Selection of Optimal Credit Card Fraud Detection Models Using a Coefficient Sum Approach

Suman Arora
sumanch09@gmail.com
Dharminder Kumar
dr.dk.kumar.02@gmail.com

Guru Jambheshwar University of Science & Technology, Hisar, India

***Abstract*---During the past years various fraud detection techniques were proposed and used to reduce fraudulent activities. Selection an optimal fraud detection model becomes keen area of interest for researchers in the field of anomaly detection. Methods and tools for fraud detection model selection which were used in the literature used a limited no of model selection criteria for finding the detection of fraud in various areas. So for the first time we propose a approach based on a Coefficient sum method. This approach is used for ranking of Fraud detection models for finding the optimal model from various fraud detection models. For ranking the FDMs, various model selection criteria, with a set of FDMs are require Real data sets are used for illustration of the Coefficient sum method. The result of this paper gives a ranking method based on the Sum value of each criteria of FDM.**

Keywords— Credit Card, Fraud, Coefficient Sum

I. INTRODUCTION

Many modern techniques for detecting fraud are continually involves and applied to many areas due to the remarkable lift of fraud which effects on financial field in each year. Fraud is defined in the Association of Certified Fraud Examiners (ACFE) as "the use of one's occupation for personal enrichment through the deliberate misuse or application of the employing organization's resources or assets [1]". With the development of latest technology and global communication, fraud is increasing noticeably, resulting in extensive sufferers to the industries. So, fraud detection has become an main area of research. Credit card fraud is a major problem for financial institutions globally. The annual cost due to it is in the billions of dollars [2].To maximize correct predictions and minimize incorrect predictions is the main aim of the fraud detection systems [3]. Performance metrics which are used for finding the performance of systems are very important to define carefully. True positive rate, false positive rate, and average time of detection are the some metrics used by the several fraud detection systems. The classical fraud detection models give maximum accuracy rate and minimize false positive rate. So all researchers have shown that some groups of models have several parameter values which are mull over better than others; for example, Fuzzy Darwinian [4], Dempster Shafer theory [5] show accuracy high in True Positive rate (TP) and false positive rate (FP). Processing speed is fast in case of BLAH-FDS and ANN in credit card [6]. Researchers only compare their TP, FP rate and accuracy to compare different models.

This study accentuate on credit card fraud detection models discussed in section II i.e. total of sixteen credit card fraud detection models. Section III presents a classification of fraud analytics techniques which are used by all the models discussed section II. Next section IV presents a comparison criterion which is used for comparison of these models. Section V proposed an approach for ranking the models. Section VI gives an example to illustrate the approach and last section VII will conclude the paper.

II. LITERATURE REVIEW

Various Fraud detection Models (FDMs) have been proposed in past years. Every model had shown its good work with a unique dataset, but no model appropriate for all datasets**.** There are various models for detecting fraud in credit card:

A. Dempster–Shafer theory and Bayesian learning [5]

Four components of Dempster Shafer Theory are: rule-based filter, Dempster–Shafer adder, transaction history database and Bayesian learner.

B. Hidden Markov Model [10]

Fraud detection system receives each incoming transaction and check the purchasing behavior for finding whether the transaction is fraud or not [13],[10].

C. Detection of Credit Card Fraud using Fuzzy[4]

Fuzzy Darwinian Detection system use fuzzy logic rules [4]. The system consists of a fuzzy expert system and a Genetic Programming (GP) search algorithm.

D. Bayesian and Neural Networks[11]

Bayesian networks or belief networks use machine learning and data mining methods of artificial intelligence.

E. Fraud detection using Association rules[12]

In this fuzzy logic is used with association rules to overcome the difficulties of minimum support and confidence, optimizes the execution time.

F. CARDWATCH[13]

CARDWATCH used neural network for detecting fraud in credit card.

ISBN: 978-1-5090-6471-7/17/$31.00 ©2017 IEEE

G. Fraud detection using SOM & PSO[14]

Self organize map and particle swarm optimization technique were combined and proposed a hybrid approach Self organizing Particle Swarm Optimization (SOPSO).

H. Genetic Algorithm and Scatter Search[15]

A method is developed using genetic algorithm (GA) and scatter search (SS) which improve fraud detection in credit card.

I. SVM and Logistic regression [16]

This paper examines the performance of two data mining techniques Support vector machine and random forest with the logistic regression in credit card fraud detection.

J. Fraud detection using Decision Tree and SVM[17]

Decision tree model built in this study use three classification models C5.0, C&RT and SVM and CHAID.

K. Fraud using computational intelligence (SOM)[18]

This approach used self organizing map for reducing the frauds in credit card.

L. Max entropy with Bayesian learning[19]

Credit card fraud detection system is proposed which detect frauds using maximum entropy and Bayesian learning.

M. Fraud detection using Rule based expert system [20]

A rule based expert is proposed for detecting fraud in credit card.

N. Fraud detection using Neural Network [21]

This system based on neural classifier for detecting fraud in credit card.

O. Game-Theory Approach [22]

Detection of frauds in credit card using game theory is proposed.

P. Fraud detection using Peer Group analysis [23]

A peer group is a group of records which behave same as the target records. When the behavior of the target record is different from its peers, an anomaly can be signed.

III. CLASSIFICATION OF FRAUD ANALYTICS TECHNIQUES

Fraud analytics techniques are classified as: Descriptive (Unsupervised), Predictive (Supervised) and Artificial & Computational Intelligence [24] in Fig. 1.

A. Descriptive or Unsupervised Techniques

1) Graphical outlier detection procedure [25]: A histogram or box plot for one dimensional and scatter plot for two or more dimensional outliers and online analytical processing (OLAP) for graphically method and multidimensional data analysis.

2) Statistical outlier detection [25]: Calculating the z-score is well known statistical outlier detection method.

3) *Break point analysis [26]:* When anomalous behavior is detected a break point is considered as observation or time.

4) Peer group analysis [26]: Peer-group analysis is also unsupervised method is used as tool for monitoring behavior over time.

5) Association rule analysis [27]: Associations between items were discovered by the frequent itemset mining in large transactional and relational datasets.

6) Clustering [28]: Main function of Clustering is to partition the set of transactions in two groups such that similarity within a group is maximized (cohesive), and the dissimilarity between groups is minimized (separated).

7) Self-Organizing Maps [31]: A self-organizing map (SOM) is a neural network technique but used unsupervised learning.SOM allows users to visualize data from high-dimensional to low-dimensional.

B. Predictive Techniques

In predictive analytics, the purpose is to construct an analytical model predicting target objects of interest [25].

1) Linear Regression: Linear regression model is represented as :

$$Z = \beta_0 + \beta_1 X_1 + \cdots + \beta_n X_n \quad (1)$$

Where Z represents the target variable, and X_1, … ,X_n the descriptive variables. The β parameters measure the effect on the target variable Y for each descriptive [25].

2) Logistic Regression: To illustrate data and to elucidate the relation between one dependent i.e. binary variable and more than one ordinal, nominal or interval variables logistic regression is used [25].

3) Decision Trees: Decision tree is a tree based organization where every non-leaf node corresponds to a testing condition of a field and each terminal node corresponds to label of class [32].

4) Neural Networks: A neural network is a computational approach which is based on a large number of neural units. These neural units are linked as input/output unit in which each link has weight associated with it. Network learns using weight adjustment during learning phase [32].

5) Support Vector Machines (SVM): SVM is statistical learning technique for classification of both linear and non-linear data[32].

6) Naïve Bayes: Naïve Bayes classification method is based on Bayes' Theorem. Bayesian classifiers are statistical classifiers [32].

7) Rule Based Classification: Rule based classification [32] is based on IF-THEN rules.

C. Artificial & Computational Intelligence Techniques

There are various artificial and computational intelligence techniques are available in literature. We discuss here some of those techniques which are used in fraud analytics mainly in credit card fraud detection.

1) Genetic Algorithm (GA): In Genetic Algorithm i.e inspired from natural evolution randomly generated rules are considered as an initial population. New populations are

generated from this population by the crossover and mutation operator [33].

2) Particle swarm optimization (PSO): Particle swarm optimization is a population based computational and optimization technique which is inspired by flocking and schooling patterns of birds and fish [34].

3) Hidden Markov Model (HMM): Hidden Markov model (HMM) is used for detecting fraud in credit card [10], [35].

4) Fuzzy logic: **In** Fuzzy logic truth values of variables may be a number between 0 and 1. It represents the degree of membership for which a particular value has in given category [36].

5) Game Theory: Game theory is used for decision making and it is the branch of mathematics which deals with the analysis of strategies.[37].

6) Dempster Shafer Theory (DST): Dempster Shafer theory or evidence theory is a general framework for reasoning with uncertainty [38].

7) Entropy: Entropy is a measure of information and uncertainty of a random variable [32][39].

IV. COMPARISON CRITERIA FOR FRAUD DETECTION MODELS

To investigate the effectiveness of techniques, various comparison criteria are proposed to compare approaches. The comparison criteria we used are described as follows. E_i and O_i : the estimated (predicted) and Observed (Actual) no of fraudulent transactions respectively in i[th] number of dataset.

A. Bias

Bias is defined as [40], [41]

$$Bias = \frac{\sum_{i=1}^{n}(E_i - O_i)}{n} \quad (2)$$

Bias is the sum of the difference between the predicted no of fraudulent transactions and the actual no of fraudulent transactions.

B. The Mean Square Error (MSE)

Mean square error or mean square deviation measure the average of the square of the errors or deviations and is defined as [42]

$$MSE = \frac{\sum_{i=1}^{n}(E_i - O_i)^2}{n} \quad (3)$$

C. The Root Mean Square Error(RMSE)

Like MSE, RMSE measure the deviation but measure using the root value of MSE. [42].

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(E_i - O_i)^2}{n}} \quad (4)$$

D. The Mean Absolute Error (MAE)

It is also same as MSE, but absolute value is used for measuring the deviation. It is defined as[42]

$$MAE = \frac{\sum_{i=1}^{n}|(E_i - O_i)|}{n} \quad (5)$$

E. The predictive-ratio risk (PRR)

PRR measures the distance of expected vale from the observed value against the expected value..

$$PRR = \sum_{i=1}^{n}\frac{(E_i - O_i)}{E_i} \quad (6)$$

F. Variance

The variance is how much the predictions for a given point vary between different realizations of the model. Mathematically variance is defined as in [40], [41]

$$Variance = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\big((E_i - O_i) - Bias\big)^2} \quad (7)$$

G. Root Mean Square Prediction Error (RMSPE)

RMSPE is a measure the proximity with which the model predict the observation. It is defined as [40], [41]

$$RMSPE = \sqrt{Variance^2 + Bias^2} \quad (8)$$

H. The Residual sum of squares (RSS):

It is the sum of the square of residual i.e deviation from predicted from actual observations. RSS is defined as [41]

$$RSS = \sum_{i=1}^{n}(E_i - O_i)^2 \quad (9)$$

I. Theil statistic (TS)

TS is the percentage of average difference for whole period examine to the observed values [44].

$$TS = \sqrt{\frac{\sum_{i=1}^{n}\big((E_i - O_i)\big)^2}{\sum_{i=1}^{n}(O_i)^2}} \quad (10)$$

J. Accuracy

Accuracy is the percentage of the correctly classified transactions. Accuracy= (TP+TN) / (TP+FP+FN+TN) [32].

V. SELECTION OF APPROACH USING SIMILAR COEFFICIENT SUM METHOD

A clustering algorithm is proposed to detect outlier based on similar coefficient sum method. This method calculates the similarity between the objects and then makes the clusters. It is described as follows [45], [46]: Let R={r1,r2,,……rn} be a set of approach to be test out, each approach with n attributes. Here we have sixteen approaches and ten selection attributes considered. We arrange the approaches and selection attributes in the form of data matrix having 16 numbers of columns (approaches) and nine numbers of rows (attributes). For finding the dissemination quantity of approaches among R, similar coefficient x_{ij} between each approach should be computed first, and then evaluated similar coefficient matrix is X.

p_i is the sum of the i[th] approach in similar coefficient matrix. Ranking of approaches are done on the basis of p_i value of approach as calculated above. Smaller the p_i value of approach represents good rank as compare to bigger p_i value of approach. So compare all p_i values and provide ranks of each approach.

$$R = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix} \quad X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{bmatrix} \quad (11)$$

$$x_{ij} = 1 - \sqrt{\frac{1}{n}\sum_{k=1}^{m}\big(r_{ik} - r_{jk}\big)^2} \quad (12)$$

$$p_i = \sum_{j=1}^{n} x_{ij} \quad (13)$$

VI. ILLUSTRATED EXAMPLE

The main motive of this illustration is to check the accuracy of the coefficient sum method so that a comparative analysis of the approaches should be done. We consider 16 credit card fraud detection models as described above and A1, A2…A16 used as abbreviations as in Table I. Dataset having fraudulent transactions has been taken for evaluation and ranking of these sixteen credit card fraud detection models according to ten criteria as discussed in above section: Variance, RSS, Bias, MSE, MAE, PRR, RMSPE, ,TS and Accuracy. The dataset was collected from banks whose information is not providing here for security reasons. The values of all ten criteria for each approach are calculated using equations given in section IV. These values are given in Table II for comparing the approaches according to the given criteria values. Now the problem arise, how we will do ranking of FDMs using these criteria because values of the selection criteria vary among different FDMs. For solving this problem we use coefficient sum method to for ranking the FDMs according to these ten criteria taken collectively. The manifestation is to check the implementation of the method, and to build up a method for ranking the considered sixteen FDMs. The matrix R can be representing the values of all parameters of all sixteen models. The coefficient matrix, X can be obtained using (12).Finally, the coefficient sum of all FDMs is calculated from (13). Table III shows the coefficient sum value and ranking of all FDMs based on their selection criteria. Ranking is based on the coefficient sum value for each of the FDMs that are calculated considering all ten attributes collectively using Coefficient sum method. FDM having smallest sum value is given rank 1 and second smallest value is given rank 2, and so on. The results, so achieved, represent that the Fraud detection using PSO & SOM is given rank 1 according to analysis using ten selection criteria and then rank 2 is given to model with max entropy and Dempster Shafer theory models is ranked 3 and so on. Peer group analysis and game theoretic approach with the maximum sum value are ranked at number 15, and 16, respectively.

VII. CONCLUSION

This study discusses the problem of optimal selection of Fraud detection models. When whole set of selection criteria and FDMs are defined, an effective process coefficient sum method can be applied. This approach is also used as a decision maker for various analyses according to his or her preferences. For all selection criteria not any one Fraud detection model is optimal. So we proposed a method which is suitable for ranking the fraud detection models according to various comparison criteria taken all collectively. A comparatively simple mathematical formulation and basic matrix operation is used in coefficient sum method. It is also used for solving complex multi-attributes decision problems; including both quantitative and qualitative factors.

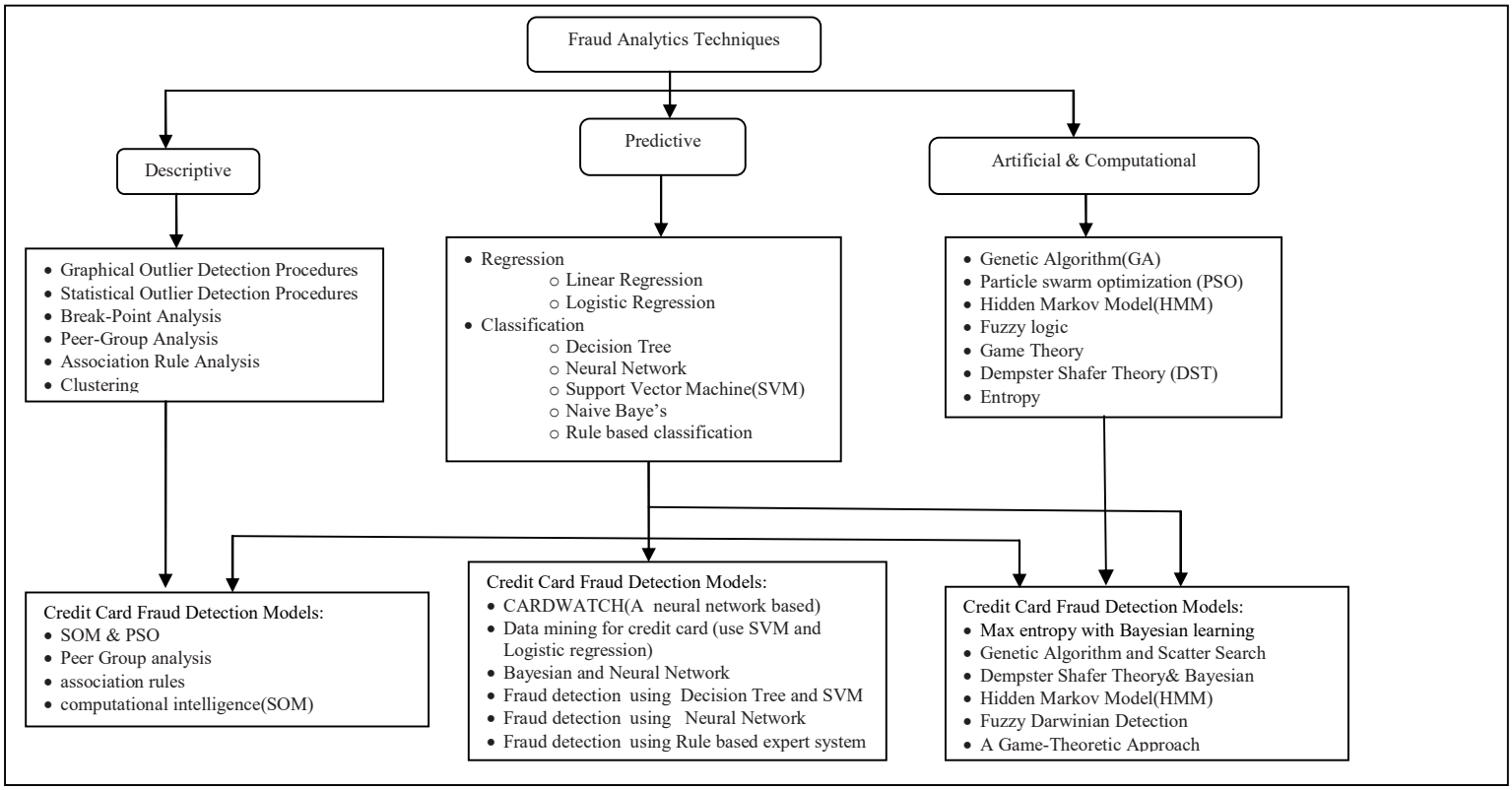

Fig. 1. Classification of Fraud Analytics Techniques

TABLE I. ABBREVATIONS OF ALL FRAUD DETECTION MODELS

Abbreviation	Name of Model	Abbreviation	Name of Model
A1	A Game-Theoretic Approach to Credit Card Fraud Detection	A9	Max entropy with Bayesian learning
A2	Fraud detection using Decision Tree and SVM	A10	Fraud detection using association rules
A3	Fraud detection using Rule based expert system	A11	Fuzzy Darwinian Detection of credit card fraud
A4	Fraud detection using Dempster Shafer Theory& Bayesian	A12	Fraud detection using SOM & PSO
A5	CARDWATCH (A Neural Network based)	A13	Fraud detection using Peer Group analysis
A6	Fraud detection using Neural Network	A14	Fraud detection using Bayesian and Neural Network
A7	Fraud detection using Hidden Markov Model (HMM)	A15	Data mining for credit card (use SVM and Logistic regression)
A8	Fraud detection using computational intelligence (SOM)	A16	Fraud detection using Genetic Algorithm and Scatter Search

TABLE II. DATABASE FOR ACTUAL AND OBSERVED VALUES OF CRITERIA FOR EACH ALTERNATIVE FDM.

Approaches	Bias	RSS	MSE	RMSE	MAE	RMSPE	TS	Variance	PRR	Accuracy
A1	14.25	847	211.75	14.55163	14.25	14.37301	0.722289	1.876388	2.358631	77.23
A2	13.25	769	192.25	13.86542	13.25	13.3822	0.682513	1.876388	2.083831	82.14
A3	13.75	797	199.25	14.11559	13.75	14.02082	0.700707	2.742414	2.142318	84.45
A4	10.5	514	128.5	11.33578	10.5	10.59874	0.556074	1.443376	1.576741	92.3
A5	10	738	184.5	13.58308	10	10.14889	0.609825	1.732051	2.025	85.32
A6	-4.75	135	33.75	5.809475	4.75	5.220153	0.323154	2.165064	-0.39528	83.57
A7	8.25	275	68.75	8.291562	8.25	8.261356	0.439832	0.433013	1.248796	90.13
A8	12.25	665	166.25	12.8938	12.25	12.25085	0.614905	0.144338	2.346949	87.36
A9	9	386	96.5	9.823441	9	9.0185	0.495852	0.57735	1.344322	92.32
A10	5.25	113	28.25	5.315073	5.25	5.251984	0.342421	0.144338	0.686214	78.26
A11	7.25	253	63.25	7.952987	7.25	7.858117	0.430958	3.031089	0.838599	88.79
A12	10.5	458	114.5	10.70047	10.5	10.59874	0.532367	1.443376	1.586077	93.12
A13	3.75	73	18.25	4.272002	3.75	3.752777	0.311432	0.144338	0.437594	79.34
A14	13.5	732	183	13.52775	13.5	13.50309	0.66291	0.288675	2.437635	88.96
A15	7.5	252	63	7.937254	7.5	7.549834	0.421335	0.866025	1.214209	89.34
A16	7.5	226	56.5	7.516648	7.5	7.505553	0.415245	0.288675	1.01837	90.34

TABLE III. FDMS RANKING BASED ON COEFFICIENT SUM METHOD

Sr. No	Fraud Detection Models (FDMs)	Coefficient Sum	Rank		Sr. No	Fraud Detection Models (FDMs)	Coefficient Sum	Rank
1	A Game-Theoretic Approach	1613.70	16		9	Max entropy with Bayesian learning	965.79	2
2	Decision Tree and SVM	1346.41	12		10	Association rules	1404.57	13
3	Rule based expert system	1432.85	14		11	Fuzzy Darwinian Detection	1046.15	5
4	Dempster Shafer Theory & Bayesian	994.62	3		12	SOM & PSO	965.84	1
5	CARDWATCH	1267.06	10		13	Peer Group analysis	1548.34	15
6	Neural Network	1337.43	11		14	Bayesian and Neural Network	1254.84	9
7	Hidden Markov Model(HMM)	1023.06	4		15	SVM and Logistic regression	1047.62	6
8	Computational intelligence(SOM)	1150.19	8		16	Genetic Algorithm and Scatter Search	1101.04	7

REFERENCES

[1] "Investigating Fraudulent Acts, University Of Houston System Administrative Memorandum", http://www.uhsa.uh.edu/samiAM/01C04.htm, 2000.

[2] Anonymous, "Credit Card Fraud — U.S.," HSN Consultants Incorporated March 2007.

[3] SAS Institute. *Using Data Mining Techniques for Fraud Detection: A Best Practices Approach* **to** *Government Technol**ogy** Solutions. Whitepapers.* hnp:iiwww.sas.com, 1996.

[4] Bentley, P. J., Kim, J., Jung, G. H., & Choi, J. U. (2000). Fuzzy Darwinian Detection of Credit Card Fraud. In *the 14th Annual Fall Symposium of the Korean Information Processing Society, 14th October*.

[5] 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

[6] Kundu, A., Panigrahi, S., Sural, S., & Majumdar, A. K. (2009). Blast-ssaha hybridization for credit card fraud detection. *IEEE Transactions On Dependable And Secure Computing*, *6*(4), 309-315.

[7] Raj, S. B. E., & Portia, A. A. (2011, March). Analysis on credit card fraud detection methods. In *Computer, Communication and Electrical Technology (ICCCET), 2011 International Conference on* (pp. 152-156). IEEE.

[8] Dorronsoro, J. R., Ginel, F., Sgnchez, C., & Cruz, C. S. (1997). Neural fraud detection in credit card operations. *IEEE transactions on neural networks*,*8*(4), 827-834.

[9] Quah, J. T., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. *Expert systems with applications*, *35*(4), 1721-1732.

[10] Khan, M. Z., Pathan, J. D., & Ahmed, A. H. E. (2014). Credit Card Fraud Detection System Using Hidden Markov Model and K-Clustering. *International Journal of Advanced Research in Computer and Communication Engineering*, *3*(2), 5458-5461.

[11] Maes, S., Tuyls, K., Vanschoenwinkel, B., & Manderick, B. (2002, January). Credit card fraud detection using Bayesian and neural networks. In *Proceedings of the 1st international naiso congress on neuro fuzzy technologies* (pp. 261-270).

[12] Sánchez, D., Vila, M. A., Cerda, L., & Serrano, J. M. (2009). Association rules applied to credit card fraud detection. *Expert Systems with Applications*, *36*(2), 3630-3640.

[13] Aleskerov, E., Freisleben, B., & Rao, B. (1997, March). Cardwatch: A neural network based database mining system for credit card fraud detection. In*Computational Intelligence for Financial Engineering (CIFEr), 1997., Proceedings of the IEEE/IAFE 1997* (pp. 220-226). IEEE.

[14] Arora S., & Kumar,D. Hybridization of SOM and PSO for detecting fraud in credit card. *International Journal of Information Systems in the Service Sector (IJISSS) (*accepted).

[15] Duman, E., & Ozcelik, M. H. (2011). Detecting credit card fraud by genetic algorithm and scatter search. *Expert Systems with Applications*, *38*(10), 13057-13063

[16] Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602-613.

[17] Şahin, Y. G., & Duman, E. (2011). Detecting credit card fraud by decision trees and support vector machines.

[18] Quah, J. T., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. *Expert systems with applications*, *35*(4), 1721-1732.

[19] Kumar, D., & Arora, S. (2016). A Hybrid Approach Using Maximum Entropy and Bayesian Learning for Detecting Delinquency in Financial Industry. *International Journal of Knowledge-Based Organizations (IJKBO)*, *6*(1), 60-73.

[20] Leonard, K. J. (1995). The development of a rule based expert system model for fraud alert in consumer credit. *European journal of operational research*, *80*(2), 350-356.

[21] Dorronsoro, J. R., Ginel, F., Sgnchez, C., & Cruz, C. S. (1997). Neural fraud detection in credit card operations. *IEEE transactions on neural networks*,*8*(4), 827-834.

[22] Vatsa, V., Sural, S., & Majumdar, A. K. (2005, December). A game-theoretic approach to credit card fraud detection. In *International Conference on Information Systems Security* (pp. 263-276). Springer Berlin Heidelberg.

[23] Weston, D. J., Hand, D. J., Adams, N. M., Whitrow, C., & Juszczak, P. (2008). Plastic card fraud detection using peer group analysis. *Advances in Data Analysis and Classification*, *2*(1), 45-62.

[24] Bolton, R. J., & Hand, D. J. (2002). Statistical Fraud Detection: A Review,*Statistical Science 17* (3): 235–255.

[25] Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection*. John Wiley & Sons.

[26] Bolton, R. J., & Hand, D. J. (2001). Unsupervised profiling methods for fraud detection. *Credit Scoring and Credit Control VII*, 235-255.

[27] Agrawal, R., Imielinski, T., & Swami, A. (1993). Mining Association Rules between Sets of Items in Massive Databases, *Proceedings of the ACM SIGMOD, International Conference on Management of Data*. Washington, D.C.

[28] Everitt, B. S., Landau, S., Leese, M., & Stahl, D. (2010). *Cluster Analysis*, 5th ed.,Hoboken, NJ: John Wiley & Sons.

[29] Jain, A. K. (2010). Data Clustering: 50 Years Beyond K-Means, *Pattern Recognition, Letters 31*(8): 651–666.

[30] MacQueen, J. (1967). Some Methods for classification and Analysis of Multivariate Observations, *Proceedings of 5th Berkeley Symposium on Mathematical Statistics and Probability*, Berkeley: University of California Press,pp. 281–297.

[31] Kohonen, T. (2000). *Self-Organizing Maps*. New York: Springer.

[32] Han, J., Pei, J., & Kamber, M. (2011). *Data mining: concepts and techniques*. Elsevier.

[33] Mitchell, M. (1998). *An introduction to genetic algorithms*. MIT press.

[34] Kennedy, J. (2011). Particle swarm optimization. In *Encyclopedia of machine learning* (pp. 760-766). Springer US.

[35] Blunsom, P. (2004). Hidden markov models. *Lecture notes, August*, *15*, 18-19.

[36] Klir, G., & Yuan, B. (1995). *Fuzzy sets and fuzzy logic* (Vol. 4). New Jersey: Prentice hall.

[37] Aumann, R. J. (1989). Game theory. In *Game Theory* (pp. 1-53). Palgrave Macmillan UK.

[38] Shafer, G. (1992). Dempster-shafer theory. *Encyclopedia of artificial intelligence*, 330-331.

[39] Shannon, C. E. (1948). A note on the concept of entropy. *Bell System Tech. J*, *27*, 379-423.

[40] Huang, C. Y., & Kuo, S. Y. (2002). Analysis of incorporating logistic testing-effort function into software reliability modeling. *IEEE Transactions on Reliability*, *51*(3), 261-270.

[41] Pillai, K., & Nair, V. S. (1997). A model for software development effort and cost estimation. *IEEE Transactions on Software Engineering*, *23*(8), 485-497.

[42] Hwang, S., & Pham, H. (2009). Quasi-renewal time-delay fault-removal consideration in software reliability modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *39*(1), 200-209.

[43] Pham, H., & Deng, C. (2003, August). Predictive-ratio risk criterion for selecting software reliability models. In *Proceedings of the 9th International Conference on Reliability and Quality in Design* (pp. 17-21).

[44] Li, P. L., Herbsleb, J., & Shaw, M. (2005, November). Forecasting field defect rates using a combined time-based and metrics-based approach: a case study of OpenBSD. In *16th IEEE International Symposium on Software Reliability Engineering (ISSRE'05)* (pp. 10-pp). IEEE.

[45] Ju, C., & Wang, N. (2009, April). Research on credit card fraud detection model based on similar coefficient sum. In *2009 First International Workshop on Database Technology and Applications* (pp. 295-298). IEEE.