IJRSET JUNE 2017 Volume 4, Issue 6 Pages: 12-18

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

ANALYSIS OF THE MODERN TECHNIQUES AND METHODS ON CREDIT CARD FRAUD DETECTION

[1] Dr. A. Prakash
[2] Assistant Professor
[3] PG & Research Dept of Computer Science,
[4] Hindutshan Colleges of Arts & Science, India.

ABSTRACT: As there is a vast advancement in the E-commerce technology, the use of credit cards has grown up. The credit card has become the crucial mode of payment so with the rise in the credit card transactions, the credit card frauds have also become frequent nowadays. Credit card frauds are increased day by day regardless of various techniques developed for its detection. Generate various new ways of committing fraudulent transactions each day which demands constant innovation for its detection techniques. Most of the modern methods are based on neural networks, Decision Tree, Fuzzy Darwinian System, Hidden Markov Model etc. This paper analyses about different types of techniques and methods to prevent the attacks and simulations.

Keywords: [Hidden Markov Model, Fuzzy Darwinian System, Neural Network, Decision Tree, Genetic Algorithm]

1. INTRODUCTION

E-commerce payment systems are increased popular due to the widespread use of the internet-based shopping and banking. Credit Card Fraud is one of the largest threats to business organizations today [1]. It is important to first understand the mechanisms of executing a fraud i.e. we need to understand the techniques of cyber credit card frauds. Since earlier the fraud is detected only when the billing for credit card is done, it is very hard to prevent fraudulent transactions. Therefore the need to assure unexposed transactions for credit-card owners when using their credit cards to make electronic payments for goods and services provided on the internet is a criterion [2]. The fraud begins to either the theft of the physical card or the compromise of data associated with the account, including the card account number or other information is routinely and necessarily available to a merchant during a legitimate transaction [3]. The compromise can occurred to many common routes and can usually be conducted without tipping off the card holder, the merchant or the issuer, at least until the account is ultimately used for fraud. Sample example is that of a store clerk copying sales receipts for later use [4] [5]. The rapid growth of credit card use on the Internet has made database security lapses particularly costly in some cases, millions of accounts are compromised. Stolen cards are reported quickly by cardholders, but a compromised account is hoarded by a thief for weeks or months before any fraudulent use, making it difficult to identify the source of the compromise. The cardholder is not discovering fraudulent use until receiving a billing statement, which may be delivered infrequently.

2. TYPES OF FRAUDS

More different types of frauds are represented into namely Credit Card Frauds, Telecommunication Frauds, and Computer Intrusions, Bankruptcy Frauds, Theft Frauds/Counterfeit Frauds, Application Frauds, Behavioural Frauds [6].

- **Credit Card Frauds:**

Credit card fraud is divided into two types. Namely, Offline fraud and On-line fraud. (1)Offline fraud is used a stolen physical card at call centre or other place. (2)On-line fraud is via internet, phone, shopping, web, or in absence of card holder.

- **Telecommunication Frauds:**

The use of telecommunication services to commit other forms of fraud. Consumers, businesses and communication service provider are the victims.

- **Computer Intrusion:**

Intrusion is defined as the act of entering without warrant or invitation that means potential possibility of unauthorized attempt to access information, manipulate information purposefully. Intruders may be from any environment, an outsider (or Hacker) and an insider who knows the layout of the system.

- **Bankruptcy Frauds:**

This column focuses on bankruptcy fraud. Bankruptcy fraud means used a credit card while being absent. Bankruptcy fraud is one of the most complicated types of fraud to predict.

- **Theft Fraud/ Counterfeit Frauds:**

Theft fraud refers to use a card that is not yours. As soon as the owner gives some feedback and contact the bank, the bank takes measures to check the thief as early as possible. Counterfeit fraud occurs to when the credit card is used remotely where only the credit card details are needed.

- **Application Frauds:**

When someone applies for a credit card with false information that is termed as application fraud. For detecting application fraud, two different situations are classified. When applications come from a same user with the same details, that is called duplicates, and when applications come from different individuals with similar details, that is termed as identity fraudsters. In most of the banks, eligibility for a credit card, applicants need to complete an application form.

Application form is mandatory except for social fields. The bank is also asked for certain details as contact details, such as e-mail address, mobile phone number and land-line number. Confidential information will be the password.

- **Behavioural Fraud:**

Behavioural fraud represented to the when sales are made on a cardholder present basis and details of legitimate cards are obtained fraudulent basis.

3. TECHNIQUES USED BY CREDIT CARD FRAUDSTERS

In order to detect cyber credit-card fraud activities on the internet, a study was conducted on how credit-card information is stolen. Here are some of the different techniques which are used for credit-card fraud information theft.

- **Credit-card fraud generator software**

This software is used to generate valid credit-card numbers and expiry dates. Some of these software are capable in generating valid credit-card numbers like credit-card companies or issuers because it uses the mathematical Luhn algorithm that credit-card companies or issuers use in generating credit-card numbers to their credit-card consumers or users [7]. In some cases, this software is written by black-hat hackers who have hacked credit-card information stored on a database file from which the software can display valid credit-card information to other type of cyber credit-card fraudsters who have bought the software to use [8].

This technique in some cases is used by black-hat hackers to sell their hacked credit-card information to other online credit-card fraudsters with little or no computer skills.

- **Key –logger and Sniffers**

The Black-hat hackers who have professional Programming or computer skills infect a computer by installing and automatically running sniffers or key-logger computer programs by which they log all the keyboard inputs made into the computer on a file with the intention of retrieving personal information like credit-card information, etc [9]. These fraudsters are able to infect the user's computers by sending infectious spam mails to computer users & asking them to download free games or software, and when those are downloaded, the sniffers of key-loggers are downloaded automatically, installed and ran on the user's computers. While the sniffer is running under the user's computer, they ken and log all the keyboard inputs made by the user over a network [10]. Therefore, any user can unknowingly share their private information through this infectious software. Sometimes this software are also shared or sold to other fraudsters who do not have computer knowledge or skills.

- **Site-cloning, Spyware and Merchant sites**

This software is also created by black-hat hackers, which are installed and ran on user's computer to keep track of all the website activities [11]. By tracking and knowing the website activities of the user on the internet, they clone the electronic or banking websites which are regularly visited by the user and send the user for using it with the intension of retrieving private or personal information [12]. Also in the case of fake merchant sites, fake websites are created on which cheap products are provided to users and thereby asking user for payment by credit cards. If any payment is made on these fake sites, the user's credit card information is then stolen.

- **Physically stolen credit-card information**

The fraudsters can steal the credit card and use the information to buying goods and products online [13].

- **CC/CVV2 shopping websites**

Cyber credit-card fraudsters who have no professional computer skills buy hacked credit-card information on these websites to use for fraudulent electronic payment for some goods and services on the internet [14].

4. CREDIT CARD FRAUD DETECTION METHODS

In Credit Card Fraud Detection there are many methods, here we present survey of some most powerful method.

- **Hidden Markov Model:**

A Hidden Markov Model is a finite set of states; every state is associated with a probability distribution. Transitions among these states are administered by a set of probabilities called transition probability [15]. In a specific state a possible outcome or observation can be produced which is associated symbol of observation of probability distribution [16].

HMM categorizes card holder's profile as low, medium and high spending based on their spending behaviour in terms of amount. A set of probabilities for amount of transaction is being assigned to each cardholder. Amount of each incoming transaction is then matched with card owner's category, if it justifies a predefined threshold value then the transaction is decided to be legitimate else declared as fraudulent. HMM never check the original user as it keeps a log. The log that is maintained will also be a proof for the bank for the transactions that are made. HMM reduces the tedious work of an employee in

bank since it maintains a log. HMM produces high false alarm as well as high false positive. HMM also works on human behaviour while doing online shopping.

- **Fuzzy Darwinian System:**

This technique is used genetic programming to develop fuzzy logic rules are capable of classifying credit card transactions into suspicious and non-suspicious ones. It elaborates the use of an evolutionary-fuzzy system that is capable of classifying suspicious and non-suspicious credit card transactions [17].

The developed system comprises of two main elements.

(i) A Genetic Programming (GP) search algorithm and **(ii)** A fuzzy expert system. When the data is provided to the FDS system, the system first clusters the data into three groups namely low, medium and high which is known as fuzzy clustering [18]. The genotypes and phenotypes of the GP System is some rules which match the incoming sequence with the past sequence. Genetic Programming is used to develop a series of variable-length fuzzy rules that characterize the differences between classes of data placed in a database. The system is developed with the definite aim for insurance-fraud detection which includes the challenging task of classifying the data into the categories are safe and suspicious [19]. For classification of transactions, when the customer's payment is not overdue or the overdue payment is less than three months, the transaction is considered as non-suspicious, otherwise it is considered as suspicious. The Fuzzy Darwinian detects suspicious and non -suspicious data easily and also detects stolen credit card Frauds. This system has very high accuracy and produces a low false alarm in comparison with other techniques, but it is highly expensive. The speed of the system is also low.

- **Neural Networks:**

Neural network is defined as a set of interconnected nodes designed to represent functioning of the human brain. Each node has a weighted connection to several other linked nodes in adjacent layers [20]. Single node take input received from linked nodes and use the weights of the connected nodes together with easy function for computation of output values. Neural networks can be created for supervised and/or unsupervised learning. The user specifies the number of hidden layers along with the number of nodes within a specific hidden layer [21]. The output layer of the neural network may contain one or several nodes depending upon the application. Recently, neural network researchers have several associated methods from statistics and numerical analysis into their networks. Neural networks can learn and summarizes the internal assumptions of data even without knowledge of the potential data principles in advance. Neural networks topologies, or architectures, formed by organizing nodes into layers and attach layers of neurons with modified weighted interconnections and it can match its own behaviour to the new environment along with the results of formation of evolution capability from present environment to the new possible situation. Statistical methods are sometime unusual in the practice research even though the common advantages of the neural networks in application of credit card fraud detection [22]. On the other side, there are still many disadvantages for the neural networks, such as

(1) Difficulty to confirm the structure,
(2) Excessive training,
(3) Efficiency of training and so on.

- **Decision Tree:**

After introducing the concept of learning system, decision tree method has been developed, that can deals with continuous

data. The decision tree is a table of tree shape with connecting lines to available nodes. Each node is either a branch node followed with more nodes or only one leaf node assigned by classification [23]. With this strategic approach of separating and resolving, decision tree usually detach the complex problem into many simple ones and resolves the sub-problems through repeatedly using, data mining method to discover training various kinds of classifying knowledge by constructing decision tree. The basis of decision tree model is how to construct a decision tree with high precision and small scale [24].There are many advantages of Decision tree method.

1. High flexibility
2. Good haleness
3. It is explainable, which is also the reason of its varied utilization. Their disadvantage is that, it requires checking each transaction one by one.

- **Genetic Algorithm:**

Genetic algorithms, inspired from natural evolution were first introduced by Holland (1975). Genetic algorithm (GA) is a search technique used in computing to find exact or approximate solutions to optimization and search problems. GA is used in data mining mainly for variable selection and is mostly coupled with other DM algorithms [25]. And their combination with other techniques has a very good performance.

They have been used in a number of applications in engineering and social science. Recently, they applied for optimization of the parameters of support vector machine for predicting bankruptcy, and hybrid with neural net work for detecting credit card fraud with high accuracy, and have been used along with Artificial Immune System for reducing a number of false alarms in credit card fraud detection [26]. GA has been used in credit card fraud detection for minimizing the wrongly classified number of transactions. And is easy accessible for computer programming language implementation, thus, make it strong in credit card fraud detection. But this method has high performance and is quite expensive.

5. COMPARISON OF DIFFERENT METHODS

Methods	Speed of detection	Accuracy	Cost
HMM	Fast	Low	Expensive
FDS	Very low	Very high	Expensive
NN	Fast	Medium	High expensive
DT	Fast	Medium	High expensive
GA	Good	Medium	In expensive

CONCLUSION AND FUTURE WORKS

In this paper analysed and some techniques, methods algorithms for credit card fraud detection. Each one method or algorithm have some performance ratio not only the advantages and also have some drawbacks within that. In future work will choose any one method which is most secure and suitable to do better accuracy for security process and then apply some enhancement within that to proof much better than the old performance.

REFERENCE

[1**]** John Akhilomen, „Data Mining Application for Cyber Credit-card Fraud Detection System", Proceedings of the World Congress on Engineering 2013 Vol III, WCE 2013, July 3 - 5, 2013, London, U.K.

[2**]** Anshul Singh, Devesh Narayan, „A Survey on Hidden Markov Model for Credit Card Fraud Detection", International Journal of Engineering and Advanced Technology

(IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-3, February 2012.

[3**]** Avinash Ingole, Dr. R. C. Thool, „ Credit Card Fraud Detection Using Hidden Markov Model and Its Performance‟, Volume 3, Issue 6, June 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[4**]** Khyati Chaudhary, Bhawna Mallick, „Credit Card Fraud: Bang in E-Commerce‟, IJCER | May-June 2012 | Vol. 2 | Issue No.3 |935-941.

[5**]** Krishna Kumar Tripathi, Mahesh A. Pavaskar, „Survey on Credit Card Fraud Detection Methods‟, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012).

[6**]** V.Dheepa1 , Dr. R.Dhanapal, „Analysis of Credit Card Fraud Detection Methods‟, International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009.

[7**]** Krishna Kumar Tripathi, Lata Ragha, „Hybrid Approach for Credit Card Fraud Detection‟, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-4, September 2013.

[8**]** Masoumeh Zareapoor, Seeja.K.R, 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.

[9**]** Francisca Nonyelum Ogwueleka, "DATA MINING APPLICATION IN CREDIT CARD FRAUD DETECTION SYSTEM‟, Journal of Engineering Science and Technology Vol. 6, No. 3 (2011) 311 - 322 © School of Engineering, Taylor‟s University.

[10**]** Suvasini Panigrahi, Amlan Kundu, Shamik Sural, A.K. Majumdar, „Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning‟, Information Fusion 10 (2009) 354–363.

[11**]** Venkata Ratnam Ganji, Siva Naga Prasad Mannem, „Credit card fraud detection using anti-k nearest neighbor algorithm‟, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 06 June 2012.

[12**]** Ganesh Kumar.Nune1, P.Vasanth Sena2 and T.P.Shekhar, „Novel Artificial Neural Networks and Logistic Approach for Detecting Credit Card Deceit‟, International Journal of Computer Science and Management Research Vol 1 Issue 3 October 2012.

[13**]** Y. Sahin and E. Duman, „Detecting Credit Card Fraud by Decision Trees and Support Vector Machines‟.

[14**]** Salvatore J. Stolfo, David W. Fan, Wenke Lee and Andreas L. Prodromidis, „Credit Card Fraud Detection Using Meta-Learning:Issues and Initial Results‟.

[15**]** 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.

[16] Venkata Ganji, Siva Naga Prasad Mannem, "Credit card fraud detection using anti-k nearest neighbor algorithm", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 06 June 2012

[17] 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.

[18] Joseph King-Fung Pun,"Improving Credit Card Fraud Detection using a Meta-Learning Strategy", Chemical Engineering and Applied Chemistry University of Toronto 2011

[19] Vladimir Zaslavsky and Anna Strizhak," CREDIT CARD FRAUD

DETECTION USING SELFORGANIZING MAPS", INFORMATION & SECURITY. An International Journal, Vol.18,2006.

[20] Khyati Chaudhary, Jyoti Yadav, Bhawna Mallick, "A review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications (0975 – 8887) Volume 45– No.1, May 2012.

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

[22] Ganesh Kumar.Nune, P.Vasanth Sena and T.P.Shekhar, "Novel Artificial Neural Networks and Logistic Approach for Detecting Credit Card Deceit", International Journal of Computer Science and Management Research Vol 1 Issue 3 October 2012

[23]. Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun K. Majumdar. "Credit Card Fraud Detection using Hidden Markov Model". IEEE Transactions on dependable and secure computing,Volume 5; (2008) (37-48).

[24]. Bidgoli, B. M., Kashy, D., Kortemeyer, G. & Punch, W. F "Predicting student performance: An Application of data mining methods with the educational web-based system LON-CAPA". In Proceedings of ASEE/IEEE frontiers in education conference. (2003).

[25]. Ekrem Duman, M. Hamdi Ozcelik "Detecting credit card fraud by genetic algorithm and scatter search". Elsevier, Expert Systems with Applications, (2011). 38; (13057–13063).

[26]. J. Hunt, J. Timmis, D. Cooke, M. Neal, C.KingDevelopment of an artificial immune system for real-world applications". Artificial Immune Systems and their Applications, Springer (1998). (157–186).