ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

A Survey of Credit Card Fraud Detection Techniques for Genetic Algorithm

Kritika Joshi[1], Dr. (Mrs) Ani Thomas[2]

M. Tech. Scholar, Department of IT (E-Security), Bhilai Institute of Technology, Durg, India[1]

Professor& HOD, Department of IT, Bhilai Institute of Technology, Durg, India [2]

ABSTRACT: Credit card plays a very important rule in today's economy. It becomes an unavoidable part of household, business and global activities. Although using credit cards provides enormous benefits when used carefully and responsibly, significant credit and financial damages may be caused by fraudulent activities. Many techniques have been proposed to confront the growth in credit card fraud. However, all of these techniques have the same goal of avoiding the credit card fraud; each one has its own drawbacks, advantages and characteristics. In this paper, after investigating difficulties of credit card fraud detection, we seek to review the state of the art in credit card fraud detection techniques, datasets and evaluation criteria. The advantages and disadvantages of fraud detection methods are enumerated and compared. Furthermore, a classification of mentioned techniques into two main fraud detection approaches, namely, misuses (supervised) and anomaly detection (unsupervised) is presented. Again, a classification of techniques is proposed based on capability to process the numerical and categorical datasets. Different datasets used in literature are then described and grouped into real and synthesized data and the effective and common attributes are extracted for further usage. Moreover, evaluation employed criterions in literature are collected and discussed. Consequently, open issues for credit card fraud detection are explained as guidelines for new researchers.

KEYWORDS:Credit Card, Fraud Classification, Fraud Detection Techniques

I. INTRODUCTION

While performing online transaction using a credit card issued by bank, the transaction may be either Online Purchase or transfer .The online purchase can be done using the credit or debit card issued by the bank or the card based purchase can be categorized into two types Physical Card and Virtual Card. In both the cases if the card or card details are stolen the fraudster can easily carry out fraud transactions which will result in substantial loss to card holder or bank. In the case of Online Fund Transfer a user makes use of details such as Login Id, Password and transaction password. Again here if the detail of the account is wrong then, as a result, it will give rise to fraud transaction. Credit card fraud is a wide-ranging term for theft and fraud committed using a credit Card or any similar Payment mechanism as a fraudulent source of funds in a transaction. The target may be to obtain goods without paying money, or to obtain unauthorized funds from an account. The fraud begins with either the theft of the physical card or the compromise of data associated with the account, it include the card account number or other information that would routinely and necessarily be available to a merchant during a legal transaction. The compromise can occur by many common routes and can usually be conducted without tipping off the card holder or the merchant at least until the account is ultimately used for fraud. A store clerk copying sales receipts for later use is a simple example. The speedy growth of credit card use on the Internet has made database security lapses particularly costly; in some cases, millions of accounts have been determined. Stolen cards can be reported emergently by cardholders, but a determined account can be cached by a thief for weeks or months before any miss use, making it difficult to identify the source of the determined. Popularity of online shopping is growing day to day. Credit card is the easy way to do online shopping. According to an ACNielsen study conducted in 2005 one-tenth of the world's population is shopping online in same study it is also mentioned that credit cards are most popular mode of online payment. In US it is found that total number of credit cards from the four credit card network(Master Card, VISA, Discover, and American Express) is 609 million and 1.28 billion credit cards from above four primary credit card networks plus some other networks (Store, Oil Company and other). If consider

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

the statistics of credit cards in India , it is found that total number of credit cards In India at the end of December-31-2012 is about 18 to 18.9 million [1]. In case of multinational banks, the usage or average balance, per borrower for credit card holder has risen up from Rs. 61,758 in 2011 to Rs. 82,455 in 2012. In the same period, private bank customers' usage rise from Rs 39,368 to Rs. 47,370 [2]. As the number of credit card users increases world-wide, the opportunities for fraudster to steal credit card details and, subsequently, commit fraud are also grew up.

II. CREDIT CARD FRAUD

Credit card fraud has been divided into two types: Offline fraud and On-line fraud.

- Offline fraud is committed by using a stolen physical card at call center or any other place.
- On-line fraud is committed via internet, phone, shopping, web, or in absence of card holder.

Telecommunication Fraud: 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 [3]. Bankruptcy Fraud: This column focuses on bankruptcy fraud. Bankruptcy fraud means using a credit card while being absent. Bankruptcy fraud is one of the most complicated types of fraud to predict [4]. Theft Fraud/ Counterfeit Fraud: In this section, we focus on theft and counterfeit fraud, which are related to one other. Theft fraud refers using a card that is not yours. As soon as the owner give some feedback and contact the bank, the bank will take measures to check the thief as early as possible. Likewise, counterfeit fraud occurs when the credit card is used remotely; where only the credit card details are needed [5]. Application Fraud: When someone applies for a credit card with false information that is termed as application fraud. For detecting application fraud, two different situations have to be 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. Phua et al. (2006) describes application fraud as "demonstration of identity crime, occurs when application form(s) contain possible, and synthetic (identity fraud), or real but also stolen identity information (identity theft)."
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 would also ask for certain details as contact details, such as e-mail address, mobile phone number and land-line number. Confidential information will be the password [6]. Behavioral Fraud: Behavioral fraud occurs when sales are made on a „cardholder present" basis and details of legitimate cards have been obtained fraudulent basis [7].

III. DIFFICULTIES OF CREDIT CARD FRAUD DETECTION

Fraud detection systems are prune to several difficulties and challenges enumerated bellow. An effective fraud detection technique should have abilities to address these difficulties in order to achieve best performance.

Imbalanced data: The credit card fraud detection data has imbalanced nature. It means that very small percentages of all credit card transactions are fraudulent. This cause the detection of fraud transactions very difficult and imprecise.

Different misclassification importance: in fraud detection task, different misclassification errors have different importance. Misclassification of a normal transaction as fraud is not as harmful as detecting a fraud transaction as normal. Because in the first case the mistake in classification will be identified in further investigations.

Overlapping data: many transactions may be considered fraudulent, while actually they are normal (false positive) and reversely, a fraudulent transaction may also seem to be legitimate (false negative). Hence obtaining low rate of false positive and false negative is a key challenge of fraud detection systems [8].

Lack of adaptability: classification algorithms are usually faced with the problem of detecting new types of normal or fraudulent patterns. The supervised and unsupervised fraud detection systems are inefficient in detecting new patterns

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

of normal and fraud behaviors, respectively.

Fraud detection cost: The system should take into account both the cost of fraudulent behavior that is detected and the cost of preventing it. For example, no revenue is obtained by stopping a fraudulent transaction of a few dollars [5, 7]. Ukraine 19% Indonesia 18% Yugoslavia 18% Malaysia 6% Turkey 9% United States 1% other country 29% Statistical Classification of Credit Card Fraud Occurrence Ukraine Indonesia Yugoslavia Malaysia Turkey United States other country 5.

Lack of standard metrics: there is no standard evaluation criterion for assessing and comparing the results of fraud detection systems.

IV. CREDIT CARD FRAUD DETECTION TECHNIQUES

The credit card fraud detection techniques are classified in two general categories: fraud analysis (misuse detection) and user behavior analysis (anomaly detection). The first group of techniques deals with supervised classification task in transaction level. In these methods, transactions are labeled as fraudulent or normal based on previous historical data. This dataset is then used to create classification models which can predict the state (normal or fraud) of new records. There are numerous model creation methods for a typical two class classification task such as rule induction [1], decision trees [2] and neural networks [3].This approach is proven to reliably detect most fraud tricks which have been observed before [4], it also known as misuse detection. The second approach deals with unsupervised methodologies which are based on account behavior. In this method a transaction is detected fraudulent if it is in contrast with user's normal behavior. This is because we don't expect fraudsters behave the same as the account owner or be aware of the behavior model of the owner [5].To this aim, we need to extract the legitimate user behavioral model (e.. user profile)for each account and then detect fraudulent activities according to it. Comparing new behaviors with this model, different enough activities are distinguished as frauds. The profiles may contain the activity information of the account; such as merchant types, amount, location and time of transactions, [6].This method is also known as anomaly detection. It is important to highlight the key differences between user behavior analysis and fraud analysis approaches. The fraud analysis method can detect known fraud tricks, with a low false positive rate. These systems extract the signature and model of fraud tricks presented in oracle dataset and can then easily determine exactly which frauds, the system is currently experiencing. If the test data does not contain any fraud signatures, no alarm is raised. Thus, the false positive rate can be reduced extremely. However, since learning of a fraud analysis system (i.e. classifier) is based on limited and specific fraud records, it cannot detect novel frauds. As a result, the false negatives rate may be extremely high depending on how ingenious are the fraudsters. User behavior analysis, on the other hand, greatly addresses the problem of detecting novel frauds. These methods do not search for specific fraud patterns, but rather compare incoming activities with the constructed model of legitimate user behavior. Any activity that is enough different from the model will be considered as a possible fraud. Though, user behavior analysis approaches are powerful in detecting innovative frauds, they really suffer from high rates of false alarm. Moreover, if a fraud occurs during the training phase, this fraudulent behavior will be entered in baseline mode and is assumed to be normal in further analysis[7].In this section we will briefly introduce some current fraud detection techniques which are applied to cr 6 together with a simple function to compute output values. Neural networks come in many shapes and architectures. The Neural network architecture, including the number of hidden layers, the number of nodes within a specific hidden layer and their connectivity, most be specified by user based on the complexity of the problem. ANNs can be configured by supervised, unsupervised or hybrid learning methods.

Supervised techniques

In supervised learning, samples of both fraudulent and non-fraudulent records, associated with their labels are used to create models. These techniques are often used in fraud analysis approach.One of the most popular supervised neural networks is back propagation network (BPN). It minimizes the objective function using a multi-stage dynamic optimization methodthat is a generalization of the delta rule.The back propagation method is often useful for feed-forward network with no feedback. The BPN algorithm is usually time-consuming and parameters like the number of hidden neurons and learning rate of delta rules require extensive tuning and trainingto achieve the best performance [10]. In the domain of fraud detection, supervised neural networks like back-propagation are known as efficient tool

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

that have numerous applications [11]. RaghavendraPatidar, et al. [12] used a dataset to train a three layers backpropagation neural network in combination with genetic algorithms (GA) forcredit card fraud detection. In this work, genetic algorithms was responsible for making decision about the network architecture, dealing with the network topology, number of hidden layers and number of nodes in each layer.

Unsupervised techniques

The unsupervised techniques do not need the previous knowledge of fraudulent and normalrecords.These methodsraise alarmfor those transactions that are most dissimilar from the normalones.These techniques are often used in user behavior approach.ANNs can produce acceptable result for enough large transaction dataset. They need a long training dataset. Self-organizing map (SOM) is one of the most popular unsupervised neural networks learning which was introduced by [13]. SOM provides a clustering method, which is appropriate for constructing and analyzing customer profiles,in credit card fraud detection, as suggested in [14]. SOM operates in two phase: training and mapping. In the former phase, the map is built and weights of the neurons are updated iteratively, based on input samples, in latter, test data is classified automatically into normal and fraudulent classes through the procedure of mapping. As stated in, after training the SOM, new unseen transactions are compared to normal and fraud clusters, if it is similar to all normal records, it is classified as normal. New fraud transactions are also detected similarly. One of the advantages of using unsupervised neural networks over similar techniques is that these methods can learn from data stream. The more data passed to a SOM model, the more adaptation and improvement on result is obtained. More specifically, the SOM adapts its model as time passes. Therefore it can be used and updated online in banks or other financial corporations. As a result, the fraudulent use of a card can be detected fast and effectively. However, neural networks has some drawbacks and difficulties which are mainly related to specifying suitable architecture in one hand and excessive training required for reaching to best performance in other hand.

IV. CONCLUSION

Credit card fraud has become more and more rampant in recent years. To improve merchants' risk management level in an automatic and efficient way and building an accurate and easy handling credit card risk monitoring system is one of the key tasks for the merchant banks. One aim of this study is to identify the user model that best identifies fraud cases. There are many ways of detection of credit card fraud. If one of these or combination of algorithm is applied into bank credit card fraud detection system, Then the probability of fraud transactions can be predicted soon after credit card transactions by the banks. This paper gives contribution towards the effective ways of credit card fraudulent detection. In our paper we survey on seven existing Techniques for credit card fraud detection with comparing their results hence we conclude that out of these method HMM model is one of the best model because in HMM model fraud detect using Card holders spending behavior, but we need to improvement HMM in future.

REFERENCES

[1] AvinashIngole, Dr. R. C. Thool, " Credit Card Fraud Detection Using Hidden Markov Model and Its Performance," International Journal of Advanced Research In Computer Science and Software Engineering (IJARCSSE), vol. 3, 6 June 2013.
[2] Srivastava, Abhinav, Kundu, Amlan, Sural, Shamik and Majumdar, Arun K., (2008) "Credit Card Fraud Detection Using Hidden Markov Model", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 1, pp. 37-48.
[3] S. Ghosh and D.L. Reilly, "Credit Card Fraud Detection with a Neural-Network," Proc. 27th Hawaii Int'l Conf. System Sciences: Information Systems: Decision Support and Knowledge Based Systems, vol. 3, pp. 621-630, 1994.
[4] Pankaj Richhariya et al "A Survey on Financial Fraud Detection Methodologies" BITS, Bhopal," International Journal of Computer Applications (0975 – 8887) Volume 45 No.22, May 2012.
[5] Dr. R. Dhanapal, Gayathiri. P, " Credit Card Fraud Detection Using Decision Tree For Tracing Email And Ip," International Journal of Computer Science Issues (IJCSI) Vol. 9, Issue 5, No 2, September 2012.
[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] Rinky D. Patel, Dheeraj Kumar Singh " Credit Card Fraud Detection & Prevention of Fraud Using Genetic Algorithm", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue6, January 2013.
[8] AmlanKundu, SuvasiniPanigrahi, Shamik Sural and Arun K. Majumdar, "Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning," Special Issue on Information Fusion in Computer Security, Vol. 10, Issue no 4, pp.354- 363, October 2009.
[9] Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick,"Credit card fraud detection using Bayesian and neural

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 7, July 2018

networks,"Interactive image-guided neurosurgery, pp.261-270, 1993.

[10] Linda Delamaire (UK), Hussein Abdou (UK), John Pointon (UK), "Credit card fraud and detection techniques: a review", Banks and Bank Systems, Volume 4, Issue 2, 2009.

[11] 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.

[12] 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.

[13] V. Bhusari, and 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.

[14] 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