Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria

Masoumeh Zareapoor
Department of computer science,
Hamdard University,
New Delhi. India

Seeja.K.R
Department of computer science,
Hamdard University,
New Delhi. India

M.Afshar.Alam
Department of computer science,
Hamdard University,
New Delhi. India

ABSTRACT
Financial fraud is increasing significantly with the development of modern technology and the global superhighways of communication, resulting in the loss of billions of dollars worldwide each year. The companies and financial institution loose huge amounts due to fraud and fraudsters continuously try to find new rules and tactics to commit illegal actions. Thus, fraud detection systems have become essential for all credit card issuing banks to minimize their losses. The most commonly used fraud detection methods are Neural Network (NN), rule-induction techniques, fuzzy system, decision trees, Support Vector Machines (SVM), Artificial Immune System (AIS), genetic algorithms, K-Nearest Neighbor algorithms. These techniques can be used alone or in collaboration using ensemble or meta-learning techniques to build classifiers. This paper presents a survey of various techniques used in credit card fraud detection and evaluates each methodology based on certain design criteria.

General Terms: Financial fraud, Fraud detection, Classification methods

Keywords: credit card fraud, fraud detection

1. INTRODUCTION
Credit card fraud can be defined as the illegal use of any system or, criminal activity through the use of physical card or card information without the knowledge of the cardholder. The credit card is a small plastic card, which issued to user as a system of payment. With rapid growth in the number of credit card transactions, the fraudulent activities are also increased. The credit card may be physical or virtual [6][3][69][5]. In a physical-card, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. In the second kind of purchase, only some important information about a card such as card number, expiration date, secure code and etc, is required to make the payment. Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. In real life, fraudulent transaction are scattered with genuine transactions and simple pattern matching
Techniques are not often sufficient to detect those frauds accurately. Outlier detection is a data mining technique commonly used for fraud detection [36][38][53][16]. Outliers are data points that are inconsistent with the reminder of the dataset or deviate so much from other observations so as to arouse suspicion that they were generated by different mechanism. The outlier detection can be achieved through techniques like neural network, SOM, HMM etc.

2. FRAUD DETECTION METHODS
The detection of fraud is a complex computational task and still there is no system that surely predicts any transaction as fraudulent. They just predict the likelihood of the transaction to be a fraudulent.
The properties of a good fraud detection system are:

1) It should identify the frauds accurately
2) It should detecting the frauds quickly
3) It should not classify a genuine transaction as fraud

In this paper, a comprehensive review of various fraud detection methods has been performed [46][8][51][23][33][48,][59].

2.1 Neural network
Fraud detection methods based on neural network are the most popular ones. An artificial neural network [56][57][50][22][54] consists of an interconnected group of artificial neurons .The principle of neural network is motivated by the functions of the brain especially pattern recognition and associative memory [52]. The neural network recognizes similar patterns, predicts future values or events based upon the associative memory of the patterns it was learned. It is widely applied in classification and clustering. The advantages of neural networks over other techniques are that these models are able to learn from the past and thus, improve results as 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. Among the reported credit card fraud studies most have focused on using neural networks [16][60]. In more practical terms neural networks are non-linear statistical data modeling tools. They can be used to model complex relationships between inputs and outputs or to find patterns in data.
There are two phases in neural network [66][20][37]- training and recognition. Learning in a neural network is called training. There are two types of NN training methods supervised and unsupervised. In supervised training, samples of both fraudulent and non fraudulent records are used to create models. In contrast, unsupervised training simply seeks those transactions, which are most dissimilar from the norm. On other hand, 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 transaction dataset. And they need a long training dataset. Two type of neural network used in credit card fraud detection; BPNN and SOMNN.

2.1.1 Back propagation neural net work

Back propagation network (BPN) is the most popular learning algorithm to train the neural network. It was developed by Arthur E. Bryson and Yu Chi Ho in 1969. They described it as a multi-stage dynamic system optimization method which minimizes the objective function. It is a supervised learning model and is a generalization of the delta rule. It is most useful for feed-forward network which is network that has no feedback.

Feed forward network [21][63][42][1] consists of three layers namely input, hidden and output layers. The incoming sequence of transactions passes from input layer through hidden layer to the output layer. This is known as forward propagation. Here the input data is repeatedly presented 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 model gets closer and closer to producing the desired output. This process is known as training.

The last one or two year data is required to train the NN about the particular pattern of using a credit card by a particular consumer [52][42][60]. During training, the network is trained to associate outputs with input patterns. After training when the network is used, it identifies the input pattern and tries to output the associated output pattern. The power of neural networks comes to life when a pattern that has no output associated with it, is given as an input. In this case, the network gives the output that corresponds to a taught input pattern that is least different from the given pattern. When credit card is being used by 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.

However, the BP algorithm requires long training times and extensive testing and retraining of parameters, such as the number of hidden neurons, learning rate and momentum, to determine the best performance [9].

2.1.2 Self Organizing Map

The self-organizing map (SOM) is an unsupervised neural network learning model that was introduced by kohonen in 1990. In credit card fraud detection SOM has been suggested for forming customer profiles and analyzing fraud patterns [72][32][77]. In process of self organization, the transaction data is first identified and pre processed. These input data are fed in to SOM and weights of the neurons are adjusted iteratively [29]. 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 nodes [20][25], an input layer and a mapping layer in the shape of a two-dimensional grid.

The layer of SOM has three purposes [32][71][59]:

- To classify and cluster the input data
- To detect and derive hidden patterns in input data
- To act as a filtering mechanism for further layers.

In this technique all transactions in the payment system are classified into genuine and fraudulent sets [29] based on two hypotheses:

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

2.2 Bayesian Network

The Bayesian belief network was first introduced by Cooper and Herskovits (1992). Bayesian belief networks are statistical techniques in data mining. Bayesian networks are very effective for modeling situations where some information is already known and incoming data is unsure or partially unavailable [60][64][18]. The goal of using Baye rules is to correctly predict the value of a designated discrete class variable given a vector of predictors or attributes [30][39][70]. In 1993, Sam maes et al [57] has been suggested BN for credit card fraud detection. For the purpose of fraud detection, two Bayesian networks hypothesis for describing the behavior of user are constructed. First, Bayesian network is constructed to model behavior that has been assumed the user is fraudulent and second model under the assumption that the user is a legitimate. The fraud net is set up by using expert knowledge. The user net is set up by using data from non fraudulent users. During operation, user net is adapted to a specific user based on emerging data. By inserting evidence to these networks, the result of any transaction has been classified as fraudulent or non fraudulent behavior. In the probability of fraud=P (F) then P (NF) =1-P (F) in general and by applying Bayes rule, it gives the probability of fraud for any incoming transaction [69]. The fraud probability that has obtained of training can be used as an alarm level. Bayesian networks allow the integration of expert knowledge, which we used to initially set up the models.

Bayesian Network needs training of data to operate and require high processing speed. BN is more accurate and much faster than neural network [57], but BBNs are slower when applied to new instances.

2.3 Support Vector Machine

The Support Vector Machines (SVM) is statistical learning techniques and has successful application in a range of problems [44][62][63]. It was first introduced by Cortes and Vapnik (1995) and it has been found to be very successful in a variety of classification tasks [10]. They are closely related to neural networks and through the use of kernel functions, they can be considered an alternative way to obtain neural network classifiers. SVM algorithm is a supervised machine learning algorithm that has been applied to anomaly detection in the one-class setting [30][10]. Such techniques use one class learning techniques for SVM and learn a region that contains the training data instances [70]. The basic idea of SVM classification algorithm is to construct a hyper plane as the decision plane which making the distance between the positive and negative mode maximum [30]. The strength of SVMs comes from two important properties they possess - kernel representation and margin optimization. Kernels, such as radial basis function (RBF) kernel, can be used to learn complex regions. A kernel function represents the dot product of projections of two data points in a high dimensional feature space. In SVMs, the classification function is a hyper-plane separating the different classes of data. The basic technique finds the smallest hypersphere in the kernel space that contains all training instances, and then determines on which side of hypersphere a test instance lies. If a test instance lies outside the hypersphere, it is confirmed to be suspicion. This

algorithm finds a special kind of linear model, the maximum margin hyper plane, and it classifies all training instances correctly by separating them into correct classes through a hyper plane. The maximum margin hyper plane is the one that gives the greatest separation between the classes. The instances that are nearest to the maximum margin hyper plane are called support vectors. There is always at least one support vector for each class, and often there are more. In credit card fraud detection, for each test instance, it determines if the test instance falls within the learned region. Then if a test instance falls within the learned region, it is declared as normal, else it is declared as anomalous. This model has been demonstrated that it possess a higher accuracy of detection compared with other algorithms. It also has a better time efficiency and generalization ability [49][58]. Performance evaluation of SVM with BPN in credit card fraud detection shows that when the data number is small, SVM can have better prediction performance than BPN in predicting the future data. But in large data BPN has a good performance.

2.4 K-Nearest Neighbor algorithm

The concept of nearest neighbor analysis has been used in several anomaly detection techniques. One of the best classifier algorithms that have been used in the credit card fraud detection is k-nearest neighbor algorithm that is a supervised learning algorithm where the result of new instance query is classified based on majority of K-Nearest Neighbor category. It was first introduced by Aha, Kibler, and Albert (1991) [30].

The performance of KNN algorithm is influenced by three main factors [Mohammed J. Islam]:

• The distance metric used to locate the nearest neighbors.

• The distance rule used to derive a classification from k-nearest neighbor.

• The number of neighbors used to classify the new sample.

Among the various credit card fraud detection methods of supervised statistical pattern recognition, the K Nearest Neighbor rule achieves consistently high performance, without a priori assumptions about the distributions from which the training examples are drawn. K- Nearest neighbor based credit card fraud detection techniques require a distance or similar the measure defined between two data instances. [70][30]. In process of KNN, we classify any incoming transaction by calculating of nearest point to new incoming transaction. Then if the nearest neighbor be fraudulent, then the transaction indicates as a fraud. The value of K is used as, a small and odd to break the ties (typically 1, 3 or 5) [40]. Larger K values can help to reduce the effect of noisy data set. In this algorithm, distance between two data instances can be calculated in different ways. For continuous attributes, Euclidean distance is a good choice, [70][65]. For categorical attributes, a simple matching coefficient is often used. For multivariate data, distance is usually calculated for each attribute and then combined [65].

The performance of KNN algorithm can be improved by using a genetic algorithm for optimizing the distance metric.

This technique required legitimate as well as fraudulent samples of data for training. It is fast technique along with high false alarm [40].

2.5 Decision tree

Decision trees are statistical data mining technique that express independent attributes and a dependent attributes logically AND in a tree shaped structure. Classification rules, extracted from decision trees, are IF-THEN expressions and all the tests have to succeed if each rule is to be generated [55]. Decision tree usually separates the complex problem into many simple ones and resolves the sub problems through repeatedly using [58][15]. Decision trees are predictive decision support tools that create mapping from observations to possible consequences. There are number of popular classifiers construct decision trees to generate class models. These classifiers first build a decision tree and then prune sub trees from the decision tree in a subsequent pruning phase to improve accuracy and prevent over fitting. These trees can be planted via machine-learning-based algorithms such as the ID3, and C4.5 and MLPC which are applied on credit card database. The core of DT model is to construct a decision tree with high accuracy and small scale [67]. There are two phases in decision tree based on credit card fraud detection, first is to generate the decision tree from the given training data and second is apply decision rules of to determine the class of any incoming transaction. Input data in decision tree, is tagged with a class label (fraudulent or legitimate). In this system, each account is monitored separately using suitable descriptors, and the transactions are attempt to be identified and flagged as legitimate or normal. In process of DT, all the training examples are at the root node and tree starts as a single node that representing the dataset. Each node is split into child nodes in a binary or a multi split fashion related to the method. Then, for each transaction to be classified, read one by one the decision rule from the Decision table. Match the fields from the transaction with each decision rule. First try to find out perfect match and indicates the Class of the transaction with that class of matched rule. If perfect match is not found then among matched rules the rule having highest risk level is chosen and the class of the transaction is filled with that class of matched rule. It means that, if the new transaction is the same type of fraud, then the node becomes a leaf and is labeled as fraud. This model is very fast and has a high flexibility [15].

MLPC algorithm is implemented with pre-pruning where while constructing the tree, growth of the tree is stopped at the set pruned level. Here the tree is constructed in a top-down recursive divide and conquer manner. In the beginning, all the training examples are kept at the root. Then partition the examples recursively based on selected attributes. Select the splitting attribute on the basis of entropy measure. Then repeat all the steps until one of the following four conditions get satisfied:

i. All samples for a given node belong to the same class.
ii. There are no remaining attributes for further partitioning.
iii. There are no samples left.
iv. Set prune level is completed.

2.6 Fuzzy logic based system

2.6.1 Fuzzy Neural Net work

The aim of FNNs is to process the massive volume of uncertain information, which is widespread applied in our life [61]. Syeda et al (2002) [41] propose fuzzy neural networks on parallel machines to speed up rule production for customer-specific credit card fraud detection. His work can be related to Data mining and Knowledge Discovery in data bases (KD). In this method syeda et al used GNN (Granular Neural Network) method that uses fuzzy neural network based on knowledge discovery (FNNKD), for how fast we can train the network and how fast a number of customers can be processed for detection in parallel. There are various fields in transaction table that include, the transaction amounts, time between transactions, statement date, transaction code, posting date, day, transaction description, and etc. But for

implementation of this credit card fraud detection method, only the relevant fields from the database were extracted into a simple text file by applying appropriate SQL queries. In this detection method the transaction amounts for any customer is the key input data. This preprocessing of data has been helped in reducing the data size and efficient processing, thus speeding up the training and making the patterns more concise. In process of fuzzy neural network data are classified into three categories- first for training, second for prediction, and third one is for fraud detection.
The detection system routine for any customer is given 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 been accepted inputs in the range 0 to 1, but the transaction amount was any number greater than or equal to zero because he considered the maximum transaction amount for that particular customer in the entire of work. In this detection method, there are two important parameters that are to be used during the training such as training error and training cycles. With increasing in training cycles the training error will be decreased. And the accuracy of results depends to these parameters. In prediction stage, the maximum absolute prediction error has to be calculated. In fraud detection stage also, the absolute detection error is calculated and then if the absolute detection error is greater than zero then it checked to see if this absolute detection error is greater than the maximum absolute prediction error or no. If it is found to be true then it indicates that transaction is fraudulent otherwise transaction is reported to be safe. Both training cycles and data partitioning were critical for better results. The more the data for training the neural network the better prediction it gives. The lower training error makes prediction and the detection more accurate. Higher fraud detection error is, greater the possibility of that transaction to be fraudulent.

2.6.2 Fuzzy Darwinian System

This technique [47][56] uses genetic programming to evolve fuzzy logic rules capable of classifying credit card transactions into "suspicious" and non-suspicious classes. It describes the use of an evolutionary-fuzzy system capable of classifying suspicious and non-suspicious credit card transactions. The system developed comprises two main elements: a Genetic Programming (GP) search algorithm and 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 (fuzzy clustering). The genotypes and phenotypes of the GP System consist of rules which match the incoming sequence with the past sequence. Genetic Programming is used to evolve a series of variable-length fuzzy rules which characterize the differences between classes of data held in a database. The system is being developed with the specific aim of insurance-fraud detection which involves the challenging task of classifying data into the categories: safe and suspicious. For classification of transactions, 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 as suspicious. The Fuzzy Darwinian detects suspicious and non - suspicious data and it easily 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 [56]. The speed of the system is low also.

2.7 Hidden Markov Model

A Hidden Markov Model is a double embedded stochastic process which is used to model much more complicated stochastic processes as compared to a traditional Markov model. If an incoming credit card transaction is not accepted by the trained Hidden Markov Model with sufficiently high probability, it is considered to be fraudulent transactions. A Hidden Markov Model [3] is initially trained with the normal behavior of a cardholder. It works on the user spending profiles which can be divided into three types such as 1) Lower profile; 2) Middle profile; and 3) Higher profile. For every credit card, the spending profile is different, so it can figure out an inconsistency of user profile and try to find fraudulent transaction. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc. Every user is represented by specific patterns of set which containing information about last 10 transaction using credit card [5][3][6]. The set of information contains spending profile of card holder, money spent in every transaction, the last purchase time, category of purchase etc. The potential threat for fraud detection will be a deviation from set of patterns.
In the process of HMM each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify whether the transaction is genuine or not. If the FDS confirms the transaction to be malicious, it raises an alarm and the issuing bank declines the transaction. The concerned cardholder may then be contacted and alerted about the possibility that the card is misused. HMM never check the original user as it maintains a log. The log which is maintained will also be a proof for the bank for the transaction 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 [56].

2.8 Artificial Immune System

Artificial immune systems (AIS) represent an important strategy inspired by biological systems and developed by Neal et al in 1998 [28]. The main developments within AIS have focused on three main immunological theories: clonal selection, immune networks and negative selection. In 2002, the journal Nature published an article on AIS where it indicated that AIS had many kinds of applications, including the detection of fraudulent financial transactions. And in 2003, a British company reported good experimental results for AIS. The AIS has successfully been used in computer security to detect network intrusion [19][11], clustering data for data mining [12], detecting computer viruses [13], and concept learning [14]. Artificial Immune Systems (AIS) are a class of bioinspired adaptive or learning algorithms, which includes the artificial immune recognition system [39], a supervised learning that has shown significant success on the classification problem in credit card fraud detection and this method can solve the classification problem in neural network. The immune system can distinguish between self and non-self. In the concept of credit card fraud detection, self (S) represents all patterns in a finite space that is legitimate and non-self ($\hat{S}$) represents all patterns that are not in self [2][45]. The AIS consists of artificial lymphocytes (ALCs) that able to classify any pattern as self or non-self by detecting only non-self patterns. When AIS The system only needs

positive examples to train on and does not require exhaustive training with negative (non-self) examples to make these distinctions, but can identify items as non-self which it has never before encountered. The system arbitrarily generates an ALC, test it against the set of self patterns and if it doesn't match any of the self patterns, it is included in the set of mature ALCs. When an ALC does match any of the self patterns, it is replaced by a new randomly generated ALC which then needs to be tested as well. The ALC becomes mature or adult, by training it with the known self patterns. This training method is known as negative selection [19].
High level model of AIS has been applied for credit card fraud detection that was influenced primarily by Hofmeyr & Forrest (1999) [26] and Wightman (2003) [74]. The AIS in CCFD has two subsystems. One part is interface system, which is included of input data. And the second one is AIS engine that is included transaction processor and the detector generator. AIS detection engines implements AIS based algorithms which can classify input data as normal or fraudulent.

The aim of the AISCCFD system is to have a high anomalous transaction detection rate and a low false positive rate [45].
Most of the models have been presented to detect the general types of fraud in the credit card, need to have both types of patterns (legitimate and illegitimate) to train on, Since negative examples (illegitimate transactions) are not always available for training. So this is a major drawback of most of these presented models that both types of patterns (legitimate and illegitimate) are necessary for the training process. But one of the main advantages of the AIS model is that the model only needs positive examples to train on, generating detectors (ALCs) with negative selection method.

2.9 Genetic Algorithm (GA)

Genetic algorithms, inspired from natural evolution were first introduced by Holland (1975). Genetic algorithm (GA) is a search technique used in computing to find exact or approximate solutions to optimization and search problems.
GA is used in data mining mainly for variable selection [7] and is mostly coupled with other DM algorithms [17]. And their combination with other techniques has a very good performance. They have been used in a number of applications in engineering and social science. Recently, they applied for optimization of the parameters of support vector machine for predicting bankruptcy [75], and hybrid with neural net work for detecting credit card fraud with high accuracy [31], and have been used along with Artificial Immune System for reducing a number of false alarm in credit card fraud detection. GA has been used in credit card fraud detection for minimizing the wrongly classified number of transactions [17]. And is easy accessible for computer programming language implementation, thus, make it strong in credit card fraud detection. But this method has high performance and is quite expensive.

3. CONCLUSION AND FUTURE WORK

In this paper, we present a comparative study of nine fraud detection methods based on credit card (Decision Tree, Neural Network, Bayesian Network, genetic algorithm, support vector machine, k nearest neighbor and Artificial Immune System, Hidden Markov Model, fuzzy neural network and fuzzy Darwinian system). The main objective of this paper is to review methodology of different detection methods based on credit card. We have considered the most important parameter in different methods such as, accuracy, speed and cost. Comparison table was prepared in order to compare various credit card fraud detection mechanisms. All the techniques of credit card fraud detection described in the table 1 have its own strengths and weaknesses. We found these result is mentioned in following table from the references that we have mentioned in end.
As the results show, the fraud detection systems based on Fuzzy Darwinian, has a very high accuracy with 100% true positive but with very low processing speed. In another view, HMM has a fast processing speed with low accuracy. And also BN is very high in speed processing with good accuracy in comparing to other techniques. At the same time, the processing speed in decision tree is very fast enough to enable detection of credit card fraud. AIS also has a good result in between other techniques, because is a fast technique with good accuracy. For comparing other classifiers such as KNN, SVM and DT: DT has a very fast processing speed in comparing with other classifiers, KNN also with large value for K, has a good result. Furthermore, the best model as obtained from the results are, FNN, AIS, BN, DT, GA, NNSOM, KNN, NNBP, SVM.
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 build a hybrid approach for developing some effective algorithms which can perform well for the classification problem with variable misclassification costs and with higher accuracy.

Methods	**Speed of detection**	**accuracy**	**cost**
HMM	Fast	Low	High expensive
FDS	Very low	Very high	High expensive
AIS	Very fast	Good	Inexpensive
FNN	Very fast	Good	Expensive
NN	Fast	Medium	Expensive
DT	Fast	Medium	Expensive
BN	Very Fast	High	Expensive
KNN	Good	Medium	Expensive
SVM	Low	Medium	Expensive
SOM	Fast	Medium	Expensive
BP	low	Low	Expensive
GA	Good	Medium	Inexpensive

Table 1: comparison of different methods

4. REFERENCES

[1] A. Vellidoa, P.J.G. Lisboaa, J. Vaughan "Neural networks in business: a survey of applications". Elsevier, Expert Systems with Applications, (1999). 17; (51–70).

[2] A.J. Graaff A.P. Engelbrecht "The Artificial Immune System for Fraud Detection in the Telecommunications Environment"; (2011). (1-4)

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

[4] Aihua Shen, Rencheng Tong, Yaochen Deng "Application of Classification Models on Credit Card Fraud Detection". (2007).

[5] Anshul Singh, Devesh Narayan "A Survey on Hidden Markov Model for Credit Card Fraud Detection". International Journal of Engineering and Advanced Technology (IJEAT), (2012). Volume-1, Issue-3; (49-52).

[6] B.Sanjaya Gandhi , R.Lalu Naik, S.Gopi Krishna, K.lakshminadh "Markova Scheme for Credit Card Fraud Detection". International Conference on Advanced Computing, Communication and Networks; (2011). (144-147).

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

[8] Bolton, R. J., Hand, D. J (2002). "Statistical fraud detection: A review". Statistical Science (1994).28(3); (235—255).

[9] Clifton Phua, Vincent Lee, Kate Smith, and Ross Gayler "A comprehensive survey of data mining-based fraud detection research". In Artificial Intelligence Review. (2005).

[10] Cortes, C. & Vapnik, V "Support vector networks, Machine Learning". . (1995). Vol. 20; (273–297).

[11] De Castro Silva, L. N., & Zuben, F. J. V "An evolutionary immune network for data clustering". In Proceedings of the IEEE SBRN (Brazilian Symposium on Artificial Neural Networks); . (2000). (84–89).

[12] De Castro, L., & Timmis, J "Artificial immune systems: a new computational approach". London, UK: Springer-Verlag. . (2002).

[13] De Castro, L.N. & Von Zuben, F.J "Artificial immune systems", part i – basic theory and applications. Technical Report, Department of Computer Engineering and Industrial Automation, School of Electrical and Computer Engineering. . (1999a).

[14] De Castro, L.N. & Von Zuben, F.J. "Artificial immune systems", part ii – a survey of applications. Technical Report, Department of Computer Engineering and Industrial Automation, School of Electrical and Computer Engineering. (1999b).

[15] Dipti D. Patil, V.M. Wadhai, J.A. Gokhale "Evaluation of Decision Tree Pruning Algorithms for Complexity and Classification Accuracy". International Journal of Computer Applications, (2010). Volume 11– No.2; (23-30).

[16] E.W.T. Ngai, Yong Hu, Y.H. Wong, Yijun Chen, Xin Sun "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature". Elsevier-Decision Support Systems(2011). 50; (559–569).

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

[18] Eugene Charniak "Bayesians networks without tears". AI Magazine. (1991).

[19] Forrest, S., Perelson, A.S., Llen, L. & Cherukuri, R. "Self-nonself discrimination in a computer". Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy; (1994). (202–212).

[20] Francisca nonyelum ogwueleka "Data Mining Application in Credit Card Fraud Detection System". Journal of Engineering Science and Technology(2011). Vol. 6, No. 3; (311 – 322).

[21] Ganesh K. Venayagamoorthy "Teaching Neural Networks Concepts and Their Learning Techniques". Proceedings of the American Society for Engineering Education Midwest Section Conference. (2004).

[22] Ghosh, D.L. Reilly "Credit Card Fraud Detection with a Neural- Network". Proceedings of the International Conference on System Science; (1994). (621-630).

[23] H. Leggatt, CyberSource "Online fraud to reach $4 billion". BizReport, December 16. (2008).

[24] Hamid Farvaresh, Mohammad Mehdi Sepehri "A data mining framework for detecting subscription fraud in telecommunication". Engineering Applications of Artificial Intelligence, (2011). 24; (182–194).

[25] Hiotis, A. "Inside a self-organizing map". AI Expert, (1993). 8(4); (38-43).

[26] Hofmeyr, S.A. & Forrest, S. "Immunity by design: an artificial immune system". Proceedings of the Genetic and Evolutionary Computation Conference (GECCO); (1999b). (1289–1296).

[27] Holland, J. H. "Adaptation in natural and artificial systems." Ann Arbor: The University of Michigan Press. (1975).

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

[29] Jon T.S. Quah, M. Sriganesh "Real-time credit card fraud detection using computational intelligence". Elsevier, Expert Systems with Applications, (2008). 35; (1721–1732).

[30] Joseph King-Fung Pun "Improving Credit Card Fraud Detection using a Meta-Learning Strategy". A thesis submitted in conformity with the requirements for the degree of Master of Applied Science Graduate Department of Chemical Engineering and Applied Chemistry University of Toronto. (2011).

[31] Kim, M., & Han, I. The discovery of experts' decision rules from qualitative bankrupcy data using genetic algorithms. Elsevier, Expert Systems with Applications(2003)., 25; (637–646).

[32] Kohonen, T. "The self-organizing map". In Proceedings of the IEEE(1990) 78 (9); (1464–1480).

[33] Kou, Y., Lu, C.-T., Sirwongwattana, S., Huang, Y.-P "Survey of fraud detection techniques". In Proceedings of the IEEE International Conference on Networking, Sensing and Control. (2004).

[34] L.N. de Castro, J. Timmis "Artificial Immune Systems". A New Computational Intelligence Approach, Springer. (2002).

[35] Lean Yu a, Wuyi Yue, Shouyang, Wang, K.K. Lai "Support vector machine based multiagent ensemble learning for credit risk evaluation". Expert Systems with Applications(2010). 37; (1351–1360).

[36] Leila Seyedhossein, mahmoud reza hashemi "Mining Information from Credit Card Time Series for Timelier Fraud Detection". IEEE-5th International Symposium on Telecommunications. (2010).

[37] M.Jeevana Sujitha, K. Rajini Kumari, 3N.Anuragamayi "The Credit Card Fraud Detection Analysis With Neural Network Methods". IJCST (2012). Vol. 3, Issue 1; (959-963).

[38] Malak Alshawabkeh, Byunghyun Jang, David Kaeli." Accelerating the Local Outlier Factor Algorithm on a GPU for Intrusion Detection Systems". ACM; (2010) (104-110).

[39] Manoel Fernando, Xidi Wang, Alair Pereira do Lago "Comparison with Parametric Optimization in Credit Card Fraud Detection". (2008) 279-285.

[40] Mohammed J. Islam, Q. M. Jonathan Wu, Majid Ahmadi, Maher A. Sid-Ahmed "Investigating the Performance of Naive- Bayes Classifiers and K-NearestNeighbor Classifiers". IEEE, International Conference on Convergence Information Technology; (2007). (1541-1546).

[41] Mubeena Syeda, 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).

[42] Mu-Chen Chena, Shih-Hsien Huang (2003). "Credit scoring and rejected instances reassigning through evolutionary computation techniques". Elsevier, Expert Systems with Applications 24; (433–441).

[43] Mukhanov "Using bayesian belief networks for credit card fraud detection". in Proc. of the IASTED International conference on Artificial Intelligence and Applications; (2008). (221– 225).

[44] N. Cristianini, J. Shawe-Taylor "An Introduction to Support Vector Machines and Other Kernel-based Learning Methods". Cambridge University Press. (2000).

[45] Nicholas Wong, Pradeep Ray, Greg Stephens & Lundy Lewis (2012). "Artificial immune systems for the detection of credit card fraud". Info Systems, Volume 22; (53–76).

[46] P.K. Chan, W. Fan, A.L. Prodromidis, S.J. Stolfo "Distributed Data Mining in Credit Card Fraud Detection". Data Mining; (1999). (67–74).

[47] Peter J. Bentley, Jungwon Kim, Gil-Ho Jung and Jong-Uk Choi "Fuzzy Darwinian Detection of Credit Card Fraud". In the 14th Annual Fall Symposium of the Korean Information Processing Society; (2000). (1-4).

[48] Phua, C, Lee, V., Smith, K., Gayler, R "A comprehensive survey of data mining-based fraud detection research". Artificial Intelligence Review. (2002).

[49] Qibei Lu, Chunhua Ju "Research on Credit Card Fraud Detection Model Based on Class Weighted Support Vector Machine". Journal of Convergence Information Technology, (2011). Volume 6, Number 1; (62-68).

[50] R. Brause, T. Langsdorf, M. Hepp "Neural Data Mining for Credit Card Fraud Detection, "International Conference on Tools with Artificial Intelligence; (1999). (103-106).

[51] R.C. Chen, T.S. Chen, C.C. Lin ("A new binary support vector system for increasing detection rate of credit card fraud". International Journal of Pattern Recognition2006). 20 (2); (227–239).

[52] Raghavendra Patidar, Lokesh Sharma "Credit Card Fraud Detection Using Neural Network". International Journal of Soft Computing and Engineering (IJSCE), (2011). Volume-1, Issue; (32-38).

[53] Raghuveer Kancherla, Ratna Venkata, Anurag Verma "Behavioral Fraud Mitigation through Trend Offsets". (2008).(1-11).

[54] Ray-I Chang, Liang-Bin Lai, Wen-De Su, Jen-Chieh Wang, Jen-Shiang Kouh "Intrusion Detection by Backpropagation Neural Networks with Sample-Query and Attribute-Query". Research India Publications; (2006). (6-10).

[55] Rekha Bhowmik "Detecting Auto Insurance Fraud by Data Mining Techniques". Journal of Emerging Trends in Computing and Information Sciences, (2011). Volume 2 No.4; (156-162).

[56] S. Benson Edwin Raj, A. Annie Portia "Analysis on Credit Card Fraud Detection Methods". IEEE-International Conference on Computer, Communication and Electrical Technology; (2011). (152-156).

[57] S. Maes, K. Tuyls, B. Vanschoenwinkel, B. Manderick "Credit card fraud detection using Bayesian and neural networks". Proceedings of the First International NAISO Congress on Neuro Fuzzy Technologies; (1993). (261-270).

[58] 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. (2010).

[59] Serrano-Cinca, C "Self-organizing neural networks for financial diagnosis". Decision Support Systems, (1996). 17; (227–238).

[60] Sherly K.K (2012) "A comparative assessment of supervised data mining techniques for fraud prevention". TIST.Int.J.Sci.Tech.Res,Vol.1; (1-6).

[61] Shifei Ding · Hongjie Jia · Jinrong Chen · Fengxiang Jin "Granular neural networks". Springer Artificial intelligence review (2012).

[62] Siddhartha Bhattacharyya, Sanjeev Jha, Kurian Tharakunnel, J. Christopher Westland "Data mining for credit card fraud: A comparative study". Elsevier, Decision Support Systems (2011).,50; (602–613).

[63] Silvia Cateni, Valentina Colla, Marco Vannucci "Outlier Detection Methods for Industrial Applications". Advances in Robotics, Automation and Control; (2008). (265-282).

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

[65] Tan, P.N., Steinbach, M, And Kumar. V "Introduction to Data Mining". (2005).

[66] Tao Guo, Gui-Yang Li "Neural Data Mining For Credit Card Fraud Detection". IEEE, Proceedings of the Seventh International Conference on Machine Learning and Cybernetics; (2008). (3630-3634).

[67] Tatsuya Minegishi1, Ayahiko Niimi "Proposal of Credit Card Fraudulent Use Detection by Online-type Decision Tree Construction and Verification of Generality". International Journal for Information Security Research (IJISR), (2011). Volume 1, Issue 4; (229-235).

[68] V. Bhusari S. Patil "Study of Hidden Markov Model in Credit Card Fraudulent Detection". International Journal of Computer Applications, (2011). Volume 20– No.5; (0975 – 8887).

[69] V.Dheepa, Dr. R.Dhanapal "Analysis of Credit Card Fraud Detection Methods". International Journal of Recent Trends in Engineering, (2009). Vol 2, No. 3; (126-128).

[70] Varun chandola, Arindam banerjee, and Vipin kumar "Anomaly Detection: A Survey. ACM Computing Surveys, Vol. 41, No. 3; (15-72).

[71] Vesanto, J., & Alhoniemi, E. (2000). "Clustering of the self-organizing map". IEEE Transactions on Neural Networks, (2009). 11; (586–600).

[72] Vladimir Zaslavsky and Anna Strizhak "Credit card fraud detection using self organizing maps". Information & Security. An International Journal, (2006). Vol.18; (48-63).

[73] W.B. Langdon, R. Poli "Foundations of Genetic Programming". Springer-Verlag, Berlin. (2002).

[74] Wightman, J. "Computer immune techniques in e-commerce fraud detection." School of Information Systems and Technology Management, The University of New South Wales, Honours Thesis.. (2003).

[75] Wu, C.-H., Tzeng, G.-H., Goo, Y.-J., & Fang, W.-C. "A real-valued genetic algorithm to optimize the parameters of support vector machine for predicting bankruptcy". Expert Systems with Applications, (2007). 32(2); (397–408).

[76] Yen-Hsien Lee, Chih-Ping Wei, Tsang-Hsiang Cheng, Ching-Ting Yang "Nearest-neighbor-based approach to time-series classification". Elsevier, Decision Support Systems(2012). 53; (207–217).

[77] Yok-Yen Nguwi, Siu-Yeung Cho "An unsupervised self-organizing learning with support vector ranking for imbalanced datasets". Expert Systems with Applications, (2010). 37; (8303–8312).

[78] Yuen, C. W. M., Wong, W. K., Qian, S. Q., Chan, L. K., & Fung, E. H. K. "A hybrid model using genetic algorithm and neural network for classifying garment defects". Expert Systems with Applications, (2009). 36(2); (2037–2047).

[81] Yufeng Kou, Chang-Tien Lu, Sirirat Sinvongwattana Yo-Ping Huang "Survey of Fraud Detection Techniques". Proceedings of the IEEE International Conference on Networking, Sensing & Control Taipei, Taiwan; (2004). (749-754)