International Journal of Research in Engineering, Science and Management
Volume 4, Issue 8, August 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

A Review on the Performance Analysis of Supervised and Unsupervised algorithms in Credit Card Fraud Detection

Prathima Gamini[1], Sai Tejasri Yerramsetti[2], Gayathri Devi Darapu[3*],
Vamsi Kaladhar Pentakoti[4], Prudhvi Raju Vegesena[5]
[1]*Assistant Professor, Department of Electronics and Communication Engineering, Sagi Ramakrishnam Engineering College, Bhimavaram, India*
[2,3,4,5]*Student, Department of Electronics and Communication Engineering, Sagi Ramakrishnam Engineering College, Bhimavaram, India*

***Abstract*: The detection of credit card fraud is the most common issue encountered in the present scenario. Generally, credit card fraud occurs when a card is stolen and used for unauthorized purposes or even when the card information is misused. This paper provides a review of performance analysis of various machine learning algorithms. Here both supervised and unsupervised learning algorithms are considered for analysis. The accuracy, precision, recall, f1score, and specificity of algorithms are regarded here for analyzing their performance.**

***Keywords*: credit card fraud detection, k-means, Local outlier factor, Neural Network, Random Forest, stacking classifier, Support Vector Machine.**

1. Introduction

A significant objective of this paper is to evaluate the performance of supervised and unsupervised algorithms used to identify fraudulent credit card transactions. Various Artificial Intelligence(AI) techniques can be used such as data mining, neural networks, machine learning and pattern recognition. The supervised and unsupervised methods of machine learning involve training computers to recognize patterns in expansive datasets and enhance those patterns naturally without the intervention of humans. Supervised learning uses labeled data to analyze and predict outcomes whereas unsupervised learning uses algorithms to analyze and cluster unlabeled data. As hybrid models incorporate both supervised and unsupervised machine learning, they may be more accurate.

Fig. 1 represents the flowchart of fraud detection. Credit fraud detection involves data splitting, training, deployment and evaluation of models. The flow chart below illustrates how to detect fraud. The process begins by cleaning up the data and obtaining the features, then train a model and apply it to various machine learning models to ensure accuracy. The credit card transaction dataset is highly imbalanced because it has more legitimate transactions than fraudulent ones. So, in order to overcome this obstacle, under-sampling and oversampling techniques can be designed to obtain comparatively balanced data. Usage of data mining techniques can lead to an improved fraud detection system. Data mining reveals meaningful patterns, turning raw data, big datasets into valuable information.

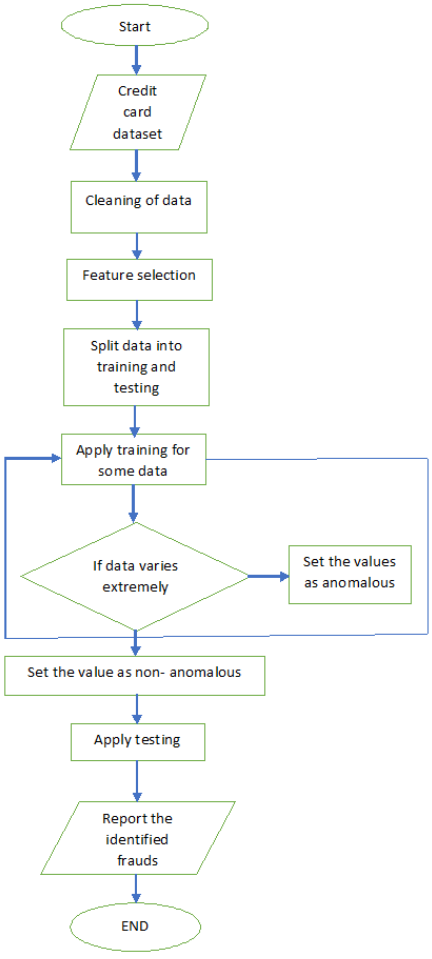

Fig. 1. Process for fraud detection

*Corresponding author: gaya3gayu2000@gmail.com

A. Dataset Used

The dataset [7] used in this paper contains the records of transactions made by European cardholders. It has 284,807 transactions recorded over two days, of which 494 were frauds. There are very few fraudulent transactions. The dataset was generated and further analyzed by Worldline and the Machine Learning Group of ULB (Universite Libre de Bruxelles). There are 28 features obtained after the analysis of the main components of the actual attributes. There is no transformation of the Time or Amount components.

2. Related Work

In all machine learning models, performance suffers due to the skewness of the training data set. For balancing an unbalanced dataset, there are two methods, intrinsic and network-based. The intrinsic features analyze past transactions of any customer to detect patterns. Network-based features calculate suspiciousness scores based on the connections between credit cardholders and merchants. Both methods result in a very high accuracy score in Random Forest(RF) results in a 1% false-positive, making this the perfect model to detect fraudulent transactions. Comparative analyses of various modelling and algorithm techniques were made on a real dataset. Some of the algorithms underperform because of the unbalanced dataset. The unbalanced dataset for learning (both non-stream and stream credit cards) comprises three methods (static, update, and data stream). Synthetic Minority Over Sampling Technique(SMOTE) and Easy Ensemble were also used to balance a dataset consisting of unbalanced data points. Random forest(RF) & Support Vector Machines(SVM) both show a decrement in Area Under Curve(AUC) and an increment in F-measure. The neural network architecture is implemented in an unsupervised manner using real-time transaction entry. Self-organizing maps of neural networks using optical classification can solve the problem for an associated group. The detection of fraud was 95% with the Receiver Operating Characteristic(ROC) curve, without any false alarms. Data Mining reports the development & implementation of a fraud detection system in a large e-commerce site. For the business outcomes to take a longer time, it was possible to train the algorithm using a cost-based performance approach. For the business outcomes to take a longer time, it is possible to train the algorithm using a cost-based performance approach.

3. Models Used

A. Supervised Algorithms

1) Stacking classifier

The stacking technique combines multiple classifiers by utilizing a meta-classifier. The whole data set has to be used to generate individual classification models and the meta-classifier is subsequently calculated based on the output features of the models. Meta-classifiers can be trained either on class labels or on probabilities derived from ensembles.

The stacking classifier method consists of two estimators stacked together to form a classification or regression model. The first layer consists of all baseline models that predicts the outputs of test datasets. The second layer consists of a Meta-Classifier or Regressor that uses all the predictions from baseline models as input and generates new predictions.

2) Random Forest (RF)

Random forests are composed of many individual decision trees that act together as an ensemble. As a result of the random forest, each tree makes a class prediction and the class with the most votes will become the prediction of this model.

As a classification task, a random forest output is a class selected by most trees. Due to decision trees' tendency to overfit their training sets, random forests help compensate for this problem. While they are generally better than decision trees, they are less accurate than gradient boosted trees. However, data characteristics can affect their performance.

3) SVM

SVM stands for Support Vector Machines. It is a supervised machine learning algorithm and used for classification or regression. To do this, it applies a technique called the kernel trick. Based on these transformations, it creates an optimal boundary between the output options.

The support-vector machine creates a set of hyperplanes in an infinite-dimensional space, which can be used for classification, regression, or other tasks like outlier detection. It is intuitively obvious that a good separation is achieved by selecting the hyperplane with the greatest distance to that class' nearest training-data point (so-called functional margin), since the greater the margin, the lower the generalization error of the classifier.

B. Unsupervised Algorithms

1) K-means clustering

K-means algorithm is an unsupervised learning algorithm used to group the unlabeled dataset. It is an algorithm that divides an unlabeled dataset into k different clusters so that each dataset belongs to only one group. Here the term 'means' represent the average of the data; that is, finding the centroid.

2) LOF

Local Outlier Factor (LOF) is a method for unsupervised anomaly detection that calculates the local deviation of a particular data point relative to its neighbors. The algorithm considers those samples as outliers that have smaller densities than their neighbors.

if LOF(k) ~ 1, then Similar density as neighbors,
if LOF(k) < 1, then Higher density than neighbors (Inlier),
if LOF(k) > 1, then Lower density than neighbors (Outlier)

3) Neural network

The neural network is an algorithm that views sensory data through a kind of machine perception, classification or clustering process. Neural network algorithms generally do not need to include rules that define what to expect from inputs. It learns from processing many labeled examples that are used during training and uses this answer key to determine what characteristics of inputs are necessary to construct the correct output. After a sufficient number of examples are processed, the neural network can begin processing new, unseen inputs and successfully return accurate results.

4. Comparison Criteria

The performance of various models is evaluated and compared using various parameters such as accuracy, precision, recall, F1-score and specificity,

Accuracy: Accuracy is one way to measure how well an algorithm can classify a data point. Based on all the data points, accuracy refers to the number of correctly predicted points.

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

Precision: The precision measures the number of observations correctly predicted out of those that are all positive.

$$\text{Precision} = \frac{TP}{TP+FP}$$

Recall: The recall is the proportion of correctly predicted positive observations to all observations in a class.

$$\text{Recall} = \frac{TP}{TP+FN}$$

F1 score: It is a weighted average of Precision and Recall forms the F1 score. As a result, this score accounts for both false positives and false negatives.

$$\text{F1 score} = \frac{2*recall*precision}{recall+precision}$$

Specificity: Specificity, which is known as the True negative rate, is the percentage of correctly identified negatives.

$$\text{Specificity} = \frac{TN}{TN+FP}$$

Here TP represents True Positive, TN represents True Negative, FP represents False Positive and FN represents False Negative.

Accuracy is enhanced if false positives and false negatives cost the same. In an unbalanced class distribution, F1-score will be helpful.

In other words, if the cost of false positives and false negatives is very different, it's better to consider both precision and recall.

5. Performance Analysis

The performance analysis is done based on the implementation of supervised learning algorithms in the "Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study" [2] and unsupervised algorithms in the "Fraud Detection in Credit Card Data using Unsupervised Machine Learning Based Scheme" [5]. Though the algorithms are highly accurate, it is necessary to consider the F1 score crucial while treating unbalanced distributions. The algorithms which have good accuracy, F1-score and specificity are more reliable. Based on the analysis in the paper of supervised learning algorithms, stacking classifiers have high accuracy followed by Random Forest(RF) and Support Vector Machine(SVM). In the paper of the unsupervised learning algorithms, Neural Networks(NN) have good accuracy followed by k-means and Local Outlier Factor(LOF).

The stacking method reduces variance and produces a more robust model by combining predictions from multiple models together. It results in improved model performance. But it takes longer to train and require more memory than simpler models. Random forest reduces overfitting in decision trees and improves accuracy. As it is rule-based, no normalization of data is required. Due to its use of many decision trees to determine classification, it takes a long time to train and makes it difficult to interpret and determine the significance of each variable.

SVM algorithms are not suitable for large data sets but the risk of over-fitting is less in SVM. K-means is easy to implement. It computes more rapidly (assuming K is small) when there are more variables to analyze. The final results may vary depending on the order of the data. It is difficult to predict the number of clusters (K-value). The final results may vary depending on the order of the data.

Local Outlier Factor (LOF) identifies an outlier based on the local neighbourhood. As there is no threshold for LOF, the choice of an outlier is up to the individual user. In Neural networks, once trained then the predictions are so fast. It is computationally time-consuming and costly to train on a traditional CPU. It depends a lot on training data. Consequently, over-fitting and generalization of samples are problems.

6. Conclusion

This review is helpful in the analysis of some of the supervised and unsupervised algorithms in credit fraud detection by considering the parameters such as accuracy, precision, recall, F1-score and specificity. Here according to review, the performance of Stacking Classifiers (SC) from supervised learning and Neural Network (NN) from unsupervised learning is better than that of other algorithms. Researchers and students can use this review to sort out algorithms to determine which is the best.

References

[1] S. Khatri, A. Arora and A. P. Agrawal, "Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison," *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2020, pp. 680-683.

[2] S. Dhankhad, E. Mohammed and B. Far, "Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study," *2018 IEEE International Conference on Information Reuse and Integration (IRI)*, 2018, pp. 122-125.

[3] R. Sailusha, V. Gnaneswar, R. Ramesh and G. R. Rao, "Credit Card Fraud Detection Using Machine Learning," *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2020, pp. 1264-1270.

[4] V. Jain, M. Agrawal and A. Kumar, "Performance Analysis of Machine Learning Algorithms in Credit Cards Fraud Detection," *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2020, pp. 86-88.

[5] A. K. Rai and R. K. Dwivedi, "Fraud Detection in Credit Card Data using Unsupervised Machine Learning Based Scheme," *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2020, pp. 421-426.

[6] O. Adepoju, J. Wosowei, S. lawte and H. Jaiman, "Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques," *2019 Global Conference for Advancement in Technology (GCAT)*, 2019, pp. 1-6.
[7] Dataset for credit card fraud, Credit Card Fraud Detection, Kaggle, 2018.
[8] A. Dal Pozzolo, O. Caelen, Y. A. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," in *Expert Syst. Appl.*, vol. 41, no. 10, pp. 4915–4928, 2014.
[9] M. A. Scholar, M. Ali, and P. Fellow, "Investigating the Performance of Smote for Class Imbalanced Learning: A Case Study of Credit Scoring Datasets," in *European Scientific Journal*, vol. 13, no. 33, pp. 340–353, 2017.
[10] H. He, W. Zhang, and S. Zhang, "A novel ensemble method for credit scoring: Adaption of different imbalance ratios," in *Expert Syst. Appl.*, vol. 98, pp. 105–117, May 2018.
[11] A. D. Pozzolo, O. Caelen, R. A. Johnson and G. Bontempi, "Calibrating Probability with Under sampling for Unbalanced Classification," *2015 IEEE Symposium Series on Computational Intelligence*, 2015, pp. 159-166.
[12] Y. Sahin and E. Duman, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines," *Int. Multiconference Eng. Comput. Sci.*, vol. 1, pp. 442–447, 2011.
[13] X. Liu, J. Wu and Z. Zhou, "Exploratory Undersampling for Class-Imbalance Learning," in *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 39, no. 2, pp. 539-550, April 2009.
[14] E. A. Mohammed, M. M. A. Mohamed, C. Naugler, and B. H. Far, "Toward leveraging big value from data: chronic lymphocytic leukemia cell classification," in *Netw. Model. Anal. Heal. Informatics Bioinforma.*, vol. 6, no. 1, p. 6, Dec. 2017.
[15] G. H. John and P. Langley, "Estimating Continuous Distributions in Bayesian Classifiers," UAI'95: Proceedings of the Eleventh conference on Uncertainty in artificial intelligence, August 1995, pp. 338–345.
[16] C. Whitrow, D. J. Hand, P. Juszczak, D. Weston, and N. M. Adams, "Transaction aggregation as a strategy for credit card fraud detection," in *Data Min. Knowl. Discov.*, vol. 18, no. 1, pp. 30–55, Feb. 2009.
[17] G. Rushin, C. Stancil, M. Sun, S. Adams, and P. Beling, "Horse race analysis in credit card fraud - Deep learning, logistic regression, and Gradient Boosted Tree," *2017 Syst. Inf. Eng. Des. Symp.* SIEDS 2017, pp. 117–121, 2017.