

ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Comparative Analysis of Credit Card Fraud Detection Using Standard Scalar and MIN-MAX Scalar

Janvi Ahuja, Abhishek Jadoun, Sadique Amin, Prof.(Dr). Parul Gandhi .

School of Computer Appplication "Manav Rachna International Institute of Research And Studies Faridabad'harayana'(121003)India"

Abstract:

Credit card transactions Fraud is a major issue in financial sector, which is causing financial harm to both individuals & businesses To mitigate these risks, machine learning models have been employed to detect fraudulent transactions. This study explores the performance of various classification models when using two different feature scaling techniques, Standard Scalar and MIN-MAX Scalar. The goal is to compare the effectiveness of these scaling methods in enhancing the accuracy and precision of credit card fraud detection. In this research, we examine five commonly used classification models: Random Forest, KNeighborsClassifier, Logistic Regression, DecisionTreeClassifier, and Gaussians. We assess their performance under two distinct scaling techniques: Standard Scalar and MIN-MAX Scalar. The analysis is carried out on a dataset of credit card transactions, where the 'Class' variable categorizes transactions into two classes: non-fraudulent (Class 0) and fraudulent (Class 1). For each model and scalar combination, we measure performance using key evaluation metrics, including accuracy, precision, recall, F1 score, and ROC AUC score. Accuracy reflects the model's overall ability to correctly classify transactions, while precision indicates its accuracy in identifying fraudulent cases. Recall measures the model's capability to capture all actual frauds, while the F1 score provides a balanced assessment of precision and recall. The ROC AUC score evaluates the model's ability to distinguish between classes. The findings of this research reveal significant variations in the performance of classification models based on the choice of scalar. Notably, the RandomForest model demonstrates remarkable performance with both Standard Scalar and MIN-MAX Scalar, achieving near-perfect accuracy, precision, and recall scores under Standard Scalar. This suggests that RandomForest is a robust choice for credit card fraud detection.KNeighborsClassifier exhibits a substantial improvement in performance when using Standard Scalar, achieving high accuracy, precision, and recall scores. LogisticRegression, too, benefits from Standard Scalar, resulting in enhanced accuracy and precision, indicating its suitability for fraud detection tasks.DecisionTreeClassifier showcases a significant performance boost with Standard Scalar, exhibiting strong accuracy and precision, making it another favorable choice for this application.GaussianNB, while less accurate than other models, still demonstrates reasonable performance, particularly with Standard Scalar. Overall, the choice of scalar plays a pivotal role in the success of credit card fraud detection models. Standard Scalar generally leads to superior model performance, particularly for RandomForest, KNeighborsClassifier, LogisticRegression, and DecisionTreeClassifier. However, model selection remains crucial, as certain algorithms have limitations in capturing specific patterns and classifying cases. This study offers practical insights for financial institutions and organizations seeking to enhance their credit card fraud detection systems. It emphasizes the importance of careful model selection and the implementation of appropriate feature scaling techniques. The findings contribute to the ongoing efforts to combat credit card fraud effectively, reducing financial losses and safeguarding the interests of cardholders and businesses.

Keywords: Credit card fraud detection, machine learning, classification ,Standard Scalar,Min-Max Scalar, model performance, feature scaling.

Introduction

In the ever-evolving landscape of financial transactions, credit cards have solidified their place as indispensable tools, facilitating seamless and expedited exchanges.

However, beneath the surface of this financial convenience lies a pervasive challenge that demands meticulous attention – the rampant issue of credit card fraud. Instances of fraudulent activities, encompassing unauthorized transactions and identity theft, not only exact a toll in terms of financial losses but also cast shadows of doubt over the trustworthiness of the entire financial ecosystem. Recognizing the gravity of this challenge, [1]there arises a compelling need for a thorough and exhaustive exploration of methodologies aimed at detecting and preventing credit card fraud.

This study, therefore, embarks on a journey to unravel the complexities inherent in credit card fraud, seeking to illuminate the nuances that surround this persistent problem. [2]As we delve into this exploration, our overarching objective is to contribute meaningful insights that will play a pivotal role in the continuous enhancement of fraud detection systems. Beyond merely mitigating financial losses, our aim is to fortify the very foundations of the financial industry, fostering an environment of heightened security, trust, and confidence in every financial transaction. Through this endeavor, we aspire to be at the forefront of shaping a financial landscape where the resilience of fraud detection mechanisms aligns seamlessly with the imperatives of safeguarding the interests of individuals and businesses alike.

Prominent statistics pertaining to credit card fraud:Credit card fraud remains a significant concern in the United States, despite a slight decrease from 2020 to 2021. The threat encompasses various scenarios, including personal information theft and data breaches affecting companies. Here are key findings from our collected data:

- In 2021, the Federal Trade Commission (FTC) received reports of over 389,000 cases of credit card fraud.

- The most extensive data breach involving credit card information occurred in 2009 at Heartland Systems, impacting 160 million credit cards (U.S. Department of Justice).

- Globally, losses attributed to credit card fraud surpassed \$32 billion in 2021, as reported by the Nilson Report, a leading trade publication in the payment card industry.

- Texas led in reported credit card fraud cases in 2021, with over 146,000 reports (FTC).

- Individuals aged 30 to 39 reported the highest number of credit card fraud cases, while those aged 80 and older experienced the highest median loss of \$1,500 per report (FTC).

According to the Nilson Report:

- Worldwide payment card fraud losses exceeded \$32 billion in 2021, with nearly \$12 billion occurring in the U.S.

- Over the next decade, the industry is projected to incur a cumulative \$397 billion in losses globally, with \$165 billion attributed to the U.S.

- Despite accounting for only 23% of card spending, the U.S. contributed to 37% of global losses to card fraud in 2021.

- Increased credit card purchases, particularly online transactions, and a surge in card-not-present transactions contributed to higher fraud losses in the U.S.

- In 2021, fraud losses in the U.S. reached \$11.9 billion, marking an 18% increase from 2020 and connected to a card volume of \$11.3 trillion.

- Fraud, expressed in basis points per \$100 in total volume, decreased slightly to 6.61ϕ in 2021, an improvement from 6.77ϕ in 2020.

David Robertson, Publisher of the Nilson Report, noted that while fraud as a percentage of total card dollar volume declined, criminals experienced a 14% growth in the money stolen, amounting to nearly \$4 billion more in 2021 compared to 2020. Losses to fraud impact card issuers, merchants, processors of card payments, and processors of card transactions from ATMs. The total worldwide spending, including cash advances and withdrawals, reached \$48.955 trillion in 2021, reflecting a 16.6% increase from 2020. This substantial payment volume involved various credit, debit, and prepaid cards, both global and domestic, used at merchants and ATMs.

Traditional fraud detection systems often rely on rulebased models that identify suspicious activities based on predefined criteria. While these systems are effective to some extent, they struggle to keep pace with the rapidly evolving techniques employed by fraudsters. This leads to a high number of false positives, which not only inconvenience legitimate cardholders but also create a significant workload for fraud investigators. [3]In essence, the battle against credit card fraud requires a more sophisticated, adaptable, and data-driven approach. The primary objective of this research is to introduce and evaluate a credit card fraud detection system that combines the K-Nearest Neighbors (KNN) [4] algorithm with an adaptive fraud detection algorithm. This novel approach aims to provide enhanced accuracy, efficiency, and adaptability in detecting fraudulent credit card transactions. [5]By leveraging machine learning techniques and the adaptability of a specialized fraud detection algorithm, this research seeks to address the limitations of traditional rule-based systems, reduce false positives, and keep pace with evolving fraud tactics.

DecisionTreeClassifier, and GaussianNB. [6]By comparing the performance of these models under different scaling techniques, [7]this study aims to provide valuable insights for financial institutions and businesses seeking to enhance their fraud detection systems.

The dataset used in this research consists of credit card transaction records, where transactions are categorized into two classes: non-fraudulent (Class 0) and fraudulent (Class 1).[8] By analyzing this data, we can evaluate how effectively the chosen classification models, in combination with distinct scaling techniques, can identify and classify fraudulent transactions.

The research focuses on key performance metrics, including accuracy, precision, recall, F1 score, and ROC AUC score. [9]Accuracy measures the overall ability of a model to accurately classify transactions. Precision assesses[10] the accuracy of the model in identifying fraudulent cases, minimizing the number of false positives.[11] Recall evaluates the model's ability to capture all actual fraudulent transactions, avoiding false negatives. The F1 score provides a balanced assessment of precision and recall.[12] Finally, the ROC AUC score gauges the model's capacity to distinguish between the two transaction classes.

The findings[13] of this research will shed light on the advantages and disadvantages of different classification models when coupled with specific scaling techniques. Understanding the impact of[14] scaling methods on model performance is crucial for making informed decisions regarding credit card fraud detection systems. The results will serve as a guide for financial institutions and businesses aiming to enhance their fraud detection capabilities,[15] thereby reducing financial losses and ensuring the security and trust of cardholders and businesses in the credit card industry.

Methodology

Dataset-In order to predict credit card fraud detection for that we have taken dataset from the Kaggle website which has been used by others researchers also. This dataset is freely available on the internet and anyone interested will be able to use and investigate on this dataset. Also, we have performed our data analysis in the python and have used the Jupyter notebook. This dataset encompasses credit card transactions carried out by European cardholders during the year 2023. With a voluminous compilation exceeding 550,000 entries, the dataset ensures the anonymity of cardholders

Fig.1: credit card transactions along with Amount and Class

life_df=pd.read_csv('credit-card-fraud-detection-dataset-2023/creditcard_2023.csv') life_df

V5	V6	V7	V8	V9	 V21	V22	V23	V24	V25	V26	V27	V28	Amount	Class
0.129681	0.732898	0.519014	-0.130006	0.727159	-0.110552	0.217606	-0.134794	0.165959	0.126280	-0.434824	-0.081230	-0.151045	17982.10	0
0.277140	0.428605	0.406466	-0.133118	0.347452	-0.194936	-0.605761	0.079469	-0.577395	0.190090	0.296503	-0.248052	-0.064512	6531.37	0
0.074062	1.419481	0.743511	-0.095576	-0.261297	-0.005020	0.702906	0.945045	-1.154666	-0.605564	-0.312895	-0.300258	-0.244718	2513.54	0
0.249486	1.143312	0.518269	-0.065130	-0.205698	-0.146927	-0.038212	-0.214048	-1.893131	1.003963	-0.515950	-0.165316	0.048424	5384.44	0
0.106125	0.530549	0.658849	-0.212660	1.049921	-0.106984	0.729727	-0.161666	0.312561	-0.414116	1.071126	0.023712	0.419117	14278.97	0
1.002401	0.481454	-0.370393	0.189694	-0.938153	0.167503	0.419731	1.288249	-0.900861	0.560661	-0.006018	3.308968	0.081564	4394.16	1
0.133660	0.237148	-0.016935	-0.147733	0.483894	0.031874	0.388161	-0.154257	-0.846452	-0.153443	1.961398	-1.528642	1.704306	4653.40	1
0.042291	0.121098	-0.070958	-0.019997	-0.122048	0.140788	0.536523	-0.211100	-0.448909	0.540073	-0.755836	-0.487540	-0.268741	23572.85	1
0.131042	-0.294148	0.580568	-0.207723	0.893527	-0.060381	-0.195609	-0.175488	-0.554643	-0.099669	-1.434931	-0.159269	-0.076251	10160.83	1
0.244976	-0.603493	-0.347613	-0.340814	0.253971	 0.534853	-0.291514	0.157303	0.931030	-0.349423	-1.090974	-1.575113	0.722936	21493.92	1

to safeguard their identities. The principal aim of this dataset is to support. The creation and enhancement of algorithms and models dedicated to fraud detection. The focus lies in identifying transactions that may exhibit characteristics indicative of potential fraudulent activity.

Inspecting the data

Exploring credit card transaction data in Jupyter for research involves importing Pandas and Matplotlib libraries. Load the dataset into a Pandas DataFrame, inspecting it with methods like head(), describe(), and info() to understand the data structure and identify missing values. Visualize transaction trends using histograms or time series plots. Calculate basic statistics for transaction amounts. Identify anomalies, patterns, and correlations within the data. Document findings and iteratively refine the analysis to gain insights into fraudulent activity or spending behavior

[12]: life_df.isnull().sum()

2]:	id	0
	V1	0
	V2	0
	V3	0
	V4	0
	V5	0
	V6	0
	V7	0
	V8	0
	V9	0
	V10	0
	V11	0
	V12	0
	V13	0
	V14	0
	V15	0
	V16	0
	V17	0
	V18	0
	V19	0
	V20	0
	V21	0
	V22	0
	V23	0
	V24	0
	V25	0
	V26	0
	V27	0
	V28	0
	Amount	0
	Class	0
	dtype:	int6

Fig. 2:Inspecting the data

Following that, we have detailed information on every single transcation that contributes to fraud detection. It can be observed that, the terms for exploring the data . id: Unique identifier for each transaction

V1-V28: Encoded features concealing diverse transaction attributes such as time, location, etc. Amount: Reflects the monetary value of the transaction. Class: Binary label indicating the fraudulent (1) or non-fraudulent (0) nature of the transaction. Potential Applications: Credit Card Fraud Detection: Develop machine learning models geared towards identifying and preventing credit card fraud. Leverage the anonymized features to detect suspicious transactions and enhance the security of credit card transactions. Merchant Category Analysis: Investigate the correlation between different merchant categories and fraudulent activities. Analyze patterns and associations within specific merchant categories to gain insights into potential vulnerabilities or risks associated with certain types of transactions.

Transaction Type Analysis: Analyze whether certain types of transactions are more prone to fraud than others.

www.jetir.org (ISSN-2349-5162)

# Column Non-Wull Count Dtype 0 id 568630 non-null int64 1 V1 568630 non-null float64 2 V2 568630 non-null float64 3 V3 568630 non-null float64 4 V4 568630 non-null float64 5 V5 568630 non-null float64 6 V6 568630 non-null float64 7 V7 568630 non-null float64 8 V8 568630 non-null float64 9 V9 568630 non-null float64 10 V10 568630 non-null float64 12 V12 568630 non-null float64 13 V13 568630 non-null float64 14 V14 568630 non-null float64 15 V15 <		≺class 'pandas.core.frame.DataFrame'> RangeIndex: 568630 entries, 0 to 568629 Data columns (total 31 columns):								
0 id 568630 non-null int64 1 V1 568630 non-null float64 2 V2 568630 non-null float64 3 V3 568630 non-null float64 4 V4 568630 non-null float64 5 V5 568630 non-null float64 6 V6 568630 non-null float64 7 V7 568630 non-null float64 8 V8 568630 non-null float64 9 V9 568630 non-null float64 10 V10 568630 non-null float64 11 V11 568630 non-null float64 12 V12 568630 non-null float64 13 V13 568630 non-null float64 14 V14 568630 non-null float64 15		# Co	lumn N	on-Null	Count	Dtype				
0 id 568630 non-null int64 1 V1 568630 non-null float64 2 V2 568630 non-null float64 3 V3 568630 non-null float64 4 V4 568630 non-null float64 5 V5 568630 non-null float64 6 V6 568630 non-null float64 7 V7 568630 non-null float64 8 V8 568630 non-null float64 9 V9 568630 non-null float64 10 V10 568630 non-null float64 11 V11 568630 non-null float64 12 V12 568630 non-null float64 13 V13 568630 non-null float64 14 V14 568630 non-null float64 15 V15 568630 non-null float64 16 V16 568630 non-null float64 17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V19 568630 non-null float64 20 V20 </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>										
0 10 556530 non-null float64 1 V1 566530 non-null float64 2 V2 566530 non-null float64 3 V3 566630 non-null float64 4 V4 568630 non-null float64 5 V5 568630 non-null float64 6 V6 568630 non-null float64 7 V7 568630 non-null float64 8 V8 568630 non-null float64 9 V9 568630 non-null float64 10 V10 568630 non-null float64 11 V11 568630 non-null float64 12 V12 568630 non-null float64 13 V13 568630 non-null float64 14 V14 568630 non-null float64 15 V15 568630 non-null float64 16 V16 568630 non-null float64 17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V19 568630 non-null float64 21 V20	~									
1 VI S00000 NON-NULL Float64 2 V2 S00000 NON-NULL Float64 3 V3 S00000 NON-NULL Float64 4 V4 S00000 NON-NULL Float64 5 V5 S00000 NON-NULL Float64 6 V6 S00000 NON-NULL Float64 7 V7 S00000 NON-NULL Float64 8 V8 S00000 NON-NULL Float64 9 V9 S00000 NON-NULL Float64 10 V10 S00000 NON-NULL Float64 11 V11 S00000 NON-NULL Float64 12 V12 S00000 NON-NULL Float64 13 V13 S00000 NON-NULL Float64 14 V14 S00000 NON-NULL Float64 15 V15 S000000-NULL Float64 16 V15 S000000-NULL Float64 17 V17 S000000-NULL Float64 18 V18 S000000-NULL Float64 19 V10 S000000-NULL Float64 20 V20 S000000-NULL Float64 21 V21 <t< td=""><td>0</td><td>10</td><td>5686:</td><td>30 non</td><td>-null</td><td>1nt64</td></t<>	0	10	5686:	30 non	-null	1nt64				
2 V2 S66630 non-null float64 4 V4 S66630 non-null float64 5 V5 S66630 non-null float64 5 V5 S66630 non-null float64 6 V6 S66630 non-null float64 7 V7 S66630 non-null float64 8 V8 S66630 non-null float64 9 V9 S68630 non-null float64 10 V10 S68630 non-null float64 11 V11 S68630 non-null float64 12 V12 S68630 non-null float64 13 V13 S68630 non-null float64 14 V14 S68630 non-null float64 15 V15 S68630 non-null float64 16 V16 S68630 non-null float64 17	2	V1 V2	50003		-null	float64				
4 V4 S66830 non-null float64 5 V5 S68630 non-null float64 6 V6 S68630 non-null float64 6 V6 S68630 non-null float64 6 V6 S68630 non-null float64 7 V7 S68630 non-null float64 9 V9 S68630 non-null float64 10 V10 S68630 non-null float64 11 V11 S68630 non-null float64 12 V12 S68630 non-null float64 13 V13 S68630 non-null float64 14 V14 S68630 non-null float64 15 V15 S68630 non-null float64 16 V16 S68630 non-null float64 17 V17 S68630 non-null float64 18	2	V2	56863	30 000	-null	float64				
5 V5 568630 non-null float64 6 V6 568630 non-null float64 7 V7 568630 non-null float64 8 V8 568630 non-null float64 9 V9 568630 non-null float64 10 V10 568630 non-null float64 11 V11 568630 non-null float64 12 V12 568630 non-null float64 13 V13 568630 non-null float64 14 V14 568630 non-null float64 15 V15 568630 non-null float64 16 V16 568630 non-null float64 17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V20 568630 non-null float64 21	4	V4	56863	30 non	- 0 1 1	float64				
5 5 5 5 6 7 7 5 5 6 7 7 7 5 6 6 7 7 7 5 6 6 7 7 7 5 6 6 7 7 7 5 6 6 7 7 7 5 6 6 7 7 7 5 6 6 7 7 7 5 6 6 9 9 5 6 6 9 7 7 5 6 6 9 7 7 7 5 6 6 9 7 7 7 7 6 6 3 7 7 7 6 6 3 7 7 7 7 6 6 3 7 7 7 7 6 6 3 7 7 7 6 6 3 7 7 7	5	VS	56863	30 000	-011	float64				
7 V7 S68630 non-null float64 8 V8 S68630 non-null float64 9 V9 S68630 non-null float64 10 V10 S68630 non-null float64 11 V10 S68630 non-null float64 12 V12 S68630 non-null float64 13 V13 S68630 non-null float64 14 V14 S68630 non-null float64 15 V15 S68630 non-null float64 16 V16 S68630 non-null float64 17 V17 S68630 non-null float64 18 V18 S68630 non-null float64 19 V19 S68630 non-null float64 20 V20 S68630 non-null float64 21 V21 S68630 non-null float64 22 </td <td>6</td> <td>VG</td> <td>56863</td> <td>30 non</td> <td>- 0 1 1</td> <td>float64</td>	6	VG	56863	30 non	- 0 1 1	float64				
8 V8 568630 non-null float64 9 V9 568630 non-null float64 10 V10 568630 non-null float64 11 V11 568630 non-null float64 12 V12 568630 non-null float64 13 V13 568630 non-null float64 14 V14 568630 non-null float64 15 V15 568630 non-null float64 16 V16 568630 non-null float64 17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V19 568630 non-null float64 20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 23	7	VZ	56863	30 non	-null	float64				
9 V9 568630 non-null float64 10 V10 568630 non-null float64 11 V11 568630 non-null float64 12 V12 568630 non-null float64 13 V13 568630 non-null float64 13 V13 568630 non-null float64 14 V14 568630 non-null float64 15 V15 568630 non-null float64 16 V16 568630 non-null float64 17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V19 568630 non-null float64 20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V26 568630 non-null float64 27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 <td>8</td> <td>V8</td> <td>56863</td> <td>30 non</td> <td>-null</td> <td>float64</td>	8	V8	56863	30 non	-null	float64				
10 V10 568630 non-null float64 11 V11 568630 non-null float64 12 V12 568630 non-null float64 13 V13 568630 non-null float64 14 V14 568630 non-null float64 15 V15 568630 non-null float64 16 V16 568630 non-null float64 17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V19 568630 non-null float64 20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 23 V23 568630 non-null float64 24 V24 568630 non-null float64 <t< td=""><td>9</td><td>V9</td><td>56863</td><td>30 non</td><td>-null</td><td>float64</td></t<>	9	V9	56863	30 non	-null	float64				
11 V11 568630 non-null float64 12 V12 568630 non-null float64 13 V13 568630 non-null float64 14 V14 568630 non-null float64 15 V15 568630 non-null float64 15 V15 568630 non-null float64 16 V16 568630 non-null float64 17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V19 568630 non-null float64 20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V26 568630 non-null float64 27 V27 568630 non-null float64 28 <	10	V10	56863	30 non	-null	float64				
12 V12 568630 non-null float64 13 V13 568630 non-null float64 14 V14 568630 non-null float64 15 V15 568630 non-null float64 15 V15 568630 non-null float64 16 V16 568630 non-null float64 17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V19 568630 non-null float64 20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V26 568630 non-null float64 <t< td=""><td>11</td><td>V11</td><td>56863</td><td>30 non</td><td>-null</td><td>float64</td></t<>	11	V11	56863	30 non	-null	float64				
13 V13 568630 non-null float64 14 V14 568630 non-null float64 15 V15 568630 non-null float64 16 V16 568630 non-null float64 17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V19 568630 non-null float64 20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 23 V23 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V26 568630 non-null float64 27 V27 568630 non-null float64 <t< td=""><td>12</td><td>V12</td><td>56863</td><td>30 non</td><td>-null</td><td>float64</td></t<>	12	V12	56863	30 non	-null	float64				
14 V14 568630 non-null float64 15 V15 568630 non-null float64 16 V16 568630 non-null float64 17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V19 568630 non-null float64 20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 23 V23 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V26 568630 non-null float64 27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null float64 30	13	V13	56863	30 non	-null	float64				
15 V15 S68630 non-null float64 16 V16 S68630 non-null float64 17 V17 S68630 non-null float64 18 V18 S68630 non-null float64 19 V19 S68630 non-null float64 20 V20 S68630 non-null float64 21 V21 S68630 non-null float64 22 V22 S68630 non-null float64 23 V23 S68630 non-null float64 24 V24 S68630 non-null float64 25 V25 S68630 non-null float64 26 V25 S68630 non-null float64 27 V26 S68630 non-null float64 28 V28 S68630 non-null float64 29 Amount S68630 non-null float64 29 Mount S68630 non-null float64 20 Lass S68630 non-null float64	14	V14	56863	30 non	-null	float64				
16 V16 S68630 non-null float64 17 V17 S68630 non-null float64 18 V18 S68630 non-null float64 19 V19 S68630 non-null float64 20 V20 S68630 non-null float64 21 V21 S68630 non-null float64 22 V22 S68630 non-null float64 23 V23 S68630 non-null float64 24 V24 S68630 non-null float64 25 V25 S68630 non-null float64 26 V26 S68630 non-null float64 27 V27 S68630 non-null float64 27 V27 S68630 non-null float64 29 Amount S68630 non-null float64 30 Class S68630 non-null float64 30 Class S68630 non-null float64	15	V15	56863	30 non	-null	float64				
17 V17 568630 non-null float64 18 V18 568630 non-null float64 19 V19 568630 non-null float64 20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 23 V23 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V26 568630 non-null float64 27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 Avant 568630 non-null float64 30 Class 568630 non-null float64 29 Avant 568630 non-null float64 30 Class 568630 non-null float64 30 Class 568630 non-null float64	16	V16	56863	30 non	-null	float64				
18 V18 566630 non-null float64 19 V19 566630 non-null float64 20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 23 V23 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V25 568630 non-null float64 27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 Amount 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null float64	17	V17	56863	30 non	-null	float64				
19 V19 568630 non-null float64 20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 23 V23 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V26 568630 non-null float64 27 V27 568630 non-null float64 28 V27 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null float64 30 Class 568630 non-null float64	18	V18	56863	30 non	-null	float64				
20 V20 568630 non-null float64 21 V21 568630 non-null float64 22 V22 568630 non-null float64 23 V23 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V25 568630 non-null float64 27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null float64 30 Class 568630 non-null float64	19	V19	56863	30 non	-null	float64				
21 V21 568630 non-null float64 22 V22 568630 non-null float64 23 V23 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V26 568630 non-null float64 27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null float64 30 Class 568630 non-null float64	20	V20	56863	30 non	-null	float64				
22 V22 568630 non-null float64 23 V23 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V26 568630 non-null float64 27 V27 568630 non-null float64 28 V27 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null float64 30 Class 568630 non-null float64	21	V21	56863	30 non	-null	float64				
23 V23 568630 non-null float64 24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V25 568630 non-null float64 26 V25 568630 non-null float64 27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null float64	22	V22	56863	30 non	-null	float64				
24 V24 568630 non-null float64 25 V25 568630 non-null float64 26 V26 568630 non-null float64 27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null float64	23	V23	56863	30 non	-null	float64				
25 V25 568630 non-null float64 26 V26 568630 non-null float64 27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null float64 30 Class 568630 non-null float64	24	V24	56863	30 non	-null	float64				
26 V26 568630 non-null float64 27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null float64	25	V25	56863	30 non	-null	float64				
27 V27 568630 non-null float64 28 V28 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null int64	26	V26	56863	30 non	-null	float64				
28 V28 568630 non-null float64 29 Amount 568630 non-null float64 30 Class 568630 non-null int64	27	V27	56863	30 non	-null	float64				
29 Amount 568630 non-null float64 30 Class 568630 non-null int64	28	V28	56863	30 non	-null	float64				
30 Class 568630 non-null int64	29	Amount	56863	30 non	-null	float64				
	30	Class	56863	30 non	-null	1nt64				

[14]: life_df.info()

Fig. 3: All numerical data is free of null values with help of Inspection of Data

Exploratory analysis

Exploratory data analysis and visualization of the distribution of classes in a DataFrame, often used in the context of binary classification problems, such as fraud detection in credit card transactions.Below is an explanation of the Jupiter code:

Distribution of Class

[23]: plt.figure(figsize=(10,8))

```
class_counts = life_df['Class'].value_counts()
```

plt.pie(class_counts, labels=class_counts.index, autopct='%1.f%%')
plt.title('Distribution of Class')
plt.legend()
plt.show()

Fig. 4: Distribution of Class



Fig. 5:Transaction Amount Distribution

Explanation:

This pie chart shows distribution of class in which 1 represents as fraudent and 0 represents non-fraudent by using plt.pie()creates a pie chart using the class counts as data points. It sets the labels for the chart as the unique values in the 'Class' column ('0' for non-fraud and '1' for fraud) and displays the percentage on each slice with no decimal places.plt.title('Distribution of Class')sets the title of the pie chart.plt.legend()adds a legend to the chart to specify the meaning of each slice (0 for non-fraud and 1 for fraud).plt.show() displays the pie chart.The code helps visualize the distribution of class labels in the 'Class' column, providing insights into the balance or imbalance between non-fraudulent and fraudulent transactions in the dataset.

And ,also shows the transaction of the above pie chart distribution of transaction amounts that results into as

```
[25]: # distribution of transaction amounts
    x = life_df['Amount']
    bins = 20
    plt.hist(x, bins, color='lightgreen')
    plt.xlabel('Amount')
    plt.ylabel('Count')
    plt.title('Transaction Amount Distribution')
    plt.show()
```

www.jetir.org (ISSN-2349-5162)



As above, but broken down by target we explicitly define the labels for the two classes ('Non-fraudulent' and 'Fraudulent') and use them in the pie chart, breaking down the chart by these two target classes. The rest of the code remains the same, providing a visual representation of the distribution of these target classes in the 'Class' column that results into:



Fig.6:Tansaction Amount By Class

After correlation heatmap is a visual representation of the correlation or relationship between different variables in a dataset. It is a commonly used tool in data analysis and visualization to understand how variables are related to each other that shows the Amounts of transaction based upon Distribution of class which Results in as shown:



Fig.7: A correlation heatmap

Created a Boxplot of class against transaction amount is a valuable data visualization technique, especially when dealing with datasets that involve binary classification, such as fraud detection in credit card transaction. The resulting boxplot allows you to visually compare the distribution of transaction amounts between nonfraudulent and fraudulent transactions, helping to identify potential differences and outliers.

Classification Of All Model Comparison Results

The dataset's features have been processed using two different scaling techniques: MIN-MAX Scalar and Standard Scalar. Each model is then trained and evaluated using both versions of the scaled data. This approach allows us to compare the performance of the models under each scaling method and determine

One is more suitable for our specific problem of all algorithms.

Model	Accurac	у	Precision		Recall		F1 Sco	re	ROC A	UC Score
	Min- Max Scalar	Standard Scalar	Min -Max Scalar	Satndard Scalar	Min- Max Scalar	Stan dard Scal ar	Min- Max Scala r	Standad Scalar	Min- Max Scala r	Standard Scalar
Random Forest	0.6480	0.999	0.5919	0.9998	0.9580	1.00 00	0.731 7	0.9999	0.647 4	0.9999
KNeighbors Classifier	0.5010	0.9978	0.5010	0.9 <mark>957</mark>	1.0000	5	0.667 5	0.9978	0.500 0	0.9978
Logistic Regression	0.5010	0.9653	0.5010	0.9773	1.0000	0.95 28	0.667 5	0.9649	0.500 0	0.9653
Decision Tree Classifier	0.5069	0.9981	0.9956	0.9972	0.0158	0.99 91	0.031	0.9981	0.507 9	0.9981
GaussianNB	0.5015	0.9180	0.5012	0.9753	1.0000	0.85 82	0.667 8	0.9130	0.500 5	0.9182

www.jetir.org (ISSN-2349-5162)

It shows that, By comparing all the models results in RandomForest: This model performs best with both scaling methods, but significantly better with Standard Scalar (F1 score close to 1) compared to MIN-MAX Scalar.

Gaussian NB: This model performs better with Standard Scalar than with Min-Max Scalar.

KNeighborsClassifier: This model has almost the same performance with both scaling methods, but slightly better with Standard Scalar.

LogisticRegression: This model performs significantly better with Standard Scalar than with MIN-MAX Scalar.

DecisionTreeClassifier: This model has the lowest F1 score with MIN-MAX Scalar, but performs well with Standard Scalar.

Summary:

In summary, this research sheds light on the intricacies of credit card fraud detection, specifically examining the influence of different feature scaling techniques on the performance of various classification models.

The results highlight notable differences in model performance based on the chosen scalar. Notably, Random Forest emerges as a dependable choice for credit card fraud detection, exhibiting impressive accuracy, precision, and recall scores, particularly when paired with Standard Scalar. KNeighborsClassifier and LogisticRegression also show improved outcomes with Standard Scalar.

While GaussianNB demonstrates comparatively lower accuracy, it still performs reasonably well, especially in

conjunction with Standard Scalar. The overarching lesson underscores the pivotal role of feature scaling techniques in optimizing credit card fraud detection models. Standard Scalar generally proves more effective

across multiple models, but the careful selection of the appropriate algorithm remains a critical factor.

		Cre

www.jetir.org (ISSN-2349-5162)

Clas

		precision	recall	f1-score	support	
	0	1.00	1.00	1.00	56750	
	1	1.00	1.00	1.00	56976	
accur	racy			1.00	113726	
macro	avg	1.00	1.00	1.00	113726	
weighted	avg	1.00	1.00	1.00	113726	

Fig. 8: Results that Random Forest has the highest accuracy

Conclusion:

In conclusion, this research delves into the realm of credit card fraud detection, exploring the impact of different feature scaling techniques on the performance of various classification models. The study focuses on five widely-used models and evaluates their effectiveness using a dataset of credit card transactions categorized as non-fraudulent or fraudulent. The findings reveal significant variations in model performance based on the choice of scalar. Notably, Random Forest emerges as a robust choice for credit card fraud detection, demonstrating remarkable accuracy, precision, and recall scores, particularly with Standard Scalar. K Neighbors Classifier and Logistic Regression also show improved performance with Standard Scalar. While Gaussians is comparatively less accurate, it still exhibits reasonable performance, especially when paired with Standard Scalar. The overall takeaway emphasizes the crucial role of feature scaling techniques in optimizing credit card fraud detection models. Standard Scalar generally leads to superior performance across multiple models, but the careful selection of the right algorithm remains pivotal. This study provides practical insights for financial institutions seeking to enhance their fraud detection systems.

References

[1]Maniraj, S. P., Saini, A., Ahmed, S., & Sarkar, S. (2019). Credit card fraud detection using machine learning and data science. International Journal of Engineering Research, 8(9), 110-115.

[2]Niu X, Wang L, Yang X. A comparison study of credit card fraud detection: Supervised versus unsupervised. arXiv preprint arXiv:1904.10604. 2019 Apr 24.

[3]Khatri, S., Arora, A. and Agrawal, A.P., 2020, January. Supervised machine learning algorithms for

credit card fraud detection: a comparison. In 2020 10th international conference on cloud computing, data science & engineering (confluence) (pp. 680-683). IEEE.

[4]Ata, O. and Hazim, L., 2020. Comparative analysis of different distributions dataset by using data mining techniques on credit card fraud detection. *Tehnički* vjesnik, 27(2), pp.618-626.

[5]Itoo, F., Meenakshi and Singh, S., 2021. Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. International Journal of Information Technology, *13*, pp.1503-1511.

[6]Alfaiz, N.S. and Fati, S.M., 2022. Enhanced credit card fraud detection model using machine learning. Electronics, 11(4), p.662.

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

[8]Singh A, Ranjan RK, Tiwari A. Credit card fraud detection under extreme imbalanced data: a comparative study of data-level algorithms. Journal of Experimental & Theoretical Artificial Intelligence. 2022 Jul 4;34(4):571-98.

[9] Cherif, Asma, Arwa Badhib, Heyfa Ammar, Suhair Alshehri, Manal Kalkatawi, and Abdessamad Imine. "Credit card fraud detection in the era of disruptive technologies: A systematic review." Journal of King Saud University-Computer and Information Sciences 35, no. 1 (2023): 145-174.

[10]Ojha, Sumit Kumar, and Padmapriya Govindhan. "Analysis of credit card fraud detection using novel ANN algorithm to improve the rate of accuracy based on assorted transactional behaviour in comparison with logistic regression." In AIP Conference Proceedings, vol. 2655, no. 1. AIP Publishing, 2023.

[11]Mirhashemi, Qazaleh Sadat, Negar Nasiri, and Mohammad Reza Keyvanpour. "Evaluation of Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison." 2023 9th International Conference on Web Research (ICWR). IEEE, 2023.

[12]Ojha, Sumit Kumar, and Padmapriya Govindhan. "Analysis of credit card fraud detection using novel ANN algorithm to improve the rate of accuracy based on assorted transactional behaviour in comparison with logistic regression." In AIP Conference Proceedings, vol. 2655, no. 1. AIP Publishing, 2023.

[13]Kaggle:Credit Card Fraud Detection 2023. https//:www.kaggle.com/code/ryanhopewell/creditcard-fraud-detection-classification/notebook.

[14]Du, H., Lv, L., Guo, A., & Wang, H. (2023). AutoEncoder and LightGBM for Credit Card Fraud Detection Problems. Symmetry, *15*(4), 870.

[15]Mienye, I. D., & Sun, Y. (2023). A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection. IEEE Access, 11, 30628-30638.