Fuzzy logic and Takagi-Sugeno Neural-Fuzzy to Deutsche Bank Fraud Transactions

Fatemeh Shafiee Nezhad
Department of Computer Engineering & IT
Amirkabir University of Technology, Tehran, Iran

Hamid Reza Shahriari
Department of Computer Engineering & IT
Amirkabir University of Technology, Tehran, Iran

Abstract

This article proposes suitable solution to detect fraud via fuzzy logic followed by Neural-fuzzy Takagi-Sugeno training method. In order for the fraud to be detected through fuzzy logic, there should be some rules stemmed from experience of the experts. These rules are expressed through information that could be registered for a given card. To come up with the fuzzy deduction, membership functions needed to be expressed over the specified input range. This issue is one of the problems of fuzzy logic. To solve this problem, fuzzy logics were established and Mamdani deduction engines were utilized as a result of which suitable responses were presented for fraud detection via Neural-fuzzy method. Despite the fact that the problem inputs were highly linear, Neural-fuzzy training was able to cope with the problem and present a suitable trained system. In other words, Neural-fuzzy training method is employed in order to optimize the fuzzy logic membership functions based on the data. Outcomes of the Neural-fuzzy training were quite satisfactory and highly precise. Thus, utilizing the research findings, Neural-fuzzy training method is proposed for upgrading fraud detection in the banking system of our country.

Keywords: Fraud detection, fuzzy logic, Neural-fuzzy, banking system

Introduction

Electronic cash dispense and bank switches have become one of the significant issues of the electronic banking in the present era. Cash card systems enjoy ever increasing high technology which demands the banks to be accountable to meet the expectations within the framework of the specified standards and guidelines. Fraud has become one of the basic problems with which the cash-card issuers and POS (**P**oint **O**f **S**ale) owners face. Fraud is mostly committed by the

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

organized professional criminals who mainly resort to the smart fraud models. Hence due to the increasing numbers of the electronic services, the banks need to immunize their switches and consider proper solutions and strategies for fraud detection. Electronic cash dispensers that are designed shall feature identification of the customer, POS-owner and transaction as well as fraud detection system. EFTPos is the commonest device of electronic cash dispense wich nowadays enjoy widespread use. The first ATM (Automated Teller Machine) was invented in 1939. Early cash dispensers worked off-line; that is to say, the money could not be automatically deducted from the customer's account. The first EFTPos was introduced in 1870 to record transactions, track monetary exchanges and prevent the user from cash theft in time of goods trading. As the EFTPOSs were developed, paper roll was used to print the receipt for customer as well as POS-owner.

Delamaire and Abdou(2009), studied various types of fraud and the way they were committed. Then they studied pertinent methods of the fraud detection and had them classified. Fraud is classified into bankruptcy fraud, theft fraud, application fraud and behavioral fraud. In order to detect the fraud, there are four common methods namely Decision Tree, Genetic Algorithms, Clustering Techniques and Neural Network. The decision tree method is based on the idea of creating a likeness tree using decision tree logic. Fan et al (2001) worked on decision tree particularly decision trees of the events for designing a system to observe troublesome behaviors of other forms of fraud. In the Genetic method some algorithms are presented as preventive measures to detect the fraud. Wheeler and Aitken (2000) proposed the idea of a combined algorithm to maximize the power of prediction.

Bolton and Hand, (2002) presented two Clustering techniques for behavioral fraud. Bayesian network is also a fraud detection technique (Maes et al., 2002) whose outcomes are promising. However, compared to neural systems, it faces more time constraint which is its main disadvantage (Maes et al., 2002). Generally, cash-card fraud can be divided into two groups namely internal and external. The internal fraud deals with cash fraud which is usually carried out through a counterfeit transaction between the channel and the card-holder. The external fraud deals mainly with stolen counterfeit cards which are used to receive money. The former approach sees transactions

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

fraud that is carried out online. In reality some money is electronically drawn out of an account illegally.

This paper deals with fraud detection through analysis of the electronic cash-dispenser's transactions by using fuzzy logic and neural-fuzzy *Takagi-Sugeno* method. Then in order to come up with highly accurate responses, Neural-fuzzy training method is utilized the outcomes of which are highly precise and can be a good intelligent method for fraud detection in the banking system of our country.

Cash dispenser is a software framework that can be the issuer or acquirer. Each cash dispenser is composed of two main sections, Front Office and Back Office. The Front office deals with Transactions management, credibility confirmation, routing and transfer of the transaction. While The Back office concerns about cash-card management, management of electronic POSs and network monitoring. Fraud detection has become one of the important issues of the country about bank switches (Res.J.Inform.Technol., 2008).

An introduction to Electronic cash-dispenser

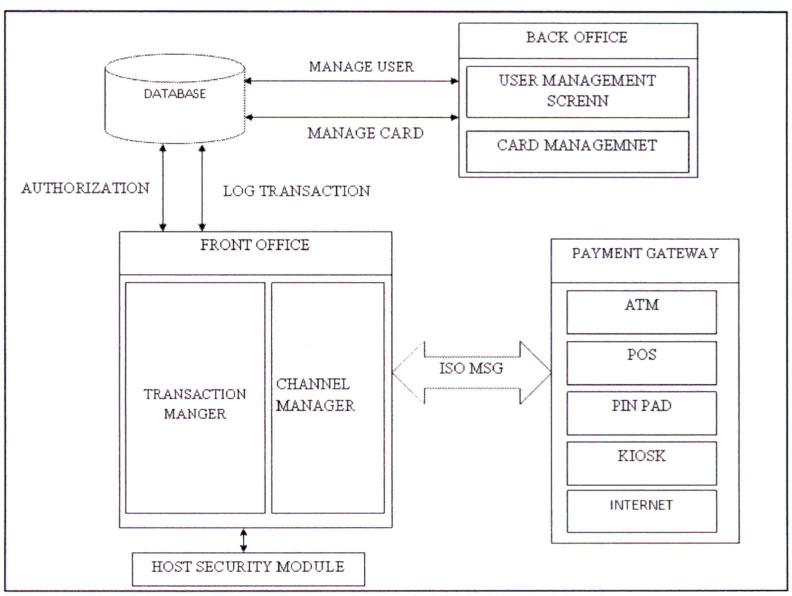

Figure 1. Schematic view of cash dispenser architecture

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

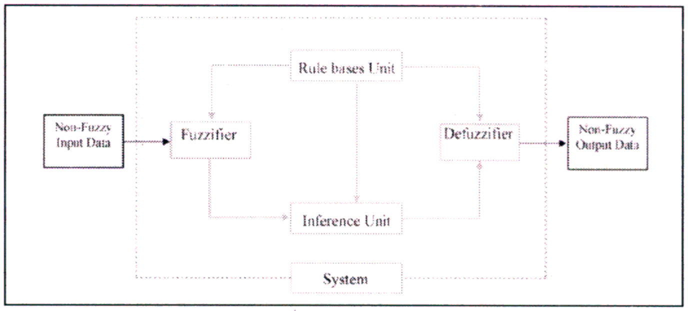

Figure 2. Demonstrates a Fuzzy system structure

An introduction to Fuzzy Systems

Fuzzy systems are accurately-defined systems. Although fuzzy systems describe uncertain and unspecified phenomena, the fuzzy theory itself is an accurate theory. In operational systems, important data result from two sources. One source is the expert whose knowledge and wisdom on system is defined using a natural language. Another source is the mathematical model and measurement emanating laws. Hence combining these two types of information is an important issue in systems design. A Fuzzy system is composed of four sections including recognition database or fuzzy rules, fuzzy-maker unit, decision-making or deduction unit and fuzzy-remover unit. Input signals are converted into fuzzy language variables in the fuzzy-maker unit. Then system output is produced in the fuzzy form by decision-making unit which uses the existing rules and combines them with recognition database information. Finally the output passes through the fuzzy-remover unit and becomes quite non-fuzzy.

Fraud-detection Implementation based on Fuzzy Method

As the first step, proper inputs and outputs are defined for the fuzzy training. The input and output parameters of the problem stem mainly from real-time transactions' data, stored information and the system expert opinion. Table 1 enumerates the input and output parameters.

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

Table 1. The input and output parameters

Number of variable	Variable	Value
1	card	New
		Old
2	number of transactions	Very few
		few
		Medium
		high
3	type of transactions	same
		different
4	Transaction amount	Very few
		few
		Medium
		high
		Very high
5	type of terminal	same
		different
6	time of transaction	Normal
		Less abnormal
		Abnormal
		High Abnormal
7	time difference of transactions	High abnormal
		Less- Abnormal
		Abnormal
		High Abnormal
	Out put	Not-suspicious
		Low-suspicious
		suspicious
		high-suspicious
		disastrous

First, transaction system is analyzed and examined as a result of which a point from 0 to 100 is dedicated to it. Then, as table 2 indicates, the transaction is identified as low-suspicious, suspicious, high-suspicious or dangerous.

Table 2. The output range

Description	Rating 0- 100
Not-suspicious	0-45
Low-suspicious	45-75
suspicious	75-85
high-suspicious	85-100

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

Second, after having defined the inputs and outputs, colloquial concepts need to be expressed for them based on the experience of experts in the banking system. Each input needs to be dedicated a membership function. For every function, Gaussian membership function has been used that presents a suitable response.

Thanks to simplicity of the formulas and optimality of the computations, Triangular and trapezoid membership functions have been widely used in the real-time systems. However, since these membership functions are based on straight lines, they do not act smoothly on the corner points specified by the parameters. Hence the present research resort to Gaussian functions to the extent possible. Double-parameter Gaussian Membership Functions are as follow:

(1)

$$gaussian(x; c, \sigma) = e^{\left[\frac{-1}{2}\left(\frac{x-c}{\sigma}\right)^2\right]}$$

C is the center of the membership function and Sigma is indicative of its width. After having parameters and verbal inputs defined, membership functions are determined according to the extent of the variability of each input. Fore example, range of variability has been considered from 0 hour to 24 hour for time input variable. In effect these membership functions are registers of variation range of the input from 0 to 1. This value (0 to 1) then is used in the fuzzy deduction engine which is a *Mamdani* deduction engine. Fuzzy rules used in this system are based on the human experience. As the next step, fuzzy deduction rules need to be developed based on experience of experts in the banking system in order to examine the inputs that have been made fuzzy. In other words, these rules – that are expressed in table3, are employed for presenting a trained expert system.

Table 3.Fuzzy rules

	If card is	**If number of transactions is**	**If type of transactions is**	**If value of transaction is**	**If type of terminal is**	**If time of transaction is**	**If time difference of transactions is**	**Then transactions is**
Rule 1	New	Very few	Different	Low	Different	Normal	Normal	Not-suspicious

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

Rule 2	Old	Few	Different	Medium	Different	Normal	Normal	Not-suspicious
Rule 3	New	Few	Different	High	Same	Normal	Normal	Low-suspicious
Rule 4	New	Medium	Same	Very high	Different	Normal	Normal	Low-suspicious
Rule 5	New	High	Same	Medium	Same	Normal	Abnormal	Suspicious
Rule 6	New	Medium	Same	High	Same	Less-Abnormal	Less-Abnormal	Suspicious
Rule 7	New	High	Same	High	Same	High - Abnormal	Less-Abnormal	Disastrous
Rule 8	New	High	Same	High	Same	Abnormal	Abnormal	Disastrous
Rule9	New	High	Same	High	Different	Normal	Abnormal	High-suspicious
Rule10	Old	High	Same	High	Different	Normal	Abnormal	High-suspicious
Rule11	Old	High	Same	High	Same	Abnormal	Abnormal	Disastrous
Rule12	Old	High	Same	High	Same	Normal	Normal	Suspicious
Rule 13	Old	High	Different	High	Different	Normal	Normal	Low-suspicious
Rule 14	Old	Medium	Different	Very high	Different	High - Abnormal	Normal	Disastrous
Rule 15	Old	Medium	Same	Medium	Different	Abnormal	Normal	Low-suspicious
Rule 16	New	High	Same	High	Different	High - Abnormal	Normal	High-suspicious
Rule 17	New	High	Different	Medium	Same	Normal	Abnormal	High-suspicious
Rule 18	New	High	Different	Medium	Same	Normal	Normal	Not-suspicious

In this research *Mamdani* fuzzy law and non-fuzzy maker (Centroied) method has been utilized for inputs and outputs connector. As a matter of fact 18 rules based on the expert opinions of the banking system have been defined.

AT last in order for the trained system's response to be examined via fuzzy method, a few series of data are introduced in table

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

4. This table helps up decide, based on the experts' opinion and system output, how the transaction behavior can be classified

.

Table 4. Results of fuzzy logic

Row	Card	Number of transaction	Type of transaction	Transaction Amount	Type of terminal	Time of transaction	Time difference of transaction	System output	Experts opinion
1.	٠	١	٠	٥٠٠٠	٠	١٢	٣	%٥٠	Not-suspicious
2.	٢.٥	٢	٠	١٠٠٠٠٠٠٠	٠	١٣	٣	%٥٠	**Not-suspicious**
3.	٠.٥	٢	٠	٥٠٠٠٠٠٠٠	١	١٦	٢.٥	%٦٣	**Low-suspicious**
4.	٠.٥	٢٠	١	٧٠٠٠٠٠٠٠	٠	٢٢.٥	٢.٨	%٦٨	**High-suspicious**
5.	٠.٢	٢٠	٠	٤٥٠٠٠٠٠٠	١	١٤	٠.٦٥	%٧٤	**Disastrous**

Outcomes of the logic are indicative of the fact that if fuzzy logic is used, suitable responses will be presented. However in order for the responses to be optimized, a more intelligent method needs to be utilized. Hence in the following section attempts are made to employ Neural-Fuzzy logic training method.

Fraud detection implementation based on Neural-Fuzzy method

In the previous section fuzzy concept was utilized in order to study the suspicious and non-suspicious behaviors of the banking transactions. As it was argued the results were good but they weren't accurate enough in some transactions. So attempts were made to achieve much more accuracy. To do so, a more advanced method, Neural-Fuzzy training method was used to overcome the weaknesses of the fuzzy method. These weaknesses could be enumerated as follow:

- Limited rule definition
- Limited membership function over the specified range
- Non optimal membership functions

Noteworthy is that neural-fuzzy method could be used to define optimal membership functions. In other words smart neural logic tries to optimize the specified range of the membership functions leading to reduced errors in definition of the membership functions

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

which itself contributes to optimization. *Sugeno* deduction rule has been used in the neural-fuzzy training where the number of inputs and outputs are 5 and 1, respectively. Input variables as well as the output variable are as follow: **Input variable 1**: Age of the card, **Input variable 2**: number of transactions, **Input variable 3**: Value of transactions, **Input variable 4**: Input time, **Input variable 5**: Time difference, **Output variable**: Transaction risk. More than 350 data, whose behaviors are presented in bellow figures, have been used for training. As it is clear from these figures, behavior is highly complex and quite nonlinear denoting the fact that it is a complicated and difficult task to train a smart system with such non-linear behaviors.

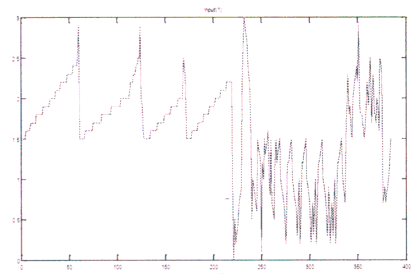

Figure 3. Behavior of Input 1

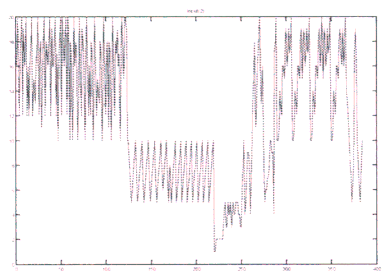

Figure 4. Behavior of Input 2

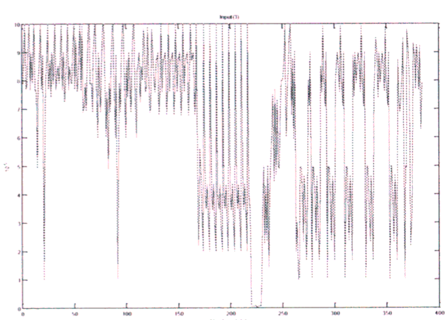

Figure 4. Behavior of Input 3

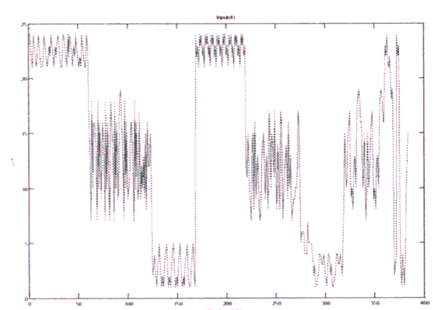

Figure 5. Behavior of Input 4

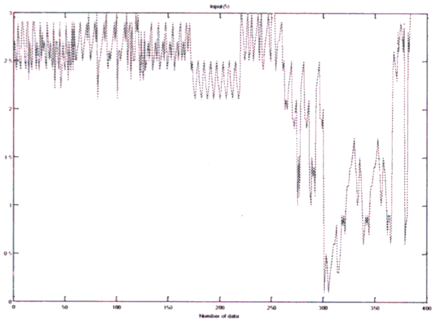

Figure 5. Behavior of Input 5

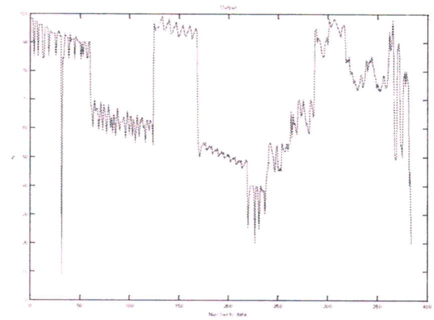

Figure 6. Behavior of output

The first step to start the training process is defining membership functions for each input. Examination of the problem's data indicated that Bell Membership Function has a better performance on these data. Hence these functions are used in the research. What follows is a brief introduction on Bell membership functions that combination of two parameters σ, c .

$$bell(x;\sigma,c) = exp\left(\frac{-(x-c)^2}{2\sigma^2}\right) \quad (2)$$

Each input has three Bell membership functions with three (a, b, c) parameters. If value of b is positive (+), the function will be Bell type; however in case it is negative (-), the function will be an inverse Bell. These membership functions are among the most popular membership functions of the Neural-Fuzzy systems because they are brief and fine [7]. The output membership function is a linear one which is common in the fuzzy deduction logic. Bellow figures demonstrate membership functions of the 2 inputs in question and indicate that how the Neural-fuzzy training has been able to detect and opt for parameters of every membership function based on the training data.

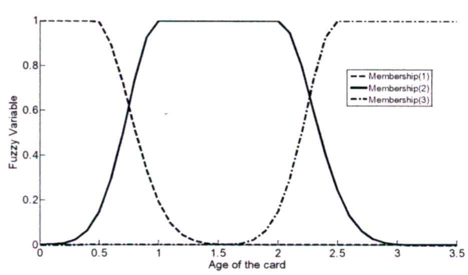

Figure 7. Membershib function of input 1

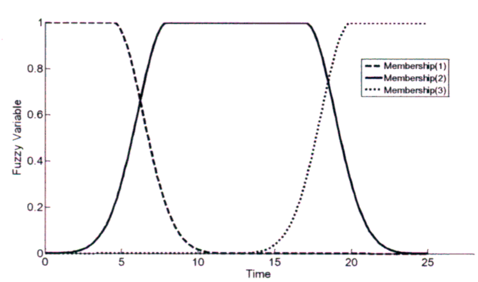

Figure 8. Membershib function of input 4

The *Sugeno* deduction rule has been used in the Neural-fuzzy training. Each base of the first-order *Sugeno* model has a numerical output and the final output is calculated based on the weighed average. As a result of which this method is free from time-consuming fuzzy-removing process of the *Mamdani* model [7]. Compared to *Mamdani* method, *Sugeno* method enjoys brief and short computations which make it the choice for adaptive techniques in modeling. These adaptive techniques have been used for customizing the membership functions. Hence fuzzy system can better model the data. Thanks to computational optimality, suitable performance along with linear systems, and optimization and adaptation techniques as well as continuity of the output surface, *Sugeno* method has been used. Table 5 shows the output of the trained system. As it is evident from this table, the rate of error is low and the system trained via *Sugeno* Neural-fuzzy network method has successfully been able to overcome the problem. The last column of the table is indicative of low errors.

Table 5. the output of the trained system

Row	Card	Number of transaction	Transaction Amount (Million)	Time of transaction	Time difference of transaction	FRAUD Rate	System FRAUD Rate	Tolerance	Normalizes *
1	1.5	16	7.9	24	2.7	98	97.674	0.326	0.332653
2	1.5	10	8.9	7	2.7	60	62.2737	2.2737	3.7895
3	1.7	12	6	9	3	60	59.2576	0.7424	1.237333
4	2.9	10	7.1	10	2.8	54	54.0009	0.0009	0.001667
5	1.5	9	6.78	5	2.5	98	98.089	0.089	0.090816
6	1.5	10	7.69	2	2.8	99	99.0863	0.0863	0.087172
7	1.5	7	10	1	2.9	97	97.0317	0.0317	0.03268
8	1	1	0.1	12	3	25	24.997	0.003	0.012
9	0	1	0.05	11	3	35	34.9999	0.0001	0.000286
10	0.5	2	0.04	15	2.8	40	40.0002	0.0002	0.0005
11	0.7	18	7.6	17	1.3	78	78	0	0

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

12	1	20	9.9	9	1.4	76	75.9974	0.0026	0.003421
13	0.2	10	8	10	1.4	77	76.9963	0.0037	0.004805
14	0.8	19	8.73	1	2.6	80	79.9999	0.0001	0.000125
15	0.9	16	7.68	4	2.9	75	74.9991	0.0009	0.0012
16	0.7	10	9.3	3	0.6	80	80.0005	0.0005	0.000625
17	0.8	8	8.73	1	0.8	78	77.9998	0.0002	0.000256
18	0.9	6	7.68	4	0.9	75	75.0001	0.0001	0.000133
19	1	5	9.23	9	2.8	40	40.0192	0.0192	0.048
20	1.2	7	6.298	12	2.6	45	44.9516	0.0484	0.107556
21	1.5	10	7.9	15	3	20	20.1945	0.1945	0.9725

$$\frac{|FRAUD\ Rate - System FRAUD\ Rate|}{FRAUD\ Rate} \times 100\ *$$

Results:

The above-mentioned table indicates the results of Neural-fuzzy training. It includes 5 inputs based on the banking system data and 1 output indicative of the degree of suspiciousness of each transaction. The system is trained using the data of the first 5 inputs and the first output. Results of the Neural-fuzzy training are expressed in the second output column. Next column shows the degree of tolerance and reflects the accuracy of the Neural-fuzzy training results. Table 2 can be referenced to use Neural-fuzzy training output in order to determine the class of each transaction. For example, it can be inferred from the table that transactions 1 and 9 are considered to be dangerous and non-suspicious, respectively. It is clear from the table that degree of the tolerance expressed in percentage is low and that response of the Neural-fuzzy training is highly accurate. To have a deeper look at the research data, normalized values of the responses have also been presented. The results reflect the high accuracy of the proposed method in this research.

Conclusion

As the world of communications is expanding with ever-increasing speed, it is necessary to take the issue of banking and particularly safe banking into consideration. Nowadays the fraud has mostly inclined toward electronic cash-card services as a result of which the issue of fraud expansion in the cash-dispenser

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

bases has drawn worldwide attention. Hence this issue needs to be considered in the banking system of the country for which the researchers have begun some research works. This paper proposes suitable solutions for fraud detection via fuzzy logic and neural-fuzzy *Takagi-Sugeno* training method. To utilized fuzzy logic for fraud detection, some rules were defined based on experience of the experts. The rules are determined using the data that could be recorded for a cash-card. These data are divided into seven parts in the fuzzy section. To develop the fuzzy deduction, membership functions needed to be expressed over the defined input range which was a problem in the fuzzy logic. So fuzzy rules were developed and *Mamdani* deduction engine was utilized leading to suitable responses for fraud detection. Then attempts were made to add up to accuracy of the proposed method. To do so, Neural-fuzzy training method was employed and neural-fuzzy rules were trained for more than 350 input data. Despite the fact that inputs of the problem were highly nonlinear, Neural-fuzzy training has successfully been able to overcome the problem and present a suitable trained system. In other words, Neural-fuzzy training method has been resorted in order to optimize the membership functions of the fuzzy logic based on the data. Results of the Neural-fuzzy training were highly satisfactory and accurate. Hence, based on the results of the research, Neural-fuzzy training is proposed for fraud detection in the future banking system of our country.

References

[1] Edge, M., Sampaio, P. Falcone, "A survey of signature based methods for financial fraud detection", Computers & Security, Vol. 28, No. 6, pp. 381-394, 2009.

[2] Krivko, M., "A Hybrid Model For Plastic Card Fraud Detection Systems", Expert Systems with Applications, Vol. 37, No. 8, pp. 6070-6076, 2010.

[3]K.Chaudhary, J.Yadav, B.Mallick "A Review of Fraud Detection Techniques: Credit Card" International Journal of Computer Application volume 45-NO.q, May 2012

[4]A.N.Ayofe, S.B.Adebayo, A.R.Ajetola, A.F.Abdulwahab "A Framework for computer Aided Investigation Of ATM Fraud in Nigeria" International Journal of soft Computing: 78-82, 2010

[5]L.Delamaire, H.Abdou, J.Pointon "Credit Card Fraud and Detection Techniques: A Review" Banks and Banks Systems, Volume 4, Issue 2, 2009

[6]C.Whitrow, D.J.hand, P.Juszczak, D.Weston, N.M.Adams "Transaction aggregation as a strategy for credit Card fraud detection"Springer Science, July.30,2008

[7] J.M.Mendel(2000). Uncertain Rule-Based Fuzzy Logic Systems.California: University of Southern California, Los Angleles, CA

[8]S.H.Ab Hamid,M.H.Nizam Md.Nasir, W.Y.Ming and H.Hassan "Improving the performance of the authorization process of credit card System Using Thread-Level Parallelism and Singleton Pattern" Research Journal of Information Technology, 2008

[9]M.Lewis, F.King, T.Arnold, W.Wright, J.Pettit "Method And Apparatus For Evaluating Fraud Risk In An Electronic Commerce Transaction" Jul.22, 2008

[10]J.Dagostino "System And method for performing secure credit card transaction" Mar.24, 2011

[11]D.Westone, N.Adams, D.Hand, C.Whitrow, P.Juszczk "Plastic Card Fraud Detection using Peer Group analysis" September, 2007

[12]A.Shen, R.Tong, Y.Deng "Application of Classification Models on Credit Card Fraud Detection"

[13]T.P.Bhatla, V.Prabhu,A.Due "Understanding Credit Card Frauds" Card Business Review, June 2003

[14]D.Anderson "Debit Card Fraud Detection And Control System" ,Card Alert Service ,Inc.Mar.16, 1999

[15]M.F.A.Gadi, X.Wang,A.P.do.Lago "Credit Card Fraud Detection with Artificial Immune System"

[16]D.Grano, M.E.Buhler, J.Milford, K.Lawson "Secure Data Processing System, Such As a system for Detecting Fraud And Expediting Note Processing" Sep.14, 2006

[17]D.Montage "Essentials of Online Payment Security and Fraud Prevention" John Wiley & Sons,Inc.

[18]D.Simic "Reducing Fraud In Electronic Payment Systems" The 7th Balkan Conference on Operational Research "BACOR 05" Constanta, May 2005, Romania

[19]S.Varadarajan,K.Kalyana "System and method for deep interaction modeling for Fraud" Apr.26, 2006

[20]"JPOS Programmer's Guide" version 1.6.1. www.jpos.org

[21] "Financial transaction card originated messages-Interchange message specification ISO 8583"Second edition 1993-12-15. Organization (in partnership with IEC and ITU) of the World Standards Cooperation academic days. http://www.iso.org.

[22]Cahill, Michael H., et. al., *Detecting Fraud in the Real World*, Handbook of massive data sets, Handbook of

978-1-4799-0393-1/13/$31.00 ©2013 IEEE

massivedata sets, Kluwer Academic ublishers, Norwell, MA, USA, 2002.

[23] de Castro, LN., Timmis, J., "Artificial immune systems: A novel paradigm to pattern recognition", Artificial Neural networks in pattern Recognition, University of Paisley, 2002.

[24] J. T. S. Quah and M. Sriganesh, "Real-time credit card fraud detection using computational intelligence," Expert Systems with Applications,2007, pp.9-17

[25] R. A. Tansel Ozyera, Ken Barker, "Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criteria for rule prescreening,"Journal of Network and Computer Applications, vol. 30, pp. 99-113,2007.

[26] D. Sanchez, M. A. Vila, L. Cerda, and J. M.Serrano, "Association rules applied to credit card fraud detection," Expert Systems with Applications, 2008, pp.1-14.

[27] M. N. Mark Jyn-Huey Lim, Jacky Hartnett,"Detecting Abnormal Changes in E-mail Traffic Using Hierarchical Fuzzy Systems," IEEE,2007, pp.1-7

[28]C.Radu "Implementing Electronic Card Payment Systems" Artech House,2003

978-1-4799-0393-1/13/$31.00 ©2013 IEEE