Unsupervised vs. Supervised Learning on Credit Card Fraud Detection

CS256 Spring 2020 Project Proposal

Yan Chen

I. Introduction

As people use credit cards in various daily activities, fraud transactions will cost huge money loss for customers. So, it is important to be able to recognize fraudulent credit card transactions accurately, that is, both in low false positive rate and low false negative rate. The project aims to identify whether a credit card transaction is fraudulent by modeling past transactions. The data will be from Kaggle [1]. In this project, both unsupervised learning algorithm, Local Outlier Factor (LOF) and supervised learning algorithm, Support Vector Machine (SVM) will be performed for the anomaly detection, and the result will be compared in terms of accuracy, precision, recall, f1-score, and time to train.

II. Related Work

M. Mahajan and S. Sharma [2] listed various techniques to detect the credit card fraud. According to their research, common approaches include Hidden Markov Model, K-means, k-nn, Decision Tree, Bayesian Network, SVM and Logistic Regression. But they only cataloged the methods without comparing the result.

Both V. Ceronmani Sharmila et al. [3] as well as H. John and S. Naaz [4] used LOF and Isolation Forest Algorithm (IFA) (both are unsupervised) to detect credit card fraud. John and S. Naaz [4] claimed LOF is better comparing with IFA with the accuracy of 97% for detecting the fraud, while V. Ceronmani Sharmila et al. [3] didn't state clearly the result in terms of accuracy nor which one did a better job.

In addition to LOF and IFA, P. Kumar and F. Iqbal [5] also used SVM, which is supervised. Different from [4], Kumar and F. Iqba claimed IFA performed better than the LOF Isolation Forest. According to ther research, IFA has detected 73 errors while Local Outlier Factor has detected 97 errors along with SVM detecting 8516 errors. Isolation Forest features a 99.74% additional correct than LOF of 99.65% and SVM of 70.09.

III. Objective and Approach

Previous works showed that both LOF and SVM can be effective ways to detect credit card fraud. But the comparison between those techniques was not clear. Therefore, this project will not only use those algorithms to identify the credit fraud but also compare the result in terms of accuracy, precision, recall, f1-score and time to train. This project will use scikit-learn [6, 7, 8] library from Python for both training and accuracy. Fig. 1 shows the architecture diagram.

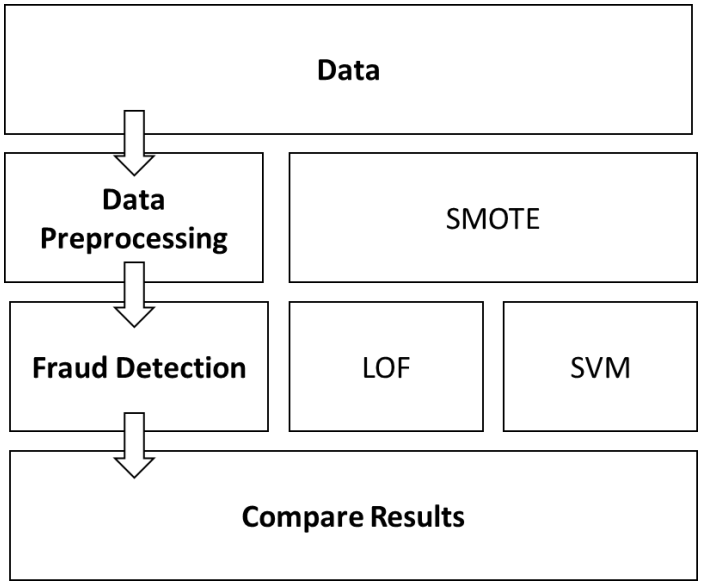

Fig. 1 Architecture diagram

IV. Data and Implementation

The dataset is from Kaggle [1], which in CSV format. The data was transformed to numerical inputs by Principal component analysis (PCA) with 28 features. Each data point is labeled 1 for fraudulent transactions, 0 otherwise. The fraud can be seen as anomaly behavior so unsupervised learning for anomaly detection can be applied. And since the data are labeled, supervised learning can also be applied.

A. Data Processing

The data does not contain any null values, but it contains duplicates. In this case since the duplicates do not provide any additional information but would take more space and time to train, they will be removed.

The original features are hidden due to confidentiality issues except for 'Time' and 'Amount', and these two features are not transformed by PCA as other features. Therefore, the data under 'Time' and 'Amount' need to be scaled so that none of the feature will weigh in a lot more in the distance calculations used to build the models.

The more important part of data processing is to balance the data since the dataset only contains 0.172% fraud cases, which means it is very unbalanced. The basic methods to solve this problem are undersampling and oversampling. Undersampling means randomly removing data from majority class (in this case, normal transactions) while oversampling means randomly duplicating data from minority class (in this case, fraud transactions). Since the gap between the two classes in this data set is too large, neigh. neither of these 2 ways can apply in this situation. In this project, both undersampling and oversampling techniques will be combined. For oversampling, SMOTE [9] will be used, which creates synthetical example of Minority data instead of duplicating them.

B. Local Outlier Factor (LOF)

LOF is an unsupervised learning used to find the anomalous data by measuring the local density of a given dataset with respect to its neighbors [6]. Locality is given by nearest neighbors and density is calculated by their distance. A data point is considered as an outlier if it has very small density as compared to its neighbors. And the outliers should be possible credit card fraud. The parameter for this algorithm is the number of neighbors considered and, in this project, 20 will be used for this parameter. Theoretically, it works well even with the unbalancing data since it only focusses on local density.

C. Support Vector Machine (SVM)

SVM is a supervised learning used for binary classification [7]. Since the data are labeled, SVM can be used to classify valid and fraud transaction. The data are first separated into two classes based on a separating hyperplane which maximizes the margin between the two classes. SVM is effective in high dimensional spaces since more space available means a higher chance of finding a separating hyperplane. Then to obtain better separation, the data is transformed by a kernel function. In this project, different kernel functions will be used, and the result will be compared.

References

[1] "Credit Card Fraud Detection," Kaggle, [Online]. Available: https://www.kaggle.com/mlg-ulb/creditcardfraud.

[2] M. Mahajan and S. Sharma, "Detect Frauds in Credit Card using Data Mining," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 2, pp. 4891-4895, 2019.

[3] V. Ceronmani Sharmila, R. Kiran Kumar, R. Sundaram, D. Samyuktha and R. Harish, "Credit Card Fraud Detection Using Anomaly Techniques," in *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*, Piscataway, NJ, USA, 2019.

[4] H. John and S. Naaz, "Credit Card Fraud Detection using Local Outlier Factor and Isolation Forest," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 4, pp. 1060-1064, 2019.

[5] P. Kumar and F. Iqbal, "Credit Card Fraud Identification Using Machine Learning Approaches," in *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*, Piscataway, NJ, USA, 2019.

[6] "sklearn.neighbors.LocalOutlierFacto," scikit-learn, [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.neighbors.LocalOutlierFactor.html.

[7] "sklearn.svm.SVC," scikit-learn, [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.svm.SVC.html.

[8] "sklearn.metrics.precision_recall_curve," scikit-learn, [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.metrics.precision_recall_curve.html.

[9] "imblearn.over_sampling.SMOTE," imbalanced-learn, [Online]. Available: https://imbalanced-learn.readthedocs.io/en/stable/generated/imblearn.over_sampling.SMOTE.html.