International Journal of Computer Architecture and Mobility (ISSN 2319-9229)
Volume 7 -Issue 3, March 2019

A Comparison Study of Various Credit Card Fraud Detection System

1st Himank Pathak
Computer Science and Engineering
SVIIT, SVVV
Indore, India
himankpathak@gmail.com

2nd Shivank Awasthi
Computer Science and Engineering
SVIIT, SVVV
Indore, India
shivankawasthi8889@gmail.com

3rd Jayant Devda
Computer Science and Engineering
SVIIT, SVVV
Indore, India
devdajayant@gmail.com

***Abstract*—Credit cards are a popular mode of payment for both online and offline purchases, which leads to increasing daily fraud transactions. There is an essential need to maintain the reliability of the payment system by using efficient fraud detection methodologies. Automated fraud behaviours detection on electronic payment platforms is a tough problem. There are many challenges for fraud detection in practice. Traditional fraud detection methods require a large-scale manually labelled dataset, which is hard to obtain in reality. Manually labelled data cost tremendous human efforts. The continuous and rapid evolution of technology and fraud users had made it harder to find new fraud patterns based on existing traditional detection rules. In this study, we perform a comparison study of credit card fraud detection by using Autoencoder Neural Network which uses the traditional autoencoder with an oversampling algorithm to provide minority class classification and Multi-perspective HMM-based feature engineering which combines its three prospective of credit card fraud with an Hidden Markov Model to provide a temporal correlation model and improve the overall effectiveness of the fraud detection process.**

***Index Terms*—fraud, detection, credit, card, machine, learning**

I. Introduction

In this era of technical evolution, the explosion of efficient potential resources and new opportunities for organization have emerged, but at the same time threats to the economy has also risen. Different from traditional cash/cheque payments, digital transactions are ensured by a third-party digital payment platform. The security of the third-party is also a major concern. The digital payment platform brings huge convenience in people's daily life, but it is also vulnerable to cybercrime attacks [1] [2]. Credit card is a very popular mode of payment online, because of its ease of use. Credit card fraud is a growing threat with far-reaching consequences in the finance industry, corporations and government. Fraud can be defined as a criminal deception with the intent of acquiring financial gain. The main reasons for fraud are due to the lack of security, which involves the use of a stolen credit card to get cash from the bank through legitimate access. This results in high difficulty of preventing credit card fraud.

So fraud detection is very significant. A lot of researchers have been proposed that detection of such credit card fraud, which account for the majority of credit card frauds. Detecting using traditional method is infeasible because of the large volume of data is generated each and every day. However, financial institutions have focused their attention on the latest computational methodologies to handle credit card fraud problems.

The classification problem is one of the key research topics in the field of machine learning. Classification methods which are currently available can only achieve preferable performance on balanced datasets. However, there are a large number of imbalanced datasets in practical application. For the fraud problem, the minority class, which is the abnormal transaction, is more important [3]. For instance, when a minority class accounts for less than 1% of the total dataset, the overall accuracy reaches more than 99% even though all the minority class has been misclassified.

This paper seeks to analyze credit card fraud detection using denoising autoencoder and oversampling and using HMM-based features to prevent credit card fraud and more generally for anomaly detection.

II. Credit Card Fraud Detection Using Autoencoder Neural Network

The process of identifying those transactions that belong to a fraud or not, which is based on the behaviors and habits of cardholder is accomplished with the help of data mining techniques such as artificial neural network [4], genetic algorithm, support vector machine, frequent itemset mining, decision tree, migrating birds optimization algorithm, Naïve Bayes. Two major data mining approaches being used majorly in classification problems are support vector machines(SVM) and random forests, together with logistic regression, as part of an attempt to better detect credit card fraud than the current use of neural network and logistic regression in credit card fraud detection problem.

A. Autoencoder

Auto-encoder is a programmatically designed neural network used for unsupervised learning. The aim of autoencoder is to learn representations of recurring features for a set of data, typically for the purpose of dimensionality reduction. The simplest autoencoder is a feedforward, non-recurrent neural network which is similar to the multilayer perceptron [5]. As depicted in figure 1, it has 2 parts: one is encoder and the

other is decoder which are consists of an input layer, one or more hidden layers and an output layer. The key feature of an autoencoder which differs from the multi-layered perceptron is that the output layer of autoencoder has the same number of neurons as the input layer. The purpose is to reconstruct its own inputs instead of predicting the target value from the given inputs as a multi-layered perceptron would.

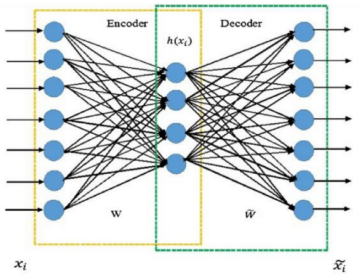

Fig. 1. Architecture of autoencoder neural network

In autoencoder, the network structure has inter-connected layers but has no connection inside each layer, xi s input sample, x'i is output feature. The training of the autoencoder neural network is to optimize reconstruction error using the given samples. The cost function of the autoencoder neural network defined in the project is (1)

$$JAE = 1m\Sigma(12||x'i - xi||2)m) \tag{1}$$

where m represents a number of input samples.

There is a variation of traditional autoencoder named denoising autoencoder which could make autoencoder neural network learn how to remove the noise and reconstruct undisturbed input as much as possible [6]. Figure 2 shows a denoising autoencoder which takes the original data x, and x' is the data corrupted with noise as input and performs the process of denoising autoencoder to give the output x'.

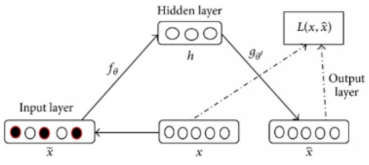

Fig. 2. Denoising autoencoder neural network

The loss function tries to minimize the difference between the output and the original data so that the autoencoder has the ability to eliminate the influence of noise and extracting features from the corrupted data. Hense the generated features from the learning of input corrupted with noise are more robust, which improved the data generalization ability of the autoencoder neural network model to input data. The cost function of the denoising autoencoder neural network is defined according to (2)

$$JDA, E = 1m\Sigma(12||x'i - xi||2)m \tag{2}$$

where

$$x' = f(\Sigma(wx' + b)) \tag{3}$$

w represents weights and b represents bias.

B. Oversampling

The imbalanced dataset is a common problem faced in machine learning since most traditional machine learning classification model can't handle imbalanced dataset. High misclassification cost often happened on minority class, because classification model will try to classify all the data sample to the majority class. Oversampling is a technique used to deal with an imbalanced dataset, its subject to create a specific class sample so the class distribution of the original dataset can be balanced. The benefit of using oversampling is shown in figure 3.

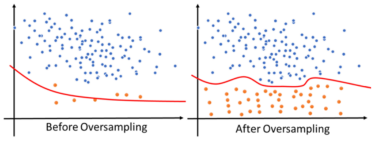

Fig. 3. Benefit of using oversampling

C. Classification fully connected model

The most common model used in classification problems is a Deep fully connected neural network with SoftMax cross-entropy function as its loss function which yields high accuracy. The SoftMax function is often used in the final layer of a neural network-based classifier, it first calculates the exponential value of each output, then normalize all the output and let the sum of the output equal to 1. The SoftMax function is often used for probability distribution transformation, since the output of SoftMax function is within range 0 to 1 that add up to 1, shown in the formula (3),

$$P(yi|xi; w) = efyi\Sigma efj \tag{4}$$

Often cross-entropy of classes is calculated and used with SoftMax function in order to increase the information being provided to the model. Entropy is a measure for information contents and could be defined as the unpredictability of an event. So, the greater the probability is, the smaller the unpredictability is, which means the information contents is also very small. If an event occurs inevitably with the probability of 100%, then the unpredictability and information content are 0. cross-entropy loss function takes advantages of feature of entropy equation, cross-entropy loss function can measure the goodness of a classification model, which is shown in formula (4),

$$J(\Theta) = -1m\Sigma\Sigma 1yloge\Theta Txi\Sigma e\Theta j \tag{5}$$

Considering the order option such as quadratic loss function cross-entropy loss function provides a better learning performance of the neural network

D. The Process

The idea is very straight forward. First, use oversampling to transform imbalanced dataset to balanced dataset. Then use denoised autoencoder to get a denoised dataset. Finally using deep fully connected neural network model for final classification.

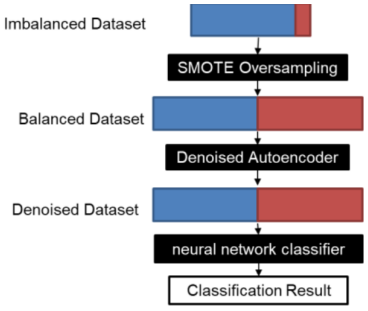

Fig. 4. Flowchart of the process

III. Multi-perspective HMM-based feature engineering

The state of the art engineering techniques for credit card fraud detection creates descriptive features. This is accomplished using the history of the cardholder (such as "money spent by a cardholder in shops in a given country in the last 24h" [7] [8]. These descriptive features present several limits that this model aims to overcome. First, they do not take the history of the seller into account even if it is clearly identified in most credit card transactions dataset. Moreover, these descriptive features don't consider dependencies between transactions of the same sequence. Therefore Hidden Markov Models is used which are generative probabilistic models and a common choice for sequence modelling [9]. Finally, the choice of the descriptive feature created using the transaction aggregation strategy [7] [8] is guided by expert knowledge. In order not to depend on expert knowledge, automated feature engineering in a supervised context is favoured.

A. Sequence Classification

Sequence classification is one of the main machine learning research fields. It considers the sequential properties of the data at the algorithmic level in order to improve the classification of sequential data. Dietterich (2002) reviewed sequential classification based on sliding windows/recurrent sliding windows [10]. However, sliding windows methods don't take into account the inner dependencies between consecutive events.

Srivastava et al. (2008) tried to overcome this limitation by using generative ML models such as Hidden Markov Models (HMMs) for fraud detection [11]. For this purpose, they created an artificial credit card transactions dataset. In their multinomial HMMs, the transactions were denoted with a symbol ('big amount', 'medium amount', 'small amount') used as the observed variable. After training, the likelihood of the sequence of recent transactions is generated by the HMMs. The decision is taken by comparing the likelihood to a threshold value.

B. Modeling of HMM

The sequence of transactions from the combinations of three binary perspectives (genuine/fraudulent, cardholder/merchant, amount/timing) is modelled and therefore learn eight different HMMs. In the end, the set of 8 HMM-based features will provide information about the fraudulence and the genuineness of both terminal and cardholder histories. In particular, we have to select three perspectives for modelling a sequence of transactions. A sequence (i) can be made only of genuine historical transactions or can include at least one fraudulent transaction in the history, sequence (ii) can come from a fixed cardholder or from a fixed terminal, and sequence (iii) can consist of amount values or of time-delta values (i.e. the difference in time between the current transaction and the previous one). We optimized the parameters of eight HMMs using all eight possible combinations (i-iii).

To learn the HMM parameters on observed data, 4 datasets are created:

- sequences of transactions from genuine credit cards (without fraudulent transactions in their history)
- sequences of transactions from compromised credit cards (with at least one fraudulent transaction)
- sequences of transactions from genuine terminals (without fraudulent transactions in their history)
- sequences of transactions from compromised terminals (with at least one fraudulent transaction)

We then extract from these sequences of transactions the symbols that will be the observed variable for the HMMs. In our experiments, the observed variable can be either:

- the amount of a transaction
- the amount of time elapsed between two consecutive transactions of a card-holder (time-delta)

The HMM models are trained on the data until the convergence of the graphical model to the observed data. The convergence can be monitored by observing the increase of the value of the likelihood that the set of observed sequences has been generated by the model. This likelihood increases over each iteration until it reaches a ceiling when the hyperparameters ruling the architecture of the generative model don't allow it to fit more to the set of observed sequences.

At the end, we obtain 8 trained HMMs which are modeling 4 types of behaviour (genuine terminal behaviour, fraudulent terminal behaviour, genuine cardholder behaviour and fraudulent card-holder behaviour) for both observed variables (amount and time-delta).

IV. Conclusion

This paper tries to provide a comparative study between the two techniques that are being used in credit card fraud detection. The first being Credit Card Fraud Detection Using Autoencoder Neural Network provides a key framework of using an autoencoder with an oversampling algorithm to

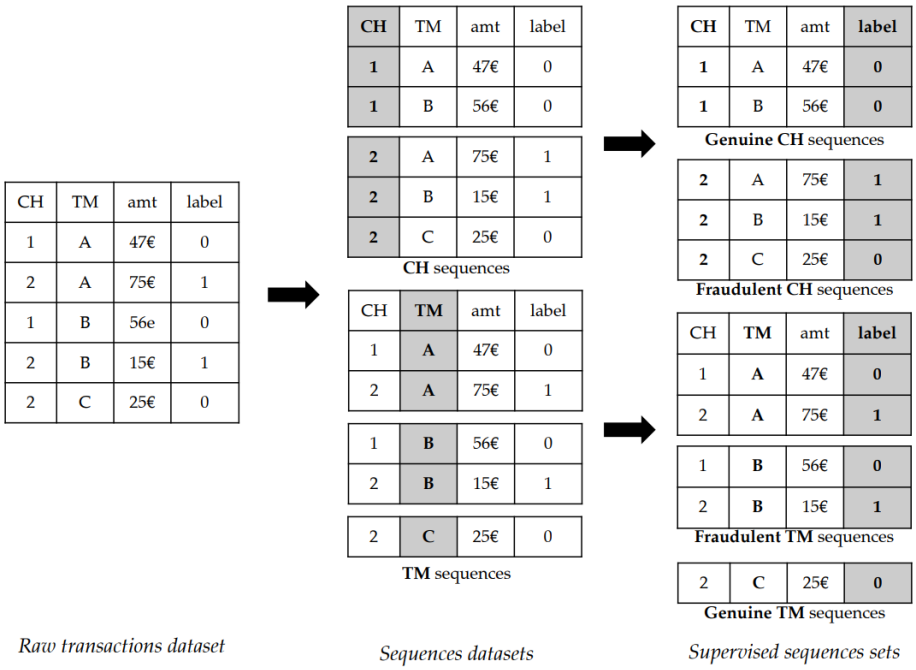

Fig. 5. Supervised selection of sequences for the training sets of the multiple perspectives Hidden Markov Models (CH=Cardholder, TM=Terminal)

increase the accuracy rate of a fraud transaction. It deals with the major problem of the fraudulent transaction being dynamic profile that is fraudulent transactions tend to look like legitimate ones by oversampling the model. The goal of using an autoencoder with an oversampling algorithm is to build a model that can achieve a minority class sampling. The accuracy of such a model can be controlled by controlling the threshold.

The multi-perspective property of the HMM-based feature engineering strategy gives us the best possibility to incorporate sequential information in a broader spectrum. In fact, the genuine and fraudulent behaviors of the merchants and the card-holders are modeled according to two features: the timing and the amount of the transactions. Also, the HMM-based features are created in a supervised way and therefore they lower the need for expert knowledge for the creation of the fraud detection system. HMM-based feature engineering is a powerful tool that is shown to present interesting properties for credit card fraud detection. We can definitely imagine building similar HMM-based features in any supervised task that involves a sequential dataset.

REFERENCES

[1] Jarrod West and Maumita Bhattacharya. 2016. Intelligent financial fraud detection: a comprehensive review, Computers & Security 57 (2016), 47–66.

[2] Yuanshun Yao, Bimal Viswanath, Jenna Cryan, Haitao Zheng, and Ben Y Zhao. 2017. Automated crowdturfing attacks and defenses in online review systems. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). ACM, 1143–1158.

[3] Y. Sahin, S. Bulkan, and E. Duman, "A cost-sensitive decision tree approach for fraud detection," Expert Systems with Applications,vol. 40, pp. 5916-5923, 2013.

[4] Ogwueleka, F. N., (2011). Data Mining Application in Credit Card Fraud Detection System, Journal of Engineering Science and Technology, Vol. 6, No. 3, pp. 311 – 322.

[5] Autoencoder for Words, Liou, C.-Y., Cheng, C.-W., Liou, J.-W., and Liou, D.-R., Neurocomputing, Volume 139, 84–96 (2014), doi:10.1016/j.neucom.2013.09.055.

[6] M. Koziarski and M. Woźniak, "CCR: A combined cleaning and resampling algorithm for imbalanced data classification", International Journal of Applied Mathematics and Computer Science, vol. 27, no. 4, 2017.

[7] Whitrow, C., Hand, D.J., Juszczak, P., Weston, D.J., Adams, N.M., 2008. Transaction aggregation strategy for credit card fraud detection. Data Mining and Knowledge Discovery 18(1).

[8] Bahnsen, A.C., Aouada, D., Stojanovic, A., Ottersten, B., 2016. Feature engineering strategies for credit card fraud detection. Expert Systems With Applications.

[9] Rabiner, L.R., Juang, B.H., 1991. Hidden markov models for speech recognition. Technometrics.

[10] Dietterich, T., 2002. Machine learning for sequential data: A review. Structural, syntactic, and statistical pattern recognition.

[11] Srivastava, A., Kundu, A., Sural, S., Majundar, A.K., 2008. Credit card fraud detection using hidden markov model. IEEE Transactions on dependable and secure computing.