DEEP NEURAL NETWORK DRIVEN INTELLIGENT METHOD FOR CREDIT CARD FRAUD DETECTION

Agnalin V

Student of Department of Computer Science and Engineering, Bethlahem Institute of Engineering, Karungal

.

ABSTRACT

Fraud detection in credit cards is one of the best test beds in computational intelligence algorithms. As fraudsters are increasing day by day and fallacious transactions are done credit cards, the safeguarding of credit card is an important application for prediction techniques. Fraud detection problem that realistically describes the operating conditions of fraud detection system (FDSs) that everyday analyze massive stream of credit card transaction. Several learning algorithm have been proposed for fraud detection, which are based on certain assumptions that hardly hold in real world Fraud detection system. In this work, a fraud detection problem that realistically describes the operating conditions of FDSs that everyday analyze the massive stream of credit card transactions is presented. Also, a learning strategy based on Deep Neural Network is proposed, that effectively addresses class imbalance, concept drift and verification latency. In addition to, the proposed makes use of four important steps such as, 1) Payment Request terminal, 2) Request based feature extraction, 3) Feature augmentation, 4) Deep Neural Network. Finally, the experimentation is performed with benchmark dataset and the results prove that the proposed method attained the accuracy of 90% which is higher when compared with the existing neural network

Keywords:- Data mining, Classification, Deep neural network, Fraud detection, Credit card.

1. INTRODUCTION

Data mining is the process of discovering patterns in large datasets involving methods at the intersection of machine learning, statistics and database systems [4]. Data mining is an interdisciplinary subfield of computer science and statistics with an overall goal to extract information (with intelligent methods) from the dataset and transform it into a comprehensive structure for further use. Data mining technique is one notable methods used in solving credit fraud detection problem. Classification of transactions done by credit cards is mostly a binary classification problem [2, 4]. Here, credit card transaction is either a legitimate transaction (negative class) or a fraudulent transaction (positive class). Fraud detection is generally viewed as a data mining classification problem, where the objective is to correctly classify the credit card transactions as legitimate or fraudulent. Fraud detection [6, 2] is a highly complex function to be performed where, there is hardly any system which can guarantee a 100% satisfaction result rate. All the existing methods can likely predict fraud transactions and not assure you about the results. The properties of good fraud detection method are: a) It must be able to identify the frauds accurately, b) It must quickly detect fraud cases, c) At any case a genuine transaction should not be considered as fraud.

Credit card fraud detection is the process of identifying those transactions that are fraudulent into two classes of legitimate (genuine) and fraudulent transactions. Credit card fraud detection is based on analysis of a card's spending behavior. Credit cards are being used everywhere and have become a successful way of modern payment, while suffering from being misused. Frauds involving computer generated financial transactions are responsible for yearly losses over billions of dollars [1].There exists high demand for means to prevent, combat and manage such fraudulent transactions. Fraud detection is an act of recognizing such an activity and stopping it as soon as possible before the transaction is accomplished. In this content we consider misusage as unauthorized account activity committed by means of credit/debit facilities of a legitimate account. Credit card fraud detection is a relevant problem that draws attention of machine learning [7] and computational intelligence communities where a large number of automatic solutions have been proposed Data mining and Artificial Intelligence are often applied in fraud detection [1, 2, 4, 5]. Many techniques have been applied to credit card fraud detection, artificial neural network [4, 5, 9], genetic algorithm [5], support vector machine, frequent item set mining, decision tree [5], migrating birds optimization algorithm, naïve Bayes [5].

This paper evaluates advanced data mining approach using deep neural network. Deep neural network is a promising tool for fault characteristic mining and intelligent diagnosis of rotating machinery with massive data. A novel intelligent diagnosis method based on deep neural networks is proposed. The method implements both fault characteristics mining and intelligent diagnosis. The method is validated by machinery massive data under various operating conditions. Accurate results are produced for fault scenarios not previously studied. The paper is organized as follows: Section 2 presents the review of the related works and section 3 describes the proposed method of credit fraud detection using deep neural network. Section 4 discusses the experimental results and section 5 concluded the paper.

2. REVIEW OF RELATED WORKS

Data-driven approaches in credit card fraud detection describes both the supervised and unsupervised [2, 4, 7] methods. Unsupervised methods consist in outlier/ anomaly detection techniques that consider any transaction as a fraud that does not confirm with the majority. Remarkably, an unsupervised DDM in an FDS can be directly configured from unlabeled transactions. A well-known method is peer group analysis which clusters customers according to their profile and identifies frauds as transactions departing from the typical cardholder's behavior. The typical cardholder's behavior has also been modeled by means of self-organizing maps. Supervised methods are by far the most popular in fraud detection, and exploit labeled transactions for training a classifier. Frauds are detected by classifying feature vectors of the authorized transactions or possibly by analyzing the posterior of the classifier. Several classification algorithms have been tested on credit card transactions to detect frauds, including neural networks logistic regression association rules, support vector machines, modified Fisher discriminant analysis, and decision trees.

Recently, in [8], a realistic modeling was developed for regulating a real-world FDS, and provided a formal model of the articulated classification problem of credit card fraud detection. The learning strategy

developed consists of separately training a classifier on feedbacks and a classifier on delayed supervised samples, and then aggregating their posteriors to identify alerts. As anticipated, the major challenges [2, 4, 8] to be addressed when designing an FDS include: 1) handling the class imbalance [6], since legitimate transactions far outnumber the fraudulent ones; 2) handling the concept drift since the statistical properties of both frauds and genuine transactions evolve with time; and 3) operating with a small number of recent supervised transactions, provided in the form of investigators' feedback.

3. PROPOSED DEEP NEURAL NETWORK DRIVEN INTELLIGENT METHOD FOR CREDIT CARD FRAUD DETECTION

This section describes the peculiarities and operating conditions of the FDS. The proposed method illustrates four layers of control such as, 1) Payment Request terminal, 2) Request based feature extraction, 3) Feature augmentation, 4) Deep Neural Network. Figure 1 shows the block diagram of the proposed deep neural network driven intelligent method for credit card fraud detection.

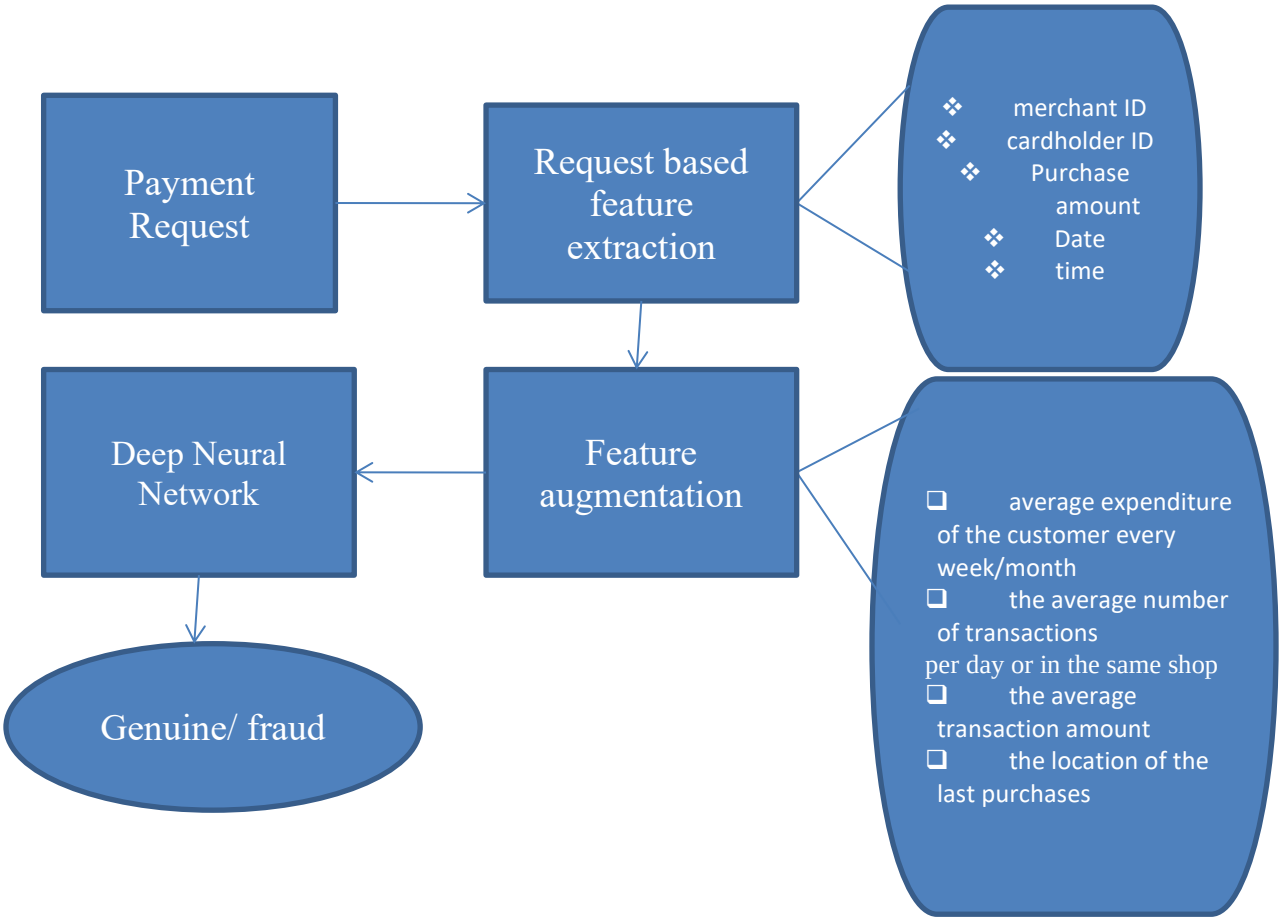

Fig.1. Block diagram of the proposed deep neural network driven intelligent method for credit card fraud detection

3.1 Payment request

The client makes the payment request at the terminal. The terminal represents the first control layer which performs conventional security checks on payment requests. Security checks include the PIN code, the card status (active or blocked), the available balance and expenditure limit. Requests that do not satisfy the above conditions are blocked. Transaction blocking rues are if-then (-else) statements meant to block the request that are clearly perceived to be fraud. These rules use information available when the payment is requested without analyzing historical records or cardholder profile. An example of blocking rule is "IF internet transactions AND unsecured website THEN deny the transaction".

3.2 Feature extraction

The request is then processed and moved to Request based feature extraction control where, features such as cardholder ID, Merchant ID, Paymentamount, date and time are extracted. Optimal selection of variables that capture the unique behavior of a credit card is done. The profile of both a legitimate and fraudulent transaction tends to be constantly changing. Thus, optimal selection of variables that greatly differentiates both profiles is needed to achieve efficient classification of credit card transaction.

3.3 Feature augmentation

After feature extraction layer of control, it moves to feature augmentation where, aggregated features such as average monthly expenditure of customer, average number of transactions done per day in the same shop, location of last transaction are extracted. Aggregated features are used to compare the previous and current transactions. The process of computing aggregated features is feature augmentation. Augmented features and current transaction data are stacked in feature vector that is supposed to be informative in determining whether the transaction authorized was fraud or genuine. Aggregated features are mostly recomputed offline for each individual cardholder on the basis of historical transactions and are stacked with transaction data in the feature vector.

3.4 Deep Neural Network

Once the features are augmented, the feature vector is given to deep neural network layer. Deep learning means using a neural network with several layers of nodes between input and output. The series of layers between input and output do feature identification and processing in a series of stages just as our brain seems to. It then finally identifies whether the transaction done was genuine or fraud.

3.4.1 Architecture

Deep neural network contains, 1) Input layer, 2) Convolution layer and pooling layer as hidden layer, 3) Classification layer and map layer as output layer. Figure 2 shows the architecture of the deep neural

network. The neural network has one or more hidden layer but deep neural network has deep and parallel connection of hidden layers to process the input and gives more accurate output. Deep learning seeks to learn rich hierarchical representation automatically through multiple stages of features learning process.

Input Layer: Input layer is the first layer of deep neural network and it contains large size of data set.

Hidden Layer: Hidden layer process the input which is from input layer. Each hidden layer must have the following two layers such as, a) Convolution layer, b) Pooling layer.

Convolution layer: It learn only related feature from input data set and this layer do mathematical operation on the input data. Hidden layer has filter and kernel matrix. Filter used to automatically filter out the needed information from the input. Kernel matrix used to extract relevant feature from the data set.

Pooling layer: The pooling layer is used to reduce the dimension of data and memory size. It also reduced amount of parameter. Pooling layer take input over certain area and reduced it to single value. Two type of pooling layer used in deep neural network, 1)Max pooling, and 2) Average pooling. Max pooling report the maximum output within a rectangular neighborhood and average pooling report the average output within a rectangle neighborhood.

Classification layer: After convolution and pooling layer, data are processed by classification layer. It only accepted one dimensional data. This analysis used to retrieve important and relevant information about data. This layer also used to classify data in different classes.

Output layer: Output layer is one which generates the output or it is the final layer of deep neural network.

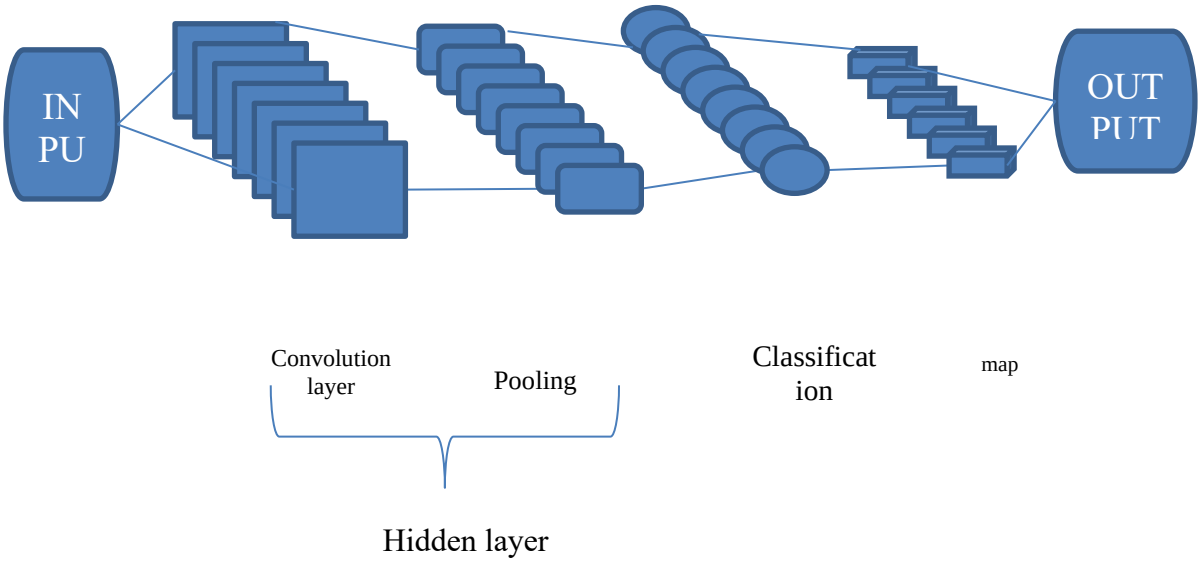

Fig.2. Architecture of the deep neural network

4. RESULTS AND DISCUSSION

This section presents the simulation results of the proposed method for credit card fraud detection. Then, the performance is analyzed with such metrics are precision and accuracy.

4.1 Dataset description

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.

4.2 Experimental set up

The proposed method of credit card fraud detection is implemented using JAVA under Netbeans framework. The proposed method is compared with the existing algorithm given in [8].

4.3 Evaluation metrics

The performance of the proposed method is analyzed by accuracy and precision. These metrics are explained as follows:

$$Accuracy = \frac{TN + TP}{TN + TP + FN + FP}$$

$$Precison = \frac{TP}{TP + FP}$$

Where, TN denotes True Negative, TP indicates True Positive, FN denotes False Negative and FP signifies False Positive.

4.4 Comparative analysis

Figure 3 shows the performance analysis of credit card fraud detection methods based on various percentage of training data. While using the percentage of training data is 50, the existing neural network achieved 60% precision. However, the proposed deep neural network acquires the higher value of 72.5%. Thus, the proposed algorithm attains higher precision value of 90% when compared with the neural network in 70% of training data. Similarly, the performance analysis of accuracy is shown in figure 4. The existing neural network obtains 67.43% while using the percentage of training data is 50 but the proposed method achieves the accuracy of 70%. Rather than the existing method, the proposed algorithm achieves 90% of accuracy value for 70% of training data.

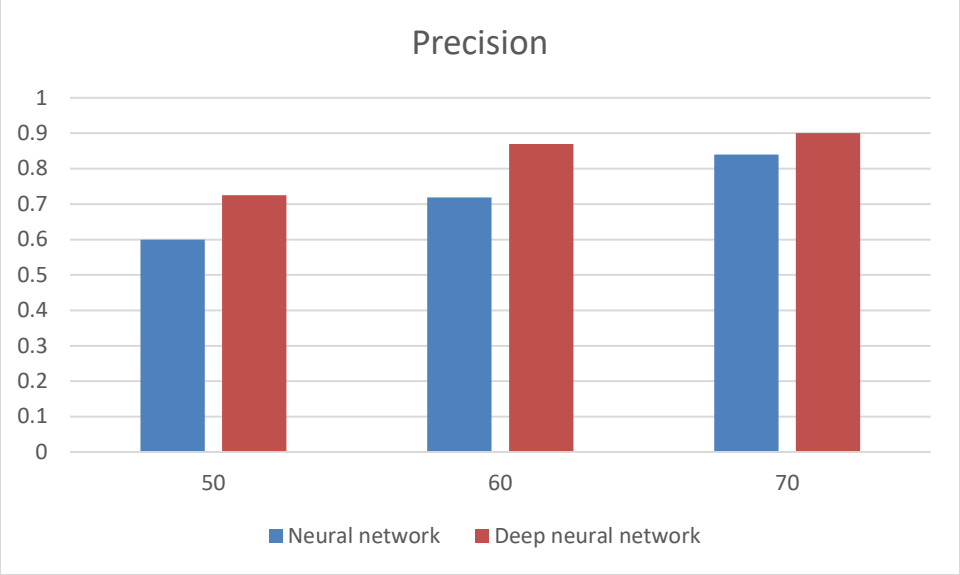

Fig.3. Comparative analysis based on precision

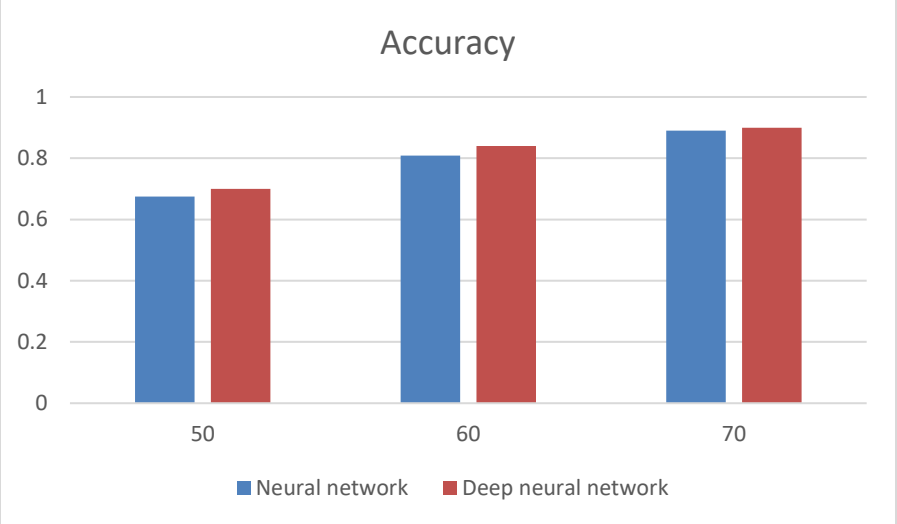

Fig.3. Comparative analysis based on accuracy

5. CONCLUSION

The alarming increase in fraudulent credit card usage has stressed the fraud management systems currently in use in banks and other institution that process credit card transaction. To progress safety measures of the monetary transaction systems in a habitual and effectual way, structure a precise and well organized credit card scam detection system is one of the essential functions for money transactions. Accordingly, deep neural network based method is developed in this paper for credit card fraud detection. Here, four important steps such as, 1) Payment Request terminal, 2) Request based feature extraction, 3) Feature augmentation, 4) Deep Neural Network is used for the detection of fraudulent behavior of the

credit card users. Finally, the experimentation is performed with benchmark dataset and the results proved that the proposed method attained the accuracy of 90% which is higher when compared with the existing neural network. In future, the optimization methods can be applied for improvement of training process of deep neural network.

REFERENCES

[1] Emanuel MinedaCarnerio, “Cluster Analysis and Artificial Neural Networks A Case Study in Credit Card Fraud Detection,” in 2015 IEEE International Conference(2015)

[2] Andrea Dal Pozzolo, Giacomo Boracchi, Olivier Caelen, Cesare Alippi, " Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy,"IEEE Transactions on Neural Networks and Learning Systems.,vol. 29, no. 8, pp.3784 - 3797, 2018

[3] Hu, H., Tang, B., Gong, X. et al.(2017). Intelligent fault diagnosis of the high-speed train with big data based on deep neural networks. IEEE Transaction on Industrial Information 13 (4): 2106-2116.

[4] John O. Awoyemi, Adebayo O. Adetunmbi , Samuel A. Oluwadare, ”Credit card fraud detection using machine learning techniques: A comparative analysis, “ 2017 International Conference on Computing Networking and Informatics (2017)

[5] N. Malini , M. Pushpa , ” Analysis on credit card fraud identification techniques based on KNN and outlier detection,” 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (2017)

[6] Ibtissam Benchaji , Samira Douzi , Bouabid ElOuahidi, ”Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Fraud Detection,”2018 2nd Cyber Security in Networking Conference (2018)

[7] Soltani,N.,Akbari,M.K.,& Javan,M.S,”A New User-Based Model for Credit Card Fraud Detection Based on Artificial Immune System,” In CSI International Symposium on Artificial Intelligence and Signal Processing(2012)

[8] 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.

[9] Ghosh, S. & Reilly, D. Credit Card Fraud Detection with a Neural Network. Proc. of 27th Hawaii International Conference on Systems Science 3: 621-630. 2004.

[10] https://data.world/raghu543/credit-card-fraud-data