INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Credit card fraud detection using Naïve Bayes model based and KNN classifier

Sai Kiran
usaikiran96@gmail.com
Bharati Vidyapeeth'S College of Engineering, Paschim Vihar, Delhi

Jyoti Guru
jguru207@gmail.com
Bharati Vidyapeeth'S College of Engineering, Paschim Vihar, Delhi

Rishabh Kumar
rishabhkumar1800@gmail.com
Bharati Vidyapeeth'S College of Engineering, Paschim Vihar, Delhi

Naveen Kumar
naveenkumarr233@gmail.com
Bharati Vidyapeeth'S College of Engineering, Paschim Vihar, Delhi

Deepak Katariya
deepak.281295@gmail.com
Bharati Vidyapeeth'S College of Engineering, Paschim Vihar, Delhi

Maheshwar Sharma
maheshwar1524@gmail.com
Bharati Vidyapeeth'S College of Engineering, Paschim Vihar, Delhi

ABSTRACT

Machine Learning is the technology, in which algorithms which are capable of learning from previous cases and past experiences are designed. It is implemented using various algorithms which reiterate over the same data repeatedly to analyze the pattern of data. The techniques of data mining are no far behind and are widely used to extract data from large databases to discover some patterns making decisions. This paper presents the Naïve Bayes improved K-Nearest Neighbor method (NBKNN) for Fraud Detection of Credit Card. Experimental results illustrate that both classifiers work differently for the same dataset. The purpose is to enhance the accuracy and enhance the flexibility of the algorithm.

Keywords: *Credit card, Fraud detection, Machine learning, Naïve Bayes, Kth nearest neighbor.*

1. INTRODUCTION

Machine learning is the technology which is nothing but the application of AI i.e., an artificial intelligence which gives computer systems the capability to learn and improve from previous cases and past experiences. Machine learning focuses on developing codes or algorithms or computer programs that are capable of accessing and analyzing given data and then later use that analyzed data to learn on their own.

The procedure of learning begins with some observations or previous data, like examples, past experiences, or instructions, in order to find and discover hidden patterns in the dataset and take better decisive actions in the future based on the examples and data that we provide[1]. The ultimate objective of machine learning is to give computers ability to earn automatically i.e., learn by themselves without any unnecessary human assistance and then scrutinize the data and take decisions accordingly.

The utilization of credit card as a mode of payment for online, along with daily purchases has increased in the last few decades[2]. As the area of information technology is developed and still developing to be better over the time and also with the improvement of communication channels, attempts in a credit card for frauds, have been increased worldwide, and because of that most organizations and people are facing huge financial losses.

This kind of illegitimate actions upon credit cards is done in possibly two ways i.e., by getting access to stolen credit cards physically (that is why this method is known as physical fraud) and by exploiting the details of the card without the knowledge of the genuine cardholder (that is why this method is known as virtual fraud) via online transactions[3]. The financial losses due to fraud in credit card worldwide are found to be very high in the past few years. Various methods, techniques, and procedures have been introduced and implemented by so many people so as to provide a solution to prevent credit card fraud[4]. So in this paper, the accuracy of Naïve Bayes and KNN has been calculated i.e., how accurately they are able to find the frauds in given credit card dataset.

The domain of detection of fraud in credit card presents numerous challenging issues, like the number of credit card transactions processed each day are in the order of millions, therefore mining of such gigantic volumes of information data requires some algorithms and techniques with very high accuracy that scale, also the data is skewed on a higher level, i.e., number of transactions done by genuine owner of the credit card is much more than the frauds and each recorded transaction has different amount, time, information and stuff, therefore, it becomes a little difficult to detect the frauds in the recorded credit card dataset[5].

This paper presents the implementation of Naïve Bayes and KNN algorithm on same credit card dataset so as to calculate the precision of algorithms to identify the fraudulent transactions in the dataset[6]. Experimental results depict that both classifiers works differently for the same dataset. The purpose is to enhance the precision, accuracy and increase the flexibility of the algorithm[7].

Bayesian network classifiers are very popular in the area of machine learning and it comes under the category of supervised classification models. Naïve Bayes classifier is also a well-known Bayesian Network that is based on Bayes theorem of conditional probability and hence, is a classifier based on probability which considers Naïve i.e., strong independence assumption[8]. It was formerly introduced with some other name, into the text retrieval community as a baseline technique for categorizing text because there was a problem of deciding in which category does the documents belongs to, with word frequencies as the feature.

The Naïve Bayes machine learning classifier tries to predict a class which is known as outcome class based on probabilities, and also conditional probabilities of how many times it occurred from the training data. This kind of learning is very efficient, fast and high in accuracy for real-world scenarios, and is known as supervised learning. Also, this is highly efficient because it estimates the parameters by using very small training data which is used for classification and is based upon word independence. Though Naïve Bayes is quite simple to implement and understand and uses strong assumptions. It gives pretty accurate results and also it has been proven over and over the time that Naïve Bayes works effectively in various areas related to machine learning.

In Naïve Bayes, the basic concept to computing the probabilities of various categories given a text is performed by using joint probabilities of categories and words.

KNN comes under a very special type of category of machine learning algorithms, known as 'Lazy Learners' because this algorithm learns very slowly as compared to other algorithms. KNN follows a process to learn in which it keeps focusing on saving the information until it is actually having the input data whose label or class is meant to be predicted[9].

KNN classifier predicts that how close the unidentified tuple is to the K^{th} training set, and KNN does this by using some distance measure. With reference to conceptuality, KNN is simple and still capable of solving complex problems as it can work relatively with little information too.

KNN is a technique which is generally used for the classification in addition to regression but it does not use any parameter since it is a non- parametric method. The output of the classification method is most prevalent cluster i.e., class membership. As the neighbors of particular objects give votes, so with the maximum votes of that objects neighbor, the object gets classified i.e., the object is classified to the K^{th} nearest neighbor which is most common to it. This rule just continues and holds the complete training set during the learning stage of the K-Nearest Neighbour algorithm and assigns each and every query through which a particular class is represented by the maximum number of labels of its k-nearest neighbors in the training dataset.
The NN rule i.e., Nearest Neighbour Rule is the most rudimentary form of K-Nearest Neighbour when the K's value is equal to 1.

Given an unknown dataset and its corresponding training sample, all the distances between the instances in the training set and the unknown sample can be calculated. Classification of that unknown sample dataset can be done upon the algorithmic basis of nearest neighbor classification technique as the smallest distance value corresponds to that instance in the training set which is closest to the unknown sample[10].

KNN is very simple, powerful, easy to implement and understand. KNN is powerful since it does not involve any kind of assumptions about the data, other than a distance measure can be calculated consistently between two instances. As such, it is called non-parametric or non-linear since it does not involve a functional form.

2. METHODOLOGY

2.1 Data Analysis

The dataset which has been selected and used holds the records of European cardholders who made transactions using their credit cards in the month of September 2013. This dataset holds the record of transactions that were made within two days and total transactions made within two days are 284,807 transactions from which 492 transactions were found as fraudulent which makes the dataset highly imbalanced, more oriented as the positive class i.e., fraud transactions are 0.172% out of total transactions. And the dataset is in CSV format i.e., in a format where the data values are separated by commas.

As PCA transformation of input values has been done in the dataset which makes the dataset contain only numerical input values. Unfortunately, the source of dataset did not provide the more background information, original features and information due to confidentiality issues.

Principal components that were obtained by PCA transformations are nothing but the numeric values under attributes V1 to V28 and the only feature that were not transformed using the transformation by Principal Component Analysis are the attributes or features 'TIME' and 'AMOUNT'.

'TIME' attribute or feature hold the data that denotes the elapsed time in between the first transaction of the dataset and each transaction. And the attribute or feature 'AMOUNT' hold the data which represents nothing but the amount of the transaction and this feature can also find its use for cost-sensitive and example-dependent machine learning. And finally the attribute or feature 'CLASS' is the response variable and it takes values '1' in the case of fraudulent transaction i.e., positive result and value '0' in the case of the genuine transaction[11].

2.2 Data Cleaning

Data cleaning is also called and known as Data cleansing because in this process the inaccurate and corrupted records from the dataset or a record-set or a table are identified and corrected i.e., removed and also this process focuses on identification of incorrect, irrelevant, inaccurate or incomplete parts of the data and then modification of that particular part by replacing it with some different value or completely deleting the dirty data[12].

In this dataset, the very first row wasn't required for the actual implementation of the algorithms which are used though it helped to analyze the dataset easily because that row is nothing but the attributes of the present data in the dataset and this is the reason why we are performing this step of data cleaning after understanding the dataset in the first step, so in this process of data cleaning or data cleansing, that particular row will be deleted from the dataset.

2.3 Implementing Naïve Bayes

The Naïve Bayes machine learning classifier tries to predict a class which is known as outcome class based on probabilities, and also conditional probabilities of its occurrence from the training data. This kind of learning is very efficient, fast and high in accuracy for real-world scenarios, and also this learning type is known as supervised learning.

The initial step for Naïve Bayes classification algorithm is the Bayes theorem for conditional probability, where 'x' is given data point and 'C' is a class:
$P(C / x) = P(x/C)/P(x)$

And further steps are done by making the assumption for a data point x = {x1 to xj}, and the occurrence probability of each of its attribute within given class is independent. So the probability of x can be computed as follows:

$$P(C/x) = P(C).\mathbf{\Pi}\ P(xi/C)$$

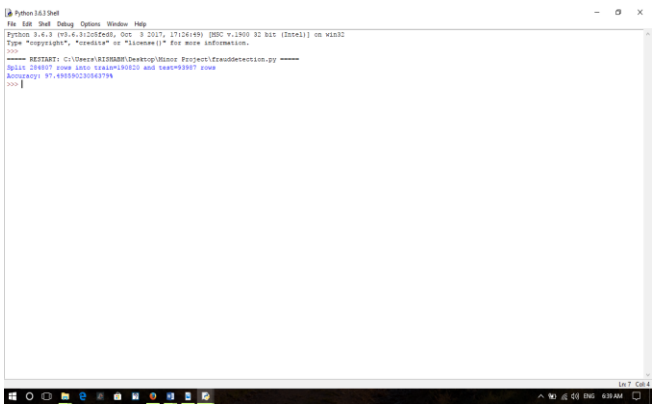

Fig. 1. Naïve Bayes Output

2.4 Implementing Kth-Nearest Neighbor

KNN come under a very special type of category of machine learning algorithms that are known as 'Lazy Learners' because this algorithm learns very slowly than compared to other algorithms.

KNN follows a process to learn in which it keeps focusing on storing the data until it is actually having the input data whose label or class is meant to be predicted. KNN classifier predicts that how close the unidentified tuple is to the K training set, and KNN does this by using some distance measure. In conceptual terms, KNN is simple and still capable of solving complex problems as it can work relatively with little information too.

`

Fig. 2. Kth-Nearest Neighbor Output

3. CONCLUSION

Credit Card Fraud Detection for given data set has been done using Naïve Bayes and KNN individually with the precision of approximately 95% and 90% respectively.

The problem faced:-

- Data Analysis and Data Cleaning is a very hard job to do.
- The algorithm takes a lot of time to iterate over the large data set.
- Optimizing an individual algorithm for doing the whole task is hard.

But Fraud Detection of Credit Card only using one individual algorithm will not be an efficient practice. As every algorithm contain their own advantages and disadvantages and so as to do credit card fraud detection effectively, we will have to combine algorithms so that we would be able to take advantages of each algorithm and get our work done effectively.

4. REFERENCES

[1] [1] N. Thai-Nghe, Z. Gantner, L. Schmidt-Thieme, Cost-sensitive learning methods for imbalanced data, in Proceeding of 2010 International Joint Conference on Neural Networks (IJCNN10), 2010.

[2] Chandel, K., Kunwar, V., Sabitha, S. et al. CSIT (2016) 4: 313. 2017 Springer International Publishing AG. Part of Springer Nature.

[3] Yang, C.C., Soh, C.S. & Yap, V.V. Energy Efficiency (2017). 2017 Springer International Publishing AG. Part of Springer Nature.

[4] Mohd Shamrie Sainin1, a), Rayner Alfred2, b), and Faudziah Ahmad1, c) AIP Conference Proceedings 1761, 020093 (2016); 2016 AIP Conference Proceedings.

[5] P.Cao, D.Zhao, O.Zaiane, An optimized cost-sensitive SVM for imbalanced data learning, in Proceedings of PAKDD2013,2013,pp.280–292.

[6] X.Zhang, Y.Li, Apositive-biased nearest neighbor algorithm for imbalanced classification, in Proceedings of PAKDD 2013, Springer, Berlin, Heidelberg, 2013,pp.293–304.

[7] Balsubramani and Y. Freund, Optimally Combining Classifiers Using Unlabeled Data, JMLR: Workshop and Conference Proceedings, 40, 1–15, (2015).

[8] Abdullah and K. R. Ku-Mahamud, Ant System-Based Feature Set Partitioning Algorithm For K-Nn And Lda Ensembles Construction, in Proceedings of the 5th International Conference on Computing and Informatics, 2015, pp. 326–332 (2015).

[9] Gandhi and M. Pandey, "Hybrid Ensemble of classifiers using voting," in International Conference on Green Computing and Internet of Things (ICGCIoT), 399 – 404 (2015).

[10] S. Sainin and R. Alfred, A Direct Ensemble Classifier for Imbalanced Multiclass Learning, in Data Mining Optimization (DMO2012), 59–66 (2012)

[11] W. Yassin, N. I. Udzir, Z. Muda, and M. N. Sulaiman, Anomaly-Based Intrusion Detection Through Kmeans Clustering And Naives Bayes Classification, in Proceedings of the 4 th International Conference on Computing and Informatics, ICOCI 2013, pp. 298–303 (2013).

[12] Y. Wan and Q. Gao, An Ensemble Sentiment Classification System of Twitter Data for Airline Services Analysis, in 15th International Conference on Data Mining Workshops, pp. 1318–1325 (2015).

