Research Article

IJCRR
Section: General Science
Sci. Journal
Impact Factor 4.016
ICV: 71.54

Analysis of Suspicious Pattern Discovery Using AI-Neural Network in Credit Card Fraud Detection

C. Sudha[1], T. Nirmal Raj[1]

Department of Computer Science and Application, SCSVMV University, Enathur, Kanchipuram, Tamil Nadu-631561, India.

ABSTRACT

In recent years, the growth of new technologies have also provided further ways in which crime as gone smart and criminal may commit fraud in a smarter way. Cases related to credit card fraud have risen exponentially over the past few years. And regrettably, fraud is one of the main challenges consumers have to deal with in their credit ratings. This is why it is vital that businesses of all sizes make network and POS security a top priority. Traditional methods of data analysis have long been used to detect fraud. They require complex and time consuming investigations that deal with knowledge of different domains like financial, economics, business practices and law. In this paper I'll analyze how neural network technique helps in credit card fraud detection. Neural network techniques which can learn suspicious patterns from samples and used later to detect them. These published findings in the credit card industry to find some of the vulnerabilities that can prepare to affect the consumers who choose to pay by credit card.

Key Words: Credit Card, Fraud Detection, Neural Network, Suspicious patterns

INTRODUCTION

In day to day life credit cards are used in shopping purpose's and the payment mode for purchasing goods and services by the help of virtual card for on-line transaction or physical card for Off-line transaction. In physical transaction, Credit cards will insert into payment machine at merchant shop to purchase goods. Tracing fraudulent transactions in this mode may not be like since the attacker already steal the credit card. The credit card corporation or company may go in monetary and financial loss if loss of credit card is not realized by credit card owner and holders. In On-line payment mode, invader needs only little data regarding the information for doing fraudulent transaction (secure code, card number, expiration date etc.,) In this purchase method, mainly transactions will be done through web mode via Internet or telephone. Small transactions are generally undergo less confirmation and verification, and are less like to be checked by either the card issuer or the card holders. Card issuers/ card holders must take more precaution against fraud detection and financial losses. Credit card fraud cases are increasing every year [1].

RELATED WORK

Srivastava, Etal: Due to a rapid advancement in the electronic commerce technology, the use of credit cards has dramatically increased. As credit cards become the most popular mode of payment for both On-line as well as regular purchase and case of fraud associated with it are also rising. In this paper, we are using hidden Markov model(HMM) the sequence of operations in credit card transactions processing and show how it can be used for the detection of fraud. An HMM is initially trained with the normal behavior of a cardholder. If trained HMM used to find out incoming credit card transaction is not accepted by sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transactions are not rejected. We are present detailed experimental results to show the effectiveness of our approach and compare it with other techniques available in the literature [2].

Abhinav, Etal: The Internet has taken its place beside the telephone and the television as an important part of people's lives. Consumers rely on the Internet to shop, bank and invest On-line. Most On-line shoppers use credit card to pay for their purchases. As credit cards become the most popular

Corresponding Author:
C. Sudha, Department of Computer Science and Application, SCSVMV University, Enathur, Kanchipuram, Tamil Nadu, India - 631561.
E-mail: srisudhasri.kpm@gmail.com

ISSN: 2231-2196 (Print) **ISSN:** 0975-5241 (Online)
Received: 22.02.2017 **Revised:** 06.04.2017 **Accepted:** 29.04.2017

mode of payment, cases of fraud associated with it are also increasing. In this paper, HMM model using a sequence of operations in credit card transaction processing and show how it can be used for the detection of frauds. An HMM is trained with normal behavior of cardholder to protect the card detection. If an incoming credit card transaction is not accepted by the HMM with adequately high probability, it's considered to be obtained. We present detailed experimental results to show the effectiveness of our approach [3].

PROPOSED CREDIT CARD FRAUD DETECTION TECHNIQUES

Let's identifies the various types of credit card fraud and reviews various credit card fraud detection techniques that are available to business owners today.

A. Objectives

Neural network technique helps in credit card fraud detection. Neural network techniques which can learn suspicious patterns from sample and used later to detect them [4]. These published findings in the credit card industry to find some of the vulnerabilities that can prepare to affect the consumers who choose to pay by credit card [4].

Following are the studies for neural network in credit card fraud detection.

1. Logistic regression
2. Network Topologies.
   a. Supervised learning.
   b. Unsupervised learning.
   c. Reinforced learning.

B. What types of fraud do we need to look out for?[5]

- Bankruptcy fraud
- Theft/counterfeit fraud
- Application fraud
- Behavioral fraud

C. Decision tree

The thought following this technique is that of a similarity tree created using decision tree logic. In this casing, a similarity tree is distinct recursively; the nodes are labeled with the use of attribute names, edges are labeled using values of characteristic, and then there are the leaves, which contain an intensity factor it is defined the ratio of the number of transactions that satisfy the outlined conditions.

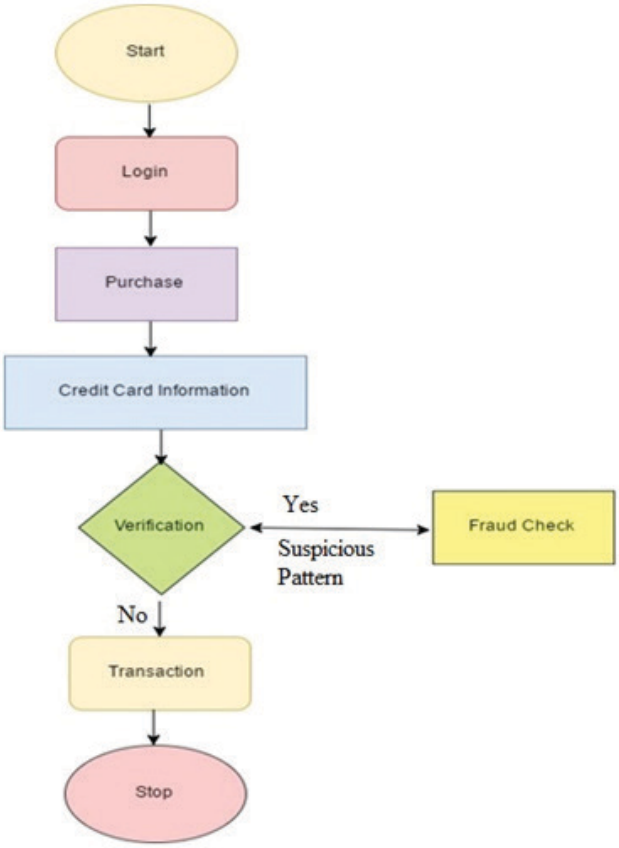

Figure 1: Existing Model HMM.

D. Equations and Algorithms

In order to define an HMM completely, following elements are needed [7].

- The number of states of the model, N. We denote the set of states S = {S1; S2; S3…SN}, where i =1; 2; . . .; N, is a number of state and Si, is an individual state. The state at time instant t is denoted by qt.
- The number of observation symbols in the alphabet, M. If the observations are continuous then M is never-ending. We denote the set of symbols V = {V1; V2; . . . VM} where Vi, is an individual symbol for a finite value of M.

$$\Lambda = \{a_{ij}\}$$

- A method is built up to determine whether the given transaction is fraud or not.
- The method uses Hidden Markov Model to detect fraud transaction.
- Hidden Markov Model works on the basis of spending habit of user.
- Classifies user into Low, Medium or High category.

E. Proposed Nerual Networks Model

Neural networks are also suggested as effective credit card fraud detection methods for finding suspicious pattern. The

only subject matter with this method is that all data has to be clustered by the kind of a/c it belongs to. Credit card fraud is a most important problem that if not dealt with well manner; it can result in myriad difficulty [6]. It is vital to try and find ways of detecting the issues and resolving them as soon as they arise.

- Neural networks provide a new alternative to linear discriminate analysis (LDA) and logistic regression, particularly in situations where the dependent and self-governing variables exhibit difficult non-linear relationships. Even though neural networks have show to effective credit scoring capability than LDA and logistic regression, they are also criticized for its long training process in designing the optimal network's topology.
- Artificial neural networks increase from the desire to artificially appearance the physiological structure and functioning of human brain structures.
- Artificial neural networks mainly used Processing Elements (PE) consist of elementary computational units, proposed by Mc Cullock and Pitts in 1943.
- As illustrated in Figure 3.2, the Input Layer will give the input neurons, which get the incoming quality. Input neurons process, according to a particular function called transfer function. The inputs selected and distribute the result to the next level of neurons.
- Then forward the information to all neurons of the layer 2 from the beginning input neurons (Middle Layers).
- Information is not simply sent to the intermediate neurons, but is weighed. It means that the result obtained from each neuron is sized according to the weight of the connection between the two neurons. Specifically, as shown in Figure 3.3, the weight of connection is represented by Wj,i.
- Each neuron must find out characterized by a transition function and a threshold value.
- The threshold must give the minimum value that input to activate the neuron. The neurons that represent the middle layer.
- Each neuron of this layer, sum of the inputs that are presented to its incoming connections. In mathematical terms, each neurons performs the summation of inputs, which given the product of output represent the first layer of the neurons. The result of this given sum is again drawn on the basis of the transfer function of each neuron. The result get turn forwarded to the next layer of neurons, multiplied by the weight between the neurons.
- Before the neural network can be applied to the problem at hand, a specific tuning of its weight must be done. This task is expert by the learning algorithm which trains the network and iteratively modifies the weights up to a specific condition is verified. In the most applications, the learning algorithm stops when the discrepancy (error) between desired output and the network falls below a predefined threshold to produce by the output. There are three topologies of learning mechanisms for neural networks

F. AI - Neural Network

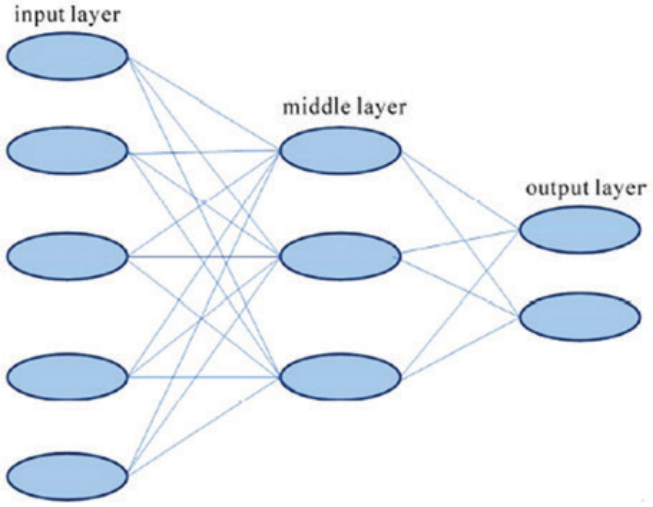

Figure 2: Neural Network.

There are three topologies of learning mechanisms for neural network.

- Supervised learning;
- Unsupervised learning;
- Reinforced learning.

Supervised learning is characterized by a training set which is correct examples of training set used to train the network. The training set is composed of pairs of inputs and corresponding desired outputs. The error produced by the network then it is used to change the weights of sets. This kind of learning is applied in some cases in which the network has to be learning to generalize the given examples.

Unsupervised learning algorithms, the network are only provided with a set of input and no desired output is given. The algorithm guides the network to self organizes and adapts its weights. This kind of learning is used for tasks such as data mining and clustering, where some regularity in a large amount of data have to be found.

Reinforced learning trains the network response by introducing prizes and penalties as a function of the network. Prizes and penalties are used to change the weights [4]. These algorithms are functional to train adaptive systems which perform a sequence of actions and task performed. The end of the outcome is result of this sequence; therefore the contribution of each action has to be produced value in the context of the action.

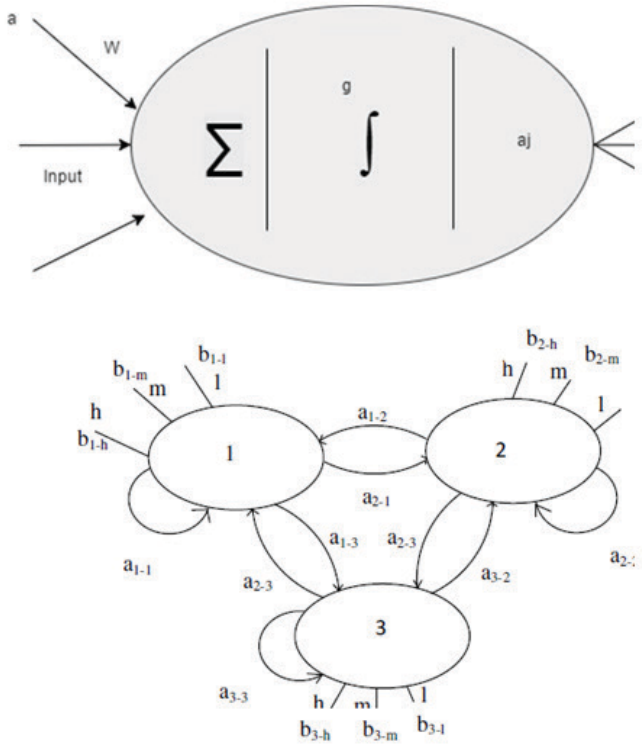

Figure 3: Graphical Representation of Neural Network and HMM.

According to the assumption for an HMM, probability that O is generated from this state sequence is given by [7][8]

P {O|q1,q2,q3,...qR,} = P(Ot|qt,)

P(O|Q,_) = bq1(O1).bq2(O2)...bqR (OR)

The probability of the state sequence Q is given as

P(Q|_) = _q1.aq1q2.aq2q3…aqR-1qR [7]s

CONCLUSION

Neural network techniques which can learn suspicious patterns from sample and used later to detect them. These published findings in the credit card industry to find some of the vulnerabilities that can prepare to affect the consumers who choose to pay by credit card holder.

Neural network is a latest technique that is being used in different areas due to its powerful capabilities of learning and predicting. In this thesis we try to use this capability of neural network in the area of credit card fraud detection.

REFERENCES

1. V. Bhusari and S. Patil, "Study of Hidden Markov Model in credit card fraudulent Detection",WCFTR'16-International Journal of Computer Applications(0975-8887), Vol 20, No.5, April 2011.
2. Abhinav Srivastava, Amlan kundu, "Credit Card fraud Detection using Hidden Markov Model", IEEE Transactions on Dependable and secure computing,Vol.5,No.1, January-March 2008.
3. Shamik Sural,"Credit card fraud Detection using Hidden Markov Model"s, IEEE Transactions on Dependable and Secure computing, Vol 5, No.1.
4. Vincenzo Pacelli, "An Artificial Neural Network Approach for credit Risk Management", Journal of Intelligent learning systems and 2011,3,103-112, published online May 2011.
5. P.Ravikumar and V.Ravi, "Bankruptcy prediction in Banks and firms via Statistical and Intelligent Techniques A Review", European Journal of operational Research, Vol.180, No.1,2007,pp.1-28.
6. Eric D.Kolaczyk,"Network Data Book", e –Book.
7. Bhusari, patil, "Application of Hidden Markov Model in Credit Card Fraud Detection",(IJDPS), Vol.2, No.6, November- 2011.
8. Mr. Matheswaran, Mr.R.Rajesh, "Fraud Detection in Credit Card using Data Mining Techniques", (IJRSET), Vol-II, issue I, pages 11-18 of 24, February – 2015.