Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Methods for Credit Card Fraud Detection Systems

Shilpa H. Taklikar
M.E Computer Engineering Student,
Sinhgad Institute of Technology
Lonavala, Maharashtra, India

Prof. R. P. Kulkarni
Professor, Department of Computer Engg.,
Sinhgad Institute of Technology
Lonavala, Maharashtra, India

Abstract— Technology has developed tremendously. The technology has been developed in such a way that it keeps in mind the new inventory will be comfortable and will be easy to use for the human beings. One such invention is the Credit card. The usages of Credit cards are for the online purchasing and for regular shopping. Credit card security is major concern to protect its misused from the fraudsters. There comes a necessity to distinguish the genuine transaction and fraudulent transaction. Financial frauds are increasing these days because of the use of plastic cards like Credit cards. There comes a necessity to identify the frauds before billing action is performed, this intern will avoid the financial losses to the banks, card owners. There are various methods to identify for the fraud detection. This paper deals with various approaches, methods that can be used in Credit card fraud detection systems.

Keywords— Artificial Immune System, Decision Tree, Genetic Algorithm, Hidden Markov Model, Outlier Detection

I. INTRODUCTION

Modern science and technology has invented many gadgets that are beneficial to the human beings and are very comfortable for the usage. One of the best inventions of the technology is the Credit cards.

Within the Europe, UK was the first country to use the creditcards. Initially, it was used for very small number of transactions. The records were initially tracked on papers . Later there came a need to have faster based approach. Banks then started to use the magnetic strips on back of the credit cards. These magnetic strips contains the confidential details of the card owner like Card Number details, Card Member name, and all the important required details. The terminals were installed at the retails so that the magnetic strips can be read and the card owner/member can perform the transaction using the credit card.

Credit cards in this ecommerce world have made remarkable usage and acceptance of usage by us for mode of payment. These plastic cards are used now-a-days everywhere for online shopping and also for regular purchasing. This is very convenient way for mode of payment. This can be best explained with the help of an example. We could find that Online Railway Reservation irctc site is many times slow due to the heavy loaded traffic. Similarly, the online shopping sites like myntra, snapdeal, flipkarts, etc have been used by many of us for online purchasing. From this we can come to know that, online shopping has increased tremendously. Thus, intern use of plastic cards / credit cards has been increased. But as we know, that every coin has two sides. Hence, the use of Credit cards has also given rise to fraudsters who may cause huge financial losses for the card holder and also fodr the card issuer's i.e. banks. Fraudsters can find it easier of misusage of the credit cards.

A. Need of Fraud Detection:

Credit cards are used as mode of payment. There comes a need wherein to identify transaction carried out by the use of credit card is true valid transaction done by card holder or it is fraud transaction done by fraudster. In traditional method, the transaction carried out is true valid transaction or fraud transaction was able to figure out once the billing has been done. This resulted in financial losses. So there is a necessity to determine the fraud transaction before the billing action is performed.

B. Credit cards Fraud Types:

1. Bankruptcy fraud: Bankruptcy fraud is the type of fraud which is very difficult to identify this fraud. The credit card's inability of a debtor to pay their debt which is also called as Insolvent gives rise to Bankruptcy fraud. The card holders may be in personal bankruptcy and failed to clear the unwanted existing loans. The banks sometimes are required to cover their losses itself. This can be prevented by passing the information or the required details to credit bureau. This is one of the ways wherein it helps to identify the past history related to its transactions and loan details of its respective customers. Depending upon the past history, further appropriate action can be taken by Banks to avoid this. Bankruptcy Foster & Stine (2004) presented a model to determine the bankruptcy fraud to forecast the details of the credit card users.

2. Application fraud: The person or the fraudster can find an alternative to commit the credit card fraud. One of the option is fraudster applies for the credit card with false or invalid information. This way of committing the fraud by fraudster is called as Application fraud.

Application fraud can be classified by two types: duplicates, identity fraudsters Whenever the application comes from same user with same individual details then it is known as duplicates. If the application comes from different individuals with the same details then it is called as identity fraudsters. To prevent this, banks uses the application form that has to be filled by the customers. It contains the mandatory fields which help to retrieve all the required details. To identify the duplicates, this can be done by cross matching with the last name or any other personal mandatory details. With this searching, it is possible to identify the duplicates.

3. Theft fraud/counterfeit fraud: This is one type of credit card fraud, which many of us can come across and may face this when the credit card is lost or the credit card details has been leaked.

Theft fraud as the name suggests that the fraud has been committed by thief. Whenever the credit card is stolen or lost and the respective stolen credit card is used by the thief or fraudster, it is called as theft fraud.

Counterfeit fraud is the type of fraud wherein the physical card is not required, only the respective credit card details are required to the fraudster. This type of fraud occurs whenever the credit card details are used from remotely without the physical card with the fraudster.

As soon as the card owner gives the details to the bank, the bank will detect or identify with the given details by card owner and try to identify the thief as soon as possible

4. Behavioural fraud: In this internet, ecommerce world, the usage of credit cards for online purchasing through ecommerce has given rise to behavioural fraud. Herein the fraudster, if he is able to retrieve the credit card details, can further use these details for fraudulent transactions by fraudster. For ecommerce, online shopping only the credit card details are required without the actual physical card for carrying out the transaction. Professional fraudsters can create an application which resembles to the exact copy of application. The credit card owner when uses the application for respective shopping or carrying out the transaction, the professional fraudster retrieves the respective card details and all required details, so that the fraudster can further use the details for carrying out the transactions. As the credit card owner uses the exact copy of application, thinking as a valid site to carry out transaction, this is called as Behavioural fraud.

II. CREDIT CARD FRAUD DETECTION METHODS

A general block diagram can be represented as below:

This diagram represents the overview to determine the given transaction is genuine transaction or the fraudulent transaction. If the given transaction is fraudulent one, then the detection system must identify the fraudulent transaction and also an alert/alarm must be generated for the same.

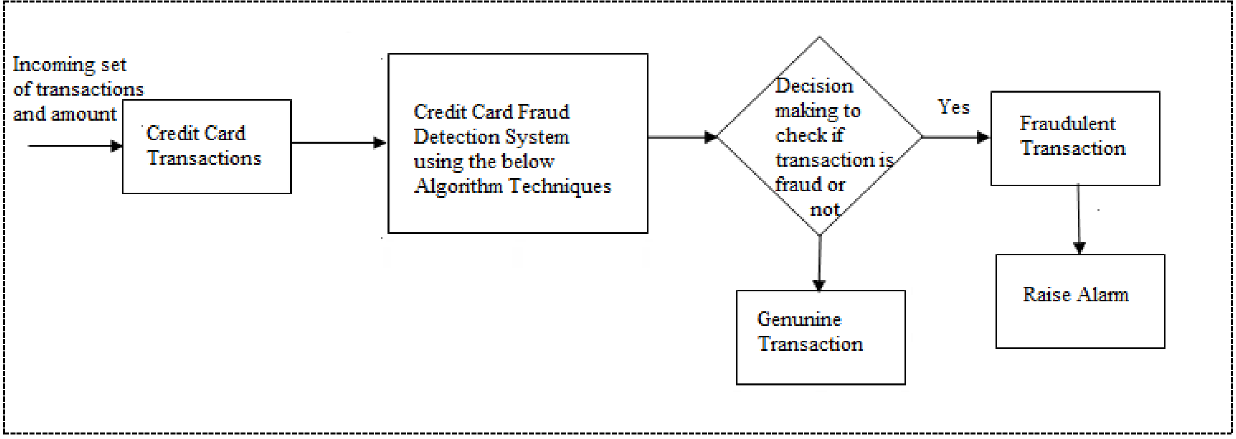
Incoming set of transactions and amount
Credit Card Transactions
Credit Card Fraud Detection System using the below Algorithm Techniques
Decision making to check if transaction is fraud or not
Yes
Fraudulent Transaction
Raise Alarm
Genuine Transaction

Fig 1: Block Diagram of Credit Card Fraud Detection System

There are various methods which can be applied to credit card fraud detection system. Below are the different ways that are obtained while doing the literature survey:

- Artificial Immune System
- Decision Tree
- Genetic Algorithm
- Hidden Markov Model
- Outlier Detection

(i) Artificial Immune System: Artificial Immune system has been inspired from natural biological immune system. The immune system can distinguish between the self and non self. Thus, artificial immune system is one of the ways which can be used in credit card fraud detection system.

The Artificial Immune system consists of artificial detectors that are able to classify any pattern as self or non-self by detecting only non-self patterns. AIS detection engines implements AIS based algorithms which can classify input data as normal or fraudulent

The main development and algorithms in Artificial Immune System [1]

- Clonal Selection
- Immune Network
- Negative Selection

The property to distinguish between self and non self helps to identify the given data or transaction is normal transaction or fraudulent transaction.

(ii) Decision Tree: Decision tree is one of the methods that can be used for fraud detection system. As the name suggests, it uses the decision tree as predictive model wherein it map the observations to get the conclusions. Here in this method, decision tree can be used to visually and represent the decisions and its respective decision making. In these tree structures, leaves represent classifications and branches represent conjuctions of features that lead to those classifications. Generally, top-down approach is used for constructing decision tree.

Below are the algorithms that are used for constructing the decision trees:

(a) Gini impurity
(b) Information gain
(c) Binary decision diagram

Decision tree can be considered as the conditional statements, wherein it is required to satisfy all the respective rules to get the result succeeded. Decision trees divide the complex problems into simple ones; this is further resolved through repeatedly.

Thus the Decision tree can be used to detect the given transaction is genuine transaction or the fraudulent transaction.

(iii) Genetic Algorithm: Genetic Algorithm is used in Data mining and has been used for credit card fraud detection. This helps in minimizing the fraudulent transactions by fraudster. This also helps in mining the fraud rates.

Pseudo code of Genetic Algorithm: [6]

```
Initialize the population
Evaluate the initial population
Repeat
Perform Competitive selection using Tournament or Roulette wheel
Apply genetic operators to generate new solutions
Evaluate solutions in population
Until some convergence criteria is satisfied.
```

The selection here deals with Tournament selection, Roulette wheel, biased selection. The process of selection is repeated to get the exact desired solutions.

There are three Genetic operators:

(i) Selection: To select in such a way that, we will get better outcomes.
(ii) Mutation: Randomly trying various combinations, so that better result can be obtained.
(iii) Crossover: Combining good portions, so that the resulting that is been created is the better one.

Genetic Algorithms are the algorithms which gives better results as the time progresses.

(iv) Hidden Markov Model: Hidden Markov model is one of the fraud detection techniques. This technique uses a finite set of states to verify the transactions. Each state has its own probabilistic distribution that is been used to verify the given transaction. The outcome of the state is given to the observer to determine its output. The internal states are hidden from the observer, Hence it is called as Hidden Markov model (HMM).

The different states in the Hidden Markov Model can be represented as shown in following diagram

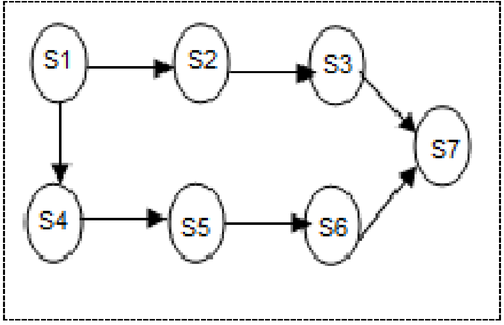

Fig 2: State representation in HMM

Hidden Markov Model can be defined with the help of following elements [2]:

a. *N*, the number of states,
b. *M* , the number of observation symbols,
c. *A*, matrix of state transition probabilities,
d. *B*, matrix of observation emission probability distribution,
e. □ □ matrix of prior probabilities

The parameter set (A, *B*,□ □) represents the overall HMM model. The parameters are selected and adjusted in HMM model by using various algorithms. One of the most important used algorithm in selecting the parameters is the (Baum Welch) B-W algorithm. HMM model initially studies the behaviour of the card owner. Depending on the observed history of the card holder, the particular transaction can thus be categorised as normal transaction or fraudulent transaction.

(vi) Outlier Detection: Outlier Detection is another form of fraud detection technique. This deals with understanding or detection the type of purchasing of usage/transaction is done by the user. The credit card when is stole, the pattern or the purchasing behavior may change. There are also the chances that there may be abnormal patterns of purchasing goods, which can also help in characterizing and thus can differentiate, if the given transaction is legal or fraudulent transaction. The ways wherein we can use for fraud detection is through Supervised learning [15], Semi-supervised and unsupervised learning.

An observation which deviates from the normal observation, may lead to the chances that the transaction needs to be investigated further and there can be possibility that it has been generated by different mechanism which can give possibility that it might be carried out by the fraudster.

III. CONCLUSIONS

The transactions that are carried with the credit card should be secure one and is very necessary to detect the fraudulent transactions carried by fraudsters. Credit card fraud detection systems by using one of the above methods can definitely help to detect the genuine transaction from the fraudulent transaction.

This will eventually help to determine fraud transactions and thus will in turn reduce the financial losses due to the fraudsters. This paper deals with the various types of credit card frauds and also its detection techniques. These techniques will help in identifying the fraudulent transaction and thus appropriate action can be taken before the billing action is performed.

REFERENCES

[1] Jianyong Tuo, Shouju Red, Wenhuane Lid, Xiu Li. Bine Li, and Lin Lei "Artificial Immune System for Fraud Detection,IEEE,2004

[2] Md. Rafiul Hassan, Baikunth Nath and Michael Kirley, "A Data Clustering Algorithm Based On Single Hidden Markov Model", Proceedings of International Multiconference on Computer Science and Information Technology, pp. 57 –66

[3] S. Benson Edwin Raj, A. Annie Portia, "Analysis on Credit Card Fraud Detection Methods", International Conference on Computer, Communication and Electrical Technology – ICCCET2011, 18th & 19th March, 2011

[4] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Credit Card Fraud Detection Using Hidden Markov Model, IEEE Transactions on Dependable and Secure Computing, VOL. 5, January-March 2008

[5] Rinky D. Patel, Dheeraj Kumar Singh, " Credit Card Fraud Detection & Prevention of Fraud Using Genetic Algorithm, "International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-6, January 2013

[6] K.RamaKalyani, D.UmaDevi "Fraud Detection of Credit Card Payment System by Genetic Algorithm", International Journal of Scientific & Engineering Research Volume 3, Issue 7, July-2012

[7] Masoumeh Zareapoor, Seeja.K.R, and M.Afshar.Alam, "Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria", International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, August 2012

[8] Krishna Kumar Tripathi, Mahesh A. Pavaskar, "Survey on Credit Card Fraud Detection Methods", International Journal Of Emerging Technology and Advanced Engineering, Volume 2, Issue 11, November 2012.

[9] V.Bhusari, S.Patil," Study of Hidden Markov Model in Credit Card Fraudulent Detection ", International Journal of Computer Applications (0975 - 8887) Volume 20- No.5, April 2011

[10] Nicholas Wong, Pradeep Ray, Greg Stephens & Lundy Lewis (2012). "Artificial immune systems for the detection of Credit card fraud". Info Systems, Volume 22.

[11] Y. Sahin and E. Duman, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines", International Multiconference of Engineers and computer scientists March, 2011.

[12] Peter J. Bentley, Jungwon Kim, Gil-Ho Jung and Jong-Uk Choi, "Fuzzy Darwinian Detection of Credit Card Fraud", 2007.

[13] Ekrem Duman, M. Hamdi Ozcelik "Detecting credit card fraud by genetic algorithm and scatter search". Elsevier, Expert Systems with Applications, 2011

[14] Daniel Garner, "Genetic algorithms for credit card fraud detection", IEEE Transactions, May 2011.

[15] Andrew Watkins, Jon Timmis, and Lois Boggess "Artificial immune recognition system (AIRS): An immune-inspired Supervised machine learning algorithm, Genetic Programming and Evolvable Machines", September 2004.

[16] A.N.Pathak, Manu Sehgal,Divya Christopher "A Study on Fraud Detection Based on Data Mining Using Decision Tree", International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011