Fraud Detection in Banking Transactions - Credit Card

Nishchal Gaur
IIIT Delhi
Roll no:2022330
Email: nishchal22330@iiitd.ac.in

Niteen Kumar
IIIT Delhi
Roll no:2022336
Email: niteen22336@iiitd.ac.in

***Abstract*—In today's digital world, detecting fraud in banking transactions, particularly credit card fraud, is a pressing concern for financial institutions and consumers alike. With the rise of online transactions, traditional fraud detection methods often fall short in identifying new and sophisticated fraud schemes. Our project delves into the realm of ML algorithms and their application in detecting fraudulent transactions. By studying a diverse dataset containing both genuine and fraudulent transactions, we aimed to understand how algorithms like logistic regression, decision trees, random forests, support vector machines, and neural networks can be utilized for fraud detection. Additionally, we explored anomaly detection techniques, including isolation forests and autoencoders, to uncover irregular patterns indicative of fraudulent activity.**

***Keywords*– Fraud detection, Semi-Supervised learning, Autoencoders Neural Network, Automated fraud detection, neural network, Imbalanced dataset.**

I. PROBLEM STATEMENT AND MOTIVATION

Credit card fraud represents a persistent threat in the digital age, posing significant challenges to both financial institutions and consumers. As online transactions continue to surge, traditional fraud detection methods are struggling to keep pace with the evolving tactics of fraudulent activities. The problem is exacerbated by the dynamic nature of fraudulent schemes, which continually adapt to circumvent existing detection mechanisms. Consequently, there is an urgent need to develop and implement advanced fraud detection systems specifically tailored for credit card transactions.

These systems must possess the capability to analyze vast volumes of transactional data in real-time, identifying subtle indicators of fraudulent behavior amidst the noise of legitimate transactions. Furthermore, they must be capable of distinguishing between legitimate and fraudulent transactions with a high degree of accuracy while minimizing false positives and negatives. Achieving this level of accuracy and efficiency is crucial not only for protecting financial institutions from substantial financial losses but also for safeguarding consumer trust and confidence in electronic payment systems.

The motivation behind addressing the problem of credit card fraud detection is multifaceted. Financial institutions face significant financial losses due to fraudulent transactions, which can result in reputational damage, regulatory penalties, and legal liabilities. Moreover, the erosion of consumer trust stemming from fraudulent activities can have far-reaching implications, deterring individuals from engaging in online transactions and undermining the viability of electronic payment systems as a whole.

On the consumer side, credit card fraud represents more than just financial loss. It can lead to identity theft, compromised personal information, and emotional distress. The aftermath of fraudulent transactions often involves lengthy and cumbersome processes to rectify the situation, causing inconvenience and frustration for affected individuals.

Addressing these challenges requires a concerted effort to develop innovative fraud detection systems that leverage advanced technologies such as machine learning, data analytics, and artificial intel-

ligence. By deploying sophisticated algorithms capable of identifying patterns indicative of fraudulent behavior, financial institutions can enhance their ability to detect and prevent fraudulent activities in real-time, thereby safeguarding the integrity of electronic payment systems and restoring consumer confidence.

II. LITERATURE REVIEW

Prajal Save et al. [18] have proposed a model based on a decision tree and a combination of Luhn's and Hunt's algorithms. Luhn's algorithm is used to determine whether an incoming transaction is fraudulent or not. It validates credit card numbers via the input, which is the credit card number. Address Mismatch and Degree of Outlierness are used to assess the deviation of each incoming transaction from the cardholder's normal profile. In the final step, the general belief is strengthened or weakened using Bayes Theorem, followed by recombination of the calculated probability with the initial belief of fraud using an advanced combination heuristic. Vimala Devi. J et al. [19] To detect counterfeit transactions, three machine-learning algorithms were presented and implemented. There are many measures used to evaluate the performance of classifiers or predictors, such as the Vector Machine, Random Forest, and Decision Tree. These metrics are either prevalence-dependent or prevalence-independent. Furthermore, these techniques are used in credit card fraud detection mechanisms, and the results of these algorithms have been compared. Popat and Chaudhary [20] supervised algorithms were presented Deep learning, Logistic Regression, Nave Bayesian, Support Vector Machine (SVM), Neural Network, Artificial Immune System, K Nearest Neighbour, Data Mining, Decision Tree, Fuzzy logic based System, and Genetic Algorithm are some of the techniques used. Credit card fraud detection algorithms identify transactions that have a high probability of being fraudulent. We compared machine-learning algorithms to prediction, clustering, and outlier detection. Shiyang Xuan et al. [21] For training the behavioral characteristics of credit card transactions, the Random Forest classifier was used. The following types are used to train the normal and fraudulent behavior features Random forest-based on random trees and random forest based on CART. To assess the model's effectiveness, performance measures are computed. Dornadula and Geetha S. [5] Using the Sliding-Window method, the transactions were aggregated into respective groups, i. , some features from the window were extracted to find cardholder's behavioral patterns. Features such as the maximum amount, the minimum amount of a transaction, the average amount in the window, and even the time elapsed are available. Sangeeta Mittal et al. [22] To evaluate the underlying problems, some popular machine learning- algorithms in the supervised and unsupervised categories were selected. A range of supervised learning algorithms, from classical to modern, have been considered. These include tree-based algorithms, classical and deep neural networks, hybrid algorithms and Bayesian approaches. The effectiveness of machine-learning algorithms in detecting credit card fraud has been assessed. On various metrics, a number of popular algorithms in the supervised, ensemble, and unsupervised categories were evaluated. It is concluded that unsupervised algorithms handle dataset skewness better and thus perform well across all metrics absolutely and in comparison to other techniques. Deepa and Akila [17] For fraud detection, different algorithms like Anomaly Detection Algorithm, K-Nearest Neighbor, Random Forest, K-Means and Decision Tree were used. Based on a given scenario, presented several techniques and predicted the best algorithm to detect deceitful transactions. To predict the fraud result, the system used various rules and algorithms to generate the Fraud score for that certain transaction. Xiaohan Yu et al. [23] have proposed a deep network algorithm for fraud detection A deep neural network algorithm for detecting credit card fraud was described in the paper. It has described the neural network algorithm approach as well as deep neural network applications. The preprocessing methods and focal loss; for resolving data skew issues in the dataset. Siddhant. Bagga et al. [24] presented several techniques for determining whether a transaction is real or fraudulent Evaluated and compared the accomplishment of 9

techniques on data of credit card fraud, including logistic regression, KNN, RF, quadrant discriminative analysis, naive Bayes, multilayer perceptron, ada boost, ensemble learning, and pipelining, using different parameters and metrics. ADASYN method is used to balance the dataset. Accuracy, recall, F1 score, Balanced Classification Rate are used to assess classifier performance and Matthews's correlation coefficient. This is to determine which technique is the best to use to solve the issue based on various metrics. Carrasco and Urban [25] Deep neural networks have been used to test and measure their ability to detect false positives by processing alerts generated by a fraud detection system. Ten neural network architectures classified a set of alerts triggered by an FDS as either valid alerts, representing real fraud cases, or incorrect alerts, representing false positives. When capturing 91.79 percent of fraud cases, optimal configuration achieved an alert reduction rate of 35.16 percent, and a reduction rate of 41.47 percent when capturing 87.75 percent of fraud cases. Kibria and Sevkli [26] Using the grid search technique, create a deep learning model. The built model's performance is compared to the performance of two other traditional machine-learning algorithms: logistic regression (LR) and support vector machine (SVM). The developed model is applied to the credit card data set and the results are compared to logistic regression and support vector machine models. Borse, Suhas and Dhotre. [27] Machine learning's Naive Bayes classification was used to predict common or fraudulent transactions. The accuracy, recall, precision, F1 score, and AUC score of the Naive Bayes classifier are all calculated. Asha R B et al. [14] have proposed a deep learning-based method for detecting fraud in credit card transactions. Using machine-learning algorithms such as support vector machine, k-nearest neighbor, and artificial neural network to predict the occurrence of fraud. used.

III. DATASET AND FEATURES

The dataset being used is collected from Kaggle.It contains 23 variables and nearly 1296675 credit card transactions labeled as either legitimate or fraudulent.Table 1 provides descriptive information about the dataset

Name of the features	**Description**
index	Serves as a unique identifier for each row in the dataset, allowing for easy referencing and data management.
trans_date_trans_time	Represents the precise date and time of each transaction, providing temporal information for analysis and tracking.
cc_num	The credit card number of the customer involved in the transaction, crucial for identifying the specific card used.
merchant	Name of the merchant where the transaction took place, providing insight into the businesses involved in the transactions.
category	Specifies the category of the merchant, offering additional context about the type of transaction.
amt	Denotes the amount of the transaction, indicating the monetary value involved in each transaction.
first	First name of the credit card holder, providing personal identification details.
last	Last name of the credit card holder, completing the personal identification details.
gender	Indicates the gender of the credit card holder, providing demographic information.
street	Specifies the street address of the credit card holder, offering location details.
city	Represents the city of residence of the credit card holder.
state	Denotes the state of residence of the credit card holder.
zip	Provides the ZIP code of the credit card holder's address, offering location-specific information.
lat	Indicates the latitude location of the credit card holder's address, providing geographical coordinates.
long	Specifies the longitude location of the credit card holder's address, providing geographical coordinates.
city_pop	Represents the population of the city where the credit card holder resides, offering demographic information.
job	Specifies the job or occupation of the credit card holder, providing additional demographic details.
dob	Stands for the date of birth of the credit card holder, providing age-related information.
trans_num	The transaction number, serving as a unique identifier for each transaction.
unix_time	Represents the UNIX time of the transaction, providing a standardized reference point for time calculations.
merch_lat	Denotes the latitude location of the merchant where the transaction took place.
merch_long	Specifies the longitude location of the merchant where the transaction took place.
is_fraud	This is the target column, indicating whether the transaction is flagged as fraudulent (1) or not (0), serving as the label for fraud detection algorithms.

IV. EVALUATION METRICS

When evaluating a Fraud Detection project for credit card transactions, it's important to consider various metrics to assess the performance of the model. Here are some common evaluation metrics

for Fraud Detection in Banking Transactions:

1. **Accuracy:**

$$\text{Formula: } \frac{TP + TN}{TP + TN + FP + FN}$$

Accuracy measures the overall correctness of the model by considering both true positives (correctly identified fraud) and true negatives (correctly identified non-fraud).

2. **Precision (Positive Predictive Value):**

$$\text{Formula: } \frac{TP}{TP + FP}$$

Precision measures the accuracy of positive predictions, providing insight into the proportion of predicted fraud cases that are actually fraud.

3. **Recall (Sensitivity, True Positive Rate):**

$$\text{Formula: } \frac{TP}{TP + FN}$$

Recall measures the ability of the model to identify all relevant instances of fraud, indicating the proportion of actual fraud cases that are correctly predicted.

4. **F1 Score:**

$$\text{Formula: } 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

The F1 Score is the harmonic mean of precision and recall, providing a balance between the two metrics. It is especially useful when there is an imbalance between fraud and non-fraud cases.

5. **Area Under the Receiver Operating Characteristic (ROC-AUC):**
ROC-AUC measures the ability of the model to discriminate between positive and negative instances. A higher ROC-AUC value indicates better performance.

6. **False Positive Rate (FPR):**

$$\text{Formula: } \frac{FP}{FP + TN}$$

FPR measures the proportion of actual non-fraud cases that are incorrectly predicted as fraud. A lower FPR is desirable in fraud detection.

7. **False Negative Rate (FNR):**

$$\text{Formula: } \frac{FN}{FN + TP}$$

FNR measures the proportion of actual fraud cases that are incorrectly predicted as non-fraud. Minimizing FNR is crucial to avoid missing fraudulent transactions.

8. **Confusion Matrix:** A table showing the counts of true positives, true negatives, false positives, and false negatives. It provides a detailed breakdown of the model's performance.

9. **Precision-Recall Curve:**
Graphical representation of the trade-off between precision and recall for different threshold values. It is particularly useful when dealing with imbalanced datasets.

10. **Cost of Misclassification:** Consider the potential financial impact of misclassifying fraud and non-fraud cases. Assign costs to false positives and false negatives based on the specific context of the application.
When evaluating a Fraud Detection model, it's essential to consider a combination of these metrics, as no single metric provides a complete picture of the model's performance. Additionally, the choice of metrics may depend on the specific goals and priorities of the banking institution deploying the model.

REFERENCES

Here, are the given reference of the DataSet for our projects.
https://www.kaggle.com/datasets/kartik2112/fraud-detection/data?select=fraudTrain.csv