Financial Fraudulent Transaction Detection Using Machine Learning Technique

Sweejalben Surti - 001127898

Abstract

Financial fraud is becoming a growing problem in the financial sector, with catastrophic implications.Payments-related fraud is a major concern for cyber-crime organisations, and recent research has demonstrated that machine learning approaches may successfully detect fraudulent transactions in vast amounts of data. Such algorithms are capable of detecting fraudulent transactions that human auditors may be unable to identify, and they can do so in real time. In this project, Using publicly available payment transaction data, we apply different supervised machine learning algorithms to the problem of fraud detection. Aim is to compare the results of several supervised machine learning algorithms, including Logistic Regression (LR), Support Vector Machines (SVM), Decision Tree (DT), and Random Forests (RF) and Neural Network.Aim is to show how supervised machine learning techniques may be utilised to accurately categorise data with substantial class imbalance.Exploratory analysis was used to distinguish between fraudulent and non fraudulent transactions. The both Decision Tree classifier and Logistic Regression outperformed the other algorithms, with an accuracy of 93.26 percent and an F1-score of 0.937500. However, the SVM Model performed worse with very low accuracy of 39.34 percent and 0.58427 F1 Score.

1. Introduction

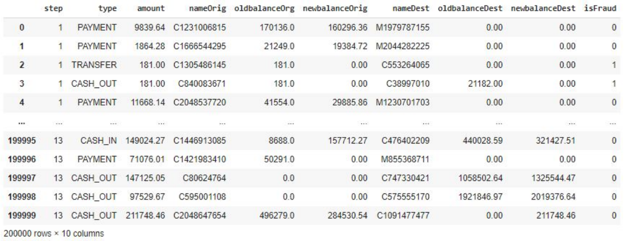
Financial fraud has a huge impact on the financial industry as well as ordinary life. Fraud can weaken confidence in the sector, undermine savings, and raise living costs. According to the PwC Global Economic Crime(PricewaterhouseCoopers nodate) and Fraud Survey 2020, respondents reported $42 billion in losses in the previous 24 months. Worse, only 56% of financial institutions asked indicated they investigated their worst fraud incidence.The ever-increasing use of technology in the finance business is contributing to the rise in fraud. While technology has made it easier to make digital payments and transactions, it has also increased the number of frauds, scams, and phishing attempts. As a result, businesses have begun to concentrate on solutions to prevent payment system vulnerabilities.

Traditionally, banks and financial institutions have used manual procedures or rule-based methods to detect fraud, which have had limited success. A rule-based method necessitates the human establishment and assessment of a complex set of criteria for identifying questionable transactions.While this is useful for spotting anomalies that follow well-known patterns, it is ineffective for detecting fraud that follows new or unexpected patterns. This provides an incentive for criminals to devise ever more sophisticated tactics to get around the regulations, and they are using new technology to do so. Machine learning is a solution that is assisting banks and financial organisations in staying one step ahead of the competition.

Machine learning is based on the idea that fraudulent transactions exhibit specific characteristics that distinguish them from legitimate ones. These tendencies are recognised by machine learning algorithms, which can distinguish between scammers and legitimate clients. Because they can use larger quantities of data, these algorithms can detect fraudulent activity much faster and with greater accuracy than traditional rules-based systems.Machine learning systems, rather than becoming more expensive to operate over time, tend to grow more effective and efficient without requiring any more specialised staff.Several studies have been conducted in the past to detect fraudulent transaction automatically using various machine learning and statistical methodologies.

For highly and anonymous datasets, a credit card fraud detection approach was proposed. To address the problem of class imbalance, frequent item set mining was utilised to identify legal and illegitimate transaction patterns for each client. The pattern of an incoming transaction was then analysed using a matching algorithm to determine if it was real or fraudulent. This model's evaluation revealed that it can both detect fraudulent transactions and improve imbalance classification(Seeja **and** Zareapoor 2014) .

Bidirec-tional neural networks were used to suggest a model for real-time fraud detection. They used a big data set of cell phone transactions given by a credit card business in their research. In terms of false positive rate, the results



	step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud
0	1	PAYMENT	9839.64	C1231006815	170136.0	160296.36	M1979787155	0.00	0.00	0
1	1	PAYMENT	1864.28	C1666544295	21249.0	19384.72	M2044282225	0.00	0.00	0
2	1	TRANSFER	181.00	C1305486145	181.0	0.00	C553264065	0.00	0.00	1
3	1	CASH_OUT	181.00	C840083671	181.0	0.00	C38997010	21182.00	0.00	1
4	1	PAYMENT	11668.14	C2048537720	41554.0	29885.86	M1230701703	0.00	0.00	0
...	...	...	...	...	...	...	...	...	...	...
199995	13	CASH_IN	149024.27	C1446913085	8688.0	157712.27	C476402209	440028.59	321427.51	0
199996	13	PAYMENT	71076.01	C1421983410	50291.0	0.00	M855368711	0.00	0.00	0
199997	13	CASH_OUT	147125.05	C80624764	0.0	0.00	C747330421	1058502.64	1325544.47	0
199998	13	CASH_OUT	97529.67	C595001108	0.0	0.00	C575555170	1921846.97	2019376.64	0
199999	13	CASH_OUT	211748.46	C2048647654	496279.0	284530.54	C1091477477	0.00	211748.46	0

200000 rows × 10 columns

Figure 1. Fraudulent Transaction Data frame

confirmed that the suggested model outperforms rule-based algorithms(Krenker **andothers** 2009).

To detect fraud, a two-layer statistical classifier was proposed for sensitive, highly skewed, and huge data sets. The method was inspired by the need to analyse a data set of over fifteen million real-world online banking transactions from 2011 to 2013 in order to spot frauds from legitimate transactions. The algorithm is especially successful at detecting abnormalities, with high true positive rates and reasonable low false positive rates, according to the results(Panaro, Riccomagno **and** Malfanti 2015).

Logistic regression, decision trees, random forests, SVM (Support Vector Machine), and neural networks are some of the common supervised machine learning methods used to handle these problems in this project. In addition, we compare the results of numerous supervised machine learning approaches to distinguish between fraud and non-fraud transactions.

1.1. Dataset

The proposed problem makes use of the publicly available dataset downloaded from the website kaggle and dataset are generated by collecting the data using payment card transaction including genuine transaction and fraudulent transactions. It consist of 10 columns, in which 9 columns are the features and the one class is the target class contain binary class which decides about whether the transaction is fraud or genuine. The shape of the data frame is 199999 records and 10 features shown in figure 1.

1.2. Exploratory Data Analysis

Exploratory Data Analysis is the crucial process of using descriptive statistics and graphical representations to undertake initial investigations on data in order to uncover patterns, spot anomalies, test hypotheses, and verify assumptions(Patil 2018). The below graphs shows how many fraud transactions and non-fraud transactions are there in our dataset.

1.2.1. Fraudulent and non-fraudulent ratio of the data

The figure 2. shows the fraud transaction ratio of the whole dataset,from table 2 we can notice there are 147 fraud transaction out of 199999 transactions.

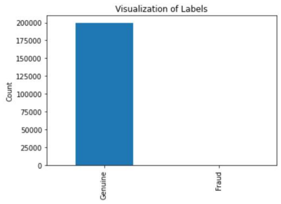


Figure 2. Fraudulent and non-fraudulent ratio

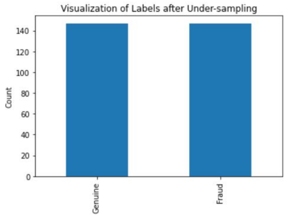


Figure 3. Fraudulent and non-fraudulent ratio

1.2.2. Missing Data

There are no missing values found in the dataset.

Table 1. Missing Values

Attributes	Counts
isFraud	0
newbalanceDest	0
oldbalanceDest	0
nameDest	0
newbalanceOrig	0
oldbalanceOrg	0
nameOrig	0
amount	0
type	0
step	0

1.2.3. Class imbalance

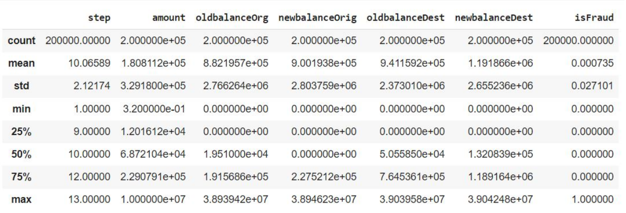
In data-driven fraud detection systems, one of the most common challenges is to tackle class imbalance. In the real world, fraudulent transactions comprise of a tiny proportional in comparison with legitimate transactions. From figure 2 and Table 2 we can notice that there are imbalance of the data.there are low amount of fraud transaction(147) compare to legit transaction(199853).As a result, AI models face risks of overfitting on the legitimate data.

Table 2. Class Imbalance

Label	Counts
non-fraud(0)	199853
Fraud(1)	147

1.2.4. Descriptive Statistics of numeric data

The below figure 4 describes the statistic of the dataset such as mean,quartile,maximum value, counts etc.The mean of the isfraud class is 0.000735.



	step	amount	oldbalanceOrg	newbalanceOrig	oldbalanceDest	newbalanceDest	isFraud
count	200000.00000	2.000000e+05	2.000000e+05	2.000000e+05	2.000000e+05	2.000000e+05	200000.000000
mean	10.06589	1.808112e+05	8.821957e+05	9.001938e+05	9.411592e+05	1.191866e+06	0.000735
std	2.12174	3.291800e+05	2.766264e+06	2.803759e+06	2.373010e+06	2.655236e+06	0.027101
min	1.00000	3.200000e-01	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000
25%	9.00000	1.201612e+04	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000
50%	10.00000	6.872104e+04	1.951000e+04	0.000000e+00	5.055850e+04	1.320839e+05	0.000000
75%	12.00000	2.290791e+05	1.915686e+05	2.275212e+05	7.645361e+05	1.189164e+06	0.000000
max	13.00000	1.000000e+07	3.893942e+07	3.894623e+07	3.903958e+07	3.904248e+07	1.000000

Figure 4. Descriptive Statistics

1.2.5. Feature Correlation

By creating correlation maps we can identify features that are closely correlated with the legitimacy of our transactions. This can be a crucial step when performing dimensionality reduction, removing/adding features.The figure 5 shows the correlation between the classes. The dark color shows the weak correlation and the light color shows very strong correlation.from that it can be notice that there are strong correlation between oldbalanceorigin,newbalanceroging and oldbalancedest, newbalancedest.Also there is no correlation found with isfraud class.

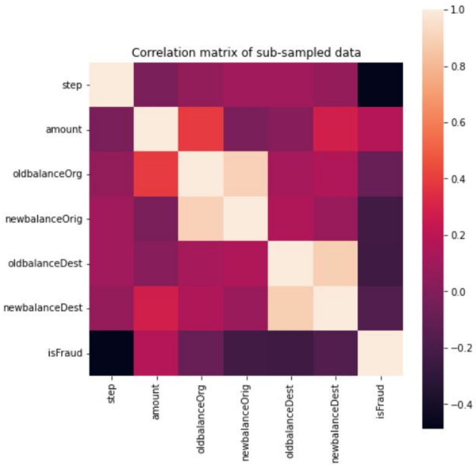


Figure 5. Correlation

2. Methods

This section explains about the implementation, which includes the algorithm used for implementation of proposed system.In this project we have used multiple supervised machine learning algorithm to find the fraudulent transaction.Such as Logistic regression, Random forest, Neural network, SVM and decision trees.

2.1. Algorithms to detect fraudulent transactions

Logistic regression is a popular method, which determines the strength of cause and effect relationships between variables in data sets. It can be used to create an algorithm which predicts whether a transaction is 'fraud' or not. Decision trees can be used to create a set of rules that model customers' normal behavior and can be trained, using examples of fraud, to detect anomalies.Random forests (boosting techniques) ensemble multiple weak classifiers into one strong classifier – they can be built using an ensemble of decision trees.Neural networks are a powerful technique inspired by the workings of the human brain. Able to learn and adapt to patterns of normal behavior, neural networks can identify fraud in real-time.

2.2. programming language used

In this project I have used Python as a programming language.Python is one of the best languages for the implementing machine learning. It provides rich packages and libraries that used in machine learning. and the libraries

2.3. Packages and libraries used

Numpy,Pandas,Scikitlearn,matplotlib,seaborn and Keras.

2.4. Data Pre-processing

we dont have a missing values in the dataset so data are cleaned already. But to balance the data we need to apply the data sampling method. Also there are some categorial values in the dataset so it needs to perform some method to make data useful.

2.4.1. Under Sampling

There are many ways to address class imbalance by using sampling techniques. but for this data we will use undersampling technique because we have 2 million samples so it will be easy to make it same as minority class size. under sampling removes records from the majority class (non-fraud)such that its size approximates the minority class's size.(See figure 3)

2.4.2. one-hot Encoding

We have categorical data as well in our dataset such as step,nameorig,namedest,hasDest. to convert it into numeric data we have performed on-hot encoding method.

2.5. Data Modeling

We have split the data into training and test sets, with a 70/30 split. Training samples are 205 and Testing samples are 89.This is done to measure and avoid possible overfitting. By measuring the model's performance on separate data, we have a more fair assessment of the model's ability to extrapolate its predictions to new or unseen information.

3. Experiments

In the Experiments section, It is to describe the dataset, experimental settings, evaluation criteria, results, and discussion.

3.1. Experimental settings

In this project different supervised machine learning models have been trained to achieve the best accuracy and F1 scores to detect the fraudulent transactions. All these models can be built feasibly using the algorithms provided by the scikit-learn package. some processing method has been performed on the data. After processing the data, Data has been splitted to perform the training and testing on the data. All the algorithm has been performed on the training data one by one to check the performance of the model on the data.

3.2. Evaluation measure

The end result is evaluated based on the confusion matrix and precision, recall and accuracy is calculated.It can be expressed as:

$$Precision = \frac{TruePositive}{TruePositive + FalsePositive}$$

$$recall = \frac{TruePositive}{TruePositive + FalseNegative}$$

$$F1 = 2X\frac{Precision * recall}{Precision + recall}$$

It contains two classes: actual class and predicted class. The confusion metrics depends on these features: True Positive: in which both the values positive that is 1. True Negative: it is case where both values are negative that is 0. False Positive: this is the case where true class is 0 and non-true class is 1. False Negative: It is the case when actual class is 1 and non-true class is 0(Asha **and** KR 2021).

Table 3. Quantifying Performance

		Actual Class	
		Positive	Negative
Predicted Class	Positive	TP	FP
	Negative	FN	TN

Typically, a confusion matrix is a visualization of a classification model that shows how well the model has predicted the outcomes when compared to the original ones.

3.3. Results

The below figure 3 shows the F1 scores and the accuracy of each model. From that It can be notice that the model Decision Tree and Logistic Regression has same and the highest accuracy(0.93258) and F1 scores(0.937500) compare to other model, It means that these two model have outperformed on this dataset of fraudulent transaction and has predicted the best compare to other models. However, the SVM has performed the worse on the dataset and gives very Low F! score and accuracy. And the other two model has very close accuracy to the best performed model.

Table 4. F1 score on the Fraud Transaction dataset. The higher the F1 score and accuracy, the better the performance.

Model	F1 score	Accuracy
Decision Tree	**0.937500**	**0.93258**
Logistic Regression	**0.937500**	**0.93258**
Random Forest	0.8320	0.86517
Neural Network	0.869565	0.73034
SVM	0.393443	0.58427

3.4. Discussion

In this Financial Fraudulent transaction detection problem first we have used the Decision tree algorithm after applying the under-sampling method to the fraud class to balance the data at minority size. Then we have checked the decision tree accuracy which performed best on this proposed system. Then we have compared the other algorithm to check the better performance than Decision tree. However at end of the all model evaluation we got best accuracy model as Decision tree as well as linear regression for the proposed problem.

4. Conclusion

To conclude, It can be notice from the above tables 4, that shows the comparison of the accuracy of the model, the best accuracy model is Decision tree and Linear regression method for the Fraud transaction prediction based on the highest accuracy and F1 scores.

References

Asha, RB **and** Suresh Kumar KR (2021). "Credit card fraud detection using artificial neural network". **in**_Global Transitions Proceedings_: 2.1, **pages** 35–41.

Krenker, Andrej **andothers** (2009). "Bidirectional Artificial Neural Networks for Mobile-Phone Fraud Detection". **in**_Etri Journal_: 31.1, **pages** 92–94.

Panaro, Delio, Eva Riccomagno **and** Fabrizio Malfanti (2015). “A Fraud Detection Algorithm For Online Banking”. **in***BOOK OF ABSTRACTS*: **page** 271.

Patil, Prasad (**may** 2018). *What is exploratory data analysis?* URL: https://towardsdatascience.com/exploratory-data-analysis-8fc1cb20fd15.

PricewaterhouseCoopers (nodate). *PWC’s Global Economic Crime and Fraud Survey 2020*. URL: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html.

Seeja, KR **and** Masoumeh Zareapoor (2014). “Fraudminer: A novel credit card fraud detection model based on frequent itemset mining”. **in***The Scientific World Journal*: 2014.