shows that the curve is in and around 1.0 almost all over the recall axis, which indicates a high precision model for a higher number of true fraudulent cases being captured as well from about halfway along the recall line. This is as a result of the Q-R combination showing high recall but drastically falling precision rates, which suggests that the model maintains a balance between more fraudulent transactions and a large number of false alarms. In general, this high stated AP score and the shape of the curve are consistent with a model that is well-attuned to effective fraud detection methods that minimize false positives in credit card fraud [19].

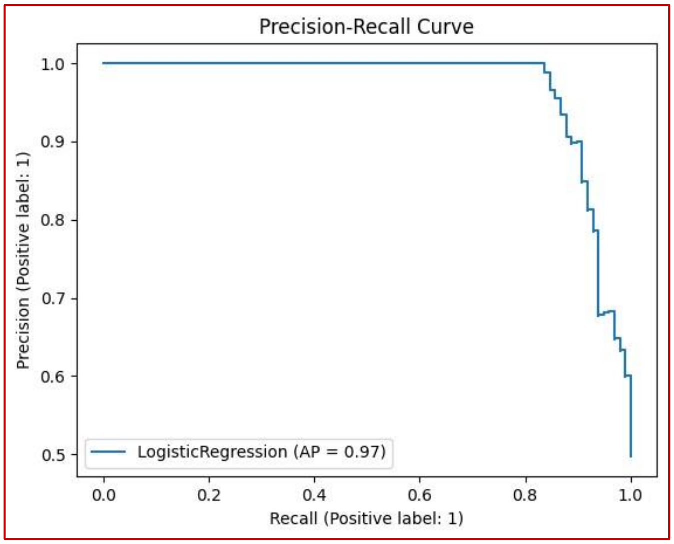

Fig. 9.Precession Recall Curve

## VII. CONCLUSION

The study reveal that credit card fraud can be detected and prevented by exploring the patterns in anonymized transactional data using machine learning models, especially random forests and logistic regression. While both models detected critical predictive attributes such as 'V17,' V14' and 'V10', the Random Forest model performed better in terms of all three performance levels (accuracy, precision, and recall). Such challenges include class imbalance, dynamic fraud patterns and the need for model interpretability. The results highlighted in this study show that financial institutions may add the proposed machine learning methods to their fraud detection systems so as to improve these situations and, therefore, enhance security levels, reduce losses associated with such crimes, and further increase customer confidence. The study also highlights the need for ethical considerations to be kept under consideration, such as bias, fairness, and privacy, when these models are deployed. In the future, more advanced techniques such as deep learning and transfer learning could be employed to enhance fraud detection across distinct financial domains.

## VIII. FUTURE WORK

The study is proposed for the future to capture some directions on employing machine learning in detecting credit card fraud prevention. We will be going through other paths as well where more qualitative data which goes beyond such regular patterns like how a user behaves or geographically could blending in to improve capturing the behavior of transactions. Finally other architectural models, like deep networks or hybrid solutions, might explore more complex data patterns. It is now imperative to work on enhancing model interpretability, and this holds especially true in the financial sector due to the importance of transparency with respect to decision-making. Methods like SHAP (Shapley Additive Explanations) or LIME (Local Interpretable Model-Agnostic Explanations) can be used to interpret black-box models such as Random Forest. Future work may focus on extending a model to new applications in domains that are similar (healthcare fraud detection) but somewhat different problematically while using transfer learning to speed up this process. For instance, one avenue of future research that has been highlighted throughout our discussion is the real-time implementation and monitoring of these models in practice both with regards to technical integration into existing systems as well as assessing ongoing model updates needed to maintain their effectiveness over additional time.

## REFERENCES

[1] R. Bin Sulaiman, V. Schetinin, and P. Sant, “Review of Machine Learning Approach on Credit Card Fraud Detection,” Human-Centric Intelligent Systems, vol. 2, May 2022, doi: https://doi.org/10.1007/s44230-022-00004-0.

[2] M. Puh and L. Brkić, “Detecting Credit Card Fraud Using Selected Machine Learning Algorithms,” IEEE Xplore, May 01, 2019. https://ieeexplore.ieee.org/document/8757212

[3] K. Yashwanth Kumar and B. Vani, “An optimal approach for fraud detection by comparing random forest algorithm and support vector machine algorithm for credit card transaction with improved accuracy,” AIP conference proceedings, Jan. 2023, doi: https://doi.org/10.1063/5.0177045.

[4] A. RB and S. K. KR, “Credit Card Fraud Detection Using Artificial Neural Network,” Global Transitions Proceedings, vol. 2, no. 1, Jan. 2021, doi: https://doi.org/10.1016/j.gltp.2021.01.006.

[5] F. Itoo, Meenakshi, and S. Singh, “Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection,” International Journal of Information Technology, vol. 13, Feb. 2020, doi: https://doi.org/10.1007/s41870-020-00430-y.

[6] A. Madhavi and T. Sivaramireddy, “Real-Time Credit Card Fraud Detection Using Spark Framework,” Machine Learning Technologies and Applications, pp. 287–298, 2021, doi: https://doi.org/10.1007/978-981-33-4046-6_28.

[7] S. Kumar, V. K. Gunjan, M. D. Ansari, and R. Pathak, “Credit Card Fraud Detection Using Support Vector Machine,” Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications, pp. 27–37, 2022, doi: https://doi.org/10.1007/978-981-16-6407-6_3.

[8] N. Boutaher, A. Elomri, N. Abghour, K. Moussaid, and M. Rida, “A Review of Credit Card Fraud Detection Using Machine Learning Techniques,” IEEE Xplore, Nov. 01, 2020. https://ieeexplore.ieee.org/abstract/document/9365916/

[9] D. Soemers, T. Brys, K. Driessens, M. Winands, and A. Nowé, “Adapting to Concept Drift in Credit Card Transaction Data Streams Using Contextual Bandits and Decision Trees,” Proceedings of the AAAI Conference on Artificial Intelligence, vol. 32, no. 1, Apr. 2018, doi: https://doi.org/10.1609/aaai.v32i1.11411.

[10] K. N. Mishra and S. C. Pandey, “Fraud Prediction in Smart Societies Using Logistic Regression and k-fold Machine Learning Techniques,” Wireless Personal Communications, Feb. 2021, doi: https://doi.org/10.1007/s11277-021-08283-9.

[11] T. Wang and Y. Zhao, “Credit Card Fraud Detection using Logistic Regression,” 2022 International Conference on Big Data, Information and

Computer Network (BDICN), Jan. 2022, doi: https://doi.org/10.1109/bdicn55575.2022.00064.

[12] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, “Random forest for credit card fraud detection,” IEEE Xplore, Mar. 01, 2018. https://ieeexplore.ieee.org/abstract/document/8361343/figures

[13] A. Gupta, M. C. Lohani, and M. Manchanda, “Utilizing mathematical concepts of heat map for an intelligent and secure approach to efficiently detect credit card fraud,” Journal of Interdisciplinary Mathematics, vol. 26, no. 8, pp. 1837–1854, Jan. 2023, doi: https://doi.org/10.47974/jim-1761.

[14] G. Moschini, R. Houssou, J. Bovay, and S. Robert-Nicoud, “Anomaly and Fraud Detection in Credit Card Transactions Using the ARIMA Model,” Engineering Proceedings, vol. 5, no. 1, p. 56, Jul. 2021, doi: https://doi.org/10.3390/engproc2021005056.

[15] V. Ceronmani Sharmila, K. K. R., S. R., S. D., and H. R., “Credit Card Fraud Detection Using Anomaly Techniques,” 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Apr. 2019, doi: https://doi.org/10.1109/iciict1.2019.8741421.

[16] E. Ileberi, Y. Sun, and Z. Wang, “A machine learning based credit card fraud detection using the GA algorithm for feature selection,” Journal of Big Data, vol. 9, no. 1, Feb. 2022, doi: https://doi.org/10.1186/s40537-022-00573-8.

[17] R. Sailusha, V. Gnaneswar, R. Ramesh, and G. R. Rao, “Credit Card Fraud Detection Using Machine Learning,” IEEE Xplore, May 01, 2020. https://ieeexplore.ieee.org/abstract/document/9121114

[18] Maureen Ifeanyi Akazue, Irene Alamarefa Debekeme, Abel Efe Edje, Clive Asuai, and Ufuoma John Osame, “UNMASKING FRAUDSTERS: Ensemble Features Selection to Enhance Random Forest Fraud Detection,” Journal of Computing Theories and Applications, vol. 1, no. 2, pp. 201–211, Dec. 2023, doi: https://doi.org/10.33633/jcta.v1i2.9462.

[19] J. Miao and W. Zhu, “Precision–recall curve (PRC) classification trees,” Evolutionary Intelligence, Apr. 2021, doi: https://doi.org/10.1007/s12065-021-00565-2.