International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 7 Issue 6, November-December 2023 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Credit Card Fraud Detection Using Hybrid Machine Learning Algorithm

Tripti Gautam[1], Ghanshyam Sahu[2], Lalit Kumar P. Bhiaya[3]

[1]M Tech Scholar, CSE Department, BCET, Durg, Chhattisgarh, India
[2]Professor, CSE Department, BCET, Durg, Chhattisgarh, India
[3]Associate Professor, Bharti University, Durg, Chhattisgarh, India

ABSTRACT

As we know and living in the era of digital world, Credit card fraud is increasing rapidly by transactions of unauthorized or any fraudulent use of someone else information of credit card to purchase and obtain benefits of financial. The victims of credit card fraud may have severe repercussions. Financial losses, harm to credit scores, and the trouble of dealing with unauthorized transactions can all arise from it. Secure your card information, keep a close eye on your account activity, and alert your card issuer right away to any odd transactions if you want to prevent credit card theft. To help combat fraud, many financial institutions additionally provide extra security features like two-factor authentication and fraud detection systems. To resolve these problem we developed a system of Credit Card Fraud detection by hybrid techniques of machine learning which combines supervised and unsupervised methods to improve the system of fraud detection. In this paper we are using machine learning algorithms like K Nearest Neighbor, Logistic Regression and XGBoost model and we had made a comparison of accuracy score with other different models by using the data of European Cardholders 2013, by that data we had make comparison and decided that which model is best for defining the fraud system of credit card.

KEYWORDS: *Credit Card, Fraud Detection, Fraud Detection Framework, Supervised and Unsupervised Techniques*

How to cite this paper: Tripti Gautam | Ghanshyam Sahu | Lalit Kumar P. Bhiaya "Credit Card Fraud Detection Using Hybrid Machine Learning Algorithm" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-7 | Issue-6, December 2023, pp.274-279, URL: www.ijtsrd.com/papers/ijtsrd60102.pdf

IJTSRD60102

INTRODUCTION

We are advancing into the digital age, and cybersecurity is playing an increasingly important role in our daily lives. The primary problem when discussing digital life security is identifying unusual behaviour. Credit cards are often preferred by many people when they transact online or buy something. Credit card credit limits occasionally enable us to make purchases even when we don't have the money on hand. On the other hand, online criminals abuse these features.

Credit card fraud can be done in various ways like

Phishing: where deceive people into entering their credit card information on phoney websites, emails or text. To win trust and obtain sensitive information, these scam pose as reliable institutions.

Data Breaching: online, it means if any company's systems are breached, hackers may able to access any credit card data of its customers. The stolen information may be utilised in fraudulent transactions or sold on the black market for their use

Card skimming: it is when a card is swiped or inserted at an ATM, a payment terminal or a petrol pump, fraudsters employ tools called skimmers to record credit card information. The stolen information is then used to build fake cards or buy things online.

The examination of a card's spending patterns and classification of its transactions into fraudulent and lawful transactions form the basis for the detection of credit card fraud. There are many challenges in detecting credit card fraud:

Due to privacy and security considerations, credit card transaction datasets are rarely available, and the ones that are are greatly skewed. Fraudulent behaviour patterns are dynamic in nature, meaning that fraudulent transactions typically look legitimate.

Related Work

In this paper we are defining and analyzing many machine learning algorithms that can help us classify abnormal transactions. The only requirement is the past data and the suitable algorithm that can fit our data in a better form. It helps you in the complete end-to-end model training process and finally, we will get the best model that can classify the transaction into normal and abnormal types.

First, we describe what is supervised and unsupervised modes and algorithms which we approached for our model. Secondly, the algorithms which we used to researched and analyzed over credit card fraud detection

1. Supervised and Unsupervised

A. Supervised Learning-A type of machine learning called supervised learning uses labelled data to teach the algorithm new things. Labelled data is a term used to describe input samples that come with the required output labels. The purpose of supervised learning is to build a model that generalises and can correctly classify or predict unknown or upcoming data.The training data serves as a teacher in supervised learning, instructing the algorithm on how to learn the correspondence between input features and their related labels. When given new, unlabeled examples, the algorithm looks for patterns, correlations, or decision boundaries in the data to create predictions.

B. Unsupervised Learning- As the name implies, unsupervised learning entails learning from unlabeled data. Without any predefined labels or goal outcomes, the algorithm in unsupervised learning investigates the data to discover innate patterns, structures, or relationships. Finding hidden patterns or clusters in the data is the goal. In unsupervised learning, the algorithm attempts to cluster or group together related data points based on their shared characteristics. It seeks to discover the data's underlying distribution or to isolate important features for future investigation or decision-making.

2. Algorithms

In this paper we used some supervised and unsupervised algorithm for the comparison and dis

A. Linear Regression- It is a simple and frequently used algorithm, by fitting and observing data in the model through connecting a dependent and independent variables. Finding the best-fitting line that reduces the discrepancy between the anticipated and actual values of the dependent variable is the aim of linear regression. The equation below represents the line:

$$y = mx + b$$

where

y is the dependent variable/ response / goal variable

x is independent variable/feature/predictor variable,

The slope of the line, m, shows how much the change in y changes when the x value changes by a unit.The value of y when x is 0 is represented by the y-intercept, or b.

B. Logistic Regression- the objective is to predict a binary outcome (e.g., true/false, yes/no, 0/1) based on a set of independent variables or features, logistic regression is a popular supervised learning approach. Contrary to its name, logistic regression is typically employed to solve classification issues as opposed to regression issues. The logistic function, also referred to as the sigmoid function, is used by the logistic regression model to translate the linear combination of independent variables to the interval [0, 1].

$$p = 1 / (1 + e^{(-z)})$$

Where:

The positive class's anticipated probability is denoted by the letter p.

The independent variables are combined linearly to form the variable z.

The feature vector (x), learning weights (coefficients) of the model, and an intercept term (b) are used to create the linear combination (z).

C. Naive Bayes -The Bayes theorem of probability serves as its foundation, and it makes the assumption that the features are conditionally independent given the class. Naive Bayes is a well-liked option for text categorization tasks like spam filtering and sentiment analysis due to its popularity and computational efficiency despite its simplicity and "naive" premise. Naïve Bayes works on Data Preparation, Calculating Class Priors, Calculating Feature Likelihoods, Calculating Posterior Probability, Class Prediction

D. K-Nearest Neighbors (KNN) -Machine learning commonly uses the K-Nearest Neighbors (KNN) algorithm for both classification and regression problems. It is a non-parametric and instance-based learning method, which means it depends on the training data alone to produce predictions rather than making firm assumptions about the distribution of the underlying data. KNN works as follows, Data Preparation, Choosing K, Calculating Distances, Finding K Neighbors,

Class Prediction (Classification), Value Prediction (Regression)

E. Random Forest - An effective and popular ensemble learning algorithm in machine learning is Random Forest. It is well-liked for both classification and regression tasks and is a member of the family of decision tree-based techniques. For more precise and reliable forecasts, Random Forest aggregates the predictions of various separate decision trees. Basically it works on Data Preparation, Random Sampling, Growing Decision Trees, Ensemble Prediction.

Because of its reliability, adaptability, and strong generalisation skills, Random Forest has gained popularity across many fields. Compared to individual decision trees, it is less prone to overfitting and is successful with complicated datasets. However, compared to simpler models, it can be more difficult to read the results and comprehend how Random Forest makes decisions.

F. Gradient Boosting Algorithms : A group of machine learning techniques known as gradient boosting algorithms combine a collection of weak prediction models, often decision trees, to produce a powerful predictive model. Gradient

boosting's main principle is to iteratively create new models that fix the errors created by the prior models, enhancing the performance of prediction as a whole. It works on Gradient Boosting Machine (GBM), XGBoost: XGBoost (Extreme Gradient Boosting), LightGBM, CatBoost, Ensemble of Weak Learners, Loss Function Optimization, Regularization

Working Performances

A. Parameters for Analysis

We use a number of parameters to assess the performance of a specific model. The number of correct predictions versus the number of incorrect guesses is plotted in a confusion matrix, a summary table that demonstrates how accurate the model is at making predictions. Four categories make up it:

True Positive (TP), where the actual value and the projected value agree. The model anticipated a positive value, and the actual result was positive.

True Negative (TN), where the actual value and the projected value are identical.

False Positive (FP) means that the predicted value in this case was incorrectly predicted. Although the model had projected a positive result, the actual value was negative.

False Negative (FN) describes a situation in which the model incorrectly predicted a result that was actually positive when it should have been negative.

Accuarcy: The number of accurate predictions your model made is a measure of accuracy. It is a solid fundamental metric to gauge a model's performance, but a simple accuracy metric has the drawback of being better in balanced datasets and worse in unbalanced datasets.

$$accuracy = (TP + TN) / TP + TN + FP + FN$$

Out of all the positives in the dataset, recall measures how many real positives are anticipated. A high recall indicates that the majority of positive cases were classified as such. There are a lot of false negatives when recall is low.

$$recall = TP/(TP + FN)$$

Precision is the degree to which a positive forecast is accurate is measured by precision. This phrase asks how certain you may be that a result is actually positive if it is projected to be positive.

$$precision = TP/TP + FP$$

F1, or their harmonic mean, combines precision and memory. When maintaining the proper balance between recall and precision, it is necessary.

$$F1 = 2\ (precision * reca\ )/\ (precision + recall)$$

B. DATA SET

We had taken a data set of the actual bank transactions that European cardholders conducted in 2018 are included in this dataset. The original variables have been changed PCA versions since sharing them would compromise security. Thus, there are 29 feature columns and 1 final class column to be found.

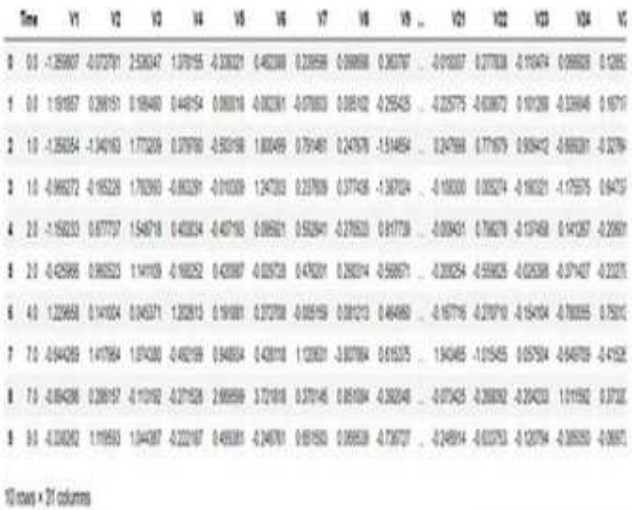

Figure 1 Sample of European Cardholder data

Importing Dataset

Importing the dataset is pretty much simple. we can use pandas module in python to import it.

Data Processing

The dataset is imbalanced towards a feature. Which seems pretty valid for such kind of data. Because today many banks have adopted different security mechanisms — so it is harder for hackers to make such moves.

Still, sometimes when there is some vulnerability in the system — the chance of such activities can increase.

That's why we can see the majority of transactions belongs to our datasets are normal and only a few percentages of transactions are fraudulent. can also check for null values

Data	columns	(total 31 columns)	:
#	column	Non- Null count	Dtype
------	-----	----------	-------
0	Time	284807 non-null	float 64
1	v1	284807 non-null	float 64
2	v2	284807 non-null	float 64
3	v3	284807 non-null	float 64
4	v4	284807 non-null	float 64
:	:	:	:
:	:	:	:
26	v26	284807 non-null	float 64
27	v27	284807 non-null	float 64
28	v28	284807 non-null	float 64
29	Amount	284807 non-null	float 64
30	Class	284807 non-null	int64
dtypes:	float64(30	int64(1)	

Figure 2 Sample of data types

Result Analysis

The experiment's dataset was obtained from the Cardholders of 2018 in website. It includes credit card transactions from 2013. The dataset has 492 out of the 284,807 total transactions that are marked as fake. Due to the 0.173% fraud cases, the data is therefore deemed to be imbalanced. The distribution of the dataset is shown in Figure 1. Without the column labels, there are 30 columns. A PCA projection was applied to all columns with the exception of the time and amount features in order to preserve privacy. All columns are therefore numerical variables. The two classes are broken down in the labels columns, where a genuine transaction is represented by a value of 0 and a fraudulent transaction by a value of 1

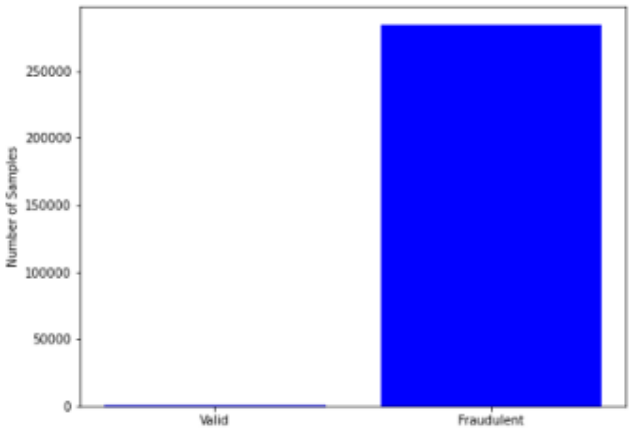

Figure 3 Distribution of Data Sets

Sno	TX_DATETIME	CUSTOMER_ID	TERMINAL_ID	TX_AMOUNT	TX_TIME_SECONDS	TX_TIME_DAYS
0	01-04-2018	0	3	123.59	26345	0
1	01-04-2018	0	3	46.51	68522	0
2	01-04-2018	0	0	77.34	64816	0
3	02-04-2018	0	2	32.35	141182	1
4	02-04-2018	0	1	63.3	137138	1
:	:	:	:	:	:	:
:	:	:	:	:	:	:
26	10-04-2018	0	2	65.78	228976	9
27	11-04-2018	0	1	54.78	453267	10
28	11-04-2018	0	2	66.89	233987	10
29	11-04-2018	0	2	44.98	221435	10
30	11-04-2018	0	2	65.89	331245	10

Figure 4 Collection of Customer profile data's in 30 rows

In figure 2 We can make a quick check that the generated transactions follow the customer profile properties:

- The terminal IDs are indeed those in the list of available terminals (0, 1, 2 and 3)
- The transaction amounts seem to follow the amount parameters of the customer (mean_amount=62.26 and std_amount=31.13)
- The number of transactions per day varies according to the transaction frequency parameters of the customer (mean_nb_tx_per_day=2.18).

Now produce the transactions for each and every customer. Using the pandas groupby and apply methods, this is simple:

"transactions_df=customer_profiles_table.

Groupby ('CUSTOMER_ID').

apply (**lambda** x: generate_transactions_table (x.iloc[0], nb_days=5)).

reset_index(drop=**True**)

transactions_df "

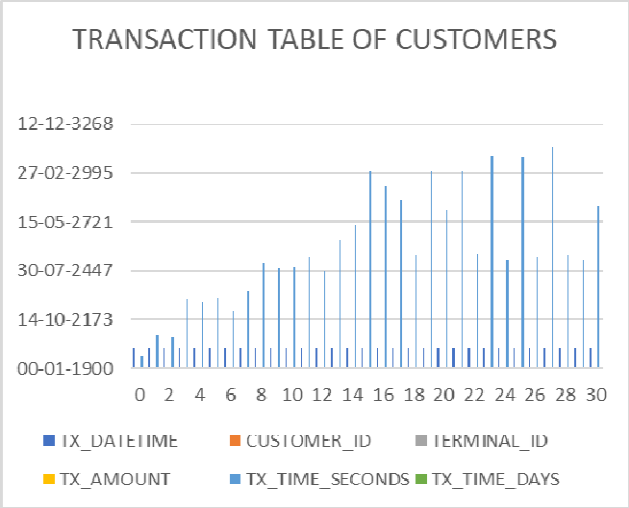

Figure 5 Graph of Transaction Table of Customers

Analysis

MODELS	ACCURACY	F1 SCORE
DECISION TREE	0.999288	0.776255
K NEAREST NEIGHBOURS	0.9995066	0.836538462
LOGISTIC REGRESSION	0.9991148	0.693467337
SUPPORT VECTOR MACHINES	0.99936154	0.77777777
RANDOM FOREST	0.999361	0.78431372
XG BOOST	0.9995211	0.842105263

Figure 6 Result Analysis

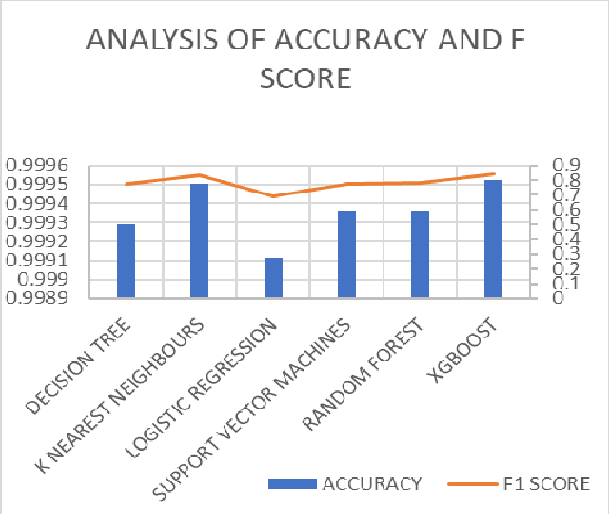

Figure 7 Graph of Accuracy and F Score

Conclusion:

In order to identify fraudulent transactions from a sizable unbalanced dataset, we have constructed different supervised models. Accuracy, and F1 score comparison statistics have been provided, and the percentage of properly recognising fraudulent transactions is the comparison parameter. In situations where it misrepresents a machine learning technique, accuracy can actually be deceptive. For instance, the local outlier factor performs poorly based on accuracy and F1 values while having a 99.67% accuracy rate. So, when choosing the optimum algorithm for fraud detection, precision, recall, and F1 score values are important considerations. The most effective supervised learning algorithm is the XGboost algorithm, and support vector machine outperforms all other algorithms.

References:

[1] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun K. Majumdar, "Credit Card Fraud Detection using Hidden Markov Model," IEEE Transactions On Dependable And Secure Computing, vol. 5, Issue no. 1, pp.37-48, January-March 2008

[2] Schneider, Gary (2010). Electronic Commerce. Cambridge: Course Technology. p. 497. ISBN 978-0-538-46924-1.

[3] S. Benson Edwin Raj, A. Annie Portia, "Analysis on Credit Card Fraud Detection Methods", International Conference on Computer, Communication and Electrical Technology – ICCCET2011, 18th & 19th March, 2011

[4] Seeja, K. R., and Zareapoor, M., (2014). FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining, The Scientific World Journal, Hindawi Publishing Corporation, Volume 2014, Article ID 252797, pp. 1 – 10, http://dx.doi.org/10.1155/2014/252797

[5] The Nilson Report. (2015). U.S. Credit & Debit Cards 2015. David Robertson

[6] Bolton, R. J. and Hand, D. J., (2001). Unsupervised profiling methods for fraud detection, Conference on Credit Scoring and Credit Control, Edinburgh.

[7] Kou, Y., Lu, C-T., Sinvongwattana, S. and Huang, Y-P., (2004). Survey of Fraud Detection Techniques, In Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, March 21-23.

[8] Bhattacharyya, S., Jha, S., Tharakunnel, K., Westland, J.C.: Data mining for credit card fraud: a comparative study. Decis. Support Syst. 50(3), 602–613 (2011)

[9] Padvekar SA, Kangane PM, Jadhav KV (2016) Credit card fraud detection system. Int J Eng Comput Sci 5(4):16183–16186

[10] Xuan S, Liu G, Li Z, Zheng L, Wang S, Jiang C (2018) Random forest for credit card fraud detection. In: ICNSC 2018—15th IEEE International conference on networking, sensing and control, pp 1–6

[11] Fernandes, E. R., & de Carvalho, A. C. "Evolutionary inversion of class distribution in overlapping areas for multi-class imbalanced learning". Information Sciences, 2019, 494, 141–154

[12] Das, S., Datta, S., & Chaudhuri, B. B., "Handling data irregularities in classification: Foundations, trends, and future challenges. Pattern Recognition", 2018, 81, 674–693.

[13] Lee, H. K., & Kim, S. B. "An overlap-sensitive margin classifier for imbalanced and overlapping data. Expert Systems with Applications",2018, 98, 72–83.

[14] Zhou, C., & Paffenroth, R. C. "Anomaly detection with robust deep autoencoders", In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2017(pp. 665–668)