IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Behaviour Based Credit Card Fraud Detection Model Using Machine Learning Based Algorithm

Govind Prasad Buddha, Feature Lead ,Computer Science ,Liutebm University, Hyderabad

Dr. NAGAMALLESWARA RAO. Department of Computer Science and Engineering, SDES, Hyderabad

ABSTRACT: Credit card frauds are easy and friendly targets. E-commerce and many other online sites have increased the online payment modes, increasing the risk for online frauds. Increase in fraud rates, researchers started using different machine learning methods to detect and analyse frauds in online transactions. The main aim of the paper is to design and develop a novel fraud detection method for Streaming Transaction Data, with an objective, to analyse the past transaction details of the customers and extract the behavioural patterns. Where cardholders are clustered into different groups based on their transaction amount. Then using sliding window strategy, to aggregate the transaction made by the cardholders from different groups so that the behavioural pattern of the groups can be extracted respectively. Later different classifiers are trained over the groups separately. And then the classifier with better rating score can be chosen to be one of the best methods to predict frauds.

INTRODUCTION:

In recent years, the prevailing data mining concerns people with credit card fraud detection model based on data mining. Since our problem is approached as a classification problem, classical data mining algorithms are not directly applicable.This project is to propose a credit card fraud detection system using supervisedlearning algorithm. supervised algorithms are evolutionary algorithms which aim at obtaining better solutions as time progresses.Credit card is the most popular mode of payment. As the number of credit card users is rising world-wide, the identity theft is increased, and frauds are also increasing.In the virtual card purchase, only the card information is required such as card number, expiration date, secure code, etc. Such purchases are normally done on the Internet or over telephone. To commit fraud in these types of purchases, a person simply needs to know the card details. The mode of payment for online purchase is mostly done by credit card. The details of credit card should be kept private. To secure credit card privacy, the details should not be leaked. Different ways to steal credit card details are phishing websites, steal/lost credit cards, counterfeit credit cards, theft of card details, intercepted cards etc. For security purpose, the above things should be avoided. In online fraud, the transaction is made remotely and only the card's details are needed. A manual signature, a PIN or a card imprint are not required at the purchase time. In most of the cases the genuine cardholder is not aware that someone else has seen or stolen his/her card information. The simple way to detect this type of fraud is to analyze the spending patterns on every card and to figure out any variation to the "usual" spending patterns. Fraud detection by analyzing the existing data purchase of cardholder is the best way to reduce the rate of successful credit card frauds. As the data sets are not available and also the results are not disclosed to the public. The fraud cases should be

detected from the available data sets known as the logged data and user behavior. At present, fraud detection has been implemented by a number of methods such as data mining, statistics, and artificial intelligence.

Credit card generally refers to a card that is assigned to the customer (cardholder), usually allowing them to purchase goods and services within credit limit or withdraw cash in advance. Credit card provides the cardholder an advantage of the time, i.e., it provides time for their customers to repay later in a prescribed time, by carrying it to the next billing cycle.

Credit card frauds are easy targets. Without any risks, a significant amount can be withdrawn without the owner's knowledge, in a short period. Fraudsters always try to make every fraudulent transaction legitimate, which makes fraud detection very challenging and difficult task to detect.

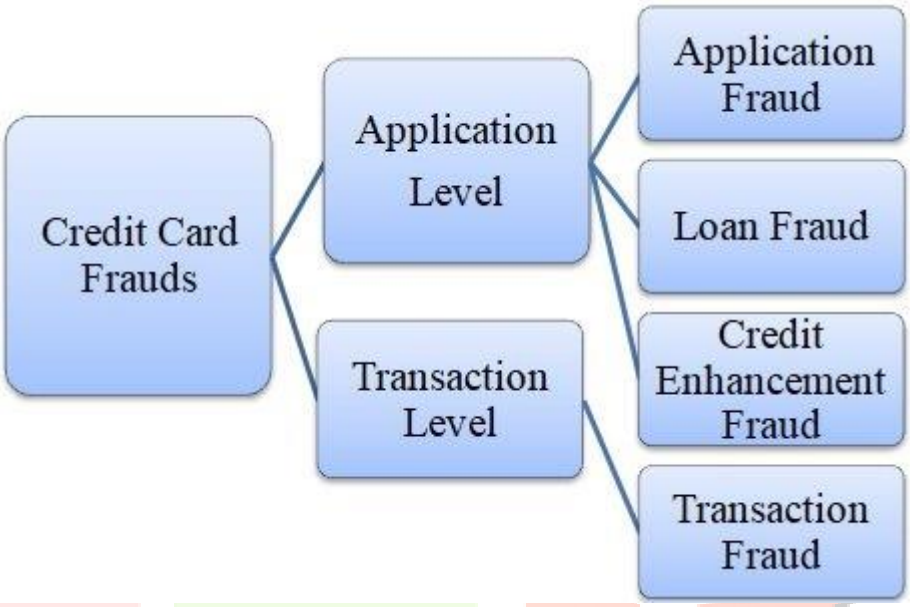

Fig: 1 Credit card frauds

Types of Algorithms

Supervised learning is built to make prediction, given an unforeseen input instance. A supervised learning algorithm takes a known set of input dataset and its known responses to the data (output) to learn the regression/classification model.An algorithm is used to learn the dataset and train it to generate the model for prediction of frauds for the response to new data or test data. Supervised learning uses classification algorithms and regression techniques to developpredictive models.

1.NAIVE BAYES: Naive Bayes classifiers calculate the probability of a sample to be of a certain category, based on prior knowledge. They use the Naïve Bayes Theorem, that assumes that the effect of a certain feature of a sample is independent of the other features. That means that each character of a sample contributes independently to determine the probability of the classification of that sample, outputting the category of the highest probability of the sample. In Bernoulli Naïve Bayes the predictors are boolean variables. The parameters that we use to predict the class variable take up only values yes or no.The basic idea of Naive Bayes technique is to find the probabilities of classes assigned to texts by using the joint probabilities of words and classes.

2.LOGISTICREGRESSION: Logistic regression is basically a supervised classification algorithm. In a classification problem, the target variable(or output), y, can take only discrete values for given set of features(or inputs), X. The logistic regression model described relationship between predictors that can be continuous, binary, and categorical. Logistic regression becomes a classification technique only when a

decision threshold is brought into the picture. The setting of the threshold value is a very important aspect of logistic regression and is dependent on the classification problem itself. It predicts the probability that a given data entry belongs to the category numbered as "1". Just like Linear regression assumes that the data follows a linear function, Logistic regression models the data using the sigmoid function.

3.RANDOM FOREST: The random forest is a supervised learning algorithm that randomly creates and merges multiple decision trees into one "forest." The goal is not to rely on a single learning model, but rather a collection of decision models to improve accuracy. The primary difference between this approach and the standard decision tree algorithm is that the root nodes feature splitting nodes are generated randomly.

4.BOOSTING TECHNIQUE: Boosting is an ensemble modeling technique which attempts to build a strong classifier from the number of weak classifiers. This procedure is continued, and models are added until either the complete training data set is predicted correctly, or the maximum number of models are added.AdaBoost was the first really successful boosting algorithm developed for the purpose of binary classification. Adaboost is short for Adaptive Boosting and is a very popular boosting techniquewhich combines multiple "weak classifiers" into a single "strong classifier".

LITERATURE REVIEW

Multiple Supervised and Semi-Supervised machine learning techniques are used for fraud detection, but we aim is to overcome three main challenges with card frauds related dataset i.e., strong class imbalance, the inclusion of labelled and unlabelled samples, and to increase the ability to process a large number of transactions.

Different Supervised machine learning algorithms like Decision Trees, Naive Bayes Classification, Least Squares Regression, Logistic Regression and SVM are used to detect fraudulent transactions in real-time datasets. Two methods under random forests are used to train the behavioural features of normal and abnormal transactions. They are Random-tree-based random forest and CART-based. Even though random forest obtains good results on small set data, there are still some problems in case of imbalanced data. The future work will focus on solving the above-mentioned problem. The algorithm of the random forest itself should be improved.

Performance of Logistic Regression, K-Nearest Neighbour, and Naïve Bayes are analysed on highly skewed credit card fraud data where Research is carried out on examining meta-classifiers and meta-learning approaches in handling highly imbalanced credit card fraud data. Through supervised learning methods can be used there may fail at certain cases of detecting the fraud cases. A model of deep Auto-encoder and restricted Boltzmann machine (RBM) that can construct normal transactions to find anomalies from normal patterns. Not only that a hybrid method is developed with a combination of Adaboost and Majority Voting methods.

Zhang Yongbin et al. suggested a behavior based credit card fraud detection model. Here they use the historical behavior pattern of the customer to detect the fraud. The transaction record of a single credit card is used to build the model. In this model, unsupervised Self organizing map method is used to detect the outliers from the normal ones.

Chuang et al. developed a model based on data mining. They used the web services to exchange data between banks and fraud pattern mining algorithm for detection. With the proposed scheme participant banks can share the knowledge about fraud patterns in a heterogeneous and distributed environment and further enhance their fraud detection capability and reduce financial loss.

Wen-Fang Yu et al. proposed an outlier mining method to detect the credit card frauds. Definitions of Distance based outliers are referred and the outlier mining algorithm was created. This model detects outlier

sets by computing distance and setting threshold of outliers. It efficiently detects the overdrafts and is also used to predict the fraudulent transactions.

Tao Guo et al. applied the neural data mining method. This model is based on customer's behavior pattern. Deviation from the usual behavior pattern is taken as an important task to create this model. The neural network is trained with the data and the confidence value is calculated. The credit card transaction with low confidence value is not accepted by the trained neural network and it is considered as fraudulent. If the confidence value is abnormal, then again it is checked for additional confirmation. The detection performance is based on the setting of threshold.

Suvasini Panigrahi et al. suggested a fusion approach. It consists of four components namely, rule based filter, DempsterShafer Adder, transaction history database and Bayesian learner. Rule based filter is used to find the suspicion level of the transaction. Dempster-Shafer Theory is used to compute the initial belief which is based on the evidences given by the rule based filter.

METHODOLOGY

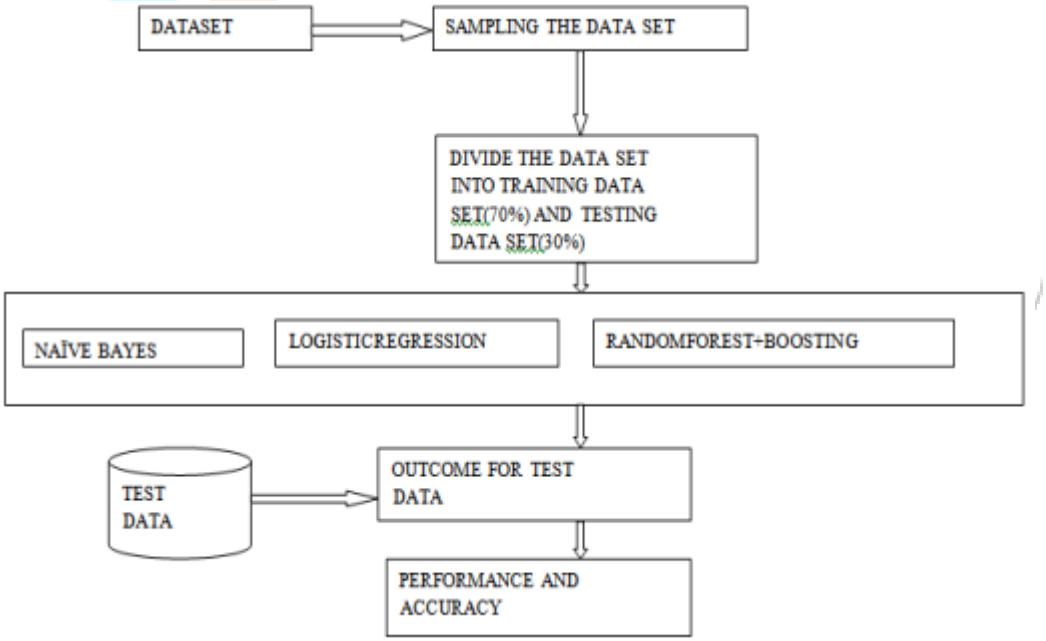

Fig: 2 System architecture

Dataset: In this paper credit card fraud detection dataset was used,which can be downloaded from Kaggle.This dataset contains transactions,occurred in two days,made in September 2013 by European cardholders. The dataset contains 31 numerical features. Since some of the input variables contains financial information, the PCA transformation of these input variables were performed in order to keep these data anonymous. Three of the given features weren't transformed. Feature "Time" shows the time between first transaction and every other transaction in the dataset. Feature "Amount" is the amount of the transactions made by credit card. Feature "Class" represents the label and takes only 2 values: value 1 in case fraud transaction and 0 otherwise.

Sampling: Further the data set is minimized to 560 transactions.Where 228 fraud and 332 normal transactions.

Divide the dataset: The dataset is divided into trained data set and test data set. 70% of the data set is under training and the remaining 30% is under testing.Here we are using some supervised machine learning

algorithms. The algorithms areNaive Bayes, Logistic RegressionandRandom Forest with boosting technique.

Naïve Bayes: Bayes theorem: Bayes theorem find probability of event occurring given probability of another event that has been alreadyoccurred.Naïve Bayes algorithm is easy and fast. This algorithm need less training data and highlyscalable

P (A/B) = (P (B/A) P (A)) / P (B)

Where, P (A) – Priority of A P (B) – Priority of B

P (A/B) – Posteriori priority of B

LogisticRegression: This algorithm similar to linear regression algorithm.But linear regression issued for predict / forecast values and Logistic regression is used for classificationtask.This algorithm easy for binary and multivariate classification task. Binomial is of 2 possible types (i.e. 0 or 1) only. Multinomial is of 3 or possible types and which are not ordered and Ordinal is in ordered in category (i.e. very poor, poor , good, very good).

Random Forest: First, start with the selection of random samples from a given dataset.Next, this algorithm will construct a decision tree for every sample. Then it will get the prediction result from every decision tree. Then voting will be performed for every predicted result. So finally, select the most voted prediction result as the final prediction result.

AdaBoost: AdaBoost is a machine learningalgorithm. Mainly developed for binary classification.For AdaBoost, Each instance in the training dataset is weighted. Initial weight is set To:

Weight (xi)= (1/n)Where, xi – i th traininginstance

n– Number of training instance

Algorithm steps for finding the Best algorithm:

Step1:Import the dataset

Step2:Convert the data into data frames format.

Step3:Do random sampling.

Step4:Decide the amount of data for training data and testing data.

Step5:Give 70% data for training and remaining data for testing(30%).

Step6:Assign train dataset to the models.

Step7:Apply the algorithm among 3 different algorithms and create the model.

Step8:Make predictions for test dataset for each algorithm.

Step9:Calculate accuracy of each algorithm by using confusion matrix.

Test data: After training is done on the datasetthen testing process take place.

Outcome for test data: We will get the respective results for each algorithm and performance is displayed in graphs.

Accuracy results: Finallyresults of each algorithm are shown with accuracy and the best algorithm is identified.

Evaluation: There are a variety of measures for various algorithms and these measures have been developed to evaluate very different things .So it should be criteria for evaluation of various proposed method. False Positive(FP),False Negative(FN),True Positive(TP),True Negative(TN) and the relation between them are quantities which usually adopted by credit card fraud detection researchers to compare the accuracy of different approaches. The definitions of mentioned parameters are presented below:

True Positive(TP): The true positive rate represents the portion of the fraudulent transactions correctly being classified as fraudulent transactions. True positive=Tp/TP+FN

TrueNegative(TN): The true negative rate represents the portion of the normal transactions correctly being classified as normal transactions. True negative=TN/TN+FP

False Positive (FP): The false positive rate indicates the portion of the non-fraudulent transactions wronglybeing classified as fraudulent transactions. False positive=FP/FP+TN

False Negative (FN): The false negative rate indicates the portion of the non-fraudulent transactions wrongly being classified as normal transactions. False negative=FN/FN+TP

Confusion matrix: The confusion matrix provides more insight into not only the performance of a predictive model, but also which classes are being predicted correctly, which incorrectly, and what type of errors are being made.The simplest confusion matrix is for a two-class classification problem, with negative and positive classes. In this type of confusion matrix, each cell in the table has a specific and wellunderstood name

Predicted	Positive	Negative
Positive	TP	FN
Negative	FP	TN

Accuracy:Accuracy is the percentage of correctly classified instances.It is one of the most widely used• classification performance metrics.

$$\text{Accuracy} = \frac{\text{Number of correct predictions}}{\text{Total Number of predictions}}$$

Or for binary classification models.The accuracy can be defined as:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

Precision and recall:Precision is the number of classifiedPositive or fraudulent instances that actually are positive instances.

Precision = Tp/(Tp+Fp)

Recall is a metric that quantifies the number of correct positive predictions made out of all positive predictions that could have been made.Unlike precision that only comments on the correct positive predictions out of all positive predictions, recall provides an indication of missed positive predictions.Recall is calculated as the number of true positives divided by the total number of true positives and false negatives.

Recall = Tp / (Tp + Fn)

F1 score: F1 Score is the weighted average of Precision and Recall. Therefore, this score takes both false positives and false negatives into account.

F1 Score = 2*(Recall * Precision) / (Recall + Precision)

Support: The support is the number of samples of the true response that lie in that class.Support is the number of actual occurrences of the class in the specified dataset. Imbalanced support in the training data may indicate structural weaknesses in the reported scores of the classifier and could indicate the need for stratified sampling or rebalancing. Support doesn't change between models but instead diagnoses the evaluation process.

RESULTS AND EVALUATION

Even though the accuracy is important, the fraud catching rate and false alarm rate are the better metrics for the fraud detection domain [26]. In this work, the confusion matrix is used for evaluating the fraud catching rate and false alarm rate. The standard confusion matrix format is shown in the following Table.1.

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

Table 1: Confusion matrix

In Confusion Matrix, the column signifies the predicted class and the row signifies the actual class. TP is True Positive (Fraud catching rate) which shows the number of genuine transactions correctly identified as non fraudulent. FP is False Positive (False alarm rate) which gives the number of genuine transactions incorrectly identified as fraudulent. FN is False Negative mistakenly consider fraudulent transaction as genuine. TN is True Negative which shows the number of fraudulent transactions correctly identified as fraudulent. Achieving highest fraud catching rate and lowest false alarm rate is the important task of this model.

The True Positive rate (TP) and False Positive rate (FP) are found by the following Eqs.

$$TP_{rate} = \frac{TP}{TP + FN}$$

$$FP_{rate} = \frac{FP}{TN + FP} \quad (1,2)$$

TPrate represents the ratio of positive class that was correctly identified. FPrate represents the ratio of the negative cases that was incorrectly identified as positive.

Accuracy represents the ratio of the total number of transactions that were correctly identified. The accuracy of the classifier is calculated by the Eq.(3) and the error rate is calculated by the Eq.(4),

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN}$$

$$Error\ Rate = \frac{FP + FN}{TP + FP + FN + TN} \quad (3,4)$$

In the Result, the TP value raises and FP value becomes low. The highest fraud catching rate and low false alarm rates are obtained by selecting the appropriate parameter values. The parameter values are found out by checking the behavior profiles of the cardholders. The parameter values of the proposed work are based on the average amount of transactions and the frequency of the card usage. This model achieves the accuracy more than 80 percent. Achieving high accuracy is a vital one and reducing the false alarms are also the important tasks in the credit card fraud detection. Too many false alarms restricted the customer from the use of credit card.

In the proposed approach false alarm rates are reduced. And also obtaining low false alarm rates will not restrict the fraud catching rate. The proposed model efficiently finds out most of the correct transactions and is well suited for fraud detection.

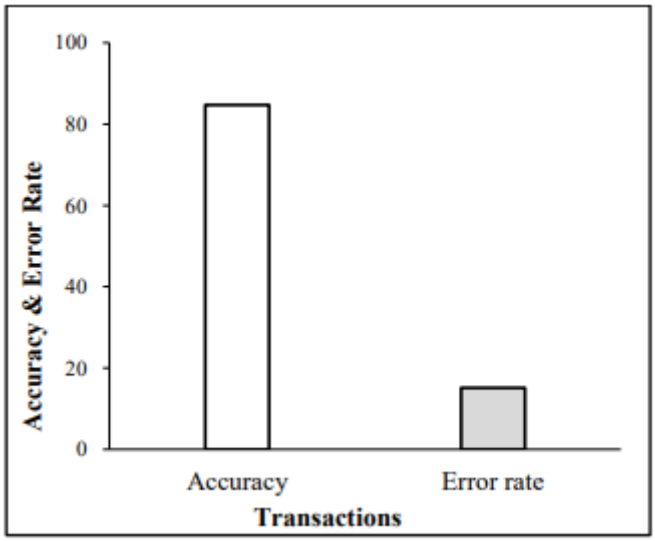

Fig: 3 Accuracy and Error rate

Conclusion:

In this paper, we studied applications of machine learning like Naïve Bayes, Logistic regression, Random forest with boosting and shows that it proves accurate in deducting fraudulent transaction and minimizing the number of false alerts. Supervised learning algorithms are novel one in this literature in terms of application domain. If these algorithmsare applied into bank credit card fraud detection system, the probability of fraud transactions can be predicted soon after credit card transactions. And a series of anti-fraud strategies can be adopted to prevent banks from great losses and reduce risks. The objective of the study was taken differently than the typical classification problems in that we had a variable misclassification cost. Percision,recall.f1-score,support and accuracy are used to evaluate the performance for the proposed system. By comparing all the three methods, we found that random forest classifier with boosting technique is better than the logistic regression and naïve bayes methods.

References

1. [7] Emin Aleskerov, Bernd Freisleben and Bharat Rao, “CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection”, Proceedings of the Computational Intelligence for Financial Engineering, pp. 220-226, 1997.
2. Zhang yongbin, You Fucheng and Liu Huaqum, “Behavior–Based Credit Card Fraud Detection Model”, Fifth International Joint Conference on INC, IMS and IDC, pp. 855-858, 2009.
3. Chuang-Cheng Chiu and Chich-Yuan Tsai, “A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection”, Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service, pp. 177-181, 2004.
4. Wen-Fang Yu and Na Wang, “Research on Credit Card Fraud Detection Model Based on Distance Sum”, Proceedings of the International Joint Conference on Artificial Intelligence, pp. 353-356, 2009.
5. Tao Guo and Gui-Yang Li, “Neural Data Mining for Credit Card Fraud Detection”, International conference on Machine Learning and Cybernetics, Vol. 7, pp. 3630-3634, 2008.

6. Salvatore J Stoflo, David W Fan, Wenke Lee and Andreas L Prodromidis and Philip K Chan, "Cost –Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project", Proceedings of the DARPA Information Survivability Conference and Exposition, Vol. 2, pp. 130- 144, 2000.
7. Pumsirirat, A. and Yan, L. (2018). Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine. International Journal of Advanced Computer Science and Applications, 9(1).
8. 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.
9. Randhawa, Kuldeep, et al. "Credit Card Fraud Detection Using AdaBoost and Majority Voting." IEEE Access, vol. 6, 2018, pp. 14277–14284., doi:10.1109/access.2018.2806420.
10. Roy, Abhimanyu, et al. "Deep Learning Detecting Fraud in Credit Card Transactions." 2018 Systems and Information Engineering Design Symposium (SIEDS), 2018, doi:10.1109/sieds.2018.8374722.
11. 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.
12. Awoyemi, John O., et al. "Credit Card Fraud Detection Using Machine Learning Techniques: A Comparative Analysis." 2017 International Conference on Computing Networking and Informatics (ICCNI), 2017, doi:10.1109/iccni.2017.8123782.
13. 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.