International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 05 May 2024
Page No: 1427 - 1434
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0196

Fraud Detection in Financial Transactions Using Credit Card: A Machine Learning Model

Dr Rakesh Kumar Pathak[1], Priyanshu Gaurav[2], Vaibhav Kumar[3], Aditya Raj[4]

[1] Assistant Professor, Department of Computer Science, St. Xavier's College of Management & Technology, Patna, India.

[2,3,4] UG, BCA Department of Computer Science, St. Xavier's College of Management & Technology, Patna, India

Emails: *rakeshkumarpathak@sxcpatna.edu.in[1], priyanshugaurav01@gmail.com[2], vaibhavkumarjak@gmail.com[3], aditya040mth@gmail.com[4]*

Abstract

Fraud in any financial transactions causes severe loss to both customer as well as the seller. The loss is not confined to financial loss only but it also causes severe dent to the confidence of the customer especially related to shopping platform and the payment instrument used. Nowadays a substantial part of buying and selling of goods and services are taking place using various e commerce platforms. Many customer use credit card as payment instrument. During the payment process, users do exposes the credit card credentials to the payment platform. These payment platforms are vulnerable to fishing and hacking attackers and the payment instrument remains highly susceptible to fraudulent activities. There are two approaches to dealing with this problem. The first step is to identify the fraudulent activities and second step is to prevent any such attempt of fraud. This paper proposes a model based on machine learning algorithms to identify fraudulent attempts by analyzing credit card transactions data set and proposes methods of preventing such fraud activities. The paper also presents the accuracy of this AI model in identifying and preventing fraudulent and mischievous activities.

Keywords: *Artificial Intelligence, Machine Learning, Fraud Detection, Fraud Prevention.*

1. Introduction

Trade and commerce is one of the most ancient endeavours of mankind across civilizations that is still in progress and will definitely exist till the doom's day. With the development of civilizations economies have also developed so has the methods of payments of any kind of transaction. Starting from the barter system economies of the world have travelled a long distance. Money has been represented in different forms like Gold, Silver, Copper and other similar precious commodities. Modern economies introduced paper money, which is a kind of promissory note that has government's endorsement. Plastic money is one of the latest tool of payment which has various forms like smart card, pre-paid card, debit card, credit card etc. Among different types of plastic money instruments, credit card is one of the most popular one. Relatively educated and well to do segment of the society is offered this tool by banking and financial institutions. In nut cell, it is a credit facility offered by the issuing authority to their customers. Against the credit limit, customers can make payment and later on they repay the debt as per the terms of the credit facility extended to them. Since it is a tool which has a hefty balance in general, people enjoy this facility of short term borrowing and repayment. On one hand this seems to be very flexible and customer friendly facility on the other hand if due care is not taken, things can go wrong and money can be stolen electronically from the credit card and the customer to whom it is issued will be liable to pay the money. This is a traumatic experience and financial hazard both. With the growth in the precision of modern algorithms and programming techniques, intruders and hackers are using cutting edge tools and techniques and a little negligence or lethargy can lead to severe financial loss to the customers. Banks and financial institutions have introduced a lot of safety measures to safeguard their customers against the fraudulent activities but they alone cannot prevent the fraud. Customers also have to be careful to protect their credentials use them with utmost care. Fraud in all financial transactions causes harm to both the customer and the seller. The damage is not only limited to financial losses, but it also undermines the confidence of the customer, especially in relation to the shopping platform and payment method used. Today, a significant part of the buying and selling of goods and services takes place through various electronic commerce platforms. Many customers use a credit card as a means of payment. During the payment process, users disclose credit card information to the payment platform. These payment platforms are vulnerable to phishing and hacking attacks, and the payment instrument remains highly vulnerable to fraudulent activity. Cyber thieves take advantage of this vulnerable period and retrieve vital user credential information and later they perform their fraudulent activities. Central and commercial banks as well as financial institutions run various types of awareness program to educate the customers of credit card to observe certain precautions but even with slight negligence or overlook on user’s part, these thieves come out victorious. There are different method that are being used by the people indulged in credit card frauds, however identity theft and impersonation are the most common and widely used techniques. The most recent data on credit card fraud and identity theft paints a dire picture. They have been among the most prevalent forms of fraud since 2020. Throughout 2023, even though reports of credit card fraud and identity theft decreased, they were still higher than they were prior to the pandemic. The identity theft statistics collected by the federal trade commission table 8 (FTC), USA revealed that in 2023 alone there were around 1 million reported cases of identity theft of credit cards. It is highly that there were a sizeable number of cases that go unreported.

Table 1 Reported Cases of Identity Theft Leading to Credit Card Frauds

Year	Reported Cases of Identity theft of credit card
2019	650000
2020	1389000
2021	1434000
2022	1108000
2023	1037000

The above table 1 shows that there is a decline in the reported cases of credit card frauds in the last two years but they still the numbers are too big to deal with. According to a report by the Javelin Strategy and Research, Identity theft case resulted in a loss of $20 billion in 2022 alone, a significant jump of 15% from 2021 figure 1.

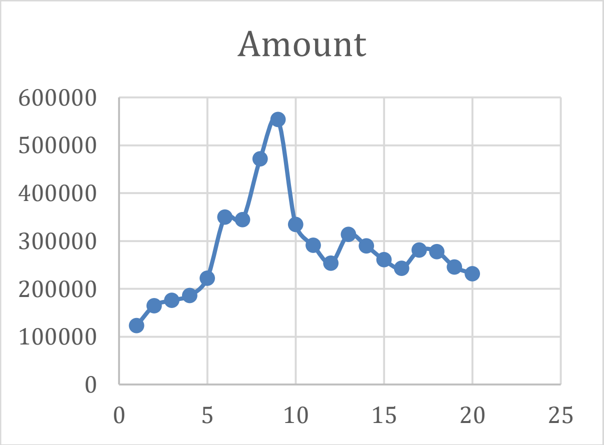

Figure 1 Federal Trade Commission, USA, and Report 2024

The culprits of credit card frauds are adopting different means to cheat people. Some of the most common techniques are that they hack payment sites or web pages where credit card credentials are punched into and later on use these vital information to carry their fraudulent activities. Similarly they make fake calls to customers impersonating bank or other officials and ask for vital information such as CVV and OTP, and those who fell into this trap, get cheated and suffer financial loss [1]. Fishing and spoofing are some other means of cheating and frauds.

1.1 Data Breaches

One method used by thieves to commit credit card fraud and identity theft is data breaches. Information obtained by hackers via data breaches is frequently sold on the dark web. Following that, buyers exploit the data for other kinds of fraud. Nationwide reports that while 69% of consumers lack cyber insurance, 58% of consumers are worried about being victims of cybercrime. According to The Identity Theft Resource Center, the number of data breaches increased to 3,205 in 2023 from 1,801 in 2022, although the number of people affected decreased by 17%, from 422 million to 352 million. The reason for dip in the number of people getting affected by data theft is that the hackers are looking for specific information to carry forward credit card frauds and not every information that they steal can be used for this purpose.

Table 2 Data Breaches

Year	Number of data compromises	Number of individuals impacted
2016	1,104	2,541,581,891
2017	1,631	2,081,515,330
2018	1,280	2,231,245,353
2019	1,362	887,286,658
2020	1,108	300,562,519
2021	1,860	300,607,163
2022	1,801	422,212,090
2023	3,205	352,027,892

2. Literature review

Theft and cheating are not new phenomenon in our life. These are as old as our civilizations. With time methods of preventing such acts have evolved and so has the cheating and fraud activities. This evolution is an ongoing process. Credit cards are relatively new tool of modern economy and their uses are growing day by day as middle class population is growing in almost all the economies globally. Similarly fraud and cheating activities have also been growing globally. Thanks to artificial intelligence and machine learning methodologies, fraud and fraudulent activities can be tracked and monitored and based on some patterns of these activities, preventive and other pro-active actions can be triggered. Many researchers have been working on these issues tirelessly and have proposed many techniques of dealing with such activities. Decision trees, Bayesian techniques, clustering algorithms like k-Nearest Neighbors, neural networks, support vector machines, regression models, gradient boosted trees, Markov models, and restricted Boltzmann Machines (RBMs) have all been used in the past to address anomaly detection in consumer behavior. To detect fraud in credit card transactions many supervised and semi supervised machine learning algorithms are used [2]. The data set used for these ML algorithms however suffer from three main deficiencies, which are, a dominant class imbalance, the data set has both labelled and unlabeled columns and these algorithms have a capacity limit when it comes to the size of data set used for credit card fraud detection. We aim to alleviate these three issues. Emad, and Behrouz [3] in their paper have stated that a plethora of machine learning algorithms like Decision Trees, Naive Bayes Classification, Least Squares Regression, Logistic Regression and SVM are used to detect fraudulent activities from real time datasets of credit card transactions. Xuan, Shiyang, et al [4], identified two methodologies under Random Forest algorithm which are Random Tree Based Random Forest and Cart Based to train the model about behavioural features of normal and fraudulent transactions. The concept of decision trees served as the basis for the development of the similarity tree idea [5]. Recursively defined similarity trees begin with labeling nodes with attribute names, labeling margins with attribute values corresponding to a necessary condition, and leaf nodes representing a percentage of the ratio between the total number of transactions that are legitimate and the number of transactions that comply with the conditions. This strategy, which is explained graphically, is very simple to comprehend and apply. The tedious aspect might be having to review every detail of every transaction to ensure it fits into a certain category. However, it turns out that similarity trees performed incredibly well in various kinds of fraud detection situations.

3. Proposed Work

In this paper we propose a machine learning model that will detect fraudulent a fraudulent transaction from a large collection of transactions performed using credit card. For this the proposed model will use machine learning algorithms to categorize the data set containing details of credit card transactions. For this classification, the proposed model uses the features of the credit card transactions contained within the dataset. The dataset retrieval of credit card transactions is a very difficult because no banking or financial institutions are willing to share their customer's transactional data, that too of the credit card transactions. This reluctance is due to the obvious reasons to protect customer credentials and maintaining the confidentiality clause. To overcome this problem, the required dataset has been downloaded from www.kaggle.com[6] portal and the dataset file name is creditcard.csv. This dataset contains roughly a collection of 285000 records of credit card transactions spanning across 31 columns. Bellow given table 2 shows the basic details of the transaction captured during the transactions made using credit card. The dataset used in this model has a total of 284807 records out of which only 492 which is a negligible 0.172 % of the total number of transactions.

Table 3 The Transactions Made Using Credit Card

Transactions Feature Name	Description
Transaction ID	Unique identification number of every transaction
Customer ID	Cardholder's Unique ID
Amount	Amount transferred or spent by the customer on the transaction
Time	Timestamp of the transaction.
Label	Feature specifying whether transaction is legitimate one or a fraudulent one.

This fact makes this dataset highly imbalance. Further table 3 disclosing the credit card transaction details of a customer will be a breach of confidentiality clause, therefore most of the features in the dataset are transformed using principal component analysis (PCA). V1, V2, V3,..., V28 are PCA applied features and rest i.e., 'time', 'amount' and 'class' are non-PCA applied features

Table 4 PCA

Serial Number	Feature Name	Description
1	Time	Time in seconds to specify the elapses between the current transaction and first transaction
2	Amount	Transaction Amount
3	Class	0= Non Fraud Transaction 1=Fraudulent Transaction

The dataset creditcasr.csv is a huge dataset containing 284807 transaction instances out of which only 492 transactions fall into the category of fraudulent transactions. To overcome this data imbalance problem, a sampling technique's need was felt. A sampling technique is a method used to select a subset of data from a large dataset to handle the imbalance ratio of the class imbalance. We have used a sampling technique called "under sampling". Under sampling is a technique used to reduce the number of instance in the majority class to match the number of instances in the minority class. This helps in balancing the class distribution and improving the performance of machine learning methods. After performing the under sampling step, we have used logistic regression method to train our model using the creditcard.csv dataset. Logistic regression is a fundamental algorithms used for binary classification tasks in machine learning. Logistic Regression is a supervised learning algorithm used for binary classification making it suitable for identifying whether a transaction is a legitimate transaction or a fraudulent one. It works by fitting a logistic curve to the data producing an "S" shaped curve. This curve maps any real world number to a value between 0 and 1. This mapping is achieved using the logistic function which transforms output of the linear regression model into a probability score between 0 and 1. To further enhance the performance of the proposed machine learning model we have used yet another ML algorithm to train our model table 5. The method name is Random Forest. Random forest is a powerful machine learning algorithm used for both classification and regression tasks. It is an ensemble learning method, which means it combines multiple individual models to create a more powerful model. In the case of Random Forest, this individual model is the decision tree. One of the key feature of Random Forest is that it reduces over fitting, which is a common problem in machine learning where a model performs well on the training data but fails to generalize to new unseen data. Random Forest achieves this by averaging the predictions of multiple decision trees which helps to smooth out the noise in the data and makes more accurate predictions on unseen data.

3.1 Data Preprocessing

To address the inherent class imbalance, wherein legitimate transactions outweigh fraudulent ones, an undersampling technique is employed. This entails randomly selecting legitimate transactions to match the volume of fraudulent ones, thereby ensuring balanced representation. Subsequently, the data is partitioned into training and testing sets using the train_test_split() function.

3.2 Model Selection and Implementation

Logistic regression is chosen as the classification algorithm due to its robust performance in binary classification tasks. By modelling the probability of an event occurrence based on input features, logistic regression provides a solid framework for discerning fraudulent transactions. The LogisticRegression() function from scikit-learn is utilized to train the model on the prepared training data.

3.3 Streamlit Application

A user-friendly interface is developed using Streamlit, allowing seamless interaction with the credit card fraud detection system. Users can upload their CSV file containing transaction data, which is then utilized to train the logistic regression model. Additionally, users have the option to input transaction features manually and receive real-time predictions regarding the transaction's legitimacy.

4. Findings

The outcome of training and test score of the model using the Logistic Regression model is Train Model Classification Report

Table 5 Train Model Classification Report

	Precision	**Recall**	**F1 Score**	**Support**
No Fraud	1.00	1.00	1.00	227468
Fraud	0.89	0.63	0.74	377
Accuracy			1.00	227845
Macro Average	0.94	0.81	0.87	227845
Weighted Average	1.00	1.00	1.00	227845

Table 6 **Test Model Classification Report**

	Precision	Recall	F1 Score	Support
No Fraud	1.00	1.00	1.00	56847
Fraud	0.83	0.61	0.70	115
Accuracy			1.00	56962
Macro Average	0.92	0.80	0.85	56962
Weighted Average	1.00	1.00	1.00	56962

For the above analytical report, a confusion matrix is used. A confusion matrix is something that are utilised to summarize the functioning of a classification algorithms. For binary classification, as in my model's case, the dimension of the confusion matrix will be 2X2. Similarly for multiclass classification, the dimension of the classification will be equal to the number of classes. For example, for N classes, the dimension of the matrix will be NXN. For binary classification, the classification model predicts the probability that each instance of the dataset belongs to one class or the other [7]. The performance matrix evaluated the similarity or differences between the actuals verses the predictions. For this it uses following evaluation methodologies [8]

True Positive (TP): True Positive measures the extent of accuracy to which it predicts the positive class.

True Negative (TN): True Negative is the measurement of accuracy of model predicting real negative values as negative.

False Positive (FP): False positive means that the model predicts that an observed value belongs to one particular [9] class whereas in in reality it does not.

False Negative (FN): False negative is the just opposite of false positive. It occurs when the model classifies a test dataset as negative while in reality it is positive [10].

5. Parameters of evaluating Prediction's using Confusion Matrix

The performance matrix or the confusion matrix uses following four parameters to evaluate the prediction models [11]

Accuracy: It is the ratio of correct prediction with that of total prediction

Accuracy= correct prediction / (Total correct + Total incorrect) predictions

Accuracy= (TP+TN) / (TP+FP+TN+FN)

Precision Score: It is the measure of proportion of positively predicted labels that are in reality true.

Precision Score=Total Positive / (True Positive + False Positive)

Recall Score: Recall score is the ratio of predicted positive value and the actual total positive values.

Recall= True Positive / (True Positive + False Negative)

Recall= TP / (TP + FN)

F1 Score: F1 score is actually the harmonic mean of the Precision and the recall scores. It is calculated using the following formula

Recall= 2 * (Recall * Precision) / (Recall + Precision)

Support: it indicates total number of true occurrences of each class. is the sum of total true instance of a label.

The above table 6 data presents a summary of the findings using the Logistic Regression model. The above precision Recall and F1-Score we are confirmed that

- our data is not overfit or underfit
- Accuracy is getting 1 that we can uderstand because of large legit transations the results are showing as 1
- we are consantrating on Fraud Transactions

Similarly the outcome of training and test score of the model using the Kneighbors Classification Model is Train Model Classification Report.

Table 7 Train Model Classification Report

	Precision	Recall	F1 Score	Support
No Fraud	1.00	1.00	1.00	227468
Fraud	0.97	0.79	0.87	377
Accuracy			1.00	227845
Macro Average	0.99	0.89	0.93	227845
Weighted Average	1.00	1.00	1.00	227845

Table 8 Test Model Classification Report

	Precision	Recall	F1 Score	Support
No Fraud	1.00	1.00	1.00	56847
Fraud	0.95	0.78	0.86	115
Accuracy			1.00	56962
Macro Average	0.97	0.89	0.93	56962
Weighted Average	1.00	1.00	1.00	56962

The model performs exceptionally well in identifying "No Fraud" instances, achieving perfect precision and recall. However, for the "Fraud" class, there is room for improvement, especially in terms of recall, as it correctly identifies only 78% of actual fraud cases table 7

ROC Curve and Optimal Thresholds for Logistic Regression and K-Neighbors Models

Model: Logistic Regression

Threshold: 0.007890862084915292

Accuracy Score: 0.9960675538078017

ROC Accuracy Score: 0.945961432709156

Model: KNeighbors Classification

Threshold: 0.25

Accuracy Score: 0.9985955549313578

ROC Accuracy Score: 0.9298718681189247

6. Result Explanation

The model is highly accurate overall but has room for improvement in precision for the "Fraud" class. The chosen threshold of 0.25 results in a trade-off between precision and recall figure 2. Depending on the specific requirements and priorities, threshold value can be adjusted to optimize precision, recall, or another metric

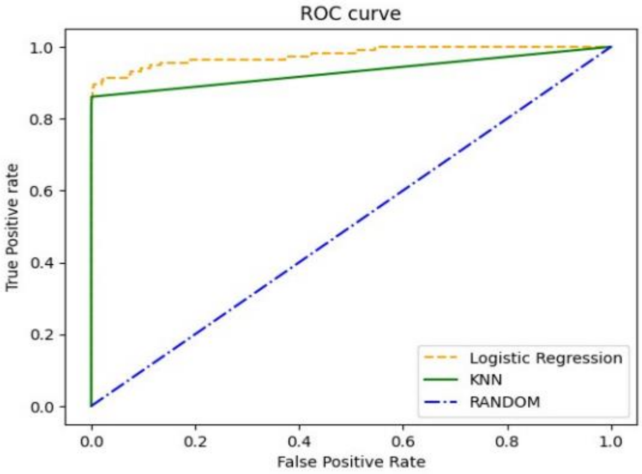

Figure 2 ROC Cure

- The ROC curves compare the performance of Logistic Regression, K-Neighbors (KNN), and a Random Classifier.
- Logistic Regression and K-Neighbors outperform the random classifier in distinguishing between classes.
- The area under the ROC curve (AUC) provides a quantitative measure of the model's discriminative ability.

7. Challenges

The above model is an attempt to present a model that identifies fraudulent transactions among a huge collections of credit card transactions. For the identification of fraud from the given dataset, this model identifies features of the dataset. The real challenge while working on this model was that not all features of the credit card transactions were available because of the obvious reasons of confidentiality and customer’s privacy. However, a few features like the amount, time and transaction ID, etc were available. The fact of the matter is that while proposing any such model one

IRJAEH

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 05 May 2024
Page No: 1427 - 1434
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0196

has to focus on a finite set of attributes and proceed further but to the contrary, frauds and cheats keep on devising new techniques and often outsmart any such preventive or identification arrangement. To cope with the dynamics of frauds and cheats especially in online mode, the model also needs dynamic data set as well as dynamic training and learning methodologies.

Conclusions

In conclusion, logistic regression proves to be a proficient tool for identifying fraudulent credit card transactions. Through meticulous data preprocessing, model training, and evaluation, our approach achieves commendable accuracy rates on both training and testing datasets. The integration of Streamlit enhances accessibility, enabling users to leverage the fraud detection system effortlessly. This project underscores the efficacy of machine learning in mitigating the risks associated with credit card fraud.

References

[1]. Federal Trade Commission Report, 2024

[2]. Melo-Acosta, German E., et al. “Fraud Detection in Big Data Using Supervised and Semi-Supervised Learning Techniques.” 2017 IEEE Colombian Conference on Communications and Computing (COLCOM), 2017, doi:10.1109/colcomcon.2017.8088206.

[3]. Mohammed, Emad, and Behrouz Far. “Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study.” IEEE Annals of the History of Computing, IEEE, 1 July 2018, doi.ieeecomputersociety.org/10.1109/IRI.2018.00025.

[4]. Xuan, Shiyang, et al. “Random Forest for Credit Card Fraud Detection.” 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), 2018, doi:10.1109/icnsc.2018.8361343.

[5]. A.I. Kokkinaki, “On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling”, Proc of IEEE Knowledge and Data Engineering Exchange Workshop; 107-113, 1997.

[6]. www.kaggle.com/creditcard.csv

[7]. S. B. Kotsiantis. (n.d.). "Decision Tree: A Recent Overview". Artificial Intelligence Review, vol. 39, no. 4, 261-28.

[8]. Kumar, A. (2023, March 17). Data Analytics - AI, Data, Data Science, Machine Learning, Blockchain, Digital. Retrieved from vitalflux.com: https://vitalflux.com/accuracy-precision-recall-f1-score-python-example/

[9]. https://www.kaggle.com/mlg-ulb/creditcardfraud

[10]. https://www.kaggle.com/uciml/default of credit-card-clients-datase

[11]. https://www.kaggle.com/ntnu-testimon/paysim1/hom