Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison

Samidha Khatri
Department of Computer Science & Engineering
Amity University Uttar Pradesh
Samidha.khatri@gmail.com

Aishwarya Arora
Department of Computer Science & Engineering
Amity University Uttar Pradesh
Aroraaishwarya99@gmail.com

Arun Prakash Agrawal
Department of Computer Science & Engineering
Sharda University Greater Noida
arun.agrawal@sharda.ac.in

***Abstract*— In today's economic scenario, credit card use has become extremely commonplace. These cards allow the user to make payments of large sums of money without the need to carry large sums of cash. They have revolutionized the way of making cashless payments and made making any sort of payments convenient for the buyer. This electronic form of payment is extremely useful but comes with its own set of risks. With the increasing number of users, credit card frauds are also increasing at a similar pace. The credit card information of a particular individual can be collected illegally and can be used for fraudulent transactions. Some Machine Learning Algorithms can be applied to collect data to tackle this problem. This paper presents a comparison of some established supervised learning algorithms to differentiate between genuine and fraudulent transactions.**

Keywords: Credit Card, Credit Card Fraud, Machine Learning, Supervised Learning.

I. INTRODUCTION

A Fraud can be described as an intentional deceit which is perpetrated for some kind of gain, mostly monetary. It is an unfair practice whose occurrences are increasing by the day. There has been a sharp increase in the usage of electronic payment methods like credit and debit cards and this has in turn led to a rise in credit card frauds. These cards may be used in both online as well as offline modes to make payments [7]. In case of the online mode of payment, the card may not have to be physically presented. In such cases the card data is prone to attack by hackers or cyber criminals. These kinds of frauds result in millions being lost every year. To overcome this obstacle, many algorithms have and are being developed. Various detection approaches are being worked upon to solve this issue most efficiently [8].

Credit card transactions are extremely commonplace now but they also come with their own set of problems. There are a lot of problems faced during fraud detection. The process of acceptance or rejection of a transaction happens within a very small-time frame, which may range between micro and milliseconds. Therefore, the process adopted for the detection of a fraudulent transaction has to be extremely quick and effective. Another problem is that there are a vast number of similar types of transactions happening at the same time. This makes it difficult to monitor each and every transaction individually and hence determine a fraud. Thus, an efficient Fraud Detection System must be put into work to be able to differentiate between a genuine and a fraud transaction. Such a system works on the principle of learning user-specific card usage behavior. Thus, existing approaches of supervised as well as unsupervised machine learning techniques can be applied to the data.

The objective of this paper is to evaluate an imbalanced dataset with the help of various supervised machine learning models and to determine which one of those is the best suited for detecting credit card frauds. We make use of 5 supervised machine learning models to evaluate a dataset on the basis of various predefined criteria.

II. RELATED WORK

Specific algorithms based on artificial intelligence and neural networks are also being proposed and implemented to predict the credit card frauds with increased accuracy. The distribution of the datasets used for fraud detection is highly imbalanced. So, to overcome this obstacle, under- sampling and oversampling techniques are being designed to obtain comparatively balanced data. Data mining techniques are also being implemented in order to create a more efficient Fraud Detection System [9]. Another important area of development is the emergence of new hybrid models. These are derived from preexisting supervised as well as unsupervised machine learning techniques. Hybrid Models may be able to produce a more accurate result as they encapture the capabilities of both supervised as well as unsupervised machine learning [15].

It is observed that the performance of all machine learning datasets is hindered due to the skewness of available data sets which are usually unbalanced. To overcome this problem, the unbalanced datasets are to be converted to balanced ones. This can be done by mainly two ways which are Intrinsic Method and Network based Method. In Intrinsic Feature Method, a pattern in the customer Activity is observed whereas in Network -based features Method, the network of users and the card merchants is exploited. These techniques may significantly improve the functioning of certain Models as they work on a more Balanced Dataset[5].

III. MACHINE LEARNING

Machine Learning is basically an application of Artificial Intelligence techniques in order to make the systems learn by themselves. This means that the system automatically learns, improvises and adapts through experience without it being programmed for performing a particular operation. This field

978-1-7281-2791-0/20/$31.00 ©2020 IEEE

deals with the coming up of programs that can deal with data on their own, that is, which can access and modify the provided data according to the need of the user. Machine Learning can be classified into 3 main categories which are Supervised Learning, Unsupervised Learning and Reinforcement Learning.

A. Machine Learning in Credit Card Fraud Detection

Machine Learning basically provides the system with the "ability to learn". The machine is able to use previously procured data and analyze it further without being explicitly commanded to. This feature is basically beneficial in detection of credit card frauds. This enables machine learning algorithms to be successfully implemented in the banking domain to identify the potentially risky transactions [13]. There are more than a million transactions which occur daily, all these need to be checked for authenticity. To carry out this task, the system can be trained to separate out the fraudulent transactions from the non-fraudulent ones. This is mostly done by feeding it past transactions data, especially the ones from the non-authentic transactions, so that all the newly approaching transactions can be labelled as normal or suspicious respectively. Subsequently, the suspicious ones will be set apart for further investigation.

B. Supervised Learning

This type of learning is also referred to as predictive learning as it predicts the class of unknown objects based on prior class-related information of similar objects. The main inspiration behind this type of learning is to learn from the information about the task, which has been provided in the past. A machine requires the basic data about the task to be provided to it. This basic input, or experience is given to it in the form of 'training data'. This is the past information or data of a particular task. In this paper, we use the supervised approach to detect fraud detection and analyze the various algorithms based on supervised machine learning [5]. In this kind of supervised approach, a database of past cases of fraudulent and genuine transactions is stored. This database acts as a reference point for the various algorithms. The process starts with the analysis of a provided dataset, then the selected algorithm produces an inferred function in order to make predictions about the possibility of getting various output values. Irrespective of the model chosen, supervised learning works as well as the data being used to train it. The prediction will be as accurate, as is the quality of data being provided to the machine. In this paper, we use various Classification models of Supervised machine learning to predict wrongful transactions with the help of an imbalanced dataset. These various models are compared after they are run on the basis of the outputs that they provide.

IV. DATASET USED

A dataset is basically a collection of related data. In this paper, we make use of a publicly available imbalanced dataset. An imbalanced dataset is one in which disparity occurs in the dependent variables. Imbalanced implies that there is an unequal distribution of classes. The particular dataset that we use is also an imbalanced one. This particular dataset contains the record of transactions made by European cardholders. It has the records of 284,807 transactions made over a span of two days, out of which 492 were found out to be fraud. The percentage of fraudulent transactions is found out to be extremely low. This dataset was made and further analyzed during a joint effort of Worldline and the Machine Learning Group of ULB (Université Libre de Bruxelles) [14]. There are 28 features obtained after the analysis of the main components of the actual attributes. The Time and Amount components are not transformed and are provided as it is.
Accuracy and some metrics cannot be used as they are not sensitive to imbalanced data [1].

V. CRITERIA FOR COMPARISON

In order to evaluate the performance of a particular model, we make use of various parameters. The models are used on the trained dataset and the outputs obtained with the use of each model are compared systematically to those produced by the other models. Based on these comparisons, a conclusion is formed as to which is the best suited model for a particular dataset or a particular type of problem. In this paper we make use of the parameters Sensitivity, Precision and Time to compare the various models being used [1][2].

A. Sensitivity

It is a measure of the proportion of actual positive cases that got predicted as positive or true positive. This actually implies that there are supposed to be some proportion of actual positive cases that would get predicted indirectly as negative. Sensitivity is also sometimes referred to as Recall. Mathematically, sensitivity can be calculated as follows:

$$Sensitivity = (TP)/(TP + FN) \quad (1)$$

Where, TP= True Positive and FN = False Negative

B. Precision

It gives a measure of the proportion of positive predictions that are truly positive. It indicates the reliability of a model in predicting a class of interest. Precision is basically a ratio of correctly positively labelled to all positively labelled. Mathematically, precision can be calculated as follows:

$$Precision = (TP)/(TP + FP) \quad (2)$$

Where, TP= True Positive and FP = False Positive

C. Time

Time is used as a parameter for performance evaluation of the various models that are used. We calculate the time for training the model and predicting the test data. The Time calculated is not the actual time, but the approximate time taken by a particular model. This parameter is used to compare the various models used based upon the time taken by them in handling the data.

VI. MODELS USED

A. Decision Tree

This is one of the most widely used predictive modelling approaches. As per the name of the model, this is built in the form of a tree like structure [16]. This model maybe used in case of a multi-dimensional analysis where there are multiple classes present. The past data also known as the past vector is used to create a model that can be used to predict the value of the output based on the input being provided. There are multiple nodes in a tree and each node corresponds to one or the other vector. The tree terminates at a leaf node where each such node represents a possible outcome or output.

B. kNN

k- Nearest Neighbor model is one the simplest but most effective models. In this model, the class label of the test datasets on the basis of the class label of the neighboring training data elements. The similarity between two elements is measured using Euclidean Distance [4][16]. It is also known as an Instance learning or Lazy model. The value of 'k' is calculated which actually the number of is nearest neighbors that have to be considered.

A suitable value for 'k' should be chosen. An appropriate distance metric is also a requirement. Sometimes, the 'Minkowski' distance may be used. It is a generalization of the Euclidean and Manhattan distance. Mathematically, it is can be represented as:

$$d\left(x^{(i)}, x^{(j)}\right) = \sqrt[p]{\sum_k |x_k^{(i)} - x_k^{(j)}|^p} \quad (3)$$

C. Logistic Regression

It is basically a statistical model which makes use of a logistic function to model a binary dependent variable. This model is mainly used where there is a chance of occurrence of a binary classification issue. It works well on linearly separable classes [4].The odds ratio is one concept using which we can also define the logit function. It is the probability of an event occurring.

$$Odds\ Ratio = p/(1-p) \quad (4)$$

Where, p = probability of the positive event

The logit function is the logarithm of the odds ratio. It takes input in the range of [0,1] and transforms them to values over the real-number range.

The logit function can be defined as follows:

$$Logit(P) = \log \frac{P}{1-P} \quad (5)$$

In this model, the sigmoid function is also used effectively

$$\emptyset(z) = \frac{1}{1-e^{-z}} \quad (6)$$

D. Random Forest

This model is basically an ensemble classifier, i.e. a combining classifier that uses and combines many decision tree classifiers. The main agenda behind using multiple trees is to be able to train the trees enough, such that, contribution from each of them comes in the form of a model. After the generation of the tree, the output is combined through majority. It uses multiple decision trees so that, the dependence of each of them is on a particular dataset possessing similar distribution throughout the tree [6]. This particular model has the quality of efficiently balancing errors in a class population of unbalanced data sets. It can be used to solve both classification as well as regression problems.

E. Naïve Bayes

It is a form of probabilistic classifier model; this implies that it has the ability to make predictions for multiple classes at once. It is based on the Bayes Theorem. Probabilistic Classifiers are those which make it possible to predict multiple classes. The decision is made based on conditional probability. This model uses a set of algorithms instead of a single algorithm, but all of these have a common principle. In this model, it is assumed that each feature makes an equal and individual contribution to the output. This model has certain advantage over other models as it requires only a small amount of training data [4].

VII. OBSERVATIONS

TABLE I
PERFORMANCE EVALUATION OF VARIOUS MODELS AT THRESHOLD VALUE OF 0.5

MODEL	SENSITIVITY	PRECISION
DECISION TREE	79.21	85.11
KNN	81.19	91.11
LOGISTIC REGRESSION	63.34	87.67
RANDOM FOREST	75.25	93.83
NAIVE BAYES	85.15	6.56

We use the imbalanced dataset to analyze the 5 supervised learning models and find out the values of sensitivity and precision for each of these models. The default threshold value is taken as 0.5 according to standards.

TABLE II
PERFORMANCE EVALUATION OF VARIOUS MODELS AT THRESHOLD VALUE OF 0.4

MODEL	SENSITIVITY	PRECISION
DECISION TREE	79.21	85.11
KNN	81.19	91.11
LOGISTIC REGRESSION	69.31	87.5
RANDOM FOREST	78.22	89.77
NAIVE BAYES	85.15	6.52

The Threshold value is changed from 0.5 to 0.4 for calculating sensitivity and precision for each model. The analysis was performed at different values, but the best output was obtained when the threshold value was taken as 0.4. When the value was changed, an increase was observed in the sensitivity and

precision of Logistic Regression, Naïve Bayes and Random Forest.

TABLE III
TIME TAKEN FOR TRAINING AND PREDICTING DATA USING VARIOUS MODELS

MODEL	TIME TAKEN FOR TRAINING THE MODEL (SECONDS)	TIME TAKEN FOR PREDICTING THE TEST DATA (SECONDS)
DECISION TREE	5s	0s
KNN	1s	462s
LOGISTIC REGRESSION	3s	0s
RANDOM FOREST	23s	0s
NAIVE BAYES	0s	0s

The time taken by all 5 models for training the model and predicting the test data was recorded. These values are not the actual values, but the approximate values of time taken by them.

VIII. CONCLUSION AND FUTURE WORK

In this study, we used an imbalanced dataset to check the suitability of different supervised machine learning models to predict the chances of occurrence of a fraudulent transaction. We used sensitivity, precision and time as the deciding parameters to come to a particular conclusion. Accuracy as a parameter was not used as it is not sensitive to imbalanced data and does not give a conclusive answer. We analyzed the kNN, Naïve Bayes, Decision Tree, Logistic Regression and Random Forest models in this study. We used these models for predicting the chances of occurrence of a fraudulent credit card transaction out of a given number of transactions. Credit Card frauds are a modern-day issue and we came to the conclusion that the best suited model for predicting such frauds is the Decision Tree model. The analysis shows that the sensitivity of the kNN model is greater than that of Decision tree, but as time taken by kNN for testing the data is very large, we choose Decision Tree over kNN. In case of fraud detection, we need to ensure that minimum time is taken for prediction, therefore, Decision Tree is the preferred model.

Future researchers in this field may apply the resampling techniques to the respective datasets being used. This technique helps to reduce the imbalance ratio of datasets which in turn produces better classification results.

After the comparative analysis of the various Supervised Learning models, we can infer that the Decision Tree Model is the best approach to be used for detecting credit card fraud detection. But, the performance of Decision Tree Model must also be evaluated with the help of unsupervised machine learning models in the future to produce a more conclusive result. This tells us whether the model which is chosen is a better option or the unsupervised machine learning techniques perform better.

REFERENCES

[1]https://www.analyticsvidhya.com/blog/2016/03/practical-guide-deal-imbalanced-classification-problems/.[Accessed: Oct 12, 2019].

[2]https://www.ritchieng.com/machine-learning-evaluate-classification-model/.[Accessed: Oct 12, 2019].

[3] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi and G. Bontempi," Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy," in IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3784-3797, Aug. 2018.

[4] J. O. Awoyemi, A. O. Adetunmbi and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, 2017, pp. 1-9.

[5] 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), Salt Lake City, UT, 2018, pp. 122-125.

[6] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang and C. Jiang, "Random forest for credit card fraud detection," 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), Zhuhai, 2018, pp. 1-6.

[7] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decis. Support Syst., vol. 50, no. 3, pp. 602–613, 2011.

[8] K. Chaudhary, J. Yadav, and B. Mallick, "A review of Fraud Detection Techniques: Credit Card," Int. J. Comput. Appl., vol. 45, no. 1, pp. 975–8887, 2012.

[9] F. N. Ogwueleka, "Data Mining Application in Credit Card Fraud Detection System," vol. 6, no. 3, pp. 311–322, 2011.

[10] O. S. Yee, S. Sagadevan, N. Hashimah, and A. Hassain, "Credit Card Fraud Detection Using Machine Learning As Data Mining Technique," vol. 10, no. 1, pp. 23–27.

[11] C. Phua, D. Alahakoon and V. Lee, "Minority report in fraud detection", *ACM SIGKDD Explorations Newsletter*, vol. 6, no. 1, p. 50, 2004.

[12] N. Sethi and A. Gera, "A Revived Survey of Various Credit Card Fraud Detection Techniques", *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 4, pp. 780-791, 2014.

[13] J. Awoyemi, A. Adetunmbi and S. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis", *2017 International Conference on Computing Networking and Informatics (ICCNI)*, 2017.

[14]http://www.ulb.ac.be/di/map/adalpozz/imbalancedatasets.zip.[Accessed: Oct 10, 2019].

[15] S. Mittal and S. Tyagi, "Performance Evaluation of Machine Learning Algorithms for Credit Card Fraud Detection", *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2019.

[16] S.Dutt, A.K.Das and S.Chandramouli, Machine Learning. Pearson Education India, 2018.