International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

# Analysis of Credit Card Fraud Detection Techniques

**Sunil Bhatia[1], Rashmi Bajaj[2], Santosh Hazari[3]**

[1]Vivekanand Education Society's Institute of Technology, Collector's Colony, Chembur, Mumbai – 400074, India

[2]Thadomal Shahani Engineering College, TPS-III Off Linking Road, Bandra (W), Mumbai – 400050, India

[3]Vivekanand Education Society's Institute of Technology, Collector's Colony, Chembur, Mumbai – 400074, India

**Abstract:** ***Due to the rise and rapid growth of E-Commerce, use of credit cards for online purchases has dramatically increased and it caused an explosion in the credit card fraud. In an era of digitalization, credit card fraud detection is of great importance to financial institutions. In this paper, we analyze credit card fraud detection using different techniques : Bayesian Learning, BLAST-SSAHA Hybridization, Hidden Markov Model, Fuzzy Darwinian detection, Neural Networks, SVM, K-Nearest Neighbour and Naïve Bayes. After analyzing through each technique, our aim is to compare all the techniques based on some parameters. The obtained results from databases of credit card transactions show the power of these techniques in the fight against banking fraud comparing them to others in the same field.***

**Keywords:** Machine Learning, Neural Networks, Blast SSAHA Hybridization, Fuzzy Darwinian Detection

## 1. Introduction

Credit card fraud can be divided into 2 types: inner card fraud and external card fraud. Inner card fraud intends to defraud the cash. Usually it is the collusion between merchants and cardholders, using false transactions to defraud banks cash. External card fraud is mainly embodied at using the stolen, fake or counterfeit credit card to consume, or using cards to get cash in disguised forms, such as buying the expensive, small volume commodities or the commodities that can easily be changed into cash.

Fraud detection is generally viewed as a data mining classification problem, where the objective is to correctly classify the credit card transactions as legitimate or fraudulent. Even though fraud detection has a long history, not that much research has appeared in this area. The reason is the unavailability of real world data on which researchers can perform experiments since banks are not ready to reveal their sensitive customer transaction data due to privacy reasons. Moreover, they used to change the field names so that the researcher would not get any idea about actual fields. Due to this scarcity of real dataset, not many fraud detection models have been developed and described in the academic literature, and even fewer are known to have been implemented in actual detection systems. Still we can find some successful applications of various data mining techniques like *BLAST-SSAHA*, neural network, Bayesian classifier, support vector machine, artificial immune system, fuzzy systems, genetic algorithm, K-nearest neighbor, and hidden Markov model in fraud detection

## 2. Related Works

Fraud detection involves monitoring the behavior of users in order to estimate, detect, or avoid undesirable behavior. To counter the credit card fraud effectively, it is necessary to understand the technologies involved in detecting credit card frauds and to identify various types of credit card frauds [20][21] [22] . There are multiple algorithms for credit card fraud detection [21] [29]. They are artificial neural-network models which are based upon artificial intelligence and machine learning approach [5][7][9][10][16][27][28] [29][30][31], distributed data mining systems [17] [19], sequence alignment algorithm which is based upon the spending profile of the cardholder [1] [6] This paper compares and analyzes some of the good techniques that have been used in detecting credit card fraud. It focuses on credit card fraud detection methods like Fusion of Dempster Shafer and Bayesian learning [2][5][12][15][25], Hidden Markov Model [3], Artificial neural networks and Bayesian Learning approach[5][25],BLAST and SSAHA Hybridization [1][6][11][14][24], Fuzzy Darwinian System[4], SVM [27], K-Nearest Neighbor[29][30], Naives Bayes[28][31]

## 3. Detection Methods

### A. A fusion approa.ch using Dempster-Shafer theory and Bayesian learning

*FDS of Dempster-Shafer theory and Bayesian learning*
Dempster-Shafer theory and Bayesian learning is a hybrid approach for credit card fraud detection [2][5][12][15] which combines evidences from current as well as past behavior. Every cardholder has a certain type of shopping behavior, which establishes an activity profile for them. This approach proposes a fraud detection system using information fusion and Bayesian learning of so as to counter credit card fraud. The FDS system consists of four components, namely, rule-based filter, Dempster-Shafer adder, transaction history database and Bayesian learner. In the rule-based component, the suspicion level of each incoming transaction based on the extent of its deviation from good pattern is determined. Dempster-Shafer's theory is used to combine multiple such evidences and an initial belief is computed. Then the initial belief values are combined to obtain an overall belief by applying Dempster-Shafer theory. The transaction is classified as suspicious or suspicious depending on this initial belief. Once a transaction is found to be suspicious, belief is

further strengthened or weakened according to its similarity with fraudulent or genuine transaction history using Bayesian learning.

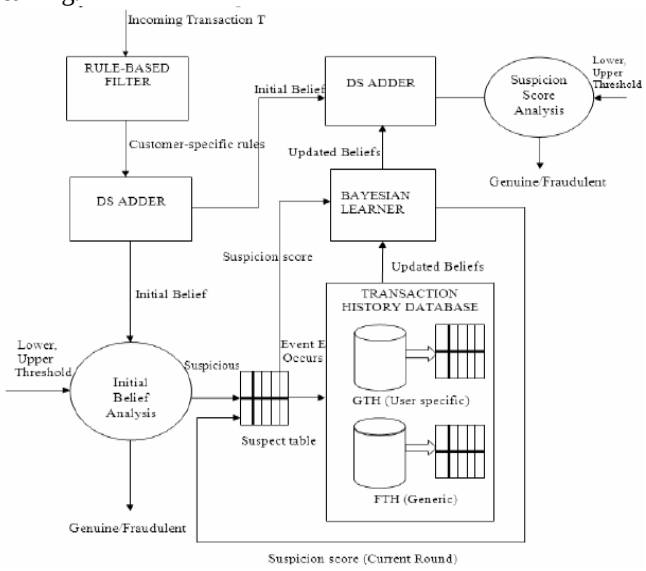


**Figure 1:** Block diagram of the proposed fraud detection system

It has high accuracy and high processing speed. It improves detection rate and reduces false alarms and also it is applicable in e-commerce. But it is highly expensive and its processing speed is low.

### B. BLAST-SSAHA Hybridization for Credit Card Fraud Detection

*BLAST-SSAHA in credit card fraud detection*

The Hybridization of BLAST and SSAHA algorithm [1][6][14] is refereed as BLAH-FDS algorithm. Sequence alignment becomes an efficient technique for analyzing the spending behavior of customers. BLAST and SSAHA are the efficient sequent alignment algorithms used for credit card fraud detection.

BLAH-FDS is a two-stage sequence alignment algorithm in which a profile analyzer (PA) determines the similarity of an incoming sequence of transactions on a given credit card with the genuine cardholder's past spending sequences. The unusual transactions traced by the profile analyzer are passed to a deviation analyzer (DA) for possible alignment with past fraudulent behavior. The final decision about the nature of a transaction is taken on the basis of the observations by these two analyzers.

BLAST-SSAHA Hybridization
If TA contains genuine transaction, then it would align well with the sequences in CPD. If there is any fraudulent transactions in TP, mismatches can occur in the alignment process.

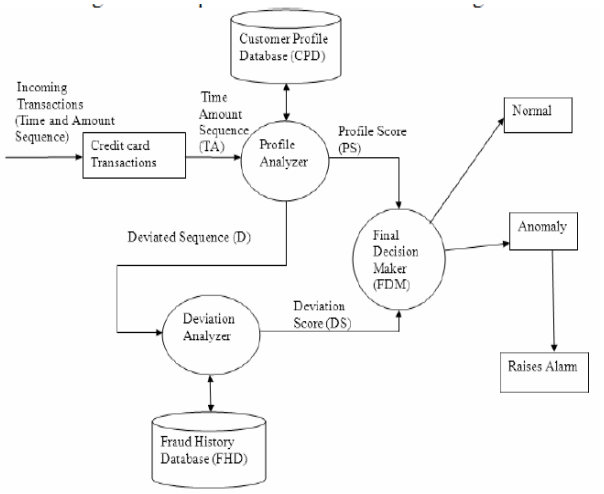


**Figure 2:** Architecture of BLAST and SSAHA Fraud Detection System

This mismatch produces a deviated sequence D which is aligned with FHD. A high similarity between deviated sequence D and FHD confirms 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. At the same time, the processing speed is fast enough to enable on-line detection of credit card fraud. It Counter frauds in telecommunication and banking fraud detection. But it does not detect cloning of credit cards or skimming.

### C. Credit Card Fraud Detection using Hidden Markov Model Hidden Markov Model

A Hidden Markov Model is a double embedded stochastic process with 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.

*Use Of HMM For Credit Card Fraud Detection*
A Hidden Markov Model [3] is initially trained with the normal behavior of a cardholder. 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 compromised.

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.

**D. Fuzzy Darwinian Detection of Credit Card Fraud**
**The Evolutionary-Fuzzy System**

Fuzzy Darwinian Detection system [4] 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 comprises of a Genetic Programming (GP) search algorithm and a fuzzy expert system.

Data is provided to the FDS system. The system first clusters the data into three groups namely low, medium and high. The GP 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". 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. The complete system is capable of attaining good accuracy and intelligibility levels for real data. It has very high accuracy and produces a low false alarm, but it is not applicable in online transactions and it is highly expensive. The processing speed of the system is low.

**E. Credit Card Fraud Detection Using Bayesian and Neural Networks**

The credit card fraud detection using Bayesian and Neural Networks are automatic credit card fraud detection system by means of machine learning approach. These two machine learning approaches are appropriate for reasoning under uncertainty. An artificial neural network [5][7][9][10][16] consists of an interconnected group of artificial neurons and the commonly used neural networks for pattern classification is the feed- forward network. It consist 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.

The ANN consists of training data which is compared with the incoming sequence of transactions. The neural network is initially trained with the normal behavior of a cardholder. The suspicious transactions are then propagated backwards through the neural network and classify the suspicious and non- suspicious transactions.

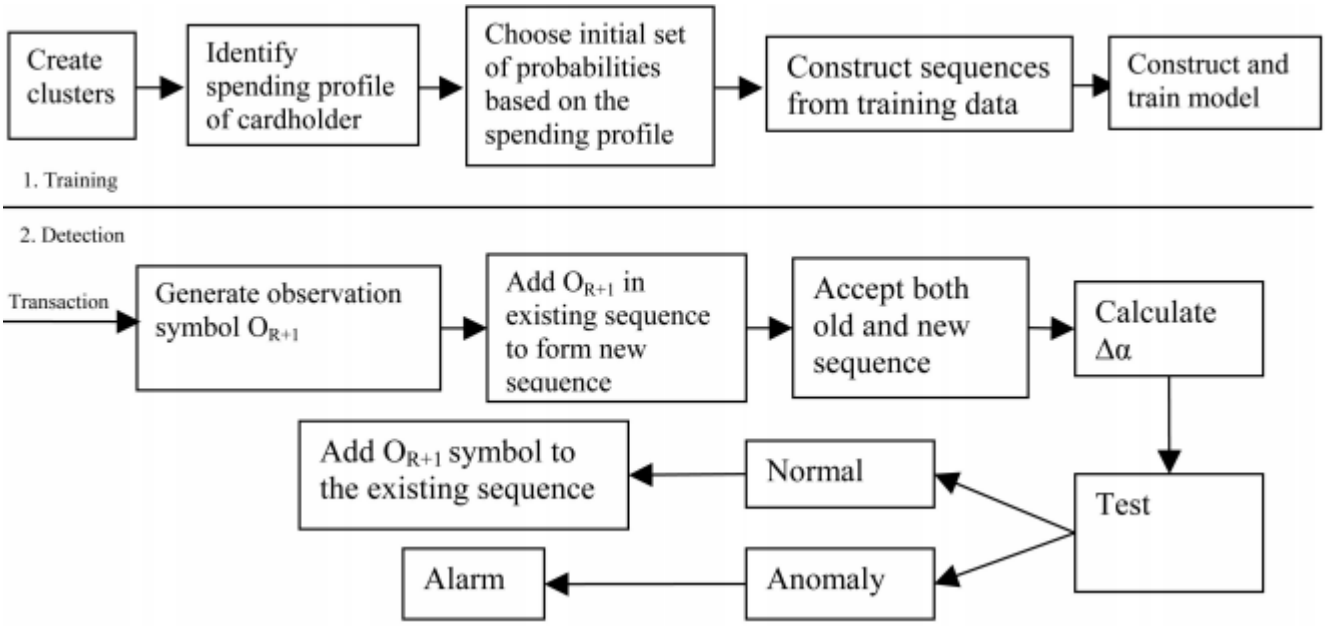


**Figure 3:** Process Flow of the Proposed FDS

Bayesian networks are also known as belief networks and it is a type of artificial intelligence programming that uses a variety of methods, including machine learning algorithms and data mining, to create layers of data, or belief. By using supervised learning, Bayesian networks are able to process data as needed, without experimentation. Bayesian belief networks are very effective for modeling situations where some information is already known and incoming data is uncertain or partially unavailable. This information or belief is used for pattern identification and data classification.

A neural network learns and does not need to be re-programmed. Its processing speed is higher than BNN. Neural network needs high processing time for large neural networks. Bayesian networks are supervised algorithms and they provide a good accuracy, but it needs training of data to operate and requires a high processing speed.

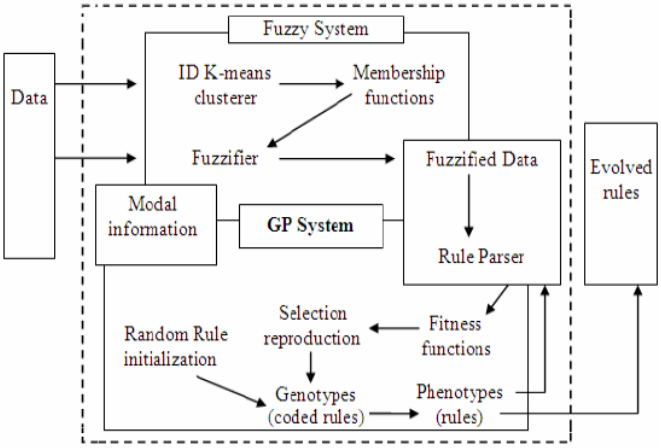


Figure 4. Block diagram of the Evolutionary-fuzzy system

### F. Support Vector Machine

The support vector machines (SVM) are statistical learning techniques first introduced by Cortes and Vapnik (1995) and they have been found to be very successful in a variety of classification tasks [27]. Support vector machines are based on the conception of decision planes which define decision boundaries. A decision plane is one that separates between a set of different classes. Basically SVM classification algorithms tend to construct a hyper plane as the decision plane which does separate the samples into the two classes—positive and negative. The strength of SVMs comes from two main properties: kernel representation and margin optimization. Kernels, such as radial basis function (RBF) kernel, can be used to learn complex regions. 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 to possess a higher accuracy and efficiency of credit card fraud detection compared with other algorithms. Even for multidimensions and continuous features SVMs are the one of first choice [27]. SVM methods require large training dataset sizes in order to achieve their maximum prediction accuracy.

### G. K-Nearest Neighbor

The K-nearest neighbor (KNN) technique [28] is a simple algorithm which stores all available instances; then it classifies any new instances based on a similarity measure. The KNN algorithm is example of an instance based learner. In the nearest neighbor classification method, each new instance is compared with existing ones by using a distance metric, and the closest existing instance is used to assign the class to the new one [30]. Sometimes more than one nearest neighbor is used, and the majority class of the closest K neighbors is assigned to the new instance. Among the various credit card fraud detection methods, the KNN achieves consistently high performance, without apriori assumptions about the distributions from which the training examples are drawn. In the process of KNN, we classify any incoming transaction by calculating nearest point to new incoming transaction. If the nearest neighbor is fraudulent, then the transaction is classified as fraudulent and if the nearest neighbor is legal, then it is classified as legal.

### H. Naıve Bayes

Naıve Bayes (NB) is a supervised machine learning method that uses a training dataset with known target classes to predict the future or any incoming instance's class value. Naıve Bayes classifier is noted as a powerful probabilistic method that exploits class information from training dataset to predict the class of future instances [29][31]. Naıve Bayes method assumes that the presence or absence of any attribute of a class variable is not related to the presence or absence of any other attributes. This technique is named –naıve" because it naıvely assumes independence of the attributes [30]. The classification is done by applying –Bayes" rule to calculate the probability of the correct class. Despite their naıve design and oversimplified assumptions, Naıve Bayes classifiers have good performance in many complex real world datasets.

## 4. Comparison of Various Fraud Detection Systems - Parameters Used for Comparison

The Parameters used for comparison of various Fraud Detection Systems are Accuracy, Fraud Detection Rate in terms of True Positive, Cost and Training required, Supervised Learning. The comparison performed is shown in Table 1.

a) Accuracy: It represents the fraction of total number of transactions (both genuine and fraudulent) that have been detected correctly.
b) Method: It describes the methodology used to counter the credit card fraud. The efficient methods like Sequence Alignment, Machine Learning and Neural Networks are used to detect and counter frauds in credit card transactions.
c) True Positive (TP): It represents the fraction of fraudulent transactions correctly identified as fraudulent and genuine transactions correctly identified as genuine.
d) Training data: It consists of a set of training examples. The fraud detection systems are initially trained with the normal behavior of a cardholder.
e) Supervised Learning: It is the machine learning task of inferring a function from supervised training data.

## 5. Comparison Results

The 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. Results show that the fraud detection systems such as Fuzzy Darwinian, Dempster and Bayesian theory have very high accuracy in terms of TP. At the same time, the processing speed is fast enough to enable on-line detection of credit card fraud in case of BLAH-FDS and ANN. Machine Learning techniques have varied accuracy depending on the case its being used.

## 6. Conclusion

Efficient credit card fraud detection system is an utmost requirement for any card issuing bank. Credit card fraud detection has drawn quite a lot of interest from the research community and a number of techniques have been proposed to counter credit fraud. The Fuzzy Darwinian fraud detection systems improve the system accuracy. Since the Fraud detection rate of Fuzzy Darwinian fraud detection systems in terms of true positive is 100% and shows good results in detecting fraudulent transactions. The neural network based CARDWATCH shows good accuracy in fraud detection and processing speed is also high, but it is limited to one-network per customer. The fraud detection rate of Hidden Markov model is very low compare to other methods. The hybridized algorithm named BLAH-FDS identifies and detects fraudulent transactions using sequence alignment tool. The processing speed of BLAST-SSAHA is fast enough to enable on-line detection of credit card fraud. BLAH-FDS can be effectively used to counter frauds in other domains such as telecommunication and banking fraud detection. The ANN and BNN are used to detect cellular phone fraud, Network Intrusion. SVM provides high accuracy and is expensive. In SVM, if a test instance lies outside the hyper sphere, it is confirmed to be suspicion transaction. K-nearest neighbor imposes high processing speed and is expensive. Naïve Bayes classification is done by applying –Bayes" rule to calculate the probability of the correct class shows good performance. All the techniques of credit card fraud detection discussed in this survey paper have its own strengths and weaknesses. Such a survey will enable us to build a hybrid approach for identifying fraudulent credit card.

**Table 1:** Comparison Of Fraud Detection Techniques

| Parameter | Fusion of Dempster-Shafer theory and Bayesian learning | Hybridization of BLAST-SSAHA | HMM | Artificial Neural Networks and Bayesian Neural Networks | | Fuzzy Darwinian detection | Support Vector Machine (SVM) | K-Nearest Neighbor | Naïve Bayes |
|---|---|---|---|---|---|---|---|---|---|
| | | | | ANN | BNN | | | | |
| Method | Machine Learning | Sequence Alignment | Hidden Markov Model | Artificial Intelligence, Machine Learning | Artificial Intelligence, Machine Learning | Genetic Programming Fuzzy Logic | Clustering | Clustering | Proabablistic classifier |
| Fraud Detection TP% | 98% | 86% | 70% | 70% | 64% | 100% | 70% | 80% | 66% |
| Processing Speed | Medium | Very high | High | High | Low | Low | Medium | High | Medium |
| Training Required | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Supervised Learning | Supervised | Unsupervised | Semi supervised | Supervised | Supervised | Supervised | Supervised | Supervised Learning | Supervised |
| Cost | Implementation is expensive | Inexpensive | Quite expensive | Expensive | Expensive | Highly expensive | Expensive | Expensive | Expensive |
| Accuracy | High | High | Medium | Medium | Medium | Very High | High | Medium | Medium |
| Research issues addressed | Intrusion detection in many database applications. Applicable in E-commerce. | Applicable in telecommunication and banking fraud detection. Online detection cost is inexpensive | Applicable in online detection of credit card fraud No need to check original user as it maintains a log. | Cellular phone fraud, Calling card fraud, Computer Networks Intrusion Applicable in E-commerce. | | Easily detect stolen credit card frauds. Detect suspicious, non-suspicious data. | If a test instance lies outside the hypersphere, it is confirmed to be suspicion transaction | classify by calculating nearest point If the nearest neighbor is fraudulent, then the transaction is classified as fraudulent | classification is done by applying "Bayes" rule to calculate the probability of the correct class shows good performance |
| Research Challenges | Processing speed is very low | Cannot detect cloning of credit card fraud | High false alarm | Needs training to operate and requires high processing time for large neural networks and BNN | | Not applicable in E-commerce. Difficult implementation | In large data BPN (Back Propagation Network) has a good performance | accuracy is highly dependent on the measure of distance | It is not capable to detect the fraud at a time when fraudulent transaction is in progress |

## References

[1] Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K.Majumdar, "BLAST-SSAHA Hybridization for Credit Card Fraud Detection," *IEEE Transactions On Dependable And Secure Computing*, vol. 6, Issue no. 4, pp.309-315, October-December 2009.

[2] Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, "Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning," *Special Issue on Information Fusion in Computer Security*, Vol. 10, Issue no 4, pp.354-363, October 2009.

[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*, vol. 5, Issue no. 1, pp.37-48, January-March 2008.

[4] 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*, 14th October 2000.

[5] Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick, "Credit card fraud detection using Bayesian and neural networks," *Interactive image-guided neurosurgery*, pp.261-270, 1993.

[6] Amlan Kundu, S. Sural, A.K. Majumdar, "Two-Stage Credit Card Fraud Detection Using Sequence Alignment," *Lecture Notes in Computer Science, Springer Verlag, Proceedings of the International Conference on Information Systems Security*, Vol. 332/2006, pp.260- 275, 2006.

[7] Simon Haykin, "Neural Networks: A Comprehensive Foundation," 2nd Edition, pp.842, 1999.

[8] A. Chiu, C. Tsai, ―A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection," *Proceedings of the IEEE InternationalConference on e-Technology, e-Commerce and e-Service*, pp.177-181, 2004.

[9] R. Brause, T. Langsdorf, M. Hepp, ―Neural Data Mining for Credit Card Fraud Detection, ―International Conference on Tools with Artificial Intelligence, pp.103-106, 1999.

[10] Ghosh, D.L. Reilly, "Credit Card Fraud detection with a Neural- Network," Proceedings of the International Conference on System Science, pp.621-630, 1994.

[11] Z. Ning, A.J. Cox, J.C. Mullikin, "SSAHA: A Fast Search Method for Large DNA Databases," Genome Research, Vol. 11, No. 10, pp.1725- 1729, 2001.

[12] Lam, Bacchus, "Learning bayesian belief networks: An approach based on the MDL principle," Computational Intelligence, Vol. 10, Issue No. 3, pp.269-293, August 1994.

[13] Manoel Fernando Alonso Gadi, Xidi Wang, Alair Pereira do Lago, "Credit Card Fraud Detection with Artificial Immune System," Lecture Notes in Computer Science, Vol. 5132/2008, pp.119-131, 2008.

[14] Tom Madden, "The BLAST Sequence Analysis Tool", 2003.

[15] M. Mehdi, S. Zair, A. Anou and M. Bensebti," A Bayesian Networks in Intrusion Detection Systems," International Journal of Computational Intelligence Research, Issue No. 1, pp.0973-1873 Vol. 3, 2007.

[16] 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 IndiaPublications, pp.6-10, November 26, 2006.

[17] C. Phua, V. Lee, K. Smith, R. Gayler, "A Comprehensive Survey of Data Mining-based Fraud Detection Research," Artificial Intelligence Review, 2005.

[18] E. Aleskerov, B. Freisleben, B. Rao, "CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection," Proceedings of IEEE/IAFE conference on Computational Intelligence for Financial Engineering (CIFEr), pp.220-226, 1997.

[19] Philip K. Chan ,Wei Fan, Andreas L. Prodromidis, Salvatore J. Stolfo, "Distributed Data Mining in Credit Card Fraud Detection," IEEE Intelligent Systems ISSN, Vol. 14 , Issue No. 6, Pages: 67 - 74, November 1999.

[20] Barry Masuda, "Credit Card Fraud Prevention: A Successful Retail Strategy," crime prevention, Vol. 6, 1986.

[21] Linda Delamaire, Hussein Abdou, John Pointon, "Credit card fraud and detection techniques: a review," Banks and Bank Systems, pp. 57-68, 2009.

[22] Tej Paul Bhatla, Vikram Prabhu & Amit Dua "Understanding Credit Card Frauds," 2003.

[23] Russell, Norvig ," Artificial Intelligence - A Modern Approach," 2nd Edition, 2003.

[24] S.F.Altschul, W. Gish, W. Miller, W. Myers, J. Lipman, "Basic Local Alignment Search Tool," Journal of Molecular Biology, Vol. 215, pp.403-410, 1990.

[25] Ezawa.K. & Norton.S,"Constructing Bayesian Networks to Predict Uncollectible Telecommunications Accounts," IEEE Expert, October;45-51, 1996.

[26] Fan, W. Miller, M.Stolfo, S.Lee & P Chan, "Using Artificial Anomalies to Detect Unknown and Known Network Intrusions," Proc. of ICDM01, pp.504-507, 2001.

[27] C. Cortes and V. Vapnik, ―Support-vector networks," Machine Learning, vol. 20, no. 3, pp. 273–297, 1995

[28] T. M. Cover and P. E. Hart, ―Nearest neighbor pattern classification," IEEE Transactions on Information Theory, vol. 13, no. 1, pp. 21–27, 1967.

[29] P. Domingos and M. Pazzani, ―Beyond independence: conditions for the optimality of the simple Bayesian classifier," Machine learning, vol. 29, no. 2-3, pp. 103–130, 1997

[30] M. Zareapoor, K. R. Seeja, and A. M. Alam, ―Analyzing credit card: fraud detection techniques based on certain design criteria," International Journal of Computer Application, vol. 52, no. 3, pp. 35–42,2012.

[31] S. Maes, K. Tuyls, B. Vanschoenwinkel, and B. Manderick, ―Credit card fraud detection using Bayesian and neural networks," in Proceedings of the 1st International NAISO Congress on Neuro Fuzzy Technologies, pp. 261–270, 1993.