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. 3, Issue. 4, April 2014, pg.780 – 791

SURVEY ARTICLE

A Revived Survey of Various Credit Card Fraud Detection Techniques

Neha Sethi[1], Anju Gera[2]

[1]B.S Anangpuria Institute of Technology & Management, Faridabad

[2]B.S Anangpuria Institute of Technology & Management, Faridabad

[1] neha.sethi1989@gmail.com ; [2] Anju.gera@faculty.anangpuria.com

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. [1] Thus, an improved fraud detection system has become essential to maintain the reliability of the payment system. The criterion is to assure secured transactions for credit card owners so that they can make electronic payment safely for the services and goods which are provided on internet. In an e-bank many transactions undergo simultaneously, so a fraud detection system should distinguish between legitimate, suspicious fraud and an illegitimate transaction.[4] There are many modern and new techniques which are based on Neural Network, Artificial Intelligence, Bayesian Network, Data mining, Artificial Immune System, K- nearest neighbor algorithm, Decision Tree, Fuzzy Logic Based System, Support Vector Machine, Machine learning, Genetic Programming etc., that has developed in detecting various credit card fraudulent transactions. This paper represents a survey of various techniques which are used in credit card fraud detection mechanisms.

Keywords: - credit card fraud detection methods; credit card fraud; E-commerce

I. INTRODUCTION

E-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking. [4] Credit Card Fraud is one of the largest threats to business organizations today. However, to overpower the fraud effectively, 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. [1] 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.

Types of Frauds:-

The credit-card fraud is divided into two types;

(i) The online credit card fraud (or no card present fraud) and
(ii) The offline credit card fraud (card present fraud)

The online credit-card fraud (also known as cyber credit card fraud) is committed with no presence of a credit-card but instead, the use of a credit-card information to make electronic purchase for goods and services on the internet. [4] The offline credit-card fraud is committed with the presence of a credit-card which in most cases have been stolen or fake and thereby used at a local store or a physical location for the purchase or some goods or services.

There are many cyber credit card fraudsters. Some of them are [1]**:**

(i) ***Credit-card information buyers*:** these are the fraudsters who either have little or no professional computer skills like computer programming, networking etc. They buy stolen or hacked credit card information on an illegal credit card sales website, with the intension of buying goods and products online.

(ii) ***Physical credit-card stealers***: these are the fraudsters who physically steal credit cards may be by pick pocketing and use the information on it for making e-payment on internet for shopping.

(iii) ***Black hat hackers****:* "Black hat hackers" which are also known as a cracker are those who violate computer security with malevolent intentions or for personal gains. They choose their targets using a two-pronged process known as the "pre-hacking stage"; which includes Targeting, Research and Information Gathering and finally finishing the Attack. These hackers are highly skilled in Computer Programming and Computer Networking and with such skills they can barge in a network of computers. The main purpose of their act of intrusion or hacking is to steal personal or private information such as credit-card information, bank-account information, etc. for their own personal gains.

II. 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. [1] Here are some of the different techniques which are used for credit-card fraud information theft**.**

(i) 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. 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. 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.

(ii) 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. 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. 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.

(iii) 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. 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. 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.

(iv) Physically stolen credit-card information: The fraudsters can steal the credit card and use the information to buying goods and products online.

(v) 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.

III. Credit Card Fraud Detection Methods

On doing the literature survey of various methods for fraud detection we come to the conclusion that to detect credit card fraud there are a lot of approaches.

- A Hybrid Approach Using Dempster-Shafer Theory and Bayesian Theory.
- Blast-Ssaha Hybridization
- Hidden Markov Model.
- Genetic Algorithm
- Neural Network
- Bayesian Network
- K- nearest neighbor algorithm
- Stream Outlier Detection based on Reverse K-Nearest Neighbors(SODRNN)
- Fuzzy Logic Based System
- Decision Tree
- Fuzzy Expert System
- Support Vector Machine
- Meta Learning Strategy

(I) A HYBRID APPROACH USING DEMPSTER-SHAFER THEORY AND BAYESIAN LEARNING

This Credit card fraud detection system is based on the integration of three approaches, i.e., rule-based filtering, Dempster–Shafer theory and Bayesian learning. Dempster's rule is applied to combine and associate multiple evidences from the rule-based component for calculation of initial belief about every incoming transaction. [10] The suspicion score is updated through Bayesian learning using history database of both genuine cardholder as well as fraudster. THD is the transaction repository component of the above fraud detection system. History records of both fraudulent as well as genuine transactions are used to construct systems which allow us to extract characteristic information of the two groups from available data. For performing this, a good transactions history (GTH) for individual customers from their past behavior and a generic fraud transactions history (FTH) from different types of past fraud data is build.

Each history transaction is represented by a set of attributes which contains information like card number, transaction amount and time since the last purchase was made. While observing the current spending behavior on a credit card, the past spending behavior in terms of the frequency of transactions on that card are also accumulated and analyzed. The transaction amount information in the THD is needed for detecting the outliers. [10] The FDS architecture is flexible so that new rules using any other effective technique can be included at a later stage to further grow the rule-based component. Bayesian learning contributes to the FDS by helping it to dynamically adapt to the changing behavior of genuine customers as well as fraudsters over time. The Dempster–Shafer theory gives good performance, especially in terms of true positives, and Bayesian learning helps to further improve the system accuracy.

It has high accuracy. It reduces false alarms and improves detection rate and also applicable in E-Commerce. But it is very expensive and its processing Speed is also low.

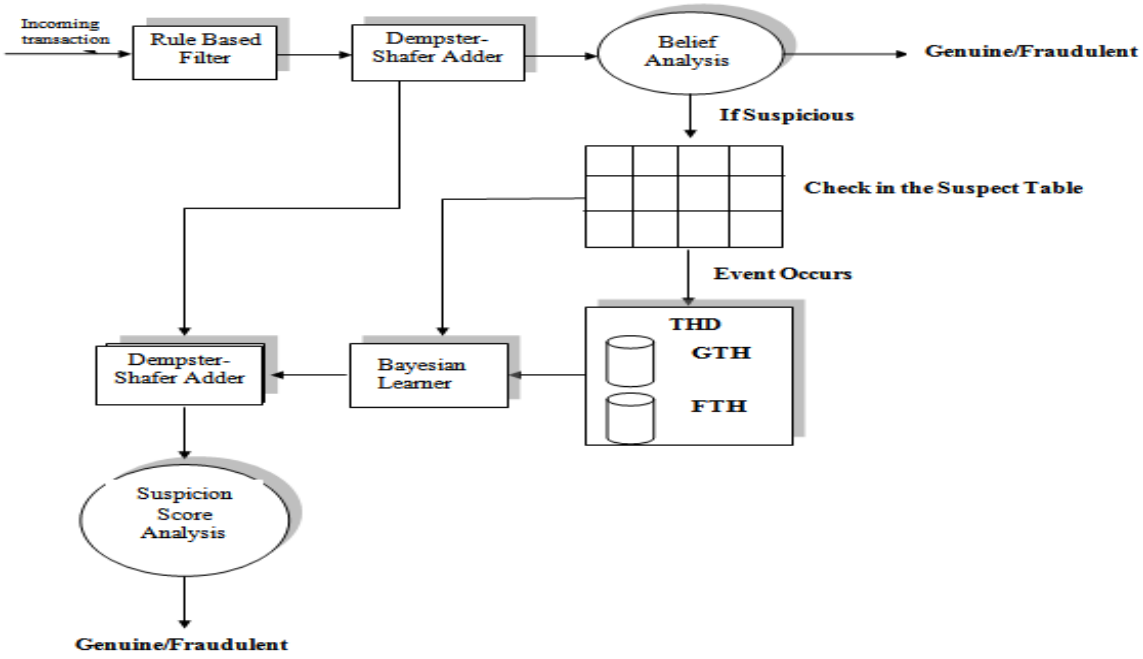

Fig 1: Block Diagram of Fraud Detection System Using Dempster-Shafer Theory and Bayesian Network.

(II) BLAST-SSAHA HYBRIDIZATION:

In this method of detecting fraud, the hybridization of BLAST and SSAHA algorithm is employed. [6] It is therefore known as BLAH-FDS Algorithm. BLAST and SSAHA algorithm are very efficient sequence alignment algorithms therefore these two algorithms are used since the alignment of sequences is an efficient technique to examine the spending behavior of customers. [7] BLAH-FDS is a two-stage sequence alignment algorithm in which a profile analyzer (PA) compares and determines the similarity of an incoming sequence of transactions on a given credit card with the genuine cardholder's past spending sequences. If there are any unusual transactions found by the profile analyzer, then they are passed to a deviation analyzer (DA) for any possible alignment with past fraudulent behavior. The final judgment about the nature of the transaction is taken on the basis of the observations made by these two analyzers.

When a transaction is carried out, the incoming sequence is merged into two sequences known as time-amount sequence (TA). The TA is aligned with the sequences that are related to the credit card in Customer Profile Database (CPD). This alignment process is done using BLAST SSAHA algorithm which increases the speed of the alignment process. If TA contains genuine transaction, then it would align well with the sequences in CPD. If there is any fraudulent transaction in TP, then mismatches occur in the alignment process. This mismatch produces a deviated sequence D which is aligned with Fraud History Database (FHD). [8] A large similarity between deviated sequence D and FHD confer the presence of fraudulent transactions. PA evaluates a Profile score (PS) according to the similarity between TA and CPD. DA evaluates a deviation score (DS) according to the similarity between D and FHD. The FDM finally raises an alarm if the total score (PS - DS) is below the alarm threshold (AT). The performance of BLAHFDS is good and it results in high accuracy. Also the processing speed is fast enough for on-line detection of credit card fraud. It enumerates frauds in telecommunication and banking fraud detection. But it does not detect cloning of credit cards.

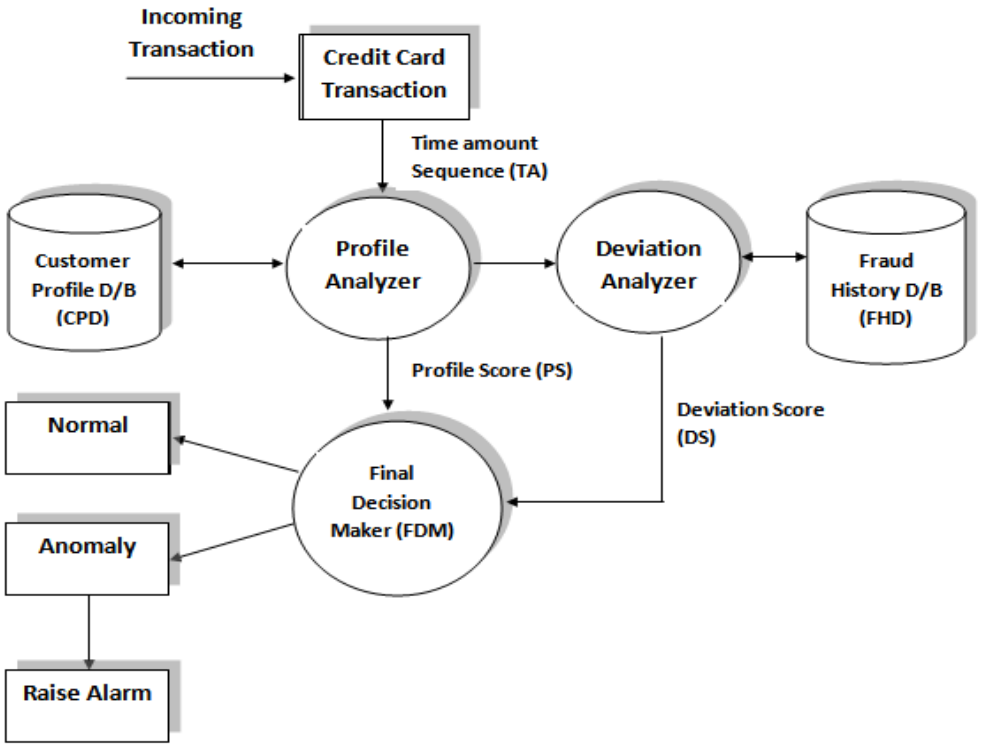

Fig 2: Architecture of BLAST-SSAHA Fraud Detection System

(III) HIDDEN MARKOV MODEL (HMM) :

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. [2] In a specific state a possible outcome or observation can be produced which is associated symbol of observation of probability distribution. HMM categorizes card holder's profile as low, medium and high spending based on their spending behavior 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.[3] 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 behavior while doing online shopping.

(IV) CREDIT CARD FRAUD DETECTION USING GENETIC ALGORITHM:

The Genetic algorithms are evolutionary algorithms which aim to obtain the better solutions to technically eliminate the fraud, a high importance have been given to develop secure and efficient e-payment system to detect whether a transaction is fraudulent or not.[8]During a credit card transaction, the fraud has to be deducted in real time and the number of false alerts are being minimized by using genetic algorithm. The fraud that is detected is based on the customer's behavior. [15]

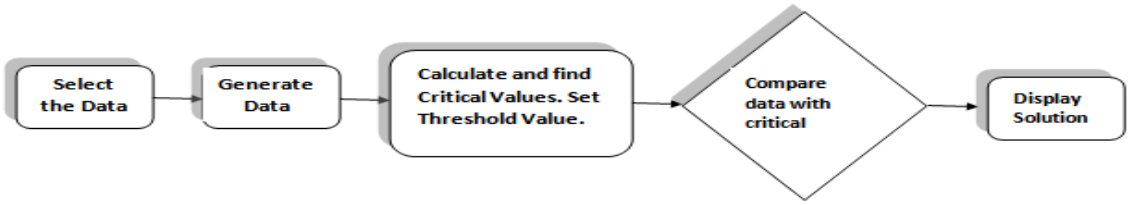

Fig 3: A simple Method Of Genetic Algorithm

Genetic algorithm procedure is repeated until a pre-specified number of iterations has passed, and the best solution is found. It is a parametric procedure and it should be problem undertaken to get a better performance. [15] The list of the parameters and the settings are needed to generate fraud transactions.Such parameters are needed to compute the critical values, to calculate the Credit Card usage frequency count, Credit Card usage location, Credit Card overdraft, current bank balance, average daily spending etc.

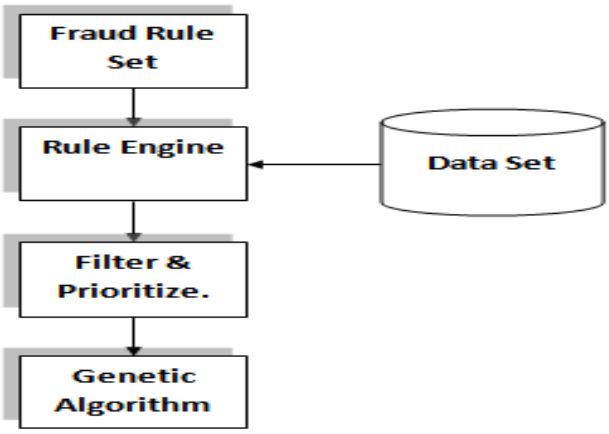

Fig 4: System Design

The aim is to obtain the better and optimal solutions.If this algorithm is applied to bank credit card fraud detection system, the probability of fraud transactions can be predicted soon after credit card transactions are done by the banks. And a series of anti-fraud strategies can be adopted to prevent banks from great losses before and reduce risks.

(V) STREAM OUTLIER DETECTION BASED ON REVERSE K-NEAREST NEIGHBORS(SODRNN)

SODRNN, standing for Stream Outlier Detection based on Reverse k Nearest Neighbors. This algorithm consists of two procedures: the Stream Manager and the Query Manager. Also the whole window should be allocated in the memory. [11] The Stream Manager receives the incoming data stream objects and efficiently updates the current window. When a new stream object comes, it only update the knnlist and rknnlist of the influenced objects in the current window, in order to maintain current window perfectly rather than all the data stream objects in the current window. When the new incoming object is inserted, it needs only one pass of scan to the current window to find all objects whose k nearest neighbors are influenced. The updating of the knnlists of the influenced objects in the current window can update their rknnlists at the same time. [11] The deletion of the expired object needs only update the rknnlists of the influenced objects in the current window according to its knnlist, and then update the knnlists of the influenced objects in the current window according to its rknnlist. When a user demands a query of the top n outliers, the Query Manager will make a scan of the current window and return n objects whose RNNk(p) is small as outliers of the query.

This algorithm reduces the number of scans to only one. Credit card validation checks and detects errors in a sequence of numbers therefore it detects valid and invalid numbers very easily.

(VI) ARTIFICIAL NEURAL NETWORK:

Artificial Neural Networks (ANN) is applied for detecting fraud, mainly in the context of supervised classification. Artificial neural network (ANN) can be used in the recognition of characteristics timely and make predictions. [12] The use of neural networking are motivated by the fact that it simulates the brain especially pattern recognition and associative memory. The neural network recognizes similar patterns, predicts future values or events based upon the associative memory of the patterns it has learned. These models are able to learn from the past and thus, improve their results as the time passes. They can also extract rules and predict future activity based on the current situation. By employing neural networks effectively, banks can detect fraudulent use of a card, faster and more efficiently.

In more practical terms neural networks are non-linear statistical data modeling tools. [12]They are used to model complex relationships between inputs and outputs and to find patterns in data.

There are two phases in neural network:

a) *Training phase and*
b) *Recognition Phase.*

Learning in a neural network is called training. There are two main types of Neural Network training methods:

a) *Supervised and*
b) *Unsupervised.*

In supervised training, samples of both fraudulent and non-fraudulent records are used to create models. On the other hand, unsupervised training simply looks for those transactions, which are most dissimilar from the normal ones. Also the unsupervised techniques do not need the previous knowledge of fraudulent and non-fraudulent transactions in database. NNs can produce best result for only large dataset of transactions. And they need a long training dataset.

Two types of neural network are used in credit card fraud detection system:

(i) *Back propagation neural network (BPNN)*

It is the most popular learning algorithm to train the neural network. It is a multi-stage dynamic system optimization method that minimizes the objective function. It is a supervised learning method and is a generalization of the delta rule. It is most useful for the feed-forward network which is network that has no feedback. It consists of three layers input, hidden and output layers. The incoming series of transactions passes from input layer through hidden layer and then to the output layer. This is also known as forward propagation. The input data is repeatedly feed to the neural network. With each presentation the output of the neural network is compared to the desired output and an error is computed. This error is then feed-back (back propagated) to the neural network and used to adjust the weights such that the error decreases with each iteration and the neural network gets closer to producing the desired output. This process is known as training. To train the NN so that it can be used for a credit card system last one or two year data is required of all the consumers. [11] During training, the network is trained to associate outputs with the input patterns. After training when the network is used, it identifies the input pattern and tries to give output the associated output pattern. The power of neural networks is tested when a pattern that has no output associated with it, is given as an input. When credit card is being used by an unauthorized user the neural network based fraud detection system check for the pattern used by the fraudster and matches with the pattern of the original card holder on which the neural network has been trained, if it recognizes a pattern match, then neural network declare the transaction ok. [12]

However, this algorithm requires long training times, extensive testing, retraining of parameters, such as the number of hidden neurons, learning rate and momentum, to determine the best performance.

(ii) *Self-Organizing Map neural network (SOMNN)*

It is an unsupervised neural network learning method. In credit card fraud detection SOM has been used for forming customer profiles and analyzing fraud patterns.[5] In this method the transaction data is first identified and pre processed. These data are fed in to SOM as input and weights of the neurons are adjusted iteratively. At the end of the

training, the data is classified into genuine and fraudulent sets through the process of self-organization. This network contains two layers of node:

a) an input layer and

b) a mapping layer

in the shape of a two-dimensional grid.

The purpose of these layers is to:

(i) classify and cluster the input data

(ii) detect and derive hidden patterns in input data

(iii) act as a filtering mechanism for further layers.

In this technique all transactions in the payment system are classified into genuine and fraudulent sets by following the two hypotheses:

1. If a new incoming transaction is similar to all previous transactions from the fraudulent set, then it is consider fraudulent.
2. If a new incoming transaction is similar to all previous transactions from genuine set, and then it is considered genuine.

(VII) DECISION TREES AND SUPPORT VECTOR MACHINES:

Classification models which are based on decision trees and support vector machines (SVM) are developed and applied on credit card fraud detection problem. In this technique, each account is tracked separately by using suitable descriptors, and the transactions are attempted to be identified and indicated as normal or legitimate. The identification is based on the suspicion score produced by the developed classifier model. When a new transaction is proceeding, the classifier can predict whether the transaction is normal or fraud.

In this approach, firstly, all the collected data is pre-processed before we start the modeling phase. Since, the distribution of data with respect to the classes is highly imbalanced, so stratified sampling is used to under sample the normal records so that the models have chance to learn the characteristics of both the normal and the fraudulent record's profile. [13] To do this, the variables that are most successful in differentiating the legitimate and the fraudulent transactions are founded. Then, these variables are used to form stratified samples of the legitimate records. Later on, these stratified samples of the legitimate records are combined with the fraudulent ones to form three samples with different fraudulent to normal record ratios. The first sample set has a ratio of one fraudulent record to one normal record; the second one has a ratio of one fraudulent record to four normal ones; and the last one has the ratio of one fraudulent to nine normal ones. [13]

The variables which are used make the difference in the fraud detection systems. Our main motive in defining the variables that are used to form the data-mart is to differentiate the profile of the fraudulent card user from the profile of legitimate card user. The results show that the classifiers of SVM and other decision tree approaches outperform SVM in solving the problem under investigation. However, as the size of the training data sets become larger, the accuracy performance of SVM based models becomes equivalent to decision tree based models, but the number of frauds caught by SVM models are still less than the number of frauds caught by decision tree methods.

(VIII) FUZZY LOGIC BASED SYSTEMS:

(i) Fuzzy Neural Network

The purpose of Fuzzy neural networks is to process the large volume of information which is not certain and is extensively applied in our lives. Syeda et al in 2002 proposed fuzzy neural networks which run on parallel machines to speed up the rule production for credit card fraud detection which was customer-specific. His work can be associated to Data mining and Knowledge Discovery in data bases (KD). In this technique, he used GNN (Granular Neural Network) method that uses fuzzy neural network which is based on knowledge discovery (FNNKD), to train the network fast and how fast a number of customers can be processed for fraud detection in parallel. [8] A transaction table is there which includes various fields like the transaction amounts, statement date, posting date, time between transactions, transaction code, day, transaction description, and etc. But for implementation of this credit card fraud detection method, only the significant fields from the database are extracted into a simple text file by applying suitable SQL queries. In this detection method the transaction amounts for any customer is the key input data. This preprocessing of data had helped in decreasing the data size and processing, which speeds up the training and makes the patterns briefer. In the process of fuzzy neural network, data is classified into three categories-

1. First for training,
2. Second for prediction, and
3. Third one is for fraud detection.

The detection system routine for any customer is as follows:

- Preprocess the data from a SQL server database.
- Extract the preprocessed data into a text file.
- Normalize the data and distribute it into 3 categories (training, prediction, detection)

For normalization of data by a factor, the GNN has accepted inputs in the range of 0 to 1, but the transaction amount was any number greater than or equal to zero because for a particular customer only the maximum transaction amount is considered in the entire work. In this detection method, there are two important parameters that are used during the training that are:

- training error and
- Training cycles.

With increase in the training cycles, the training error will be decreased. The accuracy of the results depends on these parameters. In prediction stage, the maximum absolute prediction error is calculated. [8]In fraud detection stage also, the absolute detection error is calculated and then if the absolute detection error is greater than zero then it is checked to see if this absolute detection error is greater than the maximum absolute prediction error or not. If it is found to be true then it indicates that the transaction is fraudulent otherwise transaction is reported to be safe. Both training cycles and data partitioning are extremely important for better results. The more there is data for training the neural network the better prediction it gives. The lower training error makes prediction and the detection more accurate. Higher the fraud detection error is, greater there is possibility of the transaction to be fraudulent.

(ii) Fuzzy Darwinian System

This technique uses genetic programming to develop fuzzy logic rules which 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. The developed system comprises of two main elements [8]:

(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. The genotypes and phenotypes of the GP System have 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: safe and suspicious. 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.

(IX) FRAUD DETECTION USING META-LEARNING:

Meta-learning is a strategy that provides the means of learning of how to combine and integrate a number of separately learned classifiers or models into one. Therefore, a *meta-classifier* is trained relatively with the predictions of the *base classifiers.* [14] This system has two key component technologies:

(i) ***Local fraud detection agents*** that learn how to detect fraud and provide intrusion detection services within a single collective information system, and
(ii) ***Meta-learning system*** that combines the collective knowledge attained by individual local agents. This is a secure and integrated system.

Once derived *local classifier agents* or *base classifiers* are produced at some sites, two or more such agents may be composed into a new classifier agent i.e. a *meta-classifier* by a *meta-learning agent*. [14] This meta-learning system will allow financial institutions to share their models of fraudulent transactions by exchanging classifier agents in a secured agent system without disclosing their patent data. In this way their competitive and legal restrictions can be met, and they can still share information.

IV. CONCLUSION AND FUTURE WORK

There are various methods of detecting a credit card fraud. In this paper, we've presented a comparative study of some of the fraud detection methods based on credit card. If one of these or combination of algorithms is put into practical use for bank credit card fraud detection system, the probability of fraud transactions can be known in advance soon after the credit card transactions are carried by the banks. A series of anti-fraud strategies can be adopted to prevent the banks from great losses sooner and reduce the risks. This paper gives contribution towards the effective ways of credit card fraud detection. A comparison table is prepared to compare various credit card fraud detection mechanisms based on some parameters such as, accuracy, speed and cost.

Methods	**HMM**	**FDS**	**DST & BN**	**BSH**	**GA**	**SODRNN**	**ANN**	**Meta-learning**	**FNN**	**SVM**	**SOM**
Accuracy	LOW	VERY HIGH	HIGH	HIGH	Medium	Medium	Medium	HIGH	GOOD	Medium	Medium
Speed of detection	FAST	VERY LOW	LOW	GOOD	GOOD	GOOD	FAST	LOW	VERY FAST	LOW	FAST
Cost	HIGH Expensive	HIGH Expensive	Expensive	Moderate	Inexpensive	Expensive	Expensive	Expensive	Expensive	Expensive	Expensive

Table 1:- Comparison of different Fraud detection methods.

All these techniques of credit card fraud detection discussed in this survey paper, have its own weaknesses as well as strengths. Thus, this survey enables us to create a hybrid approach for developing some effective algorithms which can perform well with minimum costs and higher accuracy.

ABBREVIATIONS:

HMM- Hidden Markov Model

FDS- Fuzzy Darwinian System

DST- Dempster-Shafer Theory

BN- Bayesian Network

BSH- Blast-Ssaha Hybridization

GA- Genetic Algorithm

SODRNN- Stream Outlier Detection Based On Reverse K-Nearest Neighbors

ANN- Artificial Neural Networks

FNN- Fuzzy Neural Network

SVM- Support Vector Machine

SOM- Self Organizing Map Neural Network

REFERENCES

[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.

