*International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868*
*Foundation of Computer Science FCS, New York, USA*
*Volume 10 – No.4, January 2016 – www.ijais.org*

# A Survey on Different Approaches used for Credit Card Fraud Detection

Anika Nahar
Department of CSE
Ahsanullah University of Science and Technology
Dhaka-1208, Bangladesh

Sharmistha Roy
Department of CSE
Ahsanullah University of Science and Technology
Dhaka-1208, Bangladesh

Syeda Shabnam Hasan
Department of CSE
Ahsanullah University of Science and Technology
Dhaka-1208, Bangladesh

## ABSTRACT

Now-a-days the use of credit card has dramatically increased due to rapid growth of e-commerce technology. It is the most popular mode of payment for both online as well as regular purchase.Credit card fraud has become a significant problem, as companies, banks other financial institutions faces huge amount of losses annually because of fraudulent activities of fraudsters. So the main aim of credit card fraud detection system is to learn different patterns used in previous frauds and train itself to identify fraudulent and non fraudulent transactions. In this paper a survey on different techniques used in credit card fraud detection such as Neural Network,Bayesian Network, Decision Trees, Hidden Markov Model, Support Vector Machines, Meta Learning, Blast-SSaha Algorithm, Fuzzy System with Neural Network, Fuzzy Darwinian System, and Genetic Algorithm is demonstrated.

## Keywords

Credit Card Fraud, Neural Network, Bayesian Network, Decision trees, Support Vector Machine, Genetic Algorithm, Hidden Markov Model, Meta Learning, Fuzzy Darwinian System.

## 1. INTRODUCTION

Credit card fraud can be defined as unauthorized use of credit card for transactions while the owner of the card and the card issuer bank are not aware of the fact that the card is being used. With rapid growth of technology, the fraudsters also change their technologies and patterns of fraudulent activities.Frauds can be broadly classified into three categories,i.e., traditional card related frauds, merchant related frauds and Internet frauds[1]. The fraudulent transactions are dispersed with non-fraudulent transactions and often simple pattern matching techniques are not sufficient to detect those fraudulent transactions accurately. So efficient technique need to be implemented in every bank or financial institutions to detect fraudulent transactions as early as possible to minimize their losses.

## 2. TECHNIQUES

### 2.1 Neural Network

Neural network is a conceptual model which is inspired by the structure and functional aspects of human brain. Human brain learns from the past experience and apply its knowledge or experience in making the decision in daily life problem and thus improves result as the time passes, the same technique is applied with the credit card fraud detection using Artificial Neural Network [2]. The neural network recognizes similar pattern, predict future values based on patterns it has learned from the past [3].

There are two distinct types of neural network learning methods:

a. Supervised

b. Unsupervised

### *2.1.1 Supervised Learning*

In supervised learning, the neural network model is trained about pattern of both fraudulent and non-fraudulent transactions faced by a particular bank previously.

### *2.1.1.1 Back Propagation Neural Network*

The most popular supervised learning algorithm to train the neural network is back propagation neural network. It is consist of 3 layers; input, hidden and output layer. It is applicable in feed forward network , means there is no recurrent loops .The incoming sequence of transactions propagates from input layer to hidden layer and then output layer. The output layer of the network is compared with the desired output given by the supervisor and for each output node the error is calculated [4]. Then the error is back propagated to the hidden layer where for each node its effect to the error is calculated and used to adjust the weights so that error is minimized in next iteration. To train the neural network so that it can be used for a credit card system last one or two year data is required [5].

### *2.1.2 Unsupervised Learning*

In unsupervised learning the previous knowledge of fraudulent and non-fraudulent transactions is not required, it find transactions that are not similar to normal ones.

### *2.1.2.1 Self-Organizing Map Neural Network (SOMNN)*

Kohonen introduced self-organizing map which is an unsupervised learning method. It has two layers of nodes- an input layer and a mapping layer in the shape of a two dimensional grid.

First the transaction data in preprocessed and fed in to SOM as input. The process is called self-organization because of iterative tuning weight of neuron [6]. At the end of training data is classified into genuine and fraudulent sets through the process of self-organization [7].

The following two hypotheses are considered as a basis for classification [8]:

1. If a transaction is similar to all previous transactions, which are carried out earlier by the cardholder, the

transaction is classified as legal.

2. If a transaction is similar to earlier executed fraudulent transactions, then it is classifies as fraudulent.

## 2.2 BAYESIAN NETWORK

The Bayesian Network was first introduced by Cooper and Herskovits in 1992.It is based on Bayes rule and these networks are very effective for modeling situations where some information is already known and incoming data is unsure or partially un available,[9].the goal of using Bayes Rules is to correctly predict the value of a discrete class given a set of attributes,[10][11].

In 1993, SAM MAES [12] suggested BN for credit card fraud detection. In the process, at first, Bayesian Network is constructed to model behavior of fraudulent user and next model is constructed taking the user as legitimate. Then transactions are classified as fraudulent or non-fraudulent by these networks. Bayes rule generates the probability for fraud for any incoming transaction,[13].Bayesian Network needs training of data to operate and require high processing speed.BN is more accurate and much faster than neural network,[14].

### *2.2.1 Combining with Dempster-Shafer theory*

A combination of Dempster-Shafer theory and Bayesian learning is used for Credit Card Fraud Detection [1]. Dempster-Shafer theory is used to combine different types of evidences and Bayesian learning is used to measure evidences supporting alternative hypothesis and arriving at optimal decisions.

The Fraud Detection System works by four components – 1) Rule-based filter 2) Dempster-Shafer adder 3) Transaction history database 4) Bayesian learner. The incoming transactions are classified by applying rules like address mismatch, outlier detection etc. to initially separate out most easily recognizable genuine transaction from the rest. Address mismatch is based on when billing address doesn't match shipping address and there are many outlier detection methods [3] but in [1], DBSCAN (Density-based spatial clustering of applications with noise)[2]is used which is based in the idea that a particular point belongs to a cluster, if it is near a lots of point to the cluster inside radius of that cluster, [5]. Then the filtered evidence goes through the Dempster-Shafer adder to combine these evidences from the previous rules and computes an overall belief value for each transaction, initially classifying each transaction as normal, abnormal or suspicious.

THD orTransaction repository component is maintained to record both fraudulent and genuine transaction to construct characteristic models. For each individual customer, a good transaction history (GTH) database of their past spending behavior is maintained, also there is a generic fraud transaction history (FTH) database from different types of past fraud data. The THD is required to detect patterns like time of the day of purchasing, spending amount, bought products. It is like a picture of fraudster behavior [4]. Suspicion score in THD of each card is updated based on time since last purchase,[1].The proposed FDS is shown in Figure 1.

So, Bayesian learning is used to update the suspicious score of each transaction according to GTH and FTH.This approach is highly accurate. It reduces false alarms which is a big improvement for detection of large set of transactions. But it is very expensive and its processing speed is also low.

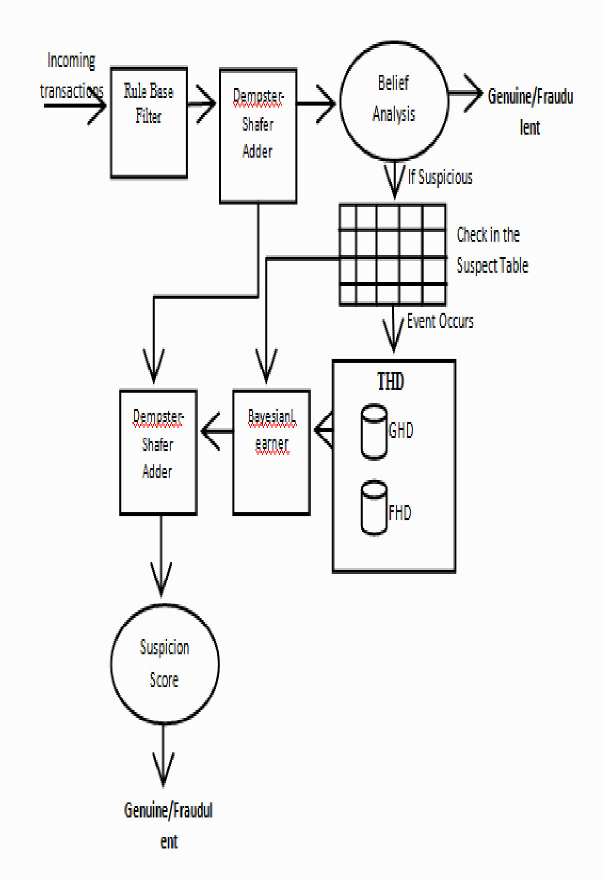

**Fig 1: Block Diagram of Fraud Detection System Using Dempster-Shafer Theory and Bayesian Network.**

## 2.3 Decision Trees

A decision tree is a kind of tree structure for separating agiven set of records into mutually exclusive subgroups. Decision trees are used for classification in which a new transaction has been given for which class label is unknown(means it is unknown whether it is fraudulent or legitimate) and the transaction value is tested against the decision tree [15].

In credit card fraud detection using decision tree there are 2 phases. First to generate a decision tree from given training data and then applying these decision rules to determine the class of any new transaction [16]. It starts form the root node then each node is split into child nodes in a binary or a multi split based on the attribute value separating the records at best. This is done recursively until the number of records for a node is too small. Each decision tree method uses its own splitting algorithms and splitting matrices[17].Some well-known tree algorithms are ID3, C5.0 and C&RT. Then for each new transaction, it must be matched to the decision table to be matched with previous generated rules to find the fraudulent or genuine transaction[18].This model is very fast and has a high flexibility [19].

## 2.4 Hidden Markov Model

A Hidden Markov Model (HMM) is a double embedded stochastic process with two hierarchy levels. It can be used to model complicated stochastic process as compared to a traditional Markov Model. In a particular state, an outcome or observation can be generated according to an associated probability distribution. It is only the outcome & not the state that is visible to an external observer.

In [20], HMM uses three behaviors of cardholder: low spending, high spending and medium spending. To find any one of the observation symbols to these behaviors corresponding to individual cardholder's transactions, k–means clustering algorithm is used [21] on past transactions. Then Baum-Welch algorithm [22] is used based on the clustering probability of each clusters to train the HMM. Then to detect fraud, the probability of initial sequence of observation symbols is calculated. A new added transaction is determined to be fraudulent if the percentage change in probability is above empirically learned threshold by Baum-Welch algorithm. Finally, the performance is calculated by using TP & FP matrices and it is observed that accuracy of system is near 75% [23].

In [24] , a multiple semi hidden Markov Model is suggested to gather multiple observations to detect fraudulent user and Cuckoo Search algorithm is used for optimizing training value. The main idea is to liberate customers from the necessity of statistical know knowledge.

HMM keeps a log rather than checking original user every time. It releases the tedious work of employees & works as a transaction proof. HMM produces high false positive [25].

## 2.5 Support Vector Machines

SVM [26] is the best tool to use for classification of data. The main idea is to find a hyper plane as a segmentation of two classes of data to minimize the classification error. It can be used on small training set, it avoids over fitting [27].

### *2.5.1 Comparison with Decision Tree*

In [28], credit card fraud detection on real data is used by applying SVM & Decision Tree base classifier models.Each account is monitored separately attempted to be flagged as legitimate or abnormal based on a suspicion score. As the credit card data set is highly imbalanced, they are preprocessed by under sampling them using stratified sampling.

The variables used to differentiate the profile of fraudulent & genuine card usage are of all transactional statistics, regional statistics, daily amount statistics & daily number of transaction statistics. From these records three samples with different ratios of fraud & normal record are formed. These are in 1:1, 1:4, 1:9ratios. TheSVM and Decision tree is applied on training set & test set.SVM kernels used here are polynomial, sigmoid, radial and linear.The result shows that as training set size increases SVM reaches higher accuracy performance [29].

### *2.5.2 Based on Personalized Approach*

In [30], personalized model based on personal data collected by an online questionnaire system is used for applying SVM and Artificial Neural Network to classify & predict newtransaction data for few data present. Questionnaires are generated for collecting personal data like age, gender, transaction item etc.SVM kernels used are dot, polynomial &radial. The SVM is used to generate classifiers of the training data and applied on the test data to show the how accurately the classifier is optimized. Then SVM is applied on future data test accuracy.

### *2.5.3 Behavioral based Fraud Detection*

This model [31], is based on transactional behavior of cardholder directly or derived. His massive amount of data is handled by using effective feature extraction method for data reduction. Then the SVM is used for classification. Only the RBF kernel is used. LIBSVM is used for training the over fitting problem is solved by cross validation the confusion matrices is used for evaluating the fraud catching rate & false alarm rate. The proposed model efficiently finds out the most of the correct transaction up to 80%.

## 2.6 Meta-Learning

The term meta-learning wasintroduced by Chan and Stolfo [32], is a methodfor combining the outputs of multiple machine-learning techniquesin a self-adaptive way to improve accuracy. Themethod has since evolved into several active streams ofresearch in a variety of application domains [33][34].

### *2.6.1 Using Learning algorithms*

In [35] meta-learning system is used to combine the collective knowledge attained by individual local fraud detection agents. Once a local classifier or base classifier is produced at some sites then any two or more are composed into meta classifier. The experiments described in this paperfocus on local fraud detection (on data from one bank), with the aim to produce the best possible (local)classifiers. Intuitively, better local classifiers will lead tobetter global (meta) classifiers.in this paper several machine learning algorithms as well as meta learning strategies on real data of one year are tested. The learning algorithms were ID3, CART [36], Ripper [37], BAYES algorithms.Finally,Meta-learning with BAYES as a meta-learner to combinebase classifiers with the highest True Positive rateslearned from 50%/50% fraud distribution is the bestmethod found thus far,[38].This system allows financial institutions to share their models of fraudulent transactions by exchanging classifier agents in a secured agent infrastructure without disclosing their proprietary data.

## 2.7 Blast-SSaha Algorithm

BLAST stands for Basic Local Alignment Search Tool whereas SSAHA stands for Sequence Search and Alignment by Hashing Algorithm,[39].BLAST is used to determine similarity of incomingsequence of transactions with the genuine card holders whileSSAHA is used to give good results of alignment of longsequences,[40].BLAST consists of three steps. At first it compiles a list of high-scoring words from given query sequence of transaction. Secondly, each word is compared with database sequences and identical ones are recorded as hit. Thirdly every hit sequence is extended until the similarity score becomes less than the threshold value.The equal or greater than threshold scored extended segment pairs are called as HIGH SCORING SEGMENT PAIRs (HSPs). SSAHA has 2 stages: one for constructing a hash table from sequences in the database and another stage for searching words from hash table [41].

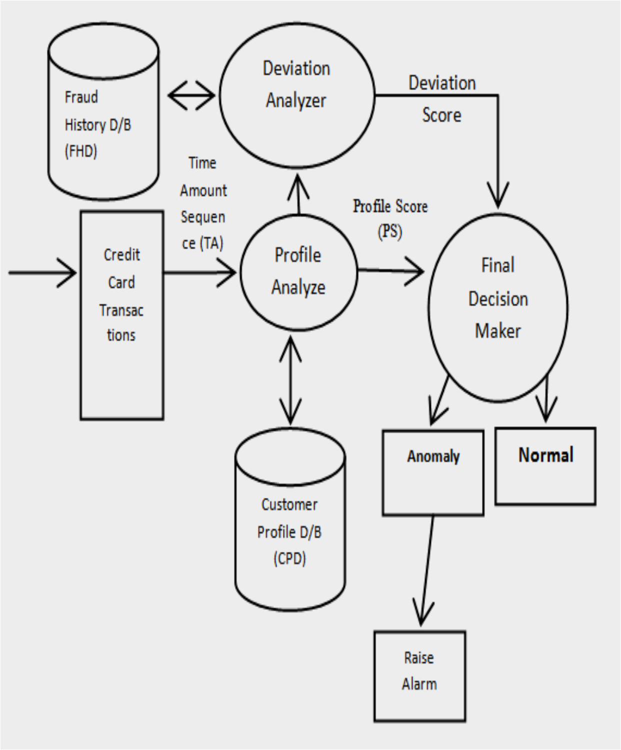

**Fig 2: Architecture of BLAST-SSAHA Fraud Detection System**

A BLAST-SSAHA Hybridization checks each new transaction to be fake or authentic. It creates a TIME AMOUNT (TA) sequence by merging the incoming sequence that is in the CUSTOMER PROFILE DATABASE for a particular card holder. Then, the PROFILE EXAMINER checks the incoming sequence with the genuine cardholder's previous spending sequence using TA and generates PROFILE SCORE (PS).If there is some deviation found by the PROFILE EXAMINER then this sequence goes to DEVIATION EXAMINER which generates DEVIATION SEQUENCE (DA) by comparing with FRAUD HISTORY DATABASE. These results in generating DEVIATION SCORE (DS) based on DA.Finally if the difference between PS and DS is found to be lesser than threshold then the transaction is blocked [42].Shown in Fig 2.

## 2.8 Fuzzy System with neural network

Fuzzy Neural Network can be used for pattern recognition if there doesn't exist any mathematical model of the given problem. A fuzzy system demand linguistic rules instead of learning examples as prior knowledge. The input and output variables have to be described linguistically. If the knowledge is incomplete, wrong or contradictory, then fuzzy system must be tunes. Since there is not any formal approach for it, the tuning is performed in a heuristic way [35].

Syeda et al in 2002 proposed fuzzy neural networks which run on parallel machine to speed up the rule production credit card fraud detection which was customer specific [36]. In this method Syeda et al used GNN (Granular Neural Network) method that uses fuzzy neural network based on knowledge discover (FNNKD), for how fast the network can be trained and how fast a number of customers can be processed for detection in parallel [37].

## 2.9 Fuzzy Darwinian System

Fuzzy Darwinian system uses genetic programming to evolve fuzzy logic rules which are capable of classifying credit card transactions into "suspicious" and "non-suspicious" classes. The evolutionary fuzzy system comprises of two main elements [38]:

1. A Genetic Programming (GP) search algorithm.
2. A fuzzy expert system.

After data is provided to the system in CSV files, the system first clusters the data using a one dimensional clustering algorithm(C-Link, S-Link, K-means) into three groups. Three membership functions are generated corresponds to the three groups where each membership function defines "degree of membership" in three fuzzy sets: low, medium and high. The GP engine is then seeded with random genotypes and evolution is initiated [31]. At the beginning of evolution random variable sized genotypes are created which are then mapped into phenotypes to obtain fuzzy rules. This system can classify credit card data into "suspicious" or "non-suspicious" one. When the customer's payment is not overdue or the number of overdue payment is less than three months, the transaction is considered as "non-suspicious", otherwise it is considered "suspicious" [38].

## 2.10 Genetic Algorithm

Genetic algorithm is an evolutionary algorithm which aims to obtain better solutions as time progress by technically eliminates the fraud, a high importance is given to develop efficient and secure e-payment system to detect if a transaction is fraudulent or not. It also been used in data mining mainly for variable selection and are mostly coupled with other data mining algorithms [39].

Flow of Genetic algorithm [40]:

- Initially the initial population is selected randomly from the sample space which has many populations.
- The fitness value is calculated for each chromosome in each population and is sorted out.
- In selection process two parent chromosomes are selected through tournament method.
- The Crossover forms new offspring (children) from the parent chromosomes using single point probability.
- Mutation mutates the new offspring using uniform probability measure.
- In elitism selection the best solution are passed to the further generation.

GA has been used in credit card fraud detection for minimizing the wrongly classified number of transactions [41]. And is easy accessible for computer programming language implementation, thus, make it strong in credit card fraud detection. A system is designed in paper [39] to detect credit card fraud and examine the result based on the principle of GA. If this algorithm is applied into bank credit card fraud detection system, the probability of fraud transactions can be predicted soon after credit card transactions by the banks. And a series of anti-fraud strategies can be adopted to prevent banks from great losses before and reduce risks [42].

## 3. CONCLUSION

In this paper various techniques used in credit card fraud detection system have been discussed. If one of these or combination of these techniques is implemented in credit card issuing bank , then fraudulent transactions will be minimized and the probability of fraud transactions can be known as early as possible, thus a series of anti-fraud strategies can be adopted to prevent fraudulent activities which reduce the losses.

## 4. REFERENCES

[1] SuvasiniPanigrahi, AmlanKundu, ShamikSural, A.K. Majumdar.2009. “Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning”, Information Fusion 10.

[2] M. Ester, H.P. Kriegel, J. Sander, X. Xu.1996.“A density-based algorithm for discovering clusters in large spatial databases with noise” .Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD).

[3] V. Hodge, J. Austin.2004. “A survey of outlier detection methodologies”. Journal of Artificial Intelligence Review 22 (2).

[4] R. Knight, 20 June, 2007. “Fraudsters favor brandy and one-way tickets”, Financial Times, UK. <http://www.ft.com/cms/s/728ff80c-1698-11da-8081-00000e2511c8.html>.

[5] Visualizing DBSCAN Clustering. http://www.naftaliharris.com/blog/visualizing-dbscan-clustering/

[6] NehaSethi, Anju Gera. 2014 . “A Revived Survey of Various Credit Card Fraud Detection Techniques”.

[7] Y. Sahin and E. Duman, “Detecting Credit Card Fraud by Decision Trees and Support Vector Machines”.

[8] Cortes, C., Vapnik, V. 1995. “Support vector network. Machine Learning”. Vol: 20 pg.(273–297).

[9] Chen, R.-C., Luo, S.-T., Liang, X. and Lee, V. C. S. 2005. “Personalized approach based on SVM and ANN for detecting credit card fraud”.

[10] V. Dheepa and R. Dhanapal. “Behavior based Credit Card Fraud Detection using Support Vector Machines”.

[11] AvinashIngole, Dr. R. C. Thool. 2013. “Credit Card Fraud Detection Using Hidden Markov Model and Its Performance”, Volume 3, Issue 6, International Journal of Advanced Research in Computer Science and Software Engineering.

[12] A. K. Jain, M. N. Murty, and P.J Flynn. “Data Clustering: A Review”. ACM comput. Surv.,31(3):263-323 September 1999

[13] J.A.“A gentle tutorial of the EM algorithm and its application to Parameter Estimation for Gaussian mixture and Hidden Markov Models”.

[14] Ganesh Kumar.Nune† and P.VasanthSena . “Novel Artificial Neural Networks and Logistic Approach for Detecting Credit Card Deceit”.

[15] Philip K. Chan and Salvatore J. Stolfo (1993), Toward Parallel and Distributed Learning by Meta-learning, in Working Notes AAAI Work. Knowledge Discovery in Databases (pp. 227-240)

[16] Brazdil, P., Giraud-Carrier, C., Soares, C., and Vilalta, R. 2008.Metalearning: Applications to Data Mining, Berlin: Springer-Verlag.

[17] Vilalta, R., and Drissi, Y. 2002. “A Perspective View and Survey of Meta-Learning,” Artificial Intelligence Review (18), pp. 77-95.

[18] Salvatore J. Stofo.Credit Card Fraud Detection Using Meta-Learning:Issues and Initial Results.

[19] W. Buntime and R. Caruana .1991. Introduction to IND and Recursive Partitioning, NASAA Research Center.

[20] Philip K. Chan and Salvatore J. Stolfo .1997. Metrics for Analyzing the Integration of Multiple Learned Classifiers

[21] William W. Cohen .1995. Fast Effective Rule Induction,in Machine Learning: Proceeding of the Twelfth International Conference, Lake Taho, California, 1995.

[22] BhaviyaRajesh Gandani. “Credit Card Fraud Detection Using BLAST-SSAHA Hybridization & Hidden Markov Model”.

[23] Avanti H. Vaidya , S. W. Mohod. “Internet Banking Fraud Detection using HMM and BLAST-SSAHA Hybridization”.

[24] AmlanKundu, SuvasiniPanigrahi, ShamikSural and Arum K. Majumdar. 2009. “BLAST-SSAHA hybridization for credit card fraud detection”, IEEE Transactions on Dependable and Secure Computing, Vol. 6, No. 4.

[25] Eugene Charniak.1991. “Bayesians networks without tears”. AI Magazine.

[26] S. Maes, K. Tuyls, B. Vanschoenwinkel, B. Manderick.1993. “Credit card fraud detection using Bayesian and neural networks”. Proceedings of the First International NAISO Congress on Neuro Fuzzy Technologies.

[27] Sherly K.K .2012. “A comparative assessment of supervised data mining techniques for fraud prevention”. TIST.Int.J.Sci.Tech.Res, Vol.1.

[28] Manoel Fernando, Xidi Wang, Alair Pereira do Lago.2008. “Comparison with Parametric Optimization in Credit Card Fraud Detection”.

[29] Varunchandola, Arindambanerjee, and Vipinkumar. “Anomaly Detection: A Survey. ACM Computing Surveys, Vol. 41, No. 3.

[30] J Han, M Kamber, J Pei. 2011. “Data Mining Concepts and Techniques”.

[31] RaghavendraPatidar, Lokesh Sharma “Credit Card Fraud Detection using Neural Network” International journal of Soft Computing(IJCSE),Volume 32,38,Issue 2011..

[32] DiptiThakur,Shalini Bhatia. 2002. “Distribution Data Mining approach to Credit card Fraud Detection”. SPIT IEEE Colloquium and International Conference, Volume 4.

[33] Suman,ResearchScholar,GJUS&THisar ,HCE Sonepat

,MitaliBansal, Mtech. C.S.E, HCE Sonepat“Survey Paper on Credit Card Fraud Detection ”

[34] vladimirzaslavsky and annastrizhak"Credit card fraud detection using self organizing maps".

[35] http://www.scholarpedia.org/article/Fuzzy_neural_network

[36] MubeenaSyeda, Yan-Qing Zhang and Yi Pan “Parallel Granular Neural Networks for Fast Credit Card Fraud Detection”. In: Proceedings of the IEEE international conference (2002). vol 1; (572–577).

[37] MasoumehZareapoor, 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.

[38] Peter J. Bentley, *Jungwon Kim, **Gil-Ho Jung and ***Jong-Uk Choi, “Fuzzy Darwinian Detection of Credit Card Fraud”.

[39] K.RamaKalyani, D.UmaDevi, “Fraud Detection of Credit Card Payment System by Genetic Algorithm”.

[40] SATVIK VATS*, SURYA KANT DUBEY, NAVEEN KUMAR PANDEY,“Genetic algorithms for credit card fraud Detection”.

[41] EkremDuman, M. HamdiOzcelik “Detecting credit card fraud by genetic algorithm and scatter search”. Elsevier, Expert Systems with Applications, (2011). 38; (13057–13063).

[42] Dipti D. Patil, V.M. Wadhai, J.A. Gokhale. 2010. “Evaluation of Decision Tree Pruning Algorithms for Complexity and Classification Accuracy”. International Journal of Computer Applications, Volume 11.