Review On Fraud Detection Methods in Credit Card Transactions

Krishna Modi
Student, Computer Department
L D College of Engineering
Ahmedabad, Gujarat, India
krishnamodi1994@gmail.com

Reshma Dayma
Assistant Professor, Computer Department
L D College of Engineering
Ahmedabad, Gujarat, India
ceradayma@gmail.com

***Abstract*— Cashless transactions such as online transactions, credit card transactions, and mobile wallet are becoming more popular in financial transactions nowadays. With increased number of such cashless transaction, number of fraudulent transactions are also increasing. Fraud can be distinguished by analyzing spending behavior of customers (users) from previous transaction data. If any deviation is noticed in spending behavior from available patterns, it is possibly of fraudulent transaction. To detect fraud behavior, bank and credit card companies are using various methods of data mining such as decision tree, rule based mining, neural network, fuzzy clustering approach, hidden markov model or hybrid approach of these methods. Any of these methods is applied to find out normal usage pattern of customers (users) based on their past activities. The objective of this paper is to provide comparative study of different techniques to detect fraud.**

Keywords— credit card fraud, online fraud, cashless transactions, neural network

I. Introduction

Banking fraud can be defined as “The unauthorized use of an individual’s confidential information to make purchases, or to remove funds from the user’s account.” As per survey of statista [1] 41% of global internet users have purchased products online in 2013. In 2011, the number of digital buyers worldwide reached 792.6 million. A year later, the number rose to 903.6 million. In 2013, 41.3% of global internet users had purchased products online. In 2017, this figure is expected to grow to 46.4%. In survey by BBC news, Losses from online banking fraud rose by 48% in 2014 compared with 2013 as consumers increasingly conducted their financial activities on the internet. So with increased number of such cashless transaction and online shopping, fraudulent transactions are also increasing. Frauds can be caused by stealing or compromising banking details by email phishing, telephonic phishing, malware, non-secure security details, social networking sites and shoulder surfing. Fraudulent transactions can be detected either classification approach or by detecting outlying transaction from normal transactions. For classification approach, first model is trained from training data. Features are extracted and transformed from raw data while giving it to train model [15]. In this paper various methods and comparison are given that is used to detect fraudulent transactions.

II. Literature Survey

Ghosh and Reilly [9] used three-layer feed forward Neural network to detect frauds in 1994. The Neural Network was trained on examples of fraud containing stolen cards, application fraud, counterfeit fraud, Non Received Issue (NRI) fraud, and mail order fraud.

Abhinav and Amlan [7] proposed a Hidden Markov Model to detect the frauds in credit cards. Proposed Model does not require fraud signatures and still it can detect frauds by considering a cardholder’s spending habit. This system is also scalable to handle large number of transactions.

Y. Sahin and E. Duman [6] proposed approach to detect credit card fraud by decision tree and Support Vector Machine. Performance of classifier models of various decision tree methods (C5.0, C&RT and CHAID) and a number of different SVM methods (SVM with polynomial, sigmoid, linear and RBF kernel functions) are compared in this study.

An approach is proposed towards fraud detection in banking transactions in [2] using fuzzy clustering and neural network. In this approach fraud detection is done in three phase. First phase is initial user authentication and verification of card details. After successfully completing this phase, fuzzy c-means clustering algorithm is performed to find out normal usage behavior of user based on past transactions. If new transaction is found to be doubtful in this phase, mechanism based on neural network based is applied to determine whether it was actually fraudulent transaction or not.

Kang Fu, Dawei Cheng, Yi Tu, and Liqing Zhang at [3] proposed a convolutional neural network (CNN) based approach to find fraudulent transactions. Convolutional Neural Network is a part of deep learning and is a type of feed-forward Neural Network that consists of more than one hidden layer. In this paper, for finding more complex fraud patterns and to improve classification accuracy, a new feature trading entropy is proposed. To relieve the problem of the imbalanced dataset, cost based sampling method is used to generate more number of frauds. Generally, CNN is used for image recognition, Character recognition, image processing, video recognition and recommender system. In this paper for the first time, CNN is used to detect frauds.

Different outlier techniques [13] can also use to differentiate fraudulent transaction as outlier data.

Table 1 Academic Survey

Title	First Author	Journal	Techniques	Dataset
Credit Card Fraud Detection with a Neural Network [9]	Sushmito Ghosh	IEEE, 1994	Feed forward Artificial Neural Network	Mallon Bank 450000 transactions to train model
Credit Card Fraud Detection Using Bayesian and Neural Netorks [11]	Sam Maes	International Naiso Congress on Neuro Fuzzy Technology, 2002	Bayesian, Neural Networks	Europay International (EPI)
Credit Card Fraud Detection Using Hidden Markov Model [7]	Avhinav Srivastava	IEEE Dep & Sec Comp. 2002	Hidden Marcov Model	Completely simulated and simplified data.
Detecting Credit Card Fraud by Decision Trees and Support Vector Machines [6]	Y. Sahin	Proc Int. MultiConf of Eng & Comp Sci 2011	Decision Tree (C5.0, C&RT and CHAID) SVM (polynomial, sigmoid, linear and RBF kernel functions)	National bank's credit card data ware house 978 fraud, 22 million normal transactions
CARDWATCH Neural Network based mining system for credit card fraud detection [10]	Emin Aleskerov		Feed forward artificial Neural Network	Synthetic data
Credit Crad Fraud Detection: A hybrid Approach using Fuzzy Clustering and Neural Network [2]	Tanmaykumar Behera	IEEE Computer Society, 2015	Fuzzy Clustering and Neural Network	Synthetic data
Credit Card Fraud Detection using Convolutional Neural Network [3]	Kang Fu	Springer,2016	Convolutional Neural Network, Cost Based Sampling for imbalance data	Commercial Bank 260 million transactions 4000 fraud

III. Problems with credit card fraud detection

One of the biggest problem associated with researchers in fraud detection is lack of real life data because of sensitivity of data and privacy issue. Many researchers have done research with real life data [3], [9], [6], [11] of bank with agreements. To deal with this problem, many tools are available to generate synthetic data.

Second problem is to deal with Imbalance data or skewed distribution because number of fraudulent transactions are very less compare to legitimate transactions. To overcome this problem, synthetic minoring oversampling methods are used to increase number of low incidence data in dataset that generate synthetic fraudulent transactions related with original data set. In [3], cost based sampling is used to generate synthetic fraudulent transactions to balance data set.

Overlapping of data is one more problem as some of transactions look like fraudulent transaction, when actually they are legitimate transactions. It is also possible that fraudulent transactions appear to be normal transactions.

IV. Various Techniques to detect fraud in banking transactions

A. Hidden Markov Model

A hidden Markov model (HMM) is a statistical Markov model in which the system being modeled is assumed to be a Markov chain with hidden states. An HMM is a double embedded probability distribution process with hierarchy levels.

Fraud detection Approach using HMM is proposed in [7]. They have considered three price ranges low, medium and high {l,m,h} as set of possible observation. For example, let l = (0,100$], m=($100,$500], h=($500,credit card limit]. If a user makes a transaction of $320, then resultant observation symbol will be m.

Each transaction amount usually depends on the equivalent type of purchase. The set of all possible types of purchase and the set of all possible lines of business of merchants forms the set of hidden states of the HMM. The proposed approach in [7], Hidden Markov Model (HMM)-based credit card FDS does not require fraud signatures and still it can detect frauds by considering a user’s spending pattern.

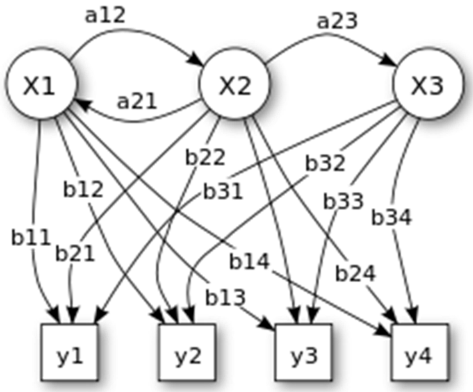

Figure 1 Probabilistic parameters of a hidden Markov model (example) [5]

B. *Artificial Neural Network*

Artificial Neural Network(ANN) is one of the powerful classifiers to find out hidden pattern among different attributes. ANN works same as human’s brain. ANN consists of different layers in which first layer is input layer and last layer is output layer. It may have number of hidden layer or no hidden layer. If Neural network consist of more than one hidden layer, then it is deep learning. Each layer has different neurons, and each neuron is connected with weighted edges. Output of each neuron is a function of its unit. This function is called activation function. Example of different activation functions used are sigmoid function, step function, threshold function, linear function etc. Most used function is Sigmoid function among all.

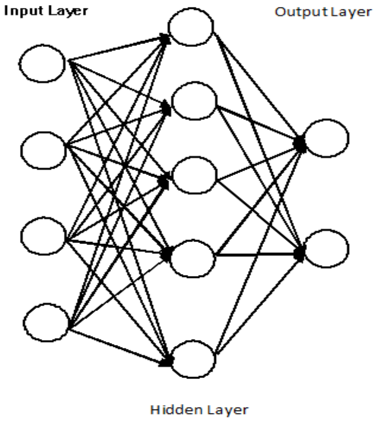

Figure 2 Structure Of Neural Network

Output layer has same number of neurons as classification label. Each neuron of output layer gives probability of being that class. In figure 2, four neurons are in input layer, which creates five decisions regarding to importance of input features. Neurons of second layer connected to output layers’ neurons. Neural network makes a decision of weights on edges from data given to it for training and adjust weights using back propagation algorithm [8]. Ghosh and Reilly [2] have proposed a three-layer feed forward neural network to detect credit card frauds. Values from 50 attributes were combined in to 20 features as input to neural network. They trained the neural network on large data set of labeled transactions taken from Mallon bank. These transactions comprise example of different fraud cases. Challenges for using neural network is to determine number of layers and number of neurons in each layer, number of iteration and learning rate. [12] Learning rate is a size of the step taken at each iteration, before correction of weights. A high value for learning rate can cause the model to train faster, but it can overshoot local minima. Choosing Activation function according dataset is also challenging task. In 1993, VISA Company had added Neural Network technology to combat card fraud. Neural network can also be combined with genetic algorithm to find parameters of Neural Network[14].

C. *Convolutional Neural Network (CNN)*

Convolutional Neural Network (CNN) is a part of deep learning. Mapping of input into hidden layer represents one feature map. Each feature map represents one characteristic. Process of compressing neurons into feature map is called convolution as shown in figure 3. Subsampling reduces parameters of feature map. Fully connected layer is same as neural network [8].

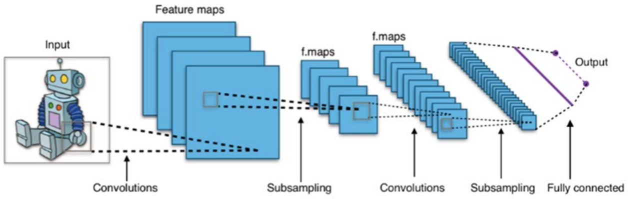

Figure 3 Structure of CNN Model

Each neuron in the first hidden layer is connected to a region of the input neurons as given in figure 4.

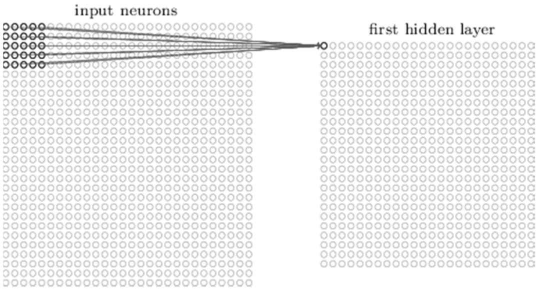

Figure 4 Making of first hidden layer

CNN is successfully applied in face recognition, character recognition, image classification etc. Kang Fu, Dawei Cheng, Yi Tu, and Liqing Zhang at [3] proposed a convolutional neural network based approach to find fraudulent transactions in credit card. Input features are transformed into feature matrices and then converted into images. For finding more complex fraud patterns and to improve classification accuracy, a new feature trading entropy is proposed. To relieve the problem of the imbalanced dataset, they used cost based sampling method to generate different number of synthetic frauds to train the model. They applied CNN model because it is suitable for training large size of data and CNN has mechanism to avoid over-fitting.

D. Decision Tree

A decision tree is a graphical representation of possible solutions to a choice based on certain situations. Decision tree starts with root node, divides into separate branches, these branches are connected with other nodes and so on. Decision tree end up in node called leaf node. Each node in Decision tree represents a test, branches associated with it represents its possible results and a leaf node has a label of class. With this tactical approach of separating and deciding, decision tree usually isolate the complex problem into simple ones. A simple example of decision tree is shown in figure 5 that distinguishes possibility of transaction being legitimate or fraudulent.

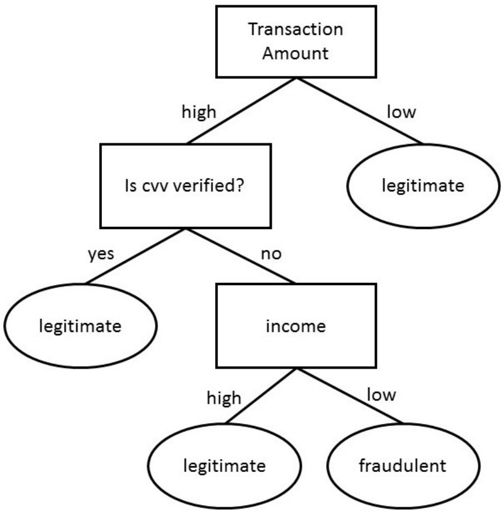

Figure 5 Example of Decision Tree

Y. Sahin and E. Duman [6] concluded that decision tree approaches outperform Support Vector Machine approaches in solving the problem under investigation.

Applied in real life, decision trees can be very complex and end up with pages of options.

E. Rule based method

Association Rules are generated to detect fraudulent transactions and normal transactions. In fraud detection, generated rules will be used to classify fraudulent and legitimate transactions. Therefor rules are generated as per behavior. This method is similar to decision tree. Example of these rules may be

R1: (transaction amount = low) → **legitimate**

R2: (transaction amount = high) ^ (is cvv verified = yes) → **legitimate**

R3: (transaction amount = high) ^ (is cvv verified = no) ^ (income=high) → **legitimate**

R4: (transaction amount = high) ^ (is cvv verified = no) ^ (income=low) → **fraudulent**

Ultimate goal in rule-based method is to mine set of rules.

Table 2 Comparison Table

Method	Advantage	Limitations
Artificial Neural Network	Can handle complex data Ability to learn itself	Very slow to train Require lot of power Hard to interpret for human.
Hidden Markov Model	Scalable for handling large volume of data	Highly expensive
Decision tree	Easy to interpret	Not powerful to handle complex data Needs data in refined form
Rule based method	Easy to understand and implement	New type of fraud will not be correctly classified after rules are generated
Convolutional Neural Network	Less training time	Avoid model overfitting.

V. MATRICS TO EVALUATE SYSTEM

As the data is highly imbalance, overall accuracy is not appropriate to evaluate model, since with very high accuracy, almost all fraudulent transactions can be misclassified.

Precision, recall, F1 score, Ratio of True Positive, True Negative, False Positive and False Negative are taken into account for evaluating binary classification.

True Positive (TP) is number of fraudulent transactions that actually predicted as fraudulent one.

True Negative (TN) is number of legitimate transactions that actually predicted as legitimate one.

False Positive (FP) is number of legitimate transactions that wrongly predicted as fraudulent one.

False Negative (FN) is number of fraudulent transactions that wrongly predicted as legitimate one.

$$\text{Precision (P)} = \frac{TP}{TP+FP} \qquad (1)$$

$$\text{Recall (R)} = \frac{TP}{TP+FN} \qquad (2)$$

F1 score is harmonic mean of precision and recall. Value of F1 score lies between 0 to 1. Higher F1 score indicates good model.

$$\text{F1 score} = 2 * \frac{precision*recall}{precision+recall} \qquad (3)$$

VI. Conclusion

In this paper, we bring together various methods to detect fraudulent transactions and comparison of these methods. One of these or combination of these methods can be used to detect fraudulent transactions. New features can be added and various sampling methods can be used to train the model more accurately.

References

[1] Statista the statistic portal (2017, March 14) available https://www.statista.com/topics/871/online-shopping/

[2] Tanmay Kumar Behera, Suvasini Panigrahi, "Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network", IEEE Computer Society, 2015

[3] Kang Fu, Dawei Cheng, Yi Tu, and Liqing Zhang, "Credit Card Fraud Detection Using Convolutional Neural Networks", Springer International Publishing AG 2016.

[4] Smt.S.Rajani, Prof.M. Padmavathamma, "A Model for Rule Based Fraud Detection in telecommunications", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 5, July – 2012.

[5] Hidden Markov model (2017, March 15) available https://en.wikipedia.org/wiki/Hidden_Markov_model

[6] Y. Sahin and E. Duman, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines", IMECS vol 1, 2011.

[7] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Senior Member, IEEE, and Arun K. Majumdar, Senior Member, IEEE , "Credit Card Fraud Detection Using Hidden Markov Model" , IEEE transactions on dependable and secure computing, vol. 5, no. 1, january-march 2008.

[8] Michael Nielsen (2017, March 15), Deep learning available http://neuralnetworksanddeeplearning.com/chap6.html

[9] Ghosh, S., Reilly, D.L.: Credit card fraud detection with a neural-network. In: Proceedings of the Twenty-Seventh Hawaii International Conference on System Sciences, 1994, vol. 3, pp. 621–630. IEEE (1994)

[10] Emin Aleskerov, Bernd fieisleben and Bharat Rao, "CARDWATCH: A Neural Network based database Mining System for Credit Card Fraud Detection"

[11] Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick, "Credit card fraud detection using bayesian and neural networks", International Naiso Congress on Neuro Fuzzy Technology, 2002.

[12] Minewiskan, Microsoft Neural Network Algorithm Technical Reference (2017, March 14) available at https://docs.microsoft.com/en-us/sql/analysis-services/data-mining/microsoft-neural-network-algorithm-technical-reference

[13] Krishna Modi, Bhavesh Oza, "Outlier Analysis Approaches in Data Mining", IJIRT vol 3 issue 7.

[14] Raghavendra Patidar, Lokesh Sharma, "Credit card fraud detection using Neural Network", IJSCE Volume-1, Issue-NCAI2011, June 2011.

[15] Alejandro Correa Bahnsen, Djamila Aouada, Aleksandar Stojanovic, Björn Ottersten, "Feature engineering strategies for credit card fraud detection", 0957-4174/ 2016 Elsevier.