Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 11, November 2015, pg.241 – 244

SURVEY ARTICLE

A SURVEY ON CREDIT CARD FRAUD DETECTION

S.Suganya MCA.,[1], **N.Kamalraj** MCA., M.Phil.[2]

[1]M.Phil Scholar (Computer Science), Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India

[2]Head & Assistant Professor, Department of Information Technology, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India

[1] sugiselvi85@gmail.com, [2] tpkamal@gmail.com

***Abstract*— In recent years credit card became one of the essential part of the people. Instead of carrying huge amount in hand it is easier to keep credit card. But now a days that too becomes unsafe. One of the issues facing credit card fraud detection systems is that a significant percentage of transactions labelled as fraudulent are in fact legitimate. The main purpose of the paper is the survey on the various methods applied to detect the credit card frauds. From the abnormalities in the transaction the fraudulent one is identified.**

***Keywords*— Data Mining, Meta –Classification, Neural Networks, Bayesian Classification, Decision Tree, SVM**

I. INTRODUCTION

In the current fast moving world the need for data mining becomes more essential huge amount of data is stored in data warehouse and it is essential to extract the needy information from warehouse. Different data mining techniques are there to get the information needed for the particular problem. Fraud can be defined as wrongful or criminal deception intended to result in financial or personal gain [1], or to damage another individual without necessarily leading to direct legal consequences.

Fraud prevention and fraud detection are two ways to avoid losses and frauds. Fraud prevention is done before the occurrence of fraud. Fraud detection is done when fraudsters passed through fraud prevention techniques and start a fraudulent transaction. None of them is sure whether the transaction passed through prevention system. Accordingly, the main aim of the detection techniques is to find whether transaction is fraudulent or not as soon as possible [2-5].

The different types of frauds that can occur are fraudulent transactions in credit card systems and e-commerce systems, fraud account in financial systems, fraudulent calls or service usages in telecommunication systems, and fraudulent claims in insurance systems.

Credit card frauds are of two types as online and offline. Simple theft, application fraud, counterfeit cards comes under offline and card holder is not needed to be present in online fraud since the transaction is

made remotely and card's details are needed. A manual signature, a PIN or a card imprint are not required at the time of purchase. Now a days, online frauds are increased a lot since usage of credit card is unavoidable. In European countries, above 50% of fraud losses in 2008 is because of online frauds which are reported by visa.

II. RELATED WORK

Some of the related work done on credit fraud detection is discussed in this section.

BASED ON FREQUENT ITEM SET MINING

K. R. Seeja and Masoumeh Zareapoor proposed a credit card fraud detection model that detects fraud from highly imbalanced and anonymous credit card transaction datasets.
Frequent item set mining is used for finding legal and illegal patterns of transactions which handles the imbalance problem in class. To find whether the incoming transactions of the customers belongs to legal or illegal pattern , a matching algorithm is proposed and according that transaction closer to the patterns are identified and decisions are made. No special attention on attributes is given to manage the anonymous nature of transaction data and every attribute is treated equally for pattern finding. On UCSD Data Ming Contest 2009 Dataset, Evaluation of performance for this model is done and found to have less false alarm rate compared to state of the art classifiers, rate of fraud detection is high, classification rate is balanced, Matthews correlation coefficient [6].

Different algorithms used by the authors are KNN, Random Forest, SVM, and Naïve Bayes. The key technique proposed is 'Fraud Miner'. Frequent item set mining is used to create patterns for legal and fraud transactions for each customer from legal and fraud transactions of them respectively in the training phase. The incoming transactions are checked by the matching algorithm to detect which pattern it belongs. The legal pattern of the customer is matched with incoming transaction then "0" is returned by the algorithm. The fraud pattern of the customer is matched with incoming transaction then "1" is returned by the algorithm [6].

DECISION TREE AND SUPPORT VECTOR MACHINE

Y. Sahin and E. Duman proposed a work that uses the real dataset for the performance comparison of decision tree algorithms and SVM. Comparatively, decision tree models are better than SVM models on test dataset. When the training datasets are used comparison results in the reverse form such that training data is over fitted by SVM models. The success factor of this problem is assignment of many fraudulent transactions as fraudulent. Regardless of whether the transaction is true fraud or true normal assignment, the rate of true assignments is shown by accuracy.

According to accuracy, when performances of models is compared as the increase in number of training data, over fitting becomes less and SVM models performance become comparable to decision tree model. SVM models caught only less number of frauds than decision tree models.
An accuracy of assignments by models is not related to the number of actual fraudulent transactions assigned as fraudulent. In this problem performance metric is not matched with accuracy accordingly. C5.0 model is the best compared to other models but C&RT model catches more frauds from samples. C&RT and C5.0 is chosen by the above key factor [7].

NEURAL NETWORKS

Raghavendra Patidar, Lokesh Sharma proposed a work on credit card fraud detection based on neural networks. Though different data mining technologies are there to detect fraud, all of them are not able to find fraudulent transaction in progress. Two peculiar characteristics of credit card fraud detection are the limited time to take decision whether to accept or reject and large amount of credit card transactions processed in stipulated time.

Working principal (Pattern Recognition)

Neural network based fraud detection is similar to the human brain working. Neural network made a computer to think as human brain that learns through past experience. The learning experience or knowledge is used to solve and make decision in problems in day today life. The same method is for credit card fraud detection. The consumer use fixed pattern of credit card use. This pattern is taken for past one or two years to train a neural network. The different other categories of information can also be stored like location for kids

purchase, frequencies of huge purchase and so on in limited time. Neural network trains the various faces of credit card fraud along with credit card usage pattern which is provided by bank. Credit card usage pattern is taken by the prediction algorithm to differentiate fraudulent and non-fraudulent. Unauthorized user's pattern is matched with original card holder's pattern which is trained by neural network, and if pattern is same the decision made as genuine transaction.

Fraud Detection

Pattern matching is not necessarily to be exact rather small variations can be accepted and if there exists big difference in pattern, then chances that particular transaction is illegal transaction is more. The output of neural network will be in between 0 and 1. If the output is below .6 or .7 it implies transaction legal and if output is above .7 then probability of an illegal transaction is high. In some occasions legal users may make transaction that will be quite different and sometimes fraudster make transactions that matches the pattern trained by neural network. Due to limitation problems, legal users will use card for limited amount but fraudster will try to do big purchase before the action taken by the credit card holder which will be a mismatch with the trained pattern by neural network. The process of business will be present always in neural network pattern recognition systems design. History descriptors provide details usage details of card and payments made. Other descriptors have information about date if issue and so on [8].

HIDDEN MARKOV MODEL

The credit card issuing bank runs a fraud detection system (FDS). FDS verifies each and every inward transaction. The card details and purchase details are used by FDS to find genuine or fake transaction. FDS checks for the difference by comparing spending details of the credit card holder, delivery address and so on. If there is a difference FDS confirms that the transaction is fake and the transaction is declined.

HMM Model for Credit Card Transaction Processing

Observation symbols should be determined to handle credit card transaction by HMM. Restrict the x values of purchase into M price ranges such as V1, V2, …, VM, establishes observation symbols to bank.

Generation of Observation Symbols

An HMM is trained for each credit card holder. A clustering algorithm is executed to get the observation symbols of individual cardholder's transaction respectively. Many attributes are stored in the database of the issuing bank.

Checking spending Profile

The spending details of card holder play a major role which can be divided into three categories namely high-spending, low – spending and medium- spending.

Model Parameter Estimation and Training

The proposed model is trained with few transactions so that it will be easier to detect frauds and which is further developed with corrections for future references to efficiently detect the fraud.

Fraud Detection

Initial symbol sequence is formed from the symbols taken from the cardholder's training data after learning HMM factors.

META CLASSIFICATION STRATEGY

Joseph Pun, Yuri Lawryshyn follows the meta-learning techniques introduced by Chan and Stolfo [10] in their proposed work. The meta-learning tries to combine the results of multiple learners to accuracy of prediction and strengths and weakness of methods are complimented with each other. The two ways of combining algorithms are arbiter and combiner methods. Through the experiments Chan and Stolfo came conclusion that combiner method is more effective compared to arbiter method. In combiner method the

attributes and correct classifications are used to train base classifiers. The resulting predictions are then fed into meta-level classifier. The combination of Original attributes, predictions from base classifier and correct classification for each and every instance is used to create a new "combined" dataset which is then used as training data for meta-classifier. In combiner strategy the final prediction is the prediction from the meta-level classifier[11].

III.FUTURE WORK

The different algorithms can be used to detect and improve the fraudulent activities done using credit card. Optimization algorithms are used with combination of algorithms or any one data mining algorithm for the best results.

IV. CONCLUSIONS

In modern world the use of credit card for multiple purposes is inevitable. The increase in the use of credit card also increases the fraudulent activities and a great loss of amount. Lot of research work has been carried in this field to develop efficient and accurate techniques for the fraud detection. Hence the careful examination of earlier proposed algorithms is necessary. In this paper the survey of the current studies on credit card fraud detection. The uniqueness of past studies is discussed. The future work determines to develop an effective data mining algorithms for credit card fraud detection.

REFERENCES

[1]. Hobson, A. 2004. The Oxford Dictionary of Difficult Words. The Oxford University Press. New York.

[2]. Bolton, R. J. and Hand, D. J. 2002. Statistical fraud detection: A review. Statistical Science 28(3):235-255.

[3]. Kou, Y. et. al. 2004. Survey of fraud detection techniques. In Proceedings of the 2004 IEEE International Conference on Networking, Sensing and Control, Taipei, Taiwan, March 21-23.

[4]. Phua, C. et al. 2005. A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review.

[5]. Sahin, Y., Duman E. An overview of business domains where fraud can take place, and a survey of various fraud detection techniques. In Proceedings of the 1st International Symposium on Computing in Science and Engineering, Aydin, Turkey, June 2010.000

[6]. K. R. Seeja and Masoumeh Zareapoor, "FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining", Hindawi Publishing Corporation ,The Scientific World Journal , Volume 2014, Article ID 252797, 10 pages , http://dx.doi.org/10.1155/2014/252797.

[7]. Y. Sahin and E. Duman, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines" , Proceedings of the International Multiconference of Engineers and Computer Scientists 2011 Vol I, IMECS 2011, March 16 -18, 2011,Hong Kong.

[8]. Raghavendra Patidar, Lokesh Sharma, "Credit Card Fraud Detection Using Neural Network", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-NCAI2011, June 2011.

[9]. Ashish Thakur, Bushra Shaikh, Vinita Jain, A. M. Magar, "Hidden Markov Model in Credit Card Fraud Detection " , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February 2015 ISSN: 2277 128X .

[10]. P. K. Chan and S. J. Stolfo, "Experiments in Multistrategy Learning by Meta-Learning," Proceedings of the second international conference on Information and knowledge management, pp. 314-323, 1993.

[11]. Joseph Pun, Yuri Lawryshyn, "Improving Credit Card Fraud Detection using a Meta-Classification Strategy ", International Journal of Computer Applications (0975 – 8887) Volume 56– No.10, October 2012 .

