Credit Card Fraud Detection Model

Prateek Shah [1], Tanmay Sanjay Dod [2] , Pratik Mahesh Tapadiya [3] , Niyati Sohni [4]

[1]Prateek Shah, Dept. of ENTC, JSPM's JSCOE, Pune, Maharashtra, India
[2]Tanmay Sanjay Dod, Dept. of ENTC, JSPM's JSCOE, Pune, Maharashtra, India
[3]Pratik Mahesh Tapadiya, Dept. of ENTC, JSPM's JSCOE, Pune, Maharashtra, India
[4]Prof. Niyati Sohni, Dept. of ENTC, JSPM's JSCOE, Pune, Maharashtra, India

Abstract: Credit card fraud presents a pressing challenge within the financial sector, posing considerable risks of monetary loss for both clients and financial institutions. Consequently, extensive research has been devoted to crafting robust fraud detection systems. These systems leverage an array of methodologies, including statistical analysis, machine learning algorithms, and deep learning models, to pinpoint suspicious transactions effectively. Rule-based systems are commonly employed for this purpose, utilizing predefined criteria to flag transactions exhibiting potential signs of fraudulence. However, these systems have inherent limitations, reliant on established rules and potentially unable to detect emerging fraud patterns.

To address these shortcomings, machine learning algorithms and statistical techniques have been harnessed for credit card fraud detection. These methods scrutinize transactional data—such as amount, location, and timing—alongside pertinent variables like the customer's transaction history and account particulars. A noteworthy example is a predictive model amalgamating Logistic Regression with rigorous evaluation metrics like accuracy, precision, and recall. These metrics furnish invaluable insights into the model's efficacy, ensuring its adeptness in accurately identifying fraudulent activities while minimizing false positives. Notably, this model has demonstrated promising outcomes by discerning patterns within data and refining fraud detection accuracy.

In summary, credit card fraud detection stands as a paramount domain of inquiry within the financial realm, offering substantial prospects for bolstering fraud detection capabilities and curtailing financial losses.

Keywords: Credit Card Fraud, Fraud Detection, Machine Learning Algorithm, Logistic Regression, Evaluation Metrics, Statistical Techniques

1. INTRODUCTION

In today's era dominated by the widespread digitization of financial transactions, safeguarding sensitive data and financial resources has emerged as a critical priority. Credit card fraud continues to pose a persistent and escalating threat, evolving in complexity and magnitude. Addressing this mounting challenge necessitates the development of resilient and adaptable fraud detection systems. This document explores the conception and assessment of a predictive model tailored for credit card fraud detection. Given the pivotal role of credit card transactions in global commerce, the ramifications of fraud are more pronounced than ever. The focal model employs Logistic Regression, a renowned method for binary classification, to scrutinize transactional data comprehensively. By distilling raw transactional information into actionable intelligence, the model evaluates the probability of a transaction being fraudulent, thereby safeguarding financial assets and bolstering customer confidence.

In an environment characterized by dynamic threats and evolving fraudulent tactics, the creation of a credit card fraud detection model is not just a necessity but also an opportunity. It is imperative for shielding financial institutions, e-commerce platforms, and diverse industries from the incessant onslaught of fraud. Concurrently, it presents an opportunity to harness machine learning capabilities to strike a delicate balance between security and operational efficiency. In the subsequent sections, we elucidate the framework of a model engineered to reinforce defenses, mitigate financial losses, and uphold customer trust in an ever-evolving digital milieu.

2. LITERATURE SURVEY

Title: Credit Card Fraud Detection using Machine Learning: A Survey, 2020; Authors: Raghavendra Srinivasaraghavan, Chiranjib Sur; Inference: This survey offers an overview of various machine learning (ML) techniques utilized in credit card fraud detection.

Title: A Study of Machine Learning Techniques for Credit Card Fraud Detection, 2019, Authors: Huanjing Wang, Zijun Yao, Zheng Wu, Yu Wang; Inference: This study conducts a comparative analysis of multiple ML techniques, such as Logistic Regression, Random Forests, Support Vector Machines, and Gradient Boosting, for credit card fraud detection.

Title: Fraud Detection of Credit Card Using Logistic Regression, 2022, Authors: Nasser Hussain Mohammed, Sai Charan Reddy Maram; Inference: This research demonstrates the application of machine learning, specifically logistic regression, in credit card fraud detection. It proposes a classifier built upon logistic regression to mitigate credit card fraud, with a preprocessing phase employed to handle data quality issues and enhance detection accuracy.

Title: Performance Analysis of Machine Learning Algorithms in Credit Cards Fraud Detection, 2020, Authors: Vinod Jain, Mayank Agrawal, Anuj Kumar; Inference: This paper evaluates three machine learning algorithms for credit card fraud detection, with the Random Forest algorithm emerging as the most accurate among the trio, outperforming Decision Tree and XGBOOST.

3. DESIGN AND METHODLOGY

Credit card fraud detection entails a methodical process that begins with the aggregation, cleansing, and preparation of historical credit card transaction data, a phase commonly referred to as data preprocessing. Subsequent to this, the data undergoes analysis to unveil transactional patterns, temporal tendencies, and distinctive attributes indicative of fraudulent activities. Following this exploratory phase, the dataset is partitioned into a training set utilized for model training and a testing set utilized for performance evaluation.

A Logistic Regression model is selected as the foundation for constructing the fraud detection system. This model is trained to ascertain the probability of a transaction being fraudulent based on input features. Upon completion of the training phase, the model undergoes rigorous evaluation employing metrics such as accuracy, precision, recall, and the F1-Score to validate its proficiency in accurately flagging fraudulent transactions while minimizing false positives. This meticulous process establishes a robust framework for safeguarding against credit card fraud.

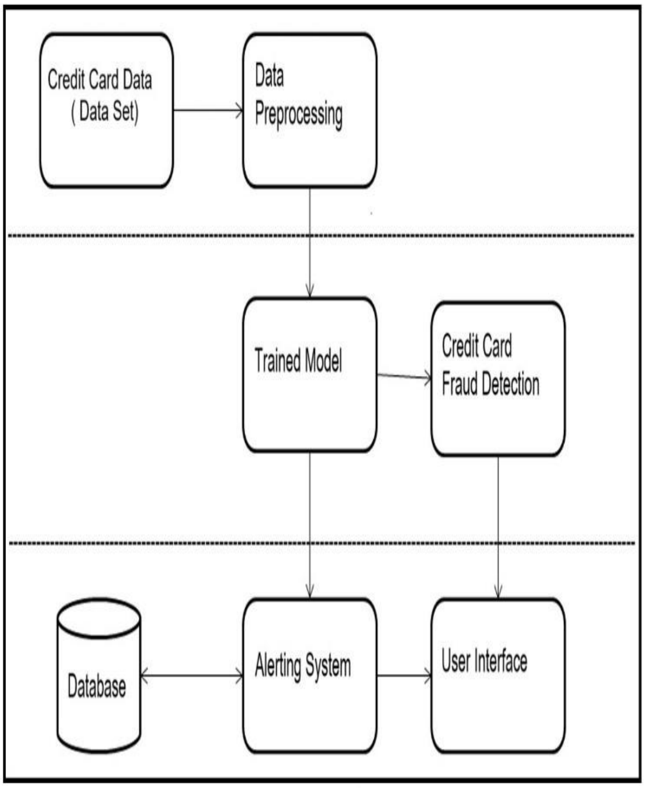


Fig 1. System Architecture

A. STEP DESCRIPTION

Credit Card Data Collection: In the initial phase, historical credit card transaction data is collected. Each data point typically includes attributes such as transaction amount, timestamp, location, merchant information, and other pertinent features. This dataset comprises both legitimate (non-fraudulent) and fraudulent transactions, forming the basis for training and testing the machine learning model.

Data Preprocessing: Data preprocessing is a crucial step aimed at ensuring the quality and reliability of the dataset. It involves several key processes: Handling Missing Values, Duplicate Removal, Data Type Consistency, Class Imbalance Handling, etc.

Data Analysis: In this phase, analysts delve into the pre-processed data to extract valuable insights, including: Feature Exploration, Identification of Fraudulent Transaction Characteristics, Feature Selection, etc.

Train-Test Split: Following preprocessing and analysis, the dataset is partitioned into a training set and a testing set: Training Set (Typically comprising 70-80% of the data) and Testing Set (Consisting of the remaining dataset, the testing set remains isolated from the training phase).

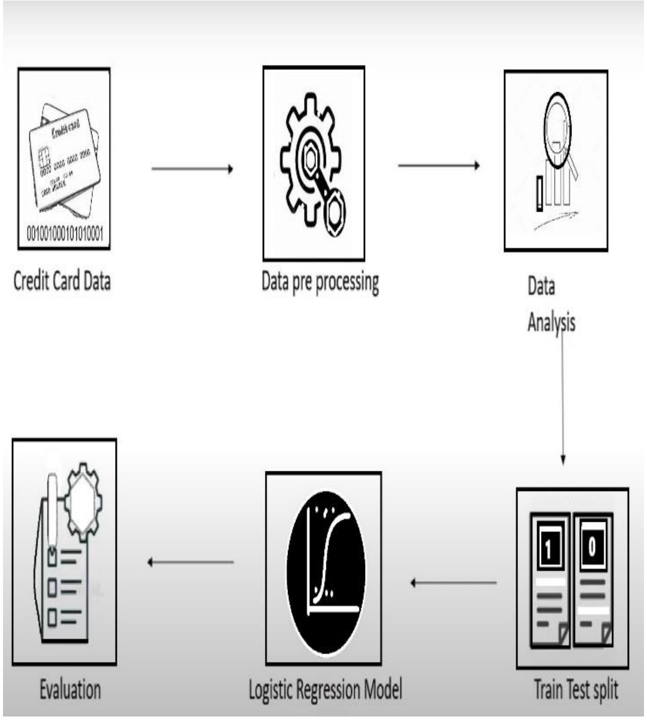


Fig 2. Step Diagram

Logistic Regression Model: The selected machine learning algorithm, Logistic Regression, is employed to construct the credit card fraud detection model: Model Training: The Logistic Regression model is trained on the training dataset, learning to compute the probability of a transaction being fraudulent based on input features such as transaction amount and time. Model

Parameters: Throughout training, the model optimizes its parameters to enhance its accuracy in predicting fraud.

Evaluation: Subsequent to model training, a comprehensive evaluation of its performance on the testing set is conducted using various metrics: Accuracy, Precision, Recall (model's ability to detect all fraudulent cases, ensuring minimal oversight), F1-Score, Receiver Operating Characteristic (ROC) Curve, etc. These evaluation metrics collectively ascertain the model's efficacy in accurately discerning fraudulent transactions while minimizing false positives, thereby ensuring the system's reliability in credit card fraud detection.

B. FLOWCHART

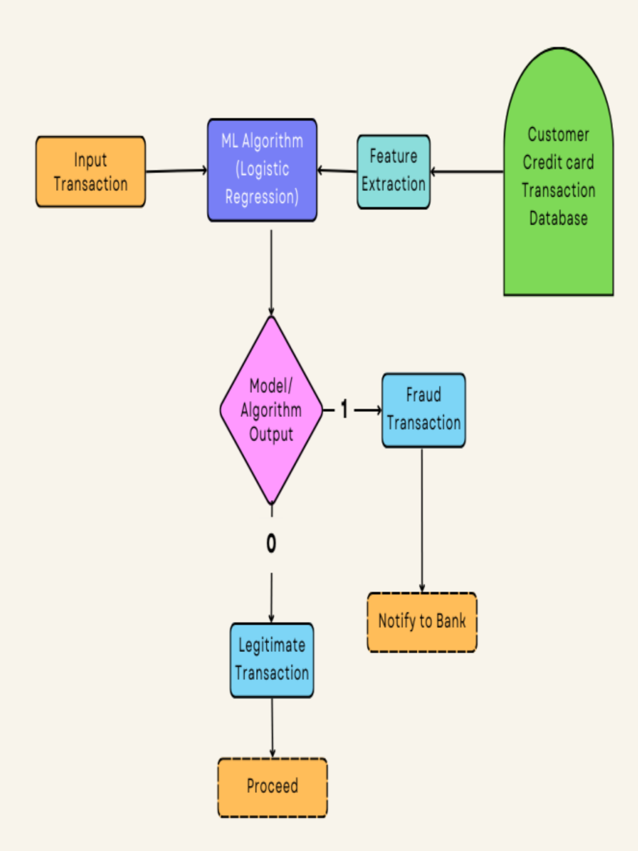


Fig 3. Flowchart of Model

Various Steps:

1. Input Transaction: This marks the initiation of the process. Each incoming credit card transaction is received and scrutinized for its authenticity.

2. Machine Learning Algorithm: Machine learning (ML) algorithms (here Logistic Regression) are utilized to scrutinize and categorize transactions as either genuine or fraudulent.

3. Feature Extraction: This phase entails extracting pertinent features from the incoming transaction data. These features may encompass transaction amount, location, timestamp, and more.

4. Customer Transaction Database: Extracted features are matched against the customer's transaction history stored in a database. This historical data provides a backdrop for evaluating the incoming transaction.

5. Model Output: If the ML algorithm yields an output of "0," it denotes that the transaction is deemed legitimate. In such instances, the system records the transaction as valid. Conversely, if the algorithm's output is "1," it indicates a fraudulent transaction. This triggers the subsequent step.

6. Alert to Bank: Upon identifying a fraudulent transaction, an alert or notification is dispatched to the bank or financial institution. This alert notifies the bank's fraud detection team, urging them to probe the suspicious transaction.

C. MODEL PREDICTION

For creating a credit card fraud detection model, the code segregates the dataset into two subsets: 'fraud' and 'valid', demarcating fraudulent and valid transactions, respectively. Through calculation, it assesses the proportion of fraudulent transactions in the dataset—a crucial metric for understanding the prevalence of fraud.

Next, it partitions the data into feature variables (X) and the target variable (Y), with X encapsulating all columns except the 'Class' column, while Y solely represents the 'Class' column—a categorical indicator of transaction legitimacy. These steps facilitate the isolation of predictor variables and the target label, a fundamental prerequisite for model training.

Following that, the dataset is split into training and testing sets. Employing the train_test_split function, the code orchestrates the division of data, allocating a subset for model training and reserving another for subsequent evaluation. This segregation ensures a rigorous assessment of the model's performance on unseen data, an indispensable aspect of model validation. With above work, the logistic regression model is instantiated and trained and later a model instance is initialized and fitted to the training data. Through this process, the model learns to discern patterns in the data, enabling it to differentiate between fraudulent and valid transactions.

Lastly, by generating predictions on the test data using the trained model, it endeavours to ascertain the model's efficacy in classifying transactions. This evaluation serves as a critical checkpoint, enabling to gauge the model's effectiveness and make informed decisions regarding its deployment.

D. EVALUATION AND RESULTS

To evaluate and analyse the model’s effectiveness in identifying fraudulent transactions, we computed several evaluation metrics to quantify the model's performance. The evaluation metrics computed here are:

1. Accuracy: It gives the overall correctness of the model's predictions. Accuracy calculates the ratio of correctly predicted transactions (both fraudulent and legitimate) to the total number of transactions. However, accuracy may not be the most informative metric when dealing with imbalanced datasets (where fraudulent transactions are rare).

2. Precision: Precision represents the number of correctly predicted fraudulent transactions out of all the transactions predicted as fraudulent. It is a crucial parameter as it helps minimize false alarms. High precision indicates that when the model predicts a transaction as fraudulent, it is likely to be correct.

3. Recall (Sensitivity): Recall, also known as sensitivity or true positive rate, measures the number of correctly predicted fraudulent transactions out of all the actual fraudulent transactions. It's essential for ensuring that fraudulent transactions are not missed. High recall means that the model is effective at identifying actual fraud cases.

4. F1-Score: F1-Score represents the harmonic mean of precision and recall metrics. It provides a balanced measure of the model's performance, considering both false alarms and missed fraud cases. It gives a perfect balance between precision and recall.

5. Confusion matrix: Confusion matrix, alternatively the error matrix, is a table that which is used to describe the performance of a classification model on a set of test data for which the true values are given. It is used to visualize the performance of an algorithm. Each row of the matrix denotes the instances in an actual class, while each column denotes the instances in a predicted class.

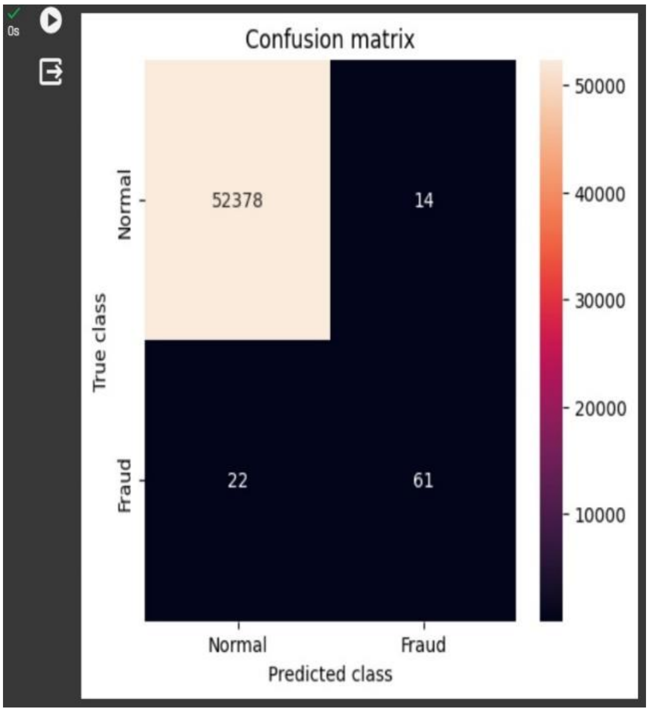
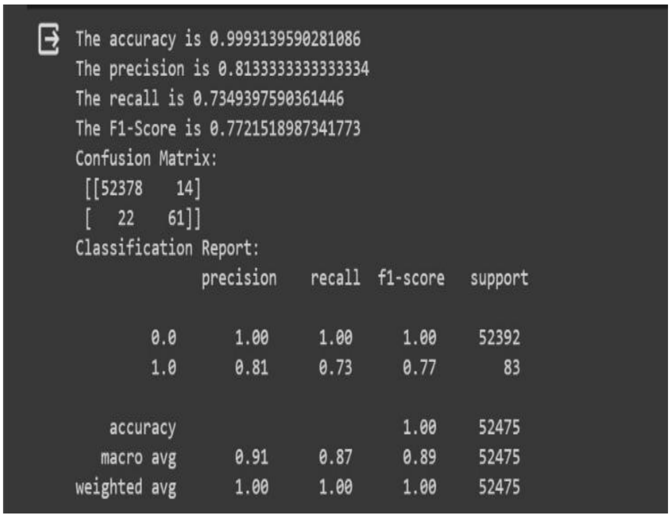


Fig 4. Confusion Matrix of Model

The confusion matrix provided a detailed breakdown of the model's classifications, distinguishing between true negatives (correctly identified valid transactions), false positives (valid transactions incorrectly classified as fraudulent), false negatives (fraudulent transactions incorrectly classified as valid), and true positives (correctly identified fraudulent transactions).

Result: This model with Logistic Regression algorithm is able to achieve high accuracy rates when predicting fraudulent transactions. However, accuracy alone is not always the best metric to evaluate the performance of a model, especially in financial application like credit card fraud detection. Other metrics like precision, recall, and F1- score are also quite satisfactory. This model achieves following scores: Precision = 0.812, Recall = 0.734 and F1-Score = 0.77.



```
The accuracy is 0.9993139590281086
The precision is 0.8133333333333334
The recall is 0.7349397590361446
The F1-Score is 0.7721518987341773
Confusion Matrix:
 [[52378    14]
 [   22    61]]
Classification Report:
              precision    recall  f1-score   support

         0.0       1.00      1.00      1.00     52392
         1.0       0.81      0.73      0.77        83

    accuracy                           1.00     52475
   macro avg       0.91      0.87      0.89     52475
weighted avg       1.00      1.00      1.00     52475
```

Fig 5. Evaluation Metrics Code Snippet

The comparison among the various ML algorithms that are used in different credit card fraud detection models is shown using several evaluation metrics:

ML Algorithm Comparison				
ML Algorithm Name	Evaluation Metrics			
	Accuracy	Precision	Recall	F1-score
Logistic Reg.	0.99931	0.8133	0.7349	0.77
Isolation Forest	0.99789	0.375	0.3367	0.35
Random Forest	0.99956	0.9740	0.7653	0.85
Decision Tree	0.99934	0.8512	0.7304	0.78

Fig 7. Comparison of various ML Algorithms

4. CONCLUSION

The domain of credit card fraud detection is in a constant state of evolution, driven by advancements in technology and data analytics. Machine learning and predictive models have emerged as pivotal tools in this arena, empowering financial institutions and businesses to combat increasingly sophisticated fraudulent activities. These technological advancements play a dual role, bolstering both security measures and customer confidence. Through real-time monitoring and predictive modelling, immediate protection against fraudulent transactions is afforded, instilling trust in customers regarding the safety of their financial transactions.

Furthermore, the realm of credit card fraud detection extends beyond national boundaries. The future trajectory emphasizes collaborative networks and information sharing among stakeholders, fostering a unified approach against fraud on a global scale. Customization and adaptability serve as cornerstone principles, enabling financial institutions to tailor fraud detection strategies to their specific requirements and risk profiles, while remaining agile in response to emerging fraud tactics.

The insights derived from data-driven models not only fortify fraud prevention efforts but also yield invaluable insights into customer behaviour and transactional patterns. This wealth of data informs strategic decision-making processes and facilitates targeted marketing endeavours, providing a comprehensive understanding of customer interactions.

As technology continues to advance, new challenges inevitably arise. The emergence of quantum computing and innovative fraud techniques underscores the need for pioneering solutions to effectively safeguard financial transactions. Regulatory compliance remains paramount, necessitating financial institutions to adhere to evolving standards while ensuring the delivery of a secure and seamless payment ecosystem.

In this dynamic landscape, the future of credit card fraud detection hinges on collaborative partnerships, tailored solutions, and relentless innovation to uphold the security of financial transactions, while concurrently nurturing customer trust and facilitating business expansion.

REFERENCES

[1] Vinod Jain; Mayank Agrawal; Anuj Kumar. Performance Analysis of Machine Learning Algorithms in Credit Cards Fraud Detection. DOI: 10.1109/ICRITO48877.2020.9197762 || IEEE || 04-05 June 2020.

[2] Dr. Yvan Lucas; Dr. Johannes Jurgovsky. Credit card fraud detection using machine learning: A survey. arXiv:2010.06479v1 [cs.LG]13 Oct 2020.

[3] Dighe D, Patil S, Kokate S. Detection of credit card fraud transactions using machine learning algorithms and neural networks: a comparative study. In: IEEE, 2018. P. 1–6.

[4] Ozlem Kilickaya. Credit Card Fraud Detection: Comparison of Different Machine Learning Techniques. www.ijlemr.com || Vol. 09 – Issue 01 || Jan 2024 || PP 15-27.

[5] Awoyemi, John O., et al. “Credit Card Fraud Detection Using Machine Learning Techniques: A Comparative Analysis” .International Conference on Computing Networking and Informatics (ICCNI), 2017; doi:10.1109/iceni.2017.8123782.

[6] Mohammed, Nasser Hussain and Maram, Sai Charan Reddy, Fraud Detection of Credit Card Using Logistic Regression (March 25, 2022) Available at SSRN: https://ssrn.com/abstract=4135514 or http://dx.doi.org/10.2139/ssrn. 4135514.

[7] M. Devika; S. Ravi Kishan; L. Sai Manohar; N. Vijaya. Credit Card Fraud Detection using Logistic Regression. IEEE || DOI: 10.1109/ICATIECE56365.2022.10046976.

[8] Arvind Rawat; Sandeep Kumar Tiwari. A comprehensive review on credit card fraud detection using machine learning techniques. Volume: 12 Issue: 2, April 2023 || DOI: 10.26671/IJIRG.2023.2.12.103.

[9] Mohammed, Emad, and Behrouz Far. “Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study.” EEE Annals o the s tory o Computing EEE1 uly 2018 doi.ieeecomputersociety.org/10.1109/ .2018.00025.

[10] https://www.kaggle.com/code/ashishkoli483/credit-card-fraud-detection/input/dataset