Probabilistic Vs. Soft Computing for Classifying Credit Card Transactions. A Case Study of Pakistani's Credit Card Data

Amjad Ali[1], Muhammad Rafi[2]

[1,2]*Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST) Karachi, Pakistan*

[1]amjad1971@gmail.com

[2]rafi.muhammad@gmail.com

Abstract— Credit cards are now widely used by consumers for purchasing various goods and services due to widespread use of internet and consequential growth of E-commerce over the past few decades. This enhanced use of credit cards has increased the associated risks such as fraudulent use of credit cards that can cause financial loss to the card holders as well as to financial institutions. It is an ethical issue and has legal implications in various countries where laws and regulations forces financial intuitions and credit card companies to employ various techniques to detect and prevent the credit card frauds. Although the changes in technological systems also change the nature of frauds but data mining techniques such as classification, regression and clustering are very useful and are widely used to prevent and detect the frauds associated with credit cards. The credit card fraud prevention and detection functionality is a type of classification problem for the new customer as well for existing customers. There are multiple data mining techniques that can be employed for classification of customers and each has its own pros and cons. This study will compare four classification techniques namely Naïve Bayes, Bayesian network, Artificial Neural Network and Artificial Immune Systems for credit card transactions classification on a dataset obtained from a commercial bank in Pakistan. The major contribution of this study is use of real data on which extensive experiments have been performed and various results have been analysed with conclusion of best technique.

***Keywords*—Credit Card, Fraud Detection, Classification data mining techniques, Credit Card Risks, E-Commerce**

I. INTRODUCTION

Fraud can be defined as wrongful or criminal deception intended to result in financial or personal gain [1]. The two mechanisms, fraud prevention and detection are used to manage the risk of fraud. The objective of fraud prevention mechanism is to prevent the occurrence of any unpleasant event and to detect the unpleasant event after occurrence as quickly as possible. Although organizations prefer that the fraud prevention mechanism should be robust and effective but it is difficult to determine at which point fraud prevention mechanism has been compromised. Thus, fraud detection system in conjunction with prevention system plays pivotal role for early detection of system penetration by illegitimate perpetrators. Therefore organizations generally deploy both systems to minimize the financial and reputational loss. Credit cards are always prone to various types of risks and therefore, deployment of both systems will assist to minimize financial loss as well as to meet the legal or regulatory requirements wherever required. These systems also provide additional advantages in terms of time and cost savings by focusing on those transactions that are marked suspicious by system.

The widespread use of internet technologies over the last two decades has resulted in the exponential growth of e-commerce that have made it possible for credit card holders to use credit cards conveniently for online purchase of goods and services. Physical use of credit cards has also increased due to acceptance of credit cards over large number of outlets. According to world payment report-2013, there were 57 billion credit card transactions globally in year 2011 that were 12.3% higher over the previous year [2].

Credit card frauds have also gain momentum over the years with the increase in use of credit cards internationally. Credit card frauds of USD 11.3 billion were reported in year 2012 that were 15% higher over the previous year [3]. Banks and credit card companies have taken various measures to reduce financial loss and to manage other multifaceted risks associated with credit cards. The most significant measure was the issuance of chip and PIN based credit cards in various countries [4]. Chip and PIN based cards contains microchip from which it is very difficult to duplicate the information and thus, these cards are more secure compared to conventional magnetic strip cards vulnerable to data cloning devices.

Provisions of secure banking environment for transactions processing is legal as well as regulatory requirements imposition in addition to maintaining customer

confidence on the system. The secure environment is most significant in the scenario of credit card transactions due to various vulnerabilities associated with credit cards. Chip and PIN based cards although have reduced the risk of counterfeiting or fake cards but risk associated with online use of card will have to be managed by issuing banks through various methods. The most common method for risk management is the monitoring of transactions to detect the suspicious spending behavior of card holders. Monitoring of each transaction is a difficult task due to high volume of credit card transactions and minimum time window to analyze each transaction. Transaction monitoring also carries the risk of offending the genuine customer if any legitimate transaction is aborted by the system. Thus banks have to be very cautious in their approach to monitor the credit card transactions.

Data mining techniques plays major role in transaction monitoring due to their scalability, efficiency in computing spending behavior and higher accuracy rate in making useful predictions on the basis of spending behavior. These techniques compute the spending patterns on the basis of transaction history by taking into account certain features such as amount, high vulnerable locations, past payment history and various fraud cases and then compare each incoming transaction with the spending pattern. They either block the transaction in case of any significant deviation or generate alarm for bank staff. Banks in addition to monitoring of transactions have adopted other mechanisms such as SMS alert generation for card holder as soon any transaction on their credit card is committed. Although monitoring of transactions and SMS alert generation are post facto mechanisms but they provides a safeguard to block subsequent transactions if credit card has been used without the knowledge of card holder. A recent development in fraud detection method at merchant side is device tracking in web based transaction where unknown device whenever connected have to be authenticated through additional information. Thus efforts are underway at merchants, credit card companies and acquirers to reduce the risk of frauds by adopting various technologies.

Our focus in this study is to apply various data mining techniques on dataset obtained from a commercial bank in Pakistan. The objective of this study is to compare probabilistic and soft computing data mining methods to determine the best method in terms of classification accuracy. The remaining part of report has been organized as under:- section 2 provides the summary of various research studies conducted in building credit card fraud detection model, section 3 narrates the problem statement, section 4 & 5 explain the experimental process, data used, data mining techniques applied and in the last section, experimental results have been compiled, discussed and conclusion has been provided.

II. RELATED WORK

The rapid development in computing and machine learning techniques has also made it possible to apply data mining techniques on the large and wide variety of data. These developments have facilitated authorities to discover patterns and relationships among data that can provide useful predictions on the basis of patterns. Although data mining techniques have their own advantages and disadvantages but techniques like Naïve Bayes, Bayesian network, decision tree, neural network and artificial intelligence are widely applied for credit card fraud detection. In this section, authors have summarized few research studies conducted by various researchers to develop the credit card fraud prevention and detection models by using various data mining techniques.

Dheepa and Dhanapal proposed credit card fraud detection model on the basis of support vector machine [5]. They computed the spending behavior of the customer on the basis of transaction history and compared each new incoming transaction against the spending behavior. The incoming transaction was classified fraudulent in case of deviation with the spending behavior. They concluded that their proposed model provides good results in terms of accuracy of fraud detection and is also highly scalable due to its capacity to provide accurate results with large set of data.

Sahin and Duman explored support vector machine and decision tree [6] to examine the best technique for fraud detection. They used historical data for building the model and accuracy rate for comparison of performance of models. They concluded that decision tree perform better over support vector machine in terms of accuracy rate for the given set of data. They mentioned the fitting problem of support vector machine with low number of instances that can be reduced with addition of instances in training set. They concluded that accuracy rate is not the best measure for the given set of data because classification of fraudulent transactions by the proposed model was not comparable with actual number of fraudulent transactions.

Patel and Singh explored genetic algorithm [7] for credit card fraud prevention and detection. Their model comprises of various stages where in the first stage, they standardized the data, get the final sample and stored it in database. In second stage, they computed critical values like credit card amount, credit card usage frequency, credit card average daily spending and etc. and in the third stage they generated the critical values by applying limited number of generations using genetic algorithm. They provided various labels to these critical values like critical fraud detected, ordinary fraud detected and etc. These critical values were then used to determine the feasibility of new credit card transactions either genuine or fraudulent.

Vats *et al* proposed credit fraud detection model based on genetic algorithm [8]. They concluded that genetic algorithm produces good results in terms of accuracy with comparatively low false generation rate compared with other data mining techniques. Another advantage of genetic

algorithm mentioned by them was its real time application on incoming transactions. This potential of algorithm can support financial institutions to adopt various risk mitigation strategies to evaluate new transactions to reduce the risk of loss to the bank and customers.

Ogwueleka explored the unsupervised method of neural networks to detect the credit card frauds [9]. He observed that most of previous fraud detection models were based on the pattern matching with major focus to identify abnormal patterns. However, instead of building spending patterns, he generated four clusters: low, high, risky and highly risky on the basis of historical transactional data. He then used self-organizing map (SOM) of neural network to optimally classify each incoming transaction against four clusters. Any transaction falls in to four clusters was not processed rather stored in database for further analysis and decision making. He concluded that four stage clusters model detected over 95% fraud cases without any significant increase in the false alarm generation rate when compared with two stage clusters models and other statistical techniques. Another advantage of proposed model was its portability to operate as background software over the banking software that can result in cost saving for banks.

Patidar and Sharma built a hybrid model by combining back propagation neural networks and genetic algorithm [10]. Both techniques represent learning as well as evolution process and they assumed combination of techniques can produce good results just like successful human beings whose success is based on their experience as well as genetic heritage. They used back propagation algorithm to build training model and then genetic algorithm was applied to identify those parameters that play significant role in the accurate performance of model. They concluded that their model can perform best if neural network is trained properly by choosing the appropriate parameters.

Fouhy *et al* highlighted the importance of feature isolation from available fraud cases that can play a significant role in predicting the behavior of fraudster [11]. They performed the analysis of various fraud cases such as internal, application frauds and credit card BIN attack cases. They manipulated and structured the data in such a way that prospective fraud can easily be detected from the already available data. They concluded that manipulation of fraud data can enable the banks to extract the latent features that can be used to predict the behavior leading towards frauds. This feature identification can enable banks to deploy the fraud detection system for on line monitoring of transactions.

Delamaire *et al* reviewed various credit card frauds detection techniques proposed by various researchers to detect the credit card frauds [12]. They mentioned one important issue in fraud detection is classifying a genuine transaction as fraudulent that can have implications for bank, customer as well as for credit card companies. Further, they mentioned that economic cost of identifying each fraud case might be high that will be difficult to justify by banks before shareholders. They proposed alternate method for fraud detection where banks can develop scoring models to allocate a score to card holder that can be used to forecast the fraudulent behaviors. They further proposed that such scoring models can be built on the basis of various features available in transactions that can likely to lead for various types of frauds.

III. PROBLEM STATEMENT

Credit card fraud detection is very important task to minimize the financial loss to the banks and to card holders. This research will explore:-

1. What will be good classification method for credit card transactions among the data mining methods: Naïve Bayes, Bayesian network, Artificial Neural Network and Artificial Immune Systems?
2. The decision will be based on the classification accuracy of each model.
3. Dataset used in this research is credit card holder dataset of a Pakistan Commercial Bank.

IV. DATASET

The authors have taken the credit card dataset from commercial bank in Pakistan. Personal information of card holders such as customer name, address and National Identity card number was not provided by bank to maintain privacy of data. Dataset consists of 500 records with 257 (51.40%) records represent the continuing customers (classified good) and 243 (48.60%) records represent customers whose cards has been blocked due to non-payment (classified bad). Main characteristics of dataset mentioned in table 1 are:

Table 1. Characteristics of credit Card Dataset

Dataset	**# Instances**	**# Classes (Good & Bad)**	**Nominal Attributes**	**Numerical Attributes**	**Good/Bad Customer %**
Pakistani	500	2	10	7	51.40/48.60

V. EXPERIMENTAL METHODOLOGY

Experimental research methodology has been used in this study where extensive experiments on the real data were performed. For our research and model validation, data has been partitioned into training sample (70%) and test sample (30%). Before partitioning, data has been randomized using WEKA and then has been divided into training and test samples in ratio of 70/30 using various tools available in WEKA. WEKA release 3.6 with graphical user interface mode was selected for various experiments.

The authors have used various algorithms under classification techniques namely Naïve Bayes, Bayesian

Network, Artificial Neural Network and Artificial Immune Systems for our experiments mentioned in table 2.

Table 2. Techniques & Algorithms

Data Mining Type	Technique	Algorithms
Probabilistic Computing	Naïve Bayes	
	Bayesnet	Hill Climber
		Simulated Annealing
Soft Computing	Artificial Neural Network	Multilayer Perceptron
		RBF Network
	Artificial Immune System	Clonalg
		CSCA

VI. EXPERIMENTAL RESULTS

In this section, brief introduction of various measures to evaluate the results have been provided. The first measure was Accuracy that can be expressed as under:-

$$\text{Accuracy} = \frac{TP+TN}{TP + TN+FP+FN} \quad \text{(i)}$$

True positive (TP) are those credit records that has been accepted correctly and true negative (TN) are those records that have been correctly rejected. False positive (FP) are those credit rejected records that have been classified as accepted and false negative (FN) are those accepted credit records that have been classified as rejected.

Another measure used for interpretation of results was Confusion Matrix that is represented as a table where column represent predictive class and rows represent the actual class.

The authors have also used Precision, recall and F score for interpretation of our results:-

$$\text{Precision} = \frac{TP}{TP + FN} \quad \text{(ii)}$$

$$\text{Recall} = \frac{TN}{FP+TN} \quad \text{(iii)}$$

F measure is harmonic mean of precision and recall:-

F-measure = 2 * ((Precision. Recall)/Precision+Recall)) (iv)

Table 3. Comparison of Classification Accuracy on Test Set

Type	Probabilistic Computing			Soft Computing			
Technique	Naïve Bayes	Bayesnet		Artificial Neural Network		Artificial Immune System	
Algorithm		Hill Climber	Simulated Annealing	Multilayer Perceptron	RBF network	Clonalg	CSCA
Classification Accuracy	61.33%	48%	48%	99.33%	64%	55.33%	72.67%
Average1	61.33%	48%		81.66%		64%	
Average2	54.66%			72.83%			

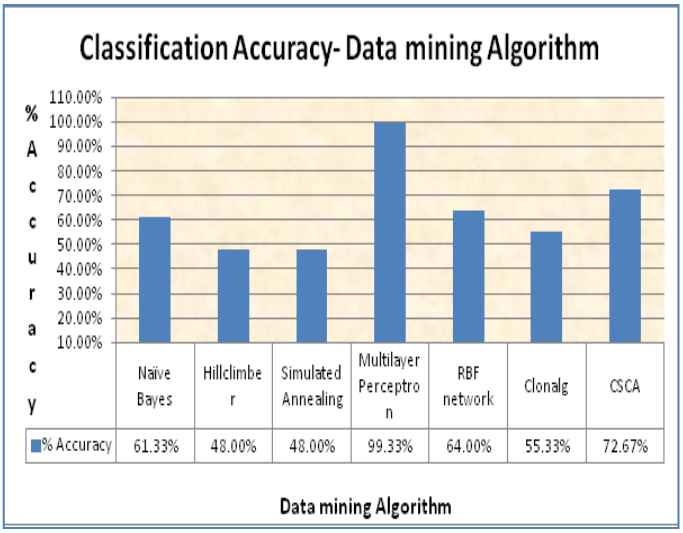

Fig. (1). Classification Accuracy- Data mining Algorithm

Table 4. Test Set Classification Results (Precision, recall and F scores)

Type	Probabilistic Computing			Soft Computing			
Technique	Naïve Bayes	Bayesnet		Artificial Neural Network		Artificial Immune System	
Algorithm		Hill Climber	Simulated Annealing	Multilayer Perceptron	RBF network	Clonalg	CSCA
Precision	0.615	0.601	0.601	0.993	0.637	0.554	0.734
Recall	0.613	0.48	0.48	0.993	0.64	0.553	0.727
F Score	0.582	0.384	0.384	0.993	0.635	0.554	0.728
Average-Precision	0.606			0.729			
Average-Recall	0.524			0.728			
Average-F Score	0.45			0.727			

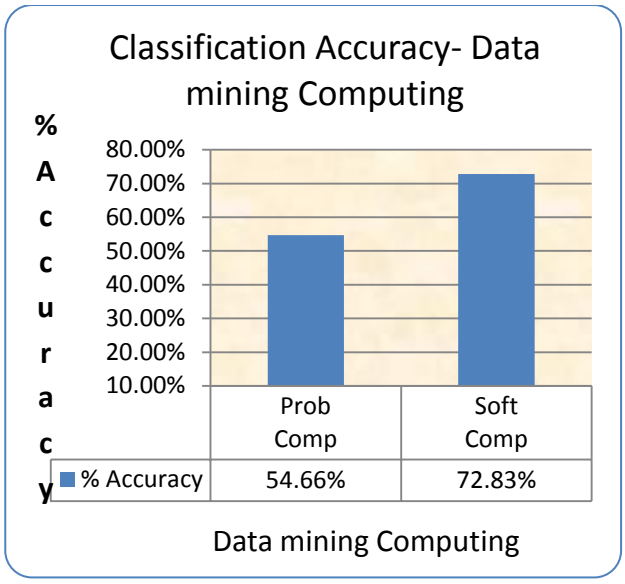

Fig. (2). Classification Accuracy- Data mining Computing Type

Table 5. Test Set AUC Results

Technique	Naïve Bayes	Bayesnet		Artificial Neural Network		Artificial Immune System	
Algorithm		Hill Climber	Simulated Annealing	Multilayer Perceptron	RBF network	Clonalg	CSCA
AUC	0.657	0.532	0.578	1	0.664	0.548	0.73
Average 1	0.657	0.555		0.832		0.639	
Average2	0.606			0.736			

Table 6. Confusion Matrices obtained in Test Dataset

Data Mining Type	Technique	Algorithm	Desired Results	Test set: Output Results Good	Bad
Probabilistic Computing	Naïve Bayes		Good	21	45
			Bad	13	71
	Bayesnet	Hill Climber	Good	62	4
			Bad	74	10
		Simulated Annealing	Good	62	4
			Bad	74	10
Soft Computing	Artificial Neural Network	Multilayer Perceptron	Good	66	0
			Bad	1	83
		RBF network	Good	34	32
			Bad	22	62
	Artificial Immune System	Clonalg	Good	33	33
			Bad	34	50
		CSCA	Good	50	16
			Bad	25	59

VII. DISCUSSION

In this section, the results observed in the study are summarized.

If the classification accuracy rate of individual data mining algorithm in table 3 is considered, Multilayer Perceptron has outperformed all other data mining algorithms whose classification accuracy is 99.33% in figure 1. It represents that Multilayer Perceptron have classified good and bad customers in the same ratio that is present in the dataset. The second highest classification accuracy is achieved under clonal selection classification algorithm (CSCA) that is 72.67%. Thus it can conclude that Multilayer Perceptron is best data mining algorithm for given dataset considering that the higher classification accuracy in fraud detection is most significant to reduce the financial loss to the customer and bank. The above comparison is based on individual algorithm and if the classification accuracy in terms of data mining techniques like artificial neural network is compared with artificial immune system then artificial neural network classification accuracy is 81.66% followed by 64% under artificial immune system. Thus, it can conclude that artificial neural network is better classification technique over artificial immune system for the given dataset. The objective of this study was the comparison of probabilistic and soft computing methods and for this comparison simple average has been used where results achieved under various algorithms were summed up and divided them by number of algorithms. Classification accuracy achieved under soft computing method is 72.83% and under probabilistic computing method is 54.66% in figure 2. It can be concluded that soft computing method is better for classifying credit card transactions for the given dataset over the probabilistic computing method.

The results have been compiled on the basis of precision, recall and F score. Multilayer Perceptron have again outperformed other data mining algorithms in terms of precision, recall and F score. Table 4 indicates that precision, recall and F score under Multilayer Perceptron is 0.993, 0.993 and 0.993. However, when comparison was carried out on the basis of objective of our study, then it can be concluded that soft computing method is better over probabilistic computing method. Precision, recall and F score under soft computing method is 0.729, 0.728 and 0.727, that is far better than the precision, recall and F score under probabilistic computing method that is 0.606, 0.524 and 0.450.

Area under ROC curve (AUC) is also used for comparison of results where AUC value indicates actual good customers have been assigned higher probability of being good customers than the bad customers. When results on the basis of objective of our study were compared, then it can be concluded that soft computing method is better over probabilistic computing method in terms of AUC value. Table 5 indicates that AUC value under soft computing method is 0.736 and probabilistic computing method is 0.606.

Results have also been compiled in confusion matrix that indicates Multilayer Perceptron have outperformed other algorithms while predicting the good and bad customers. Table 6 indicated that Multilayer Perceptron has classified 100% good customer while only identified one bad customer as good customer.

VIII. CONCLUSION AND FUTURE WORK

Credit card fraud is an ethical issue and has legal implications in various countries where laws and regulations forces financial intuitions and credit card companies to employ various techniques to detect and prevent the credit card frauds. The objective of this study was comparison of probabilistic and soft computing methods to determine the best method in terms of classification accuracy. The authors have used four classification techniques namely Naïve Bayes, Bayesian network, Artificial Neural Network and Artificial Immune Systems on a real data set obtained from commercial bank. Various algorithms available in WEKA were used to perform extensive experiments. Six iterations of experiments were performed to determine the statistical soundness of the results. Analytic results depicts that better classification accuracy rate was achieved under soft computing method when compared with probabilistic computing method. In the soft computing method, classification accuracy under Multilayer Perceptron was approximately 100%. Multilayer Perceptron is back propagation algorithm that maps the inputs against the desired output and performs several iterations until the desired results approximately matches with the actual results. Thus it can be concluded that artificial neural network is better data mining technique for classification accuracy for the given set of data.

This study has many limitations like proposed model is based on certain data patterns and will become outdated as soon as data patterns changes. So, it needs to be constantly updated considering the changes in data patterns to minimize the number of false generation alarms. Further, the nature of frauds changes with evolution of technology; therefore, any proposed model should be dynamic enough to integrate the attributes of various types of frauds. Other limitation of this research is that the data of one financial institution from Pakistan with limited number of instances has been used. Any actual model building requires large dataset that should be used to evaluate the existing results and to get better experimental results.

In future work, more experiments can be performed on the dataset by using other algorithms available in WEKA. Dataset from other banks with same set of attributes can be used for comparison of results. More attributes can be added to data to determine the impact of attributes on classification accuracy.

IX. ACKNOWLEDGEMENT

The author would like to express gratitude to Mr. Muhammad Rafi for supervising this study, providing technical knowledge and support, extending valuable time for meticulously reviewing work and providing extremely useful and critical suggestions in all matters.

REFERENCES

[1] *The Oxford Dictionary of Difficult Words*. The Oxford University Press. New York, 2004.

[2] J. Lassignardie and K. Brown. "World Payments Report (WPR)," Capgemini and Royal Bank of Scotland (RBS), 2013.

[3] "Skimming off the top", print edition, finance and economics, The Economist, The Economist Newspaper Limited, February, 2014.

[4] Tom Groenfeldt. (2014) *More Secure Credit Cards With Chips Coming To The U.S* [Online]. Available FTP: http://www.forbes.com/sites/tomgroenfeldt/2014/06/23/more-secure-credit-cards-with-chips-coming-to-the-u-s/

[5] V. Dheepa and R. Dhanapal, "Behavior Based Credit Card Fraud Detection Using Support Vector". *ICTACT Journal on Soft Computing*, vol. 2, no. 4, July 2012.

[6] Y. Sahin and E. Duman, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines". In *Proceedings of International Multi conference of Engineers and Computer Scientists (IMECS 2011)*, 2011, vol. 1.

[7] R. D. Patel and D. K. Singh, "Credit Card Fraud Detection & Prevention of Fraud Using Genetic Algorithm". *International Journal of Soft Computing and Engineering* , vol. 2, no. 6, January 2013.

[8] S. Vats, S. K. Dubey and N. K. Pandey, "Genetic Algorithms for Credit Card Fraud Detection". In *Proceedings of the International Conference on Education and Educational Technologies,* 2013.

[9] F. N. Ogwueleka, "Data Mining Application In Credit Card Fraud Detection System". *Journal of Engineering Science and Technology*, vol. 6, no. 3, pp: 311-322, 2011.

[10] R. Patidar and L. Sharma, "Credit Card Fraud Detection Using Neural Network". *International Journal of Soft Computing and Engineering*, vol. 1, no. NCAI2011, June 2011.

[11] J. C. Fouhy, P. J. Bracewell, G. L. Gee1 and C. H. Messom, "Importance of Feature Isolation in Detecting Fraud". *International Journal of Principles and Applications of Information Science and Technology,* vol. 3, no.1, February 2010.

[12] L. Delamaire, H. Abdou and J. Pointon. "Credit Card Fraud and Detection Techniques: A Review". *Banks and Bank Systems*, vol. 4, no. 2, 2009.