Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network

Tanmay Kumar Behera
Department of CSE & IT
Veer Surendra Sai University of Technology
Burla-768018, Odisha, India
tanmay.vssut@gmail.com

Suvasini Panigrahi
Department of CSE & IT
Veer Surendra Sai University of Technology
Burla-768018, Odisha, India
suvasini26@gmail.com

***Abstract*—Due to the rapid progress of the e-commerce and online banking, use of credit cards has increased considerably leading to a large number of fraud incidents. In this paper, we have proposed a novel approach towards credit card fraud detection in which the fraud detection is done in three phases. The first phase does the initial user authentication and verification of card details. If the check is successfully cleared, then the transaction is passed to the next phase where fuzzy c-means clustering algorithm is applied to find out the normal usage patterns of credit card users based on their past activity. A suspicion score is calculated according to the extent of deviation from the normal patterns and thereby the transaction is classified as legitimate or suspicious or fraudulent. Once a transaction is found to be suspicious, neural network based learning mechanism is applied to determine whether it was actually a fraudulent activity or an occasional deviation by a genuine user. Extensive experimentation with stochastic models shows that the combined use of clustering technique along with learning helps in detecting fraudulent activities effectively while minimizing the generation of false alarms.**

Keywords—Fraud, credit card, suspicion score, fuzzy clustering, neural network.

I. INTRODUCTION

Credit card has become the most popular mode of payment for both online as well as daily purchases. As a result, cases of fraud associated with it are also growing. Fraud can be defined as the unlawful usage on any system or goods. Credit card fraud is done through the use of the credit card details, with an intension of obtaining goods without paying for it. The loss due to credit card fraud has become so high that it seems to be a menace to the economy.

Statistics shows that on-line banking has been the fastest growing sector in this current scenario. During 2012, losses due to credit card accounted around 5.22 per $100 in total volume, up from 5.07 per $100 in 2011 [1]. As e-commerce continues to rise up over the past few years, losses to internet merchants were projected to be between $5 and $15 billion in 2005. Hacking, publication of obscene contents, credit cards and banking frauds among other cyber-crimes have filed an annual increase of more than 40% only in India in the past few years [2]. The credit card fraud is classified into two groups as physical fraud and virtual fraud. Physical fraud is the fraud that is being conducted using the stolen card whereas virtual fraud is the fraud which is done by misusing someone’s card details through internet and other channels. A study of over 160 companies revealed that online fraud or virtual fraud (committed over the Web or e-shopping) is 12 times higher than offline fraud or physical fraud (committed by using a stolen physical card) [3]. Thus, the virtual fraud possess a bigger problem in the financial sector and causes great losses as it may remain undetected for long time by the genuine user. For this reason, we focus on identifying this kind of fraud by behavioural analysis.

To address this problem, financial institutions apply various fraud prevention strategies such as credit card authorization, address verification system (AVS), rule-based detection, etc. However, fraudsters are adaptive and come up with several tricks and ideas to break the existing prevention mechanisms. Once the fraud prevention techniques fail, there is the requirement of devising an efficient fraud detection system (FDS) for detecting credit card frauds and maintaining the viability of the payment system.

The focus of this paper is to analyze the spending behaviour of credit card users based on the deviation from their past usage patterns so as to classify the transactions as fraudulent or genuine. Learning is also carried out on the suspicious transactions to minimize the misclassification of transactions.

II. RELATED WORK

Various techniques used in detecting fraud in credit card usage include genetic algorithm, neural network, data mining, game-theoretic approach and support vector machine. The solution using genetic algorithm and scatter search is proposed by Duman and Ozcelik [4]. Each transaction is associated with some score and based on which the transactions are classified as fraudulent or genuine. Ghosh and Reilly [5] have done a feasibility study for Mellon bank to check the effectiveness of the neural network for detection of credit card fraud and they have achieved the

978-1-4799-1734-1/15 $31.00 © 2015 IEEE
DOI 10.1109/ICACCE.2015.33

reduction of around 20%-40% in the overall loss. A new approach to this problem is given by Aleskerov et al. [6] as CARDWATCH, a neural network based data-mining system for credit card fraud detection (CCFD). Quah and Sriganesh [7] proposed a framework that can be applied in real-time where first an outlier analysis is done separately for each customer using self-organizing map (SOM) and classification algorithm is used to classify a transaction as fraudulent or genuine. A four component fraud detection system that is connected serially is proposed by Panigrahi et al. [8]. The main idea is to determine the suspicious transaction by applying Bayesian learning to identify the fraudulent activities. Srivastava et al. [9] proposed a new model which uses the Hidden Markov Model (HMM) that is trained with normal behavior of the card holders and based on it the classification is done. An automated credit card fraud detection system by applying Artificial Neural Network (ANN) and Bayesian Belief Network (BBN) is outlined by Maes et al. [10].

Fraud detection can be visualized as a data mining problem, where the target is to classify the transactions as legitimate or fraudulent. Chan et al. [11] made a division of the large sets of transactions into smaller subsets and then applied distributed data mining for building models of user behavior. The application of data mining is also carried out in the work of Chiu and Tsai [12]. They have considered the web services for data exchange among banks.

A meta-learning system helps in allowing financial institutions to share their frameworks of fraudulent transactions by exchanging classifier agents. Stolfo et al. [13] has applied four base classifiers namely, ID3, CART, Bayes RIPPER and the class-combiner strategy is used to select the best classifier for meta-learning. The game theory concept is given by Liu and Li [14] where the technique is used to predict the attacks on IDS protected system. Vasta et al. [15] have designed a model to show the interaction between an attacker and a FDS as the repeated game occurs between the two players, each trying to maximize its payoff.

A lot of variation is observed in the accuracy of most of the FDSs as mentioned above. The main challenge in this problem is that the numbers of occurrences of fraud are relatively small and thus requires detecting a rare event from a very large collection of legitimate transactions. This results the generation of false alarms, hence needs to be minimized. While failure to detect a fraud cases results in direct loss to the company, but the follow up actions required for pursuing the alse alarms also tend to be costly. In this work, our attempt is not only to detect the fraudulent usage of credit cards, but also to reduce the false alarm rate.

Every card holder has a particular type of spending behavior, which creates an activity profile for the user. Almost all the fraud detection methodologies capture the behavioral patterns as rules and check for any violation in subsequent transactions. However, the target of a reliable FDS is to learn the behavior of the users dynamically so as to minimize the losses. Thus, it is required to develop a FDS which can detect frauds effectively as well as learn the dynamic change of users and fraudsters' behavior over time.

We have proposed a FDS for detecting credit card frauds by applying the fuzzy clustering technique for determining the deviation of sending patterns of users. Due to the overlapping nature of cluster boundaries, the use of hard clustering is limited in real life applications. To reduce such limitations fuzzy clustering has been applied so that individual data points may belong to more than one cluster [16]. Moreover, neural network based learning is further applied to verify the suspicious cases. As neural network matches human intuition very closely, hence it provides a promising role model for modeling the neurological processes.

The rest of the paper is organized as follows. In the next section, the proposed work is described in detail along with the flow of events as shown in Fig. 2. In Section IV, the simulation results of the proposed method have been indicated. Finally we conclude the paper in Section V along with directions for future research.

III. PROPOSED WORK

The proposed FDS can be abstractly represented as a 5-tuple $< C, P, SC, \Phi_{Uth,} \Phi_{Lth}>$, where:

a) $C = \{C_1, C_2, \ldots\ldots, C_n\}$ is the set of cards on which the detection is performed.
b) $P = \{P(C_1), P(C_2), \ldots.., P(C_n)\}$ is the set of profiles of the card holders, where $P(C_k)$ represents the profile of the cardholder having card C_k. The profile is a set of patterns that contains information like transaction amount, items purchased, time of transaction, etc.
c) SC is the suspicion score for measuring the extent of deviation from normal profile.
d) Φ_{Uth} is the upper threshold value, where $0 \leq \Phi_{Uth} \leq 1$.
e) Φ_{Lth} is the lower threshold value, where $0 \leq \Phi_{Lth} \leq 1$ and $\Phi_{Lth} \leq \Phi_{Uth}$.

The hybrid approach towards credit card fraud detection is best modelled by the prototype as shown in Fig.1. It is a multi-layered approach consisting of:

- Initial Authentication and Verification
- Behavioural Analysis Phase by using Fuzzy C-Means Clustering
- Learning Phase by applying Neural Network.

The details of the credit card fraud detection process are described as follows:

A. Initial Authentication and Verification

The first layer is the layer for initial verification and screening where the credit card details such as credit card pin, transaction amount within the card limit and credit card expiry date are checked and user authenticity is verified.

B. Behavioural Analysis Phase

A cardholder generally carries out similar types of transactions in terms of amount and types of products, which can be viewed as a part of a cluster. However, the behaviour of the fraudster is expected to deviate from the usual card holder's profile as the fraudster is unaware of the normal patterns. Thus, the transactions carried out by the fraudsters can be observed as exception to the cluster known as outliers.

Fuzzy c-means (FCM) is a clustering algorithm that allows individual data to belong to two or more clusters [17]. This method has a great advantage to overcome the limitations of the hard clustering, and hence widely applied in many real life applications. Let $C_l = \{c_1,\ldots..,c_n\}$ be the clusters belonging to the datasets for a particular card C_k and $A = \{a_1,a_2,\ldots..,a_n\}$ be the possible attributes in a transaction. In this work, the attributes used for clustering are transaction amount and items purchased. Suppose, transaction made on a card C_k is denoted as T_{Ck}. The cluster is formed based on the spending patterns followed by cardholder C_k. The Euclidian distance d_{ik} from the cluster head p_i to the object point x_k of the transaction T_{Ck} is calculated by using the following expression:

$$SC = d_{ik} = \|x_k - p_i\| \tag{1}$$

The *SC* is then compared with the already pre-set threshold values i.e. upper threshold (Φ_{Uth}) and the lower threshold (Φ_{Lth}) which are determined experimentally. Depending on the result of comparison, three rules are defined as follows:

a) If ($SC < \Phi_{Lth}$), then the credit card transaction is allowed. (Genuine)
b) Else if ($\Phi_{Lth} \leq SC \leq \Phi_{Uth}$), then move the transaction to the suspicious table for applying the learning mechanism for strengthening the initial observation. (Suspicious)
c) Else, reject the transaction i.e. when $SC > \Phi_{Uth}$. (Fraudulent)

The transactions those are found to be suspicious are passed to the learning phase before taking the final decision.

C. Learning Phase

The suspicious transactions are moved to the suspicious table where they are kept for further analysis and classification which is done by using the feed forward neural networks with backpropagation (FFNNBP). A supervised learning algorithm is used for learning which is based on the conjugate gradient method that is well known as Scale Conjugate Gradient (SCG) [18]. It has set a benchmark against the performance and accuracy of the standard backpropagation algorithm (BP) due to its faster execution. Moreover, SCG also eliminates some of the disadvantages of other backpropagation algorithms such as low convergence rate and poor behavior on large scale of datasets.

In the current work, we have used the attributes such as items purchased and the time of purchase. Based on these attribute values, fraud cases are statistically examined to determine the relationships among input data and values for certain prime parameters in order to understand various patterns of fraud. This knowledge of fraud is then iteratively fed to the feed-forward neural networks. A suspicious transaction is finally classified as fraudulent or genuine based on similarity with the trained patterns. The learning component is included in our proposed system so as to reduce the misclassification rate.

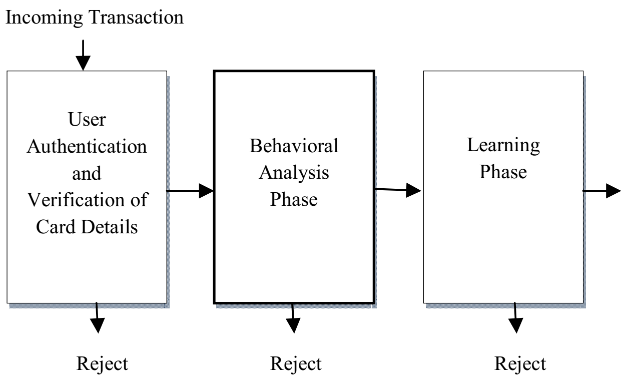
Incoming Transaction
User Authentication and Verification of Card Details
Behavioral Analysis Phase
Learning Phase
Reject
Reject
Reject

Fig.1. Prototype Structure

IV. SIMULATION AND RESULTS

We demonstrate the performance of our proposed FDS by testing it with large scale data.

A. Simulation

The datasets developed by Panigrahi et al. [8] has been employed for testing due to the unavailability of the real life credit card datasets or any benchmark datasets. The simulator uses the Gaussian distribution to generate the synthetic transactions that represents the behavior of the genuine users as well as fraudsters. Large scale datasets are being produced on which testing of the proposed system is performed. The simulator has been designed to handle various real life scenarios those are usually seen in credit card transaction processing systems.

B. Results and Discussions

The implementation of the proposed FDS has been done in MATLAB-2014. The experiments are carried out by giving input vectors to the fuzzy c-means algorithm module. The Euclidian distance is measured based on which suspicion score is calculated for each of the data points present in the clusters. In our experiment, we have empirically determined the threshold values as: lower threshold (Φ_{Lth}) = 0.28 and upper threshold value (Φ_{Uth}) = 0.72. The basic parameters through which the system performance is being evaluated are True Positive (TP)/Sensitivity, True Negative (TN)/Specificity and False Positive (FP). TP is the percentage of correctly classified fraudulent transactions, TN is the percentage of correctly classified genuine transactions and FP refers to the percentage of incorrectly categorized genuine transactions.

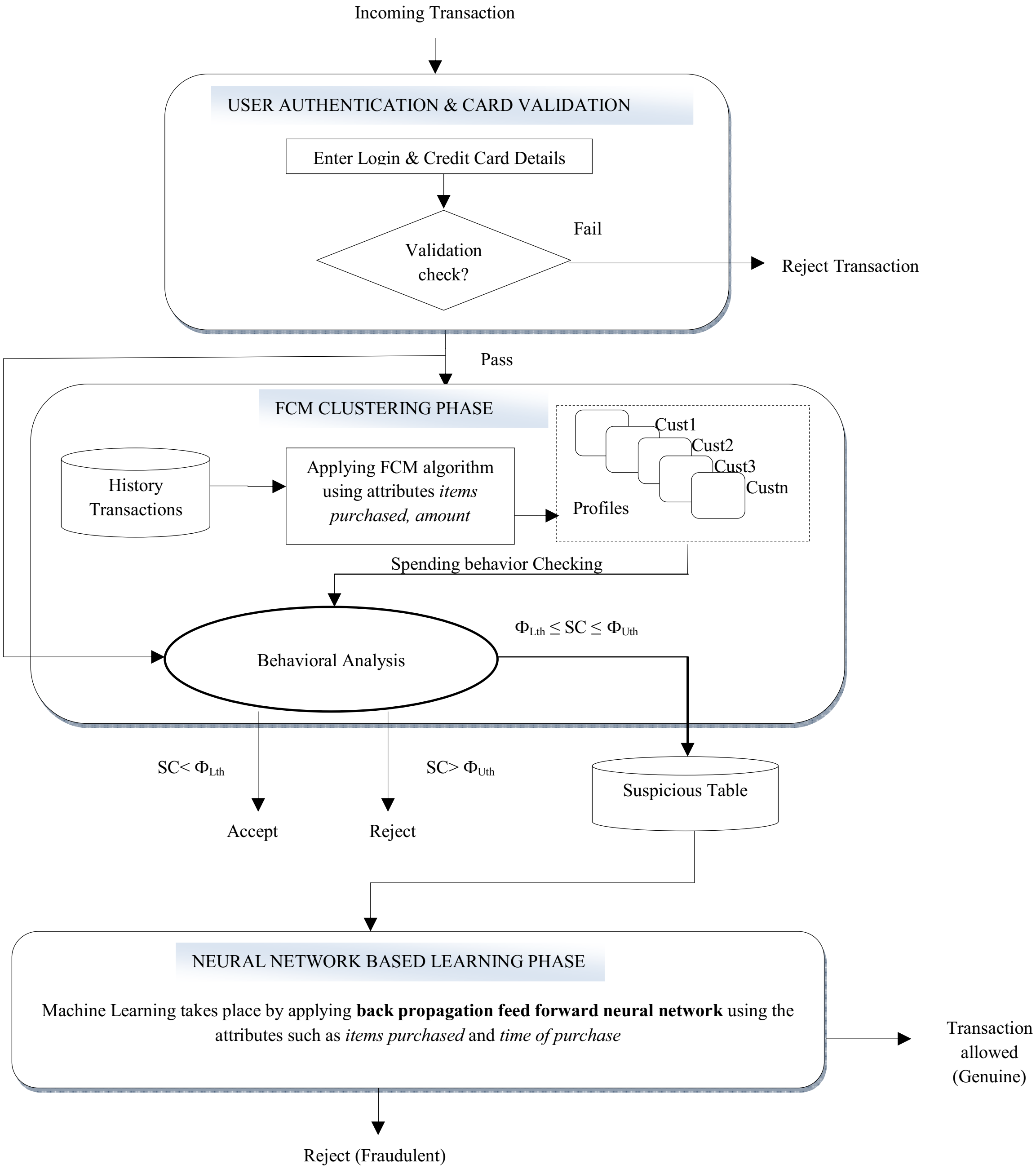
Incoming Transaction
USER AUTHENTICATION & CARD VALIDATION
Enter Login & Credit Card Details
Validation check?
Fail
Reject Transaction
Pass
FCM CLUSTERING PHASE
History Transactions
Applying FCM algorithm using attributes items purchased, amount
Cust1
Cust2
Cust3
Custn
Profiles
Spending behavior Checking
Behavioral Analysis
ΦLth ≤ SC ≤ ΦUth
SC< ΦLth
SC> ΦUth
Suspicious Table
Accept
Reject
NEURAL NETWORK BASED LEARNING PHASE
Machine Learning takes place by applying back propagation feed forward neural network using the attributes such as items purchased and time of purchase
Transaction allowed (Genuine)
Reject (Fraudulent)

Fig.2. Flow of events in the proposed Credit Card Fraud Detection System

The transactions having suspicion score values higher than that of the upper threshold value (Φ_{Uth}) are simply discarded in the clustering phase. Only the transactions having threshold values in between Φ_{Lth} and Φ_{Uth} are termed as suspicious and are kept in a suspicious table. The transactions in the suspicious table are fed to the machine learning layer where learning takes place using the SCG backpropagation algorithm. The network is used to train the datasets with 5-hidden layers. As we increase the number of hidden layers, better results are obtained but the computation time also increases. The whole dataset is divided into three categories i.e. 70% for training phase, 15% for validation, 15% for testing. The learning component classifies the suspicious transactions and gives the following results: 93.90% correctly classified transactions and 6.10% incorrectly classified transactions.

We have shown the Receiver-Operating Characteristics (ROC) curve as shown in Fig. 3. The ROC is a metric that is used to check the quality of the classifier by plotting the true positive rate against the false positive rate. A perfect ROC shows points in the upper left corner with 100% sensitivity and 100% specificity. It is evident from the curve in Fig. 3 that the performance of the proposed FDS is correct in terms of ROC.

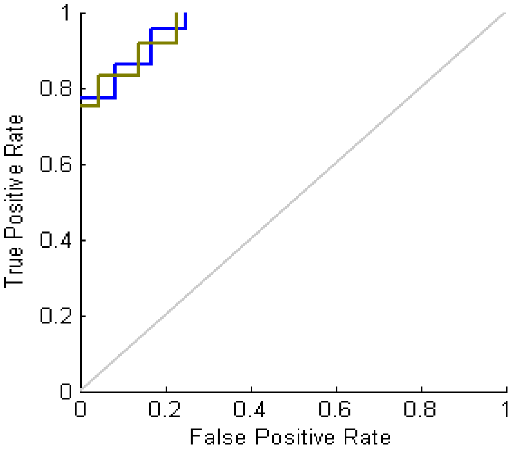

Fig. 3 ROC Curve

It can be clearly seen from Fig. 4 that, as we increase the size of the genuine transactions, percentage of FP decreases over a time period, thus the behavior of the user is being captured more consistently by the FDS. The TP rate also increases accordingly. Similarly, Fig. 5 shows that when we increase the number of the fraudulent transactions (size), TP rate increases and the FP rate decreases.

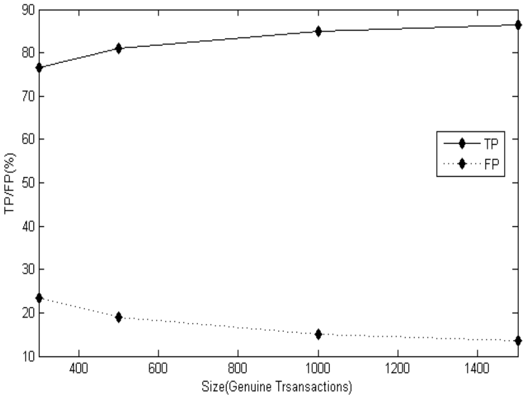

Fig. 4 Variation of TP/FP with size of genuine transaction

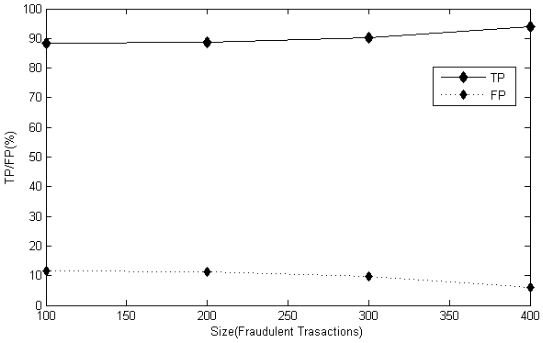

Fig. 5 Variation of TP/FP with size of fraudulent transaction.

V. CONCLUSIONS

Though most of the fraud detection systems show good results in detecting fraudulent transactions, they also lead to the generation of too many false alarms. This assumes significance especially in the domain of credit card fraud detection where a credit card company needs to minimize its losses but, at the same time, does not wish the cardholder to feel restricted too often. We have proposed a novel credit card fraud detection system based on the integration of two approaches that is fuzzy clustering and neural network. We have used the fuzzy c-means clustering technique for the grouping of the similar datasets and employed the neural network as a learning technique to reduce the misclassification rate based on the attributes transaction amount, type of items purchased and time of transaction.

We have used stochastic models for analysing the performance of the proposed system. The simulation yielded up to 93.90% TP and less than 6.10% FP. Based on the results, we conclude that combinatorial use of fuzzy clustering and learning are the appropriate approaches for addressing this type of real world problems. The system can be further improved by using additional attributes like location of transaction, time gap between transactions, etc. for framing rules. Moreover, other learning techniques needs to be experimented and comparison between them are required to be done in future research.

References

[1] Credit Card Fraud Statistics-2013,<http: www.cardhub.com/edu/credit-fraud-statistics >, 5 Feb, 2015.

[2] A Tale of two fraud stats, < www.pymts.com/in-depth/2014/a-tale-of-two-fraud-stats/#.VN01GJ3F9PS >, 5 Feb,2015.

[3] Online fraud is 12 times higher than offline fraud,<http:// sellitontheweb.com/ezine/news0434.shtml>, 20 June, 2007

[4] E. Duman, and M.H. Ozcelik, “Detecting credit card fraud by genetic algorithm and scatter search,” Expert Systems with Applications, 38, pp. 13057–13063, 2011.

[5] S. Ghosh and D.L.Reilly, "Credit card fraud detection with a neural-network," in: Proceedings of the Annual International Conference on System Science, pp. 621–630, 1994.

[6] E. Aleskerov, B. Freisleben & B. Rao, "CARDWATCH: a neural network based database mining system for credit card fraud detection," in: Proceedings of the Computational Intelligence for Financial Engineering, pp. 220–226, 1997.

[7] J. T. S. Quah and M. Srinagesh, "Real-time credit fraud detection using computational intelligence," Expert Systems with Applications, 35, pp. 1721–1732, 2008

[8] S. Panigrahi, A. Kundu, S. Sural, & A. Majumdar, "Credit card fraud detection a fusion approach using Dempster–Shafer theory and bayesian learning," Information Fusion, pp. 354–363, 2009.

[9] A. Shrivastava, A. Kundu, S. Sural and A.K. Majumdar, "Credit Card Fraud Detcetion using Hidden Markov Model," IEEE transactions on dependable and secure computing, Vol. 5, pp.37-48, 2008.

[10] S. Maes, K. Tuyls, B. Vanschoenwinkel and B. Manderick, "Credit card fraud detection using Bayesian and neural networks," in: Proceedings of the First International NAISO Congress on Neuro Fuzzy Technologies, 2002.

[11] P.K. Chan, W. Fan, A.L. Prodromidis, S.J. Stolfo, "Distributed data mining in credit card fraud detection," in: Proceedings of the IEEE Intelligent Systems, pp. 67–74, 1999.

[12] C. Chiu and C. Tsai, "A web services-based collaborative scheme for credit card fraud detection," in: Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service, pp. 177–181, 2004.

[13] S.J. Stolfo, D.W. Fan, W. Lee and A.L. Prodromidis, "Credit card fraud detection using meta-learning: issues and initial results," in: Proceedings of the Workshop on AI Methods in Fraud and Risk Management, pp. 83–90, 1997.

[14] P. Liu and L. Li, "A Game-Theoretic Approach for Attack Prediction," Technical Report, PSU-S2-2002-01, Penn State University, 2002.

[15] V. Vatsa, S. Sural, A.K. Majumdar, "A game-theoretic approach to credit card fraud detection," in: Proceedings of the International Conference on Information Systems Security, Lecture Notes in Computer Science, vol. 3803, pp. 263–276, 2005.

[16] J. Nayak, B. Naik, and H. S. Behera, " Fuzzy C-Means (FCM) Clustering Algorithm: A Decade Review from 2000 to 2014," In Computational Intelligence in Data Mining-Volume 2, Springer India, pp. 133-149, 2015.

[17] James C. Bezdek, "FCM: The fuzzy *c*-means clustering algorithm," Computers & Geosciences, Elsevier, Volume 10, Issues 2–3, pp. 191–203, 1984.

[18] M. F. Moller, "A scaled conjugate gradient algorithm for fast supervised learning," Neural Networks , Elsevier, Volume 6, Issue 4, pp. 525–533, 1993.