A Survey of Fraud Detection Techniques for Credit Card based Transaction Processing

Siddhartha Choubey
Shri Shankaracharya Technical Campus, Bhilai

Vaibhav Lal
Shri Shankaracharya Technical Campus, Bhilai

Abha Choubey
Shri Shankaracharya Technical Campus, Bhilai

ABSTRACT
The wide emergence of electronic-commerce has widened the extensive usage of credit card for online transactions. However, there is also a high rise in malicious transaction and fraudulent associated with the credit cards. In this study we present several models and algorithm used in data mining for the detection of such malicious fraudulent or thefts. Such algorithm learns the transaction patterns and cluster the pattern of sequences usually involving with the processing of transactions to inhibit such malicious transactions made in the future.

Keywords
Online Transactions, credit card, credit card fraud, detection techniques, credit bureaux, data mining techniques, fraud detection.

1. INTRODUCTION
For quite some time there is a noticeable rise in the banking ethics and cyber fraudulent [1-3]. The illegal or unauthorized access to the credit card or its details is a criminal offence and there is nonexistence of an effective way to inhibit such thieve ies until the past decade [4-7]. The security and surety for the making of secured transaction has been an extensive research topic for the growth of business, financial institution and electronic commerce [7-14]. In the few other studies the credit card fraud is divided into certain types such as [15]:

1. Bankruptcy fraud.
2. Theft fraud/counterfeit fraud.
3. Application fraud
4. Behavioral fraud

Out of this four types of fraud the second one which implies towards the illegal accusation of the credit card and making personal transaction is what has been in rise and there were few studies made on it to define an approach to inhibit such types of electronic frauds [15-18]. Let alone Germany in 2004 has face over 345 billion pounds of credit card fraud, as been stated by the Euromonitor international in a series of report at the year 2006 [19-25]. In this study we discussed such techniques which has been proven successful against the cyber frauds over European Markets. This techniques aid in detecting such frauds by learning the pattern of the previous transaction of the card holder and each time verifying it with the previously trained pattern to allow the next transactions to take place.

2. TAXONOMY OF FRAUD DETECTION TECHNIQUES
2.1. Decision Tree based Technique

Figure 1. Illustration of credit card fraud detection through decision tree

Here the idea is to find the similarity of the tree formed during the previous transaction to that of the transaction being processed [26-29]. The similarity tree is generated recursively during each transaction and it’s weighted based on the validation of the previous ones. The similarity tree consists of nodes of attributes such as names, amount and edges with certain labelled factors or values of attributes in order to satisfactorily check for its similarity or dissimilarity. It legitimize the transaction and validate the transaction to update with the previous value or attributes that are encountered in new ones. The advantage of this method is that it is easy to implement, can be easily comprehended and visualized. It has its proven results and effectivity in countering numerous anomalistic scenarios.
2.2. Genetic Algorithm based Techniques

The evolutionary algorithm is more advantageous for fraud detection in comparison to that of the similarity tree method [30-34]. It is more of a predictive based method for identifying and classifying the transactions as suspicious or not. The advantage of this method is that it always cope up with the anomalistic scenario of validating a transaction. The method evaluates and form a logical relationship between the various attributes of the card holder and of its previous transactions, which enable it in classifying the suspicious or non-suspicious transactions for over 62 attribute fields. This method has proven results for various scenarios encountered in the past [35]. The major advantage posed by such a method is its predictability which can be increased by training unit with more and more credible data sets. There where also few studies which combines a probabilistic based approach in combination with the evolutionary algorithms [36].

2.3. Clustering based Techniques

Figure 2. Illustration of simple tree based fraud detection algorithm

Figure 3. Illustration of simple clustering based fraud detection algorithm
The clustering based technique is relied more over behavioral anomalies in order to detect for the malicious transaction. This system analyzes the behavioral conditions of the accounts that made improper or anomalistic transactions in the past [37-43]. Though this method isn’t applicable at the time of making transactions but it’s an algorithm that can be used to verify the transactions made in the past and such accounts are flagged as suspicious. This followed by several legal investigation to prove the fraudulent.

2.4. Neural Network based Technique

The application of the neural network is increasing at wide range because of its low computational cost. Fraud detection scenario is not left out with its advantages. Thus, several studies made in the past has shown the improved fraud detection algorithm while primarily based on neural network [44-49]. In this technique a neural classifier is used to form the synaptic linkage between various attributes of the datasets used in training the classifier. The system has a huge accuracy in comparison with the previously discussed methods. As the fraudsters are prone to developing new techniques or ways thus in this case with the help of neural classifier there isn’t a requirement to update the neural network with several other training sets but it train itself and update its feature as the time goes on. It constantly, check for the regularity and helps the banking or financial institution to instantly keep checks on false account claims.

3. CONCLUSION

Clearly, the various data mining techniques currently employed for fraud detection isn’t superior of confronting several issues and parameters at the same instance. Therefore, there is still a wide room of imprudent in the existing techniques. We hope that our work of summarizing several techniques under one documentation will help other researchers to look for the pro-and-cons of these techniques under a single roof and consequently aid in coming up with the new one or improving the existing ones.

4. REFERENCES


[41] Phua, C., Gayler, R., Lee, V., & K Smith. 2006. On the Approximate Communal Fraud Scoring of Credit Applications, Proceedings of Credit Scoring and Credit Control IX.


