Vol 7. No. 2 - June, 2014

African Journal of Computing & ICT

www.ajocict.net

An Intelligent Financial Fraud Indication System Using Fuzzy Logic

[1]D. Maliki, [2]A. M. Aibinu and [1]O. M.Olaniyi
[1]Computer Engineering Department
, [2]Telecommunication Engineering Department
Federal University of Technology, Minna, Nigeria
danlami.maliki@futminna.edu.ng, abiodun.aibinu@futminna.edu.ng, mikail.olaniyi@futminna.edu.ng

ABSTRACT

The issue of financial fraud is taking different dimensions in various countries due to rise in fraud enabling factors emanating from internal and external challenges. The internal challenges from unemployment rate depend on overpopulation, poor standard of living and nature of existing leadership of government. Recent advancement in modern technology and increase in tourist activities have contributed to the existing external challenges. In this paper, an intelligent financial fraud indication system using fuzzy logic is proposed, which involves the use of fuzzy arithmetic, fuzzy degree of association, fuzzy inference, fuzzy rules and different surface plot in determination of different relationship as it relate to certain choice of inputs. The selected input indices were meant to determine how certain degree of changes in inputs can affect the nature of fraud indication. The proposed system also depends on fraud enabling factors in the determination of appropriate fraud indication level. From the results obtained, it is shown that people from areas with high population, high political activities and high education are likely to be engaged in more financial fraud compared to an area in which population, political activities and education are low.

Keywords- Financial fraud, Financial institution, Fuzzy logic, Intelligent system, Membership function.

African Journal of Computing & ICT Reference Format:
M. Danlami, A. M. Aibinu &. M.Olaniyi (2014). An Intelligent Financial Fraud Indication System Using Fuzzy Logic.
Afr J. of Comp & ICTs. Vol 7, No. 2. Pp 77-84.

1. INTRODUCTION

Financial transactions have been recognized to be major activities in any financial institution [1]. The financial investment sector and internet technology was originally created with the expectation of an ideal world where every individual honestly carry out sincere and efficient transaction. However, the dark side begins to surface with issue of Financial Fraud (FF) [2]. FF is a deliberate act by a person or group of people with the aim of violating trust and protocol in any financial transaction [3]. FF pattern involving forgery, digital property right violation, phishing attack, stolen card and incorrect auditing process are attracting a great deal of attention [4]. To this great extent, Financial Fraud Detection (FFD) and Indication System are of paramount importance, in which different systems will be developed.

The developed system should have the capability of detecting, indicating, analyzing and even preventing any attack capable of undermining business or government transactions [5]. Indication of fraud due to breach of security and protocol still remain a critical issue [6]. Traditional methods of FFD depend only on client level of education and information contained in the database. In this case, time of intelligent response against any potential fraud is very low [7].

In the context of latest techniques in carrying out fraud indication and detection, the concept of Artificial Intelligence (AI) was used to provide high level of intelligent response based on classification from statistical evidences [8]. The discovery of supervised and unsupervised techniques of fraud indication in recent years, serve as a better improvement upon the traditional method of FFD [9]. Some of the AI techniques used in indicating and preventing the existence of financial fraud usually depend on the knowledge of independent analysis, learning, probability and decision making [10].

Artificial Neural Networks (ANN) can be used in prediction of unknown financial fraud base on available data of previous learning experiences that serve as a benchmark for decision taking [12]. The idea of fuzzy logic can also serve as a tool in combining human thinking and reasoning in prediction of transaction fraud in complex and confusing situation [11]. The remaining part of this paper is organised as follows: Section 2 discusses on determinant of financial fraud; Section 3 discusses various methods of detecting financial fraud; Section 4 discusses financial fraud indicator system; Section 5 discusses result and Section 6 discusses conclusion from the overall review.

2. DETERMINANTS OF FINANCIAL FRAUD

Rapid growth in population coupled with low employment rate can easily result to FF [13]. Other effects from the fast population growth range from poor standard of living, slow economic growth and social disorder [14]. The educational improvement from Information and Communication Technology (ICT) has led to a situation whereby some individual in the society are using it as a medium for financial fraud. A decade ago, not every part of the world had access to internet technology and the rate of internet fraud was minimal [15]. One of the objectives of using ICT in committing fraud started with the belief of some individuals of being potential hackers or defrauding others for personal profit gain [16]. Also, political leadership resulting from the election of various political office holders are among the causes of corruption that result to financial fraud [17].

3.METHODS FOR DETECTING FINANCIAL FRUAD

There is different artificial intelligence techniques use in detecting FF. The techniques involved the use of different data set as input variable.

3.1 *Bayesian Belief Network*

The concept of Bayesian Belief Network was used in detecting fraudulent financial statement using certain transaction class. If H can be a transaction and X belonging to a particular transaction class C. The probability of certain transaction to hold is given in (1).

$$P(H/X) = \frac{(P(X/H) \times P(H))}{P(X)} \quad (1)$$

$$\text{Classifier} = P(C_i/X) \quad (2)$$

$$P(x_1, x_2, \dots x_n) = \pi P(x_i/\text{parents}(x_1)) \quad (3)$$

The calculation of true transaction is done by the classifier in (2). The parent serves as the overall transaction which can be use in comparison with the customer financial account over the set of $(x_1, x_2, \dots x_n)$ in determining score for genuine and fraudulent transactions [18].

3.2 *Application Fraud Approach*

Support Vector Machine (SVM) and Random Forest was used in detecting FF that exists in credit card [19]. The concept was built around application fraud resulting from the use of fake credit card and behavioural fraud that result from stolen credit card. The two type of identified fraud was also used to form different transaction data set which SVM base it own comparison upon. The determination of Accuracy in (4), Sensitivity (existence of fraud) in (5), Precision (predicted fraud) in (6) and Specificity (no fraud case) in (7) was used as measure of performance while Random Forest performed the function of selecting the infected data set over a given period of time [19].

$$\text{Accuracy} = \frac{(TP+TN)}{TP+FP+TN+FN} \quad (4)$$

$$\text{Sensitivity} = \frac{TP}{(TP+FN)} \quad (5)$$

$$\text{Precision} = \frac{TP}{(TP+FP)} \quad (6)$$

$$\text{Specificity} = \frac{TN}{(FP+TN)} \quad (7)$$

3.3 *Associate Rule Approach*

An associated data mining rule was used to detect FF using credit card [20]. The associated rules was developed using Fuzzy logic to differentiate between genuine and fraudulent card user. Information from a certain repository containing the status of every card user, including previous transaction was utilized in developing rules that rank the level of detection. This is represented as:

$$I = \{I_1, I_2, I_3 \dots . I_m\} \quad (8)$$

$$T_i = \frac{\sum_{I \in} ti}{t} \quad (9)$$

If I_1 is high and I_2 is low and T_i < C_A THEN C_k = 1
If I_2 is low and I_3 is high and T_i > C_A THEN C_k = 0

Let I be a set of any choice of transaction stated in (8) and T be a fuzzy combination during the transaction. Whenever a transaction takes place $I \in T$ and $t(i)$ is a membership degree of I for which C_k represents the validity of a transaction and $C_A$total amount in credit card. When C_k= 1, then transaction is valid and when C_k = 0, transaction is invalid (recognize as fraud) [20].

3.4 *Financial Text Predictor*

The financial text predictor used an automatic text analyzer in differentiating between companies experiencing fraud and bankruptcy [21]. The automatic text analyzer starts by collecting financial document and proceed to analyze the text in the document with the extraction of certain key words from an inbuilt dictionary. Each document can be represented mathematically by a vector space given in (10), with the number of keywords represented as *n*; and w_{ij} represents the weight of the keywords *i* in document *j* in (11); tf_{ij} is the frequency of the term d_j and *N* is the number of collected documents.

$$d_j = (w_{1j}, w_{2j}, \dots w_{nj}) \quad (10)$$

$$w_{ij} = tf_{ij} \times \log\frac{N}{n} \quad (11)$$

$$idf_{ij} = \log\frac{N}{n} \quad (12)$$

© 2014 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net

Thus, a WorldNet was used in conjunction with Word Sense Disambiguation (WSD) to understand the meaning of some financial activities as presented in financial reports [21]. Detection of fraud or bankruptcy depends on ranking repetition of '0' and '1' in similar and dissimilar words that exist in financial report [21].

3.5 *Fusion Approach*

Fusion techniques combines Bayesian learner, rule based filter, transaction history and dempster-shafer adder in detecting credit card fraud [22]. Fraud detection was performed on $C_1, C_2, C_3, \dots C_n$ as a set of transaction data set in which $P(C_1), P(C_2), \dots . P(C_1)$ stand for information on a particular credit card. A suspicious score of $\varphi\left(T_{j,p}^{ck}\right)$ was applied for a credit card in which C_k and ρ were used to determine the time difference between the present and past transaction. The upper detection boundary $(0 \leq \theta_{UT} \leq 1)$ and lower detection boundary $(0 \leq \theta_{LT} \leq 1)$ were set up as thresholds for classification. The detection of normal and abnormal transaction is done by the rule filter in order to determine the existence of any fraud during a financial transaction [22].

4. FINANCIAL FRAUD INDICATOR SYSTEM

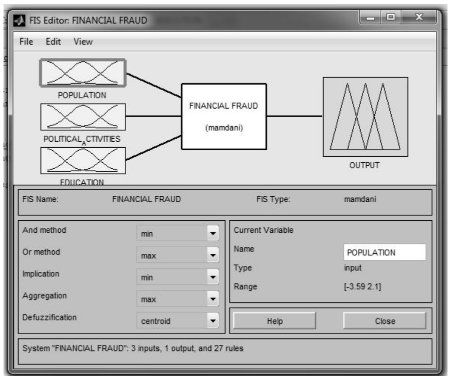
Financial fraud indicator system is developed using the fuzzy inference system, degree of membership function, fuzzy rules and rule viewer. Detail description is presented here with.

4.1 Fraud Input Indices

The system fraud indices include POPULATION, POLITICAL ACTIVIES and EDUCATION. These input indices serve as the three inputs to the fuzzy logic system.

4.2 Fuzzy Inference System

The fuzzy inference system serves as an entry point for three fuzzy inputs. A Mamdani inference method was used along with the three inputs to provide a logical AND combination method to obtain an output as shown in Fig 1.

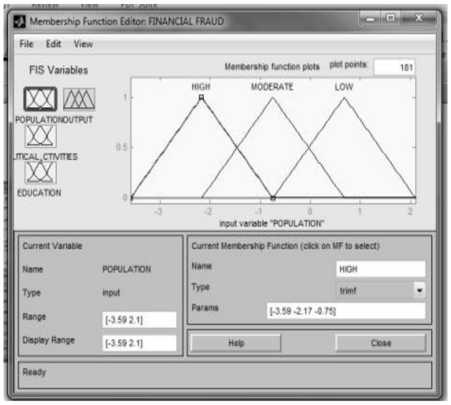


FIS Name: FINANCIAL FRAUD
FIS Type: mamdani
And method: min
Or method: max
Implication: min
Aggregation: max
Defuzzification: centroid
Current Variable
Name: POPULATION
Type: input
Range: [-3.59 2.1]
System "FINANCIAL FRAUD": 3 inputs, 1 output, and 27 rules

Figure 1: Input Membership Function

4.3 Population Membership Function

The population membership function was developed using range of values as shown in Figure 2 with a maximum value at -3.590 and minimum value at 2.100.

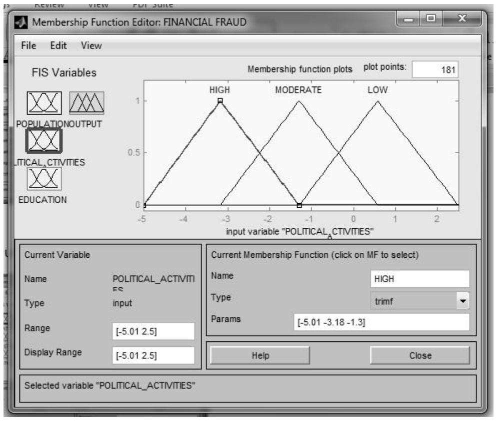


plot points: 181
Current Variable
Name: POPULATION
Type: input
Range: [-3.59 2.1]
Display Range: [-3.59 2.1]
Current Membership Function (click on MF to select)
Name: HIGH
Type: trimf
Params: [-3.59 -2.17 -0.75]
Ready

Figure 2: Population fuzzy set

4.4 Political Activities Membership Degree

Three degree of membership function was used to develop the political activities membership set with maximum range at -5.100 and a minimum value at 2.500 as shown in Figure 3.

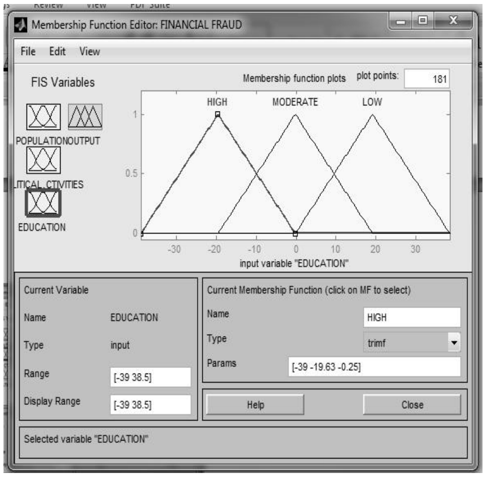


plot points: 181
Current Variable
Name: POLITICAL_ACTIVITIES
Type: input
Range: [-5.01 2.5]
Display Range: [-5.01 2.5]
Current Membership Function (click on MF to select)
Name: HIGH
Type: trimf
Params: [-5.01 -3.18 -1.3]
Selected variable "POLITICAL_ACTIVITIES"

Figure 3: Political activities fuzzy set

4.5 Education Membership Function

The education membership functions used have its highest value at -39.000 and a minimum value at 38.500 as shown in Figure 4.



plot points: 181

Current Variable
Name EDUCATION
Type input
Range [-39 38.5]
Display Range [-39 38.5]

Current Membership Function (click on MF to select)
Name HIGH
Type trimf
Params [-39 -19.63 -0.25]

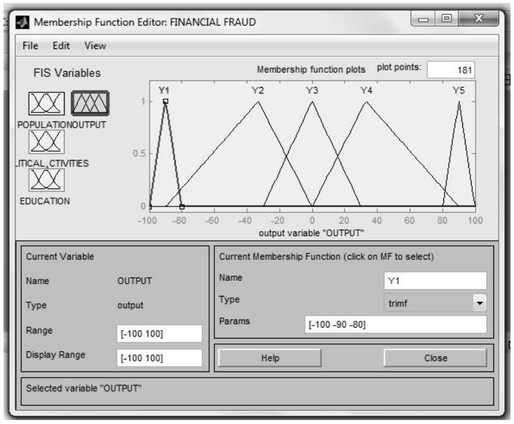
Selected variable "EDUCATION"

Figure 4: Education fuzzy set

4.6 Output Membership Function

Five output membership functions are use to set up five output condition for financial fraud indication which ranges from Y1, Y2, Y3, Y4 and Y5 as shown in figure 5.

Y1 = Extremely High Crime Rate
Y2 = High Crime Rate
Y3 = Moderate Crime Rate
Y4 = Low Crime Rate
Y5 = No Crime Rate



plot points: 181

Current Variable
Name OUTPUT
Type output
Range [-100 100]
Display Range [-100 100]

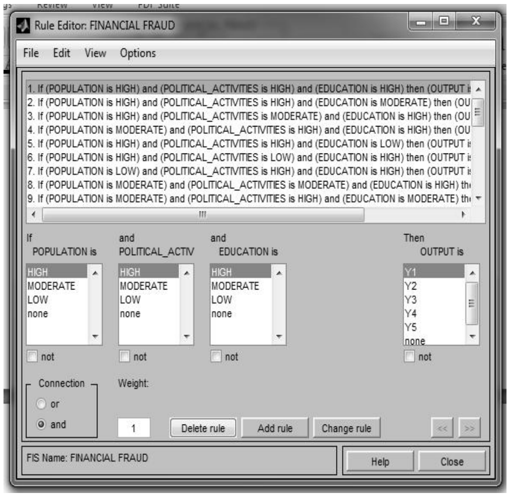
Current Membership Function (click on MF to select)
Name Y1
Type trimf
Params [-100 -90 -80]

Selected variable "OUTPUT"

Figure 5: Output membership function

4.7 Fuzzy Rules Development

About 27 fuzzy rules are developed. The rules depend on the number of available inputs and the degree of membership as shown in figure 6.



1. If (POPULATION is HIGH) and (POLITICAL_ACTIVITIES is HIGH) and (EDUCATION is HIGH) then (OUTPUT i
2. If (POPULATION is HIGH) and (POLITICAL_ACTIVITIES is HIGH) and (EDUCATION is MODERATE) then (OU
3. If (POPULATION is HIGH) and (POLITICAL_ACTIVITIES is MODERATE) and (EDUCATION is HIGH) then (OU
4. If (POPULATION is MODERATE) and (POLITICAL_ACTIVITIES is HIGH) and (EDUCATION is HIGH) then (OU
5. If (POPULATION is HIGH) and (POLITICAL_ACTIVITIES is HIGH) and (EDUCATION is LOW) then (OUTPUT i
6. If (POPULATION is HIGH) and (POLITICAL_ACTIVITIES is LOW) and (EDUCATION is HIGH) then (OUTPUT i
7. If (POPULATION is LOW) and (POLITICAL_ACTIVITIES is HIGH) and (EDUCATION is HIGH) then (OUTPUT i
8. If (POPULATION is MODERATE) and (POLITICAL_ACTIVITIES is MODERATE) and (EDUCATION is HIGH) th
9. If (POPULATION is MODERATE) and (POLITICAL_ACTIVITIES is HIGH) and (EDUCATION is MODERATE) th

If POPULATION is	and POLITICAL_ACTIV	and EDUCATION is	Then OUTPUT is
HIGH	HIGH	HIGH	Y1
MODERATE	MODERATE	MODERATE	Y2
LOW	LOW	LOW	Y3
none	none	none	Y4
			Y5
			none
□ not	□ not	□ not	□ not

Connection
○ or
● and

Weight: 1

FIS Name: FINANCIAL FRAUD

Figure 6: Rule editor.

5. RESULTS AND DISCUSSION

The five output conditions are evaluated by comparing the rules that were activated with the rule viewer output of Extremely High Crime Rate, High Crime Rate, Moderate crime Rate, Low Crime Rate and No Crime Rate.

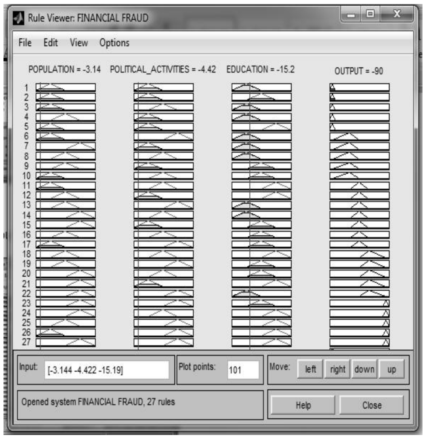
5.1 Extremely High Crime Rate

R1 and R2 were activated in Figure 7, which indicates an output of -90 for Extremely High Crime Rate. The R1 and R2 rules are given as:

R1: IF (POPULATION is HIGH) and (POLITICAL ACTIVITIES is HIGH) and (EDUCATION is HIGH) THEN (OUTPUT is Y1)

R2: IF (POPULATION is HIGH) and (POLITICAL ACTIVITIES is HIGH) and (EDUCATION is MODERATE) THEN (OUTPUT is Y1)

© 2014 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net



POPULATION = -3.14 POLITICAL_ACTIVITIES = -4.42 EDUCATION = -15.2 OUTPUT = -90

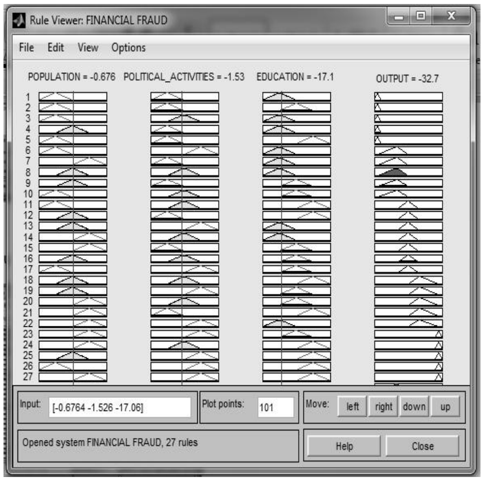
Input: [-3.144 -4.422 -15.19] Plot points: 101

Opened system FINANCIAL FRAUD, 27 rules

Figure 7: Extremely high crime rate output

5.2 High Crime Rate

R8 was activated in Figure 8 which indicates an output of -32.7 for High Crime Rate. The R8 rule is given as:
R8: IF (POPULATION is MODERATE) and (POLITICAL ACTIVITIES is MODERATE) and (EDUCATION is HIGH) THEN (OUTPUT is Y2)



POPULATION = -0.676 POLITICAL_ACTIVITIES = -1.53 EDUCATION = -17.1 OUTPUT = -32.7

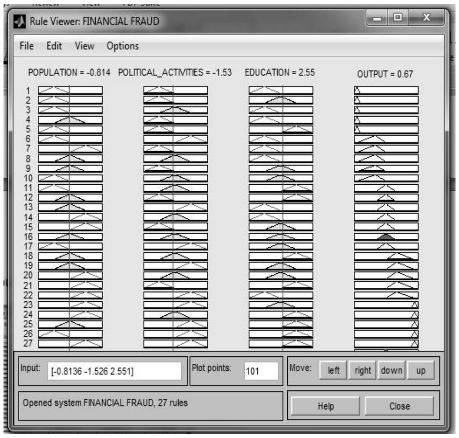
Input: [-0.6764 -1.526 -17.06] Plot points: 101

Opened system FINANCIAL FRAUD, 27 rules

Figure 8: High crime rate output

5.3 Moderate Crime Rate

A Moderate crime Rate provides an indication at R16 with an output of 0.67 in Figure 9. The R16 rule is given as:
R16: IF (POPULATION is MODERATE) and (POLITICAL ACTIVITIES is MODERATE) and (EDUCATION is MODERATE) THEN (OUTPUT is Y3)



POPULATION = -0.814 POLITICAL_ACTIVITIES = -1.53 EDUCATION = 2.55 OUTPUT = 0.67

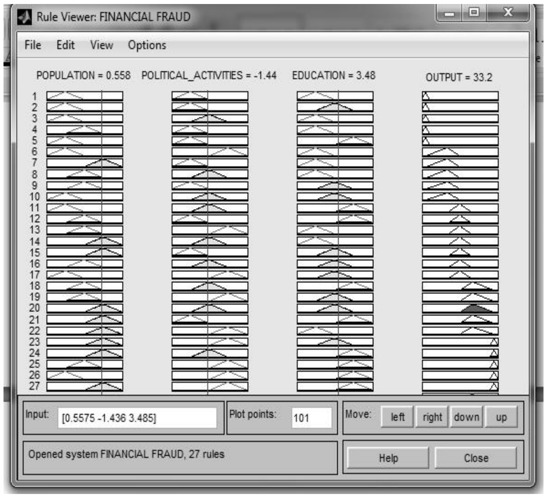
Input: [-0.8136 -1.526 2.551] Plot points: 101

Opened system FINANCIAL FRAUD, 27 rules

Figure 9: Moderate crime rate output

5.4 Low Crime Rate

A Low Crime Rate provides an indication at R20 at an output of 33.2 in Figure 9. The R20 rule is given as:
R20: IF (POPULATION is LOW) and (POLITICAL ACTIVITIES is MODERATE) and (EDUCATION is MODERATE) THEN (OUTPUT is Y4)



POPULATION = 0.558 POLITICAL_ACTIVITIES = -1.44 EDUCATION = 3.48 OUTPUT = 33.2

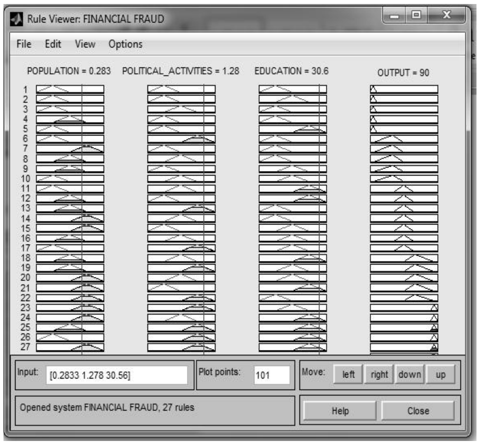
Input: [0.5575 -1.436 3.485] Plot points: 101

Opened system FINANCIAL FRAUD, 27 rules

Figure 10: Low crime rate output

5.5 No Crime Rate

A condition of No Crime Rate was triggered by R25 and R27 in Figure 10. The R25 and R27 rules are given as:
R25: IF (POPULATION is MODERATE) and (POLITICAL ACTIVITIES is LOW) and (EDUCATION is LOW) THEN (OUTPUT is Y5)
R27: IF (POPULATION is LOW) and (POLITICAL ACTIVITIES is LOW) and (EDUCATION is LOW) THEN (OUTPUT is Y5)


Rule Viewer: FINANCIAL FRAUD

POPULATION = 0.283 POLITICAL_ACTIVITIES = 1.28 EDUCATION = 30.6 OUTPUT = 90

Input: [0.2833 1.278 30.56]

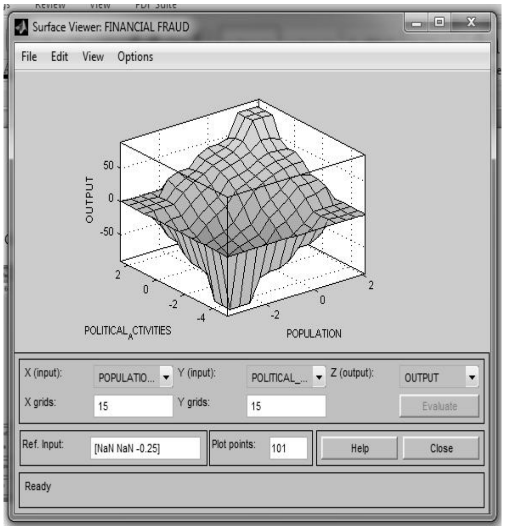
Plot points: 101

Opened system FINANCIAL FRAUD, 27 rules

Figure 10: No crime rate output

5.6 Population and Political Activities Relationship

A 3D graph in Figure 11, shows two inputs and one output relationship. The extreme rate of FF is given at -50 with input range of -4 for political activities and -2 for populations. This relationship indicate that at a very high population the rate of voters registration at a particular region is always very high which directly represent the high level of political activities that will be experienced at a particular period of time. The high level of such activities easily results to FF due to cases of unemployment and accessibility to fund for political activities. The rate of fraud starts to reduce at an output range of 0 to 50 with an input range of 0 to 2 on both population and political activities axis.


Surface Viewer: FINANCIAL FRAUD

X (input): POPULATIO... Y (input): POLITICAL_... Z (output): OUTPUT

X grids: 15 Y grids: 15

Ref. Input: [NaN NaN -0.25]

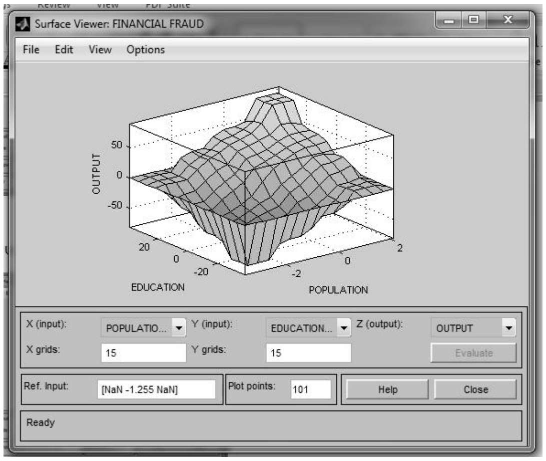
Plot points: 101

Ready

Figure 11: Population and political activities

5.7 Population and Education Relationship

The surface viewer in Figure 12 indicate that at high rate of education and at high rate of population, a condition of extremely high crime will be experienced as a result of acquiring more technological education and issue of unemployment that originate from high population. With this, people might be encouraged to commit fraud due to availability of the skills and financial hardship from unemployment. Condition of low rate in financial fraud exist an output above 0 with moderate situation of fraud at an output of 0.


Surface Viewer: FINANCIAL FRAUD

X (input): POPULATIO... Y (input): EDUCATION... Z (output): OUTPUT

X grids: 15 Y grids: 15

Ref. Input: [NaN -1.255 NaN]

Plot points: 101

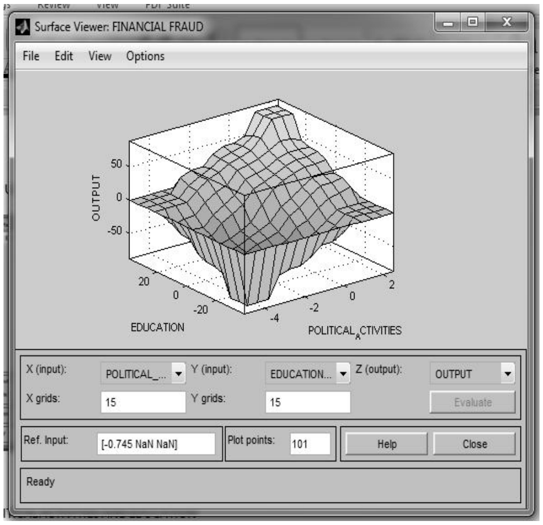
Ready

Figure 12: Population and education

5.8 Political Activities and Education Relationship

The relationship between political activities and education is given in figure13. The input at high rate of education and high rates of political activities experience a very high rate of financial fraud with an output of -50. This provides an indication that an increase in number of educated people in an environment will enhance high political activities, which easily result to different issues of fraud. A low range of fraud begins to surface above 0 up to maximum output point of 50.

© 2014 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net



X (input): POLITICAL_...
Y (input): EDUCATION...
Z (output): OUTPUT
X grids: 15
Y grids: 15
Ref. Input: [-0.745 NaN NaN]
Plot points: 101
Ready

Figure 13: Political activities and education relationship

6. CONCLUSION

This paper presented the development of FF indication of individual likely potential level to commit financial fraud using fuzzy logic as an artificial intelligence approach. In this paper, different relationships among the inputs were also studied. The study further aid in determining the variation of output as related to the selection of two or three different input membership function which was indicated in the rule viewer and surface plots.

REFERENCE

[1] Akiyom, O.J. (2012). Examination of Fraud In Nigerian Banking Sector and It Prevention. Asian Journal of Management Research, 3, 184-192.

[2] Won, K., Ok, R.J., Chulyun, K., & Jungmin, S. (2011). The Dark Side of Internet: Attack, Costs and Responses. Journal of Information Systems, 36, 675-705.

[3] Adeyemo, A.K. (2012). Fraud in Nigerian Banks, Nature, Deep Seated Causes, Aftermaths and Probable Remedies. Mideteranian Journal of Social Science, 3, 279-289.

[4] Ngai, E.w.T., Yong, H. W., Yijun, C.,& Xin, S. (2011). The Application of Data Mining Techniques In Financial Fraud Detection: A Classification Frame Work and Academic Review of Literature. Elsevier Journal of Decision Support Systems, 559-569.

[5] Angus, O.U. (2013). Advance In Modelling for Falsified Financial Statements. International Journal of Finance and Accounting, 37-54.

[6] John. L, & Ali A.G. (2012). Improved Competite Learning Neural Networks For Network Intrusion and Fraud Detection. Journal of Neurocomputing , 135-145.

[7] Nitin M., Ranjit, K., & Shishir, K.S. (2012). Credit Card Transaction Fraud Detection by Using Hidden Markov Model. International Journal of Scientific Engineering and Technology, 139-142.

[8] Antonio, M.R.S., Jao, P.C.L .D. C., & Carlos, H.C. (2010). Neural Network Predictor For Fraud Deteection: A Study Case for the Federal Patrimony Department. The Seventh International Conference on Forensic Computer Science, 61-66.

[9] Dharminder, K., Suman & Nutan. (2013). Anormaly Detection Using Support Vector Machine. International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 2363-2368.

[10] Nikita, G., Archana, D., Karan, S. R., & Shiyya, N. (2012). Credit Card Fraud Detection Using Rough Sets and Artificial Neural Network. Journal of Computer Application, 5, 11-20.

[11] Adeyiga, J.A., Ezekie, J.O.J, & Adegbola, O.M. (2012). An Intelligent System for Detecting Irregularities In Electronics Banking Transactions. Journal of computing, Information Systems and Development Informatics, 57-66.

[12] Bingyi, K., Yong, D., Rehan, S., & Sankaran, M. (2012). Evidential Cognitive Maps. Journal of Knowledge- Based Systems, 77-86.

[13] Ayandike, K., & Emeh, I.E., & Ukah, F.O. (2012). Entrepreneurship Development and Employment Generation In Nigeria: Problems and Propects. Universal Journal of Education and General Studies, 88-102.

[14] Chimobi, U. (2010). Poverty In Nigeria: Some Dimensions and Contributing Factors. Global Majority E-journal, 1, 46-56.

[15] Longe, O. Oneurine, N., Friday , W., & Victor, M. (2009). Criminal Uses of Information and Communication Technologies. Journal of Information Technology Impact, 9, 155-172.

[16] Anah, B.H., Funmi, D.L., & Julius, M. (2012). Cybercrime In Nigeria: Causes, Effect and The Way Out. ARPN journal of Science and Technology, 626-631.

[17] Michael, E. E., & Pedro, R.F.S. (2009). A Survey of Signature Based Methods for Financial Fraud Detection. Journal of Computers and Security, 381-394.

[18] Estathios, K., Charalambo, S., & Yannis, M. (2007). Data Minning Techniques for The Detection of Fraudulent Financial Statements. Journal of Expert Systems With Applications, 995-1003.

[19] Siddhartha, B., Sanjeev, J., Kurain, T., & Christopher, W. (2011). Data Mining For Credit Card Fraud: A Comparative Study. Journal of Decision Support Systems, 602-613.

[20] Sanchez, D., Vila, M.A., Cerda, L., & Serrano, J.M. (2009). Association Rules Applied To credit Card Fraud Detection. Journal of Expert System With Application, 3630-3640.

[21] Mark, C., Haldun, A., Gray, J.K. & Praveen, P. (2010). Making Words Works: Using Financial Text As a predictor of Financial Event, Journal of Decision Systems, pp.164-175.

[22] Wen-His, C. & Jau-Shien, C. An Effective Early Fraud Detection Method For Online Auctions, Journal of Electronic Commerce research and Application, pp.346-360, 2012.

AUTHORS' PROFILES

Maliki Danlami is a Lecturer in the Department of Computer Engineering, Federal University of Technology, Minna, Niger State.

Abiodun Musa Aibinu is a Lecturer in the Department of Telecommunication Engineering, Federal University of Technology, Minna, Niger State.

Olaniyi O. Mikail is a Lecturer in the Department of Computer Engineering, Federal University of Technology, Minna, Niger State. He had his First Degree in Computer Engineering at the Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria and M.Sc. Degree in Electronic and Computer Engineering at Lagos State University, Lagos. He is currently a doctoral student at the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria. He is a member of International Association of Engineers and Computer Scientists and Registered with the Council of Regulation of Engineering in Nigeria.