SOFT COMPUTING APPROACH FOR CREDIT CARD FRAUD DETECTION

1 Kushal S, 2Brunda S A, 3Dr. H S Prasantha
1Student, 2Student, 3Professor
Department of Electronics and Communication Engineering
Nitte Meenakshi Institute of Technology, Bangalore, India

Abstract: Financial fraud is an ever-growing menace with far consequences in the financial industry. Data mining has played an imperative role in the detection of credit card fraud in online transactions. Credit card fraud detection, which is a data mining problem, becomes challenging due to two major reasons-first, the profiles of normal and fraudulent behavior change constantly and secondly, credit card fraud data sets are highly skewed. The performance of fraud detection in credit card transactions is greatly affected by the sampling approach on the dataset, selection of variables and detection technique(s) used. This paper investigates the performance of naïve bayes, logistic regression and many others on highly skewed credit card fraud data detection. A hybrid technique of under-sampling and oversampling is carried out on the skewed data. The three techniques are applied on the raw and preprocessed data. The work is implemented in Python. The performance of the techniques is evaluated based on accuracy, sensitivity, specificity, precision. The results show the optimal accuracy for naïve bayes, logistic regression and support vector machine algorithms respectively. The comparative results show that a support vector machine performs better than naive bayes and logistic regression.

Keywords- fraudulent, skewed, sampling approach, under-sampling, oversampling, accuracy, sensitivity, specificity, precision.

1. INTRODUCTION

Machine learning was defined in the 90's by Arthur Samuel described as the,” it is a field of study that gives the ability to the computer for self-learning without being explicitly programmed”, that means imbuing knowledge to machines without hard-coding it.

• It can process massive data faster with the learning algorithm. For instance, it will be interested in learning to complete a task, make accurate predictions, or behave intelligently.

• Why Machine Learning? To develop systems that can automatically adapt and customize themselves to individual users. It can mimic human and replace certain monotonous tasks, which require some intelligence from large data bases (Data mining). We can also implement it on difficult/expensive to construct to manually because they require specific detailed skills and knowledge tuned to a specific task.

CREDIT CARD: Credit cards offer you a line of credit that can be used to make purchases, balance transfers or cash advances and require that you pay back the loan amount in the future.

• When using a credit card, you will need to make at least the minimum payment every month by the due date on the balance.

• What is credit card fraud detection?

It’s a set of activities aimed to save the money and assets being stolen by criminals. There are a lot of traditional methods, which worked perfectly fine for some time.

However now, it is a kind of area where constant improvement is crucial for survival. That’s why it is important to talk about what Machine Learning, a subdivision of Artificial Intelligence, can do here. You need a team of Data Science experts and main information on credit card transactions in your organization, such as Amount, Date, User Location, Usual Behavioral Patterns of your clients, etc. Experts, obtaining that, will be able to develop a model that will be able to prevent and reveal any fraudulent activity among your transactions. This model will be fine-tuned in the process, and there are few ways to make it work, we will talk about it later. Now, let’s move on to the most common scenarios, which ML powered Fraud Detection could handle easily.
Causes of credit card fraud:
- This growth in losses is partially caused by the rise of electronic transactions.
- Fraudulent methods are getting more sophisticated and thus harder to spot by traditional fraud detection methods.

How machine learning helps with fraud detection:
The key objective of any credit card fraud detection system is to identify suspicious events and report them to an analyst while letting normal transactions be automatically processed. But now they increasingly turn to a machine learning approach, as it can bring significant improvements to the process.

- Higher accuracy of fraud detection:
  Compared to rule-based solutions, machine learning tools have higher precision and return more relevant results as they consider multiple additional factors. This is because ML technologies can consider many more data points, including the tiniest details of behavior patterns associated with a particular account.

- Less manual work needed for additional verification:
  Enhanced accuracy leads reduce the burden on analysts. People are unable to check all the transactions manually even in small banks.

- Fewer false declines:
  False declines or false positives happen when a system identifies a legitimate transaction as suspicious and wrongly cancels it. Unsupervised learning techniques may be applied to analyze available data and find patterns of fraudulent behavior.

- Ability to identify new patterns and adapt to changes:
  Unlike rule-based systems, ML algorithms are aligned with a constantly changing environment and financial conditions. They enable analysts to identify new suspicious patterns and create new rules to prevent new types of scams.
2. LITERATURE SURVEY

Literature survey is done for this project and the brief description of some paper is as follows:

STUDY ON SUPPORT VECTOR MACHINE BASED LINEAR AND NON-LINEAR PATTERN CLASSIFICATION:
In this paper concept of SVM along with its various models has been presented. Phenomenon which leads to the concept of SVM back in the 90s’ is mentioned. SVMs are mainly used for classification and regression analysis both for linear and nonlinear decision boundaries.

COMPARATIVE STUDY OF BIG DATA CLASSIFICATION ALGORITHM BASED ON SVM:
The emergence of linear support vector machines algorithm package LIBLINEAR has solved the problem. In fact, LIBLINEAR is originally designed to solve the problem of large amount of data. Using completely different optimization algorithms from LIBSVM, LIBLINEAR greatly reduces training computational complexity and time consumption while maintaining similar effects in linear SVM classification.

SUPPORT VECTOR MACHINE ACCURACY IMPROVEMENT WITH CLASSIFICATION:
The report represents superiority to the presented approach (SVM based on RBF) which delivers extensively enhanced value against the other classifiers. The misclassification value is removed from the final Support Vector Classification. An improved accuracy is obtained after a certain modification on the epsilon and cost parameter in radial basis function. It has been observed in the experiment that the trained SVM gives 98% accuracy.

CLASSIFICATION MECHANISM OF SUPPORT VECTOR MACHINES:
This formulation results in a global quadratic optimization problem with convex constraints, which is readily solved by interior point methods. The kernel mapping provides a unifying framework for most of the commonly employed model architectures.

RESEARCH ON SVM IMPROVED ALGORITHM FOR LARGE DATA CLASSIFICATION:
In view of the two problems of the SVM algorithm in processing large data, the paper proposed a weighted Euclidean distance, radial integral kernel function SVM and dimensionality reduction algorithm for large data packet classification. The improved algorithm reconstructs the data feature space, makes the boundary of different data samples clearer, shortens the modeling time, and improves the accuracy of classification.

IMPROVING CLASSIFICATION ACCURACY USING SVMS WITH NEW KERNEL:
In this paper, they introduce a new kernel function called polynomial radial basis function (PRBF) that could improve the classification accuracy of support vector machines (SVMs). The proposed kernel function combines both Gauss (RBF) and Polynomial (POLY) kernels and is stated in general form. It is shown that the proposed kernel converges faster than the Gauss and Polynomial kernels.

BEHAVIOR BASED CREDIT CARD FRAUD DETECTION USING SUPPORT VECTOR MACHINES:
Along with the great increase of internet and e-commerce, the use of credit card is an unavoidable one. Due to the increase of credit card usage, the frauds associated with this have also increased. There are a lot of approaches used to detect the frauds. In this paper, behavior-based classification approach using Support Vector Machines are employed and efficient feature extraction method also adopted. If any discrepancies occur in the behavior’s transaction pattern, then it is predicted as suspicious and taken for further consideration to find the frauds. Generally, credit card fraud detection problem suffers from a large amount of data, which is rectified by the proposed method. Achieving finest accuracy, high fraud catching rate and low false alarms are the main tasks of this approach.

IMPLEMENTATION OF CREDIT CARD FRAUD DETECTION USING SUPPORT VECTOR MACHINE:
Credit card fraud has without hesitation an expression of criminal deception. Fraud identification seems to be a complicated problem that requires a significant amount of skill until throwing algorithms regarding machine learning into it. However, it is an implementation for both the better of machine learning as well as artificial intelligence, ensuring that perhaps the funds of both the customer seems to be secure and therefore not manipulated. The whole research article addressed an effective system of identifying fraud depending on machine learning methodologies, with such a feedback system. Its feedback process relates to enhancing the classifier's detection rate as well as effectiveness. The state of art approaches failed to detect the frauds through credit card transactions. Thus, to solve these drawbacks, the proposed system is implemented with the Support vector machine (SVM) classification to detect the frauds. The simulation results show that the proposed method gives the better classification accuracy compared to the state of art approaches.
CREDIT CARD FRAUD DETECTION USING WEIGHTED SUPPORT VECTOR MACHINE

Credit card fraudulent data is highly imbalanced, and it has presented an overwhelmingly large portion of nonfraudulent transactions and a small portion of fraudulent transactions. The measures used to judge the veracity of the detection algorithms become critical to the deployment of a model that accurately scores fraudulent transactions taking into account case imbalance, and the cost of identifying a case as genuine when, in fact, the case is a fraudulent transaction. In this paper, a new criterion to judge classification algorithms, which considers the cost of misclassification, is proposed, and several under sampling techniques are compared by this new criterion. At the same time, a weighted support vector machine (SVM) algorithm considering the financial cost of misclassification is introduced, proving to be more practical for credit card fraud detection than traditional methodologies. This weighted SVM uses transaction balances as weights for fraudulent transactions, and a uniformed weight for nonfraudulent transactions. The results show this strategy greatly improve performance of credit card fraud detection.

SELECTION FEATURES AND SUPPORT VECTOR MACHINE FOR CREDIT CARD RISK IDENTIFICATION

For identifying credit card risk in massive and high dimensionality data, feature selection is considered very important to improve classification performance and fraud identification process. One of the commonly used feature selection methods is Random Forest Classifier (RFC), which is very suitable for large dataset. RFC has a good performance; it tends to identify the most predictive features, which may provide a significant improvement in classification performance of credit card risk identification model. In this paper, we propose an enhanced Credit Card Risk Identification (CCRI) method based on the features selection algorithm as Random Forest Classifier and Support Vector Machine to detecting fraud risk. Our experimental results show that the proposed algorithm outperforms the Local Outlier Factor, Isolation Forest and Decision Tree in term of classification performance on a larger dataset.

METHODOLOGY

- Feature engineering to transform historical data into feature and label inputs for a machine learning algorithm.
- Split the data into two parts, one for building the model and one for testing the model.
- Build the model with the training features and labels.
- Test the model with the test features to get predictions. Compare the test predictions to the test labels.
- Loop until satisfied with the model accuracy:
  - Adjust the model fitting parameters, and repeat tests.
  - Adjust the features and/or machine learning algorithm and repeat tests.

Algorithms used for Credit Card Fraud Detection:

1. Naive Bayes.
2. Logistic regression.

1. **Naive Bayes**: Naive Bayes is one of the most popular and simple machine learning classification algorithms, in Naive Bayes algorithm the classification technique based on Bayes Theorem with an assumption of independence among predictors. In simple terms, the classifier assumes that the presence of a particular feature in a class is unrelated to the presence of any other feature. It’s easy to build and particularly useful for large data sets, hence its known to outperform even highly sophisticated classification models and can be implemented easily.

Using Probabilistic Model: When we try to calculate probability on a condition, i.e., probability of happening of event A when event B has already taken place.

\[
P(c/x) = \frac{P(x/c) \cdot P(c)}{P(x)}
\]

\[
P(c) = P(x1/c) \cdot P(x2/c) \cdot \ldots \cdot P(xn/c) \cdot P(c)/P(x)
\]
• Likelihood: Indicates how probable is the evidence given that our hypothesis is true.
• Posterior Probability: Indicates how probable is our hypothesis given from the observed evidence (Not directly Computable).
• Predictor Prior Probability: Indicates how probable is the new evidence under all possible hypotheses.
• Class Prior Probability: Indicates how probable our Hypotheses are before observing the evidence.

Steps to implement Naive Bayes Algorithm:
Step 1: Handling the data and summarizing. It can even involve converting the table into frequency.
Step 2: Making predictions and creating likelihood to evaluate accuracy.
Step 3: Trying all together and to calculate the posterior probability of each class. The class with the highest prediction is considered for the ideal output.

Applications of Naive Bayes Algorithms:
1. Text classification/ Spam Filtering/ Sentiment Analysis
Recommendation System: Naive Bayes Classifier uses machine learning and data mining techniques to filter unseen information and predict whether a user would like a given resource or not.

2. Logistic Regression: Logistic regression is a supervised learning classification algorithm used to predict the probability of a target variable. The nature of target or dependent variable is dichotomous, which means there would be only two possible classes. In simple words, the dependent variable is binary in nature having data coded as either 1 (stands for success/yes) or 0 (stands for failure/no). Mathematically, a logistic regression model predicts \( P(Y=1) \) as a function of \( X \). It is one of the simplest ML algorithms that can be used for various classification problems such as spam detection, Diabetes prediction, cancer detection etc

Figure 4 : Linear regression graph

Types of Logical Regression:
• Binary or Binomial: In such a kind of classification, a dependent variable will have only two possible types either 1 and 0. For example, these variables may represent successor failure, yes or no, win or loss etc.
• Multinomial: In such a kind of classification, dependent variables can have 3 or more possible unordered types or the types having no quantitative significance. For example, these variables may represent “Type A” or “Type B” or “Type C”.
• Ordinal: In such a kind of classification, dependent variables can have 3 or more possible ordered types or the types having a quantitative significance. For example, these variables may represent “poor” or “good”, “very good”, “Excellent” and each category can have the scores like 0,1,2,3. In the Credit Card Fraud Detection project, we use Binary Type of Logical Regression

Sigmoid Function: Logistic Regression uses a more complex cost function also known as Sigmoid Function. Hypothesis of logistic regression tends to limit the cost function instead of a linear function. The hypothesis of logistic regression tends to limit the cost function between 0 and 1. Therefore linear functions fail to represent it as it can have a value greater than 1 or less than 0 which is not possible as per the hypothesis of logistic regression
**Sigmoid function**

\[ f(x) = \frac{1}{1 + e^{-x}} \]

**Steps To implement Logistic Regression:**

To implement the Logistic Regression, we will use the same steps as we have done in previous topics of Regression.

- **Step 1:** Data Preprocessing. We will prepare the data so that we can use it in our code.
- **Step 2:** Fitting Logistic Regression to the Training set.
- **Step 3:** Predicting the test result.
- **Step 4:** Test accuracy of the result (Creation of Confusion matrix) and the verification process is done at this step.

**Application of Logistic Regression:**

1. **Sentiment Analysis:** Analyzing the sentiment using the review or tweets is the objective of this use case. Most of the brands and companies use this to increase customer experience.
2. **Image segmentation, recognition and classification:** The objective of all these use cases is to identify the object in the image and classify it.
3. **Support Vector Machine Algorithm:** Support Vector Machine (SVM) is a supervised machine learning algorithm used for both classification and regression and it is particularly applicable for small and medium sized datasets. Support Vector Machine or SVM is one of the most popular Supervised Learning algorithms, which is used for Classification as well as Regression problems. However, primarily, it is used for Classification problems in Machine Learning. The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in future.

**Figure 6 : Block diagram of SVM**

This best decision boundary is called a hyperplane. SVM chooses the extreme points/vectors that help in creating the hyperplane. These extreme cases are called support vectors, and hence the algorithm is termed as Support Vector Machine. Consider the below diagram in which there are two different categories that are classified using a decision boundary or hyperplane.
Types of SVM:
1. **Linear SVM**: Linear SVM is used for linearly separable data, which means if a dataset can be classified into two classes by using a single straight line, then such data is termed as linearly separable data, and classifier is used called as Linear SVM classifier.
2. **Non-linear SVM**: Non-Linear SVM is used for non-linearly separated data, which means if a dataset cannot be classified by using a straight line, then such data is termed as non-linear data and classifier used is called as Non-linear SVM classifier.

**Hyperplane and Support Vectors in the SVM algorithm:**

**Hyperplane**: There can be multiple lines/decision boundaries to segregate the classes in n-dimensional space, but we need to find out the best decision boundary that helps to classify the data points. This best boundary is known as the hyperplane of SVM. The dimensions of the hyperplane depend on the features present in the dataset, which means if there are 2 features (as shown in image), then the hyperplane will be a straight line. And if there are 3 features, then the hyperplane will be a 2- dimension plane. We always create a hyperplane that has a maximum margin, which means the maximum distance between the data points.

**Support Vectors**: The data points or vectors that are the closest to the hyperplane and which affect the position of the hyperplane are termed as Support Vector. These vectors support the hyperplane, hence called a Support vector.

**Applications of Support Vector Machine Algorithm:**
1. Handwriting analysis.
2. Protein fold and remote homology detection.

**Steps to implement support vector machine algorithm:**
Step 1: Collect a training set.
Step 2: Choose a kernel and its parameters as well as any regularization needed.
Step 3: Extract from the correlation matrix.
Step 4: Train your machine exactly or approximately to get contraction coefficients.
Step 5: Use the coefficients to create your estimator.

### 3. IMPLEMENTATION

In this project we have used Python as programming language for implementation of credit card fraud detection project. For python we have used Jupyter notebook as python tool which is used to run various code, to visualize data, for computational data where this tool uses python as programming language. Also using python in jupyter notebook we have imported many inbuilt python libraries for analysis, visualization, for using higher complex mathematical functions etc.

In this project dataset used for credit card fraud detection is :

- The dataset contains transactions made by credit cards in September 2013 by European cardholders.
- This dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced, the positive class (frauds) account for 0.172% of all transactions.
- It contains only numerical input variables which are the result of a PCA transformation. Unfortunately, due to confidentiality issues, we cannot provide the original features and more background information about the data.
- Features V1, V2, … V28 are the principal components obtained with PCA, the only features which have not been transformed with PCA are ’Time’ and ’Amount’.
- Feature ’Time’ contains the seconds elapsed between each transaction and the first transaction in the dataset.
- The feature ’Amount’ is the transaction Amount, this feature can be used for example-dependent cost-sensitive learning.
- Feature ’Class’ is the response variable and it takes value 1 in case of fraud and 0 otherwise.
Credit card fraud detection is a classification problem. Target variable values of Classification problems have integer(0,1) or categorical values (fraud, non-fraud). The target variable of our dataset ‘Class’ has only two labels - 0 (non-fraudulent) and 1 (fraudulent).

The comparison parameters used are performance metrics
- **Metrics** are measures of quantitative assessment commonly used for assessing, comparing, and tracking performance or production.
- It can also be **defined** as the number of correct predictions made as a ratio of all predictions made.

**Types of Classification Metrics used:**
- **Accuracy**: It is defined as Number of correct predictions to the Total number of predictions.

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

- **Precision**: Precision tells us how many of the correctly predicted cases actually turned out to be positive. Precision is a useful metric in cases where False Positive is a higher concern than False Negatives.

\[
\text{Precision} = \frac{TP}{TP + FP}
\]

- **Recall**: Recall tells us how many of the actual positive cases we were able to predict correctly with our model. Recall is a useful metric in cases where False Negative trumps False Positive.

\[
\text{Recall} = \frac{TP}{TP + FN}
\]

- **F1-score**: F1-score is a harmonic mean of Precision and Recall, and so it gives a combined idea about these two metrics. It is maximum when Precision is equal to Recall. In practice, when we try to increase the precision of our model, the recall goes down, and vice-versa. The F1-score captures both the trends in a single value. But there is a limitation here. The interpretability of the F1-score is poor. This means that we don’t know what our classifier is maximizing – precision or recall? So, we use it in combination with other evaluation metrics which gives us a complete picture of the result.

\[
\text{F1 score} = \frac{2 \cdot \text{Recall} \cdot \text{Precision}}{\text{Recall} + \text{Precision}}
\]

- **AUC-ROC**: The Receiver Operator Characteristic (ROC) curve is an evaluation metric for binary classification problems. It is a probability curve that plots the TPR against FPR at various threshold values and essentially separates the ‘signal’ from the ‘noise’. The Area Under the Curve (AUC) is the measure of the ability of a classifier to distinguish between classes and is used as a summary of the ROC curve.

The higher the AUC, the better the performance of the model at distinguishing between the positive and negative classes.

**Confusion matrix**: A Confusion matrix is an N x N matrix used for evaluating the performance of a classification model, where N is the number of target classes. The matrix compares the actual target values with those predicted by the machine learning model. This gives us a holistic view of how well our classification model is performing and what kinds of errors it is making.

For a binary classification problem, we would have a 2 x 2 matrix as shown below with 4 values:
- The target variable has two values: Positive or Negative
- The columns represent the actual values of the target variable
- The rows represent the predicted values of the target variable

![2x2 Confusion matrix](image)
4. RESULT AND OUTPUT GRAPH

Figure 9: ROC curve of Naïve bayes

Figure 10: Logistic Regression Degree 2

Figure 12: Support Vector Machine
Table 1 : Comparison of results of different classification algorithm

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>F1 score</th>
<th>AUC-ROC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naïve Bayes</td>
<td>99.30</td>
<td>84.10</td>
<td>66.10</td>
<td>23.25</td>
<td>82.76</td>
</tr>
<tr>
<td>Logistic Regression</td>
<td>99.21</td>
<td>86.31</td>
<td>60.29</td>
<td>70.99</td>
<td>92.46</td>
</tr>
<tr>
<td>Support Vector Machine</td>
<td>99.92</td>
<td>85.56</td>
<td>61.09</td>
<td>64.80</td>
<td>97.18</td>
</tr>
</tbody>
</table>

5. CONCLUSION

By seeing the results, we can clearly conclude that Support Vector Machine (SVM) is the best performing algorithm over Logistic regression & Naïve Bayes. So, we can use SVM in production environment to predict whether the transaction is fraud or not.
REFERENCES