Computing, Information Systems
& Development Informatics Journal

Volume 3. No. 2. May, 2012

An Intelligent System for Detecting Irregularities in Electronic Banking Transactions

[1]Adeyiga,, J.A, Ezike, J.O.J & Adegbola, O.M.
Dept. of Computer Science
Bells University of Technology
Ota, Ogun State, Nigeria
[1]jadeyiga, [2]josephezike, [3]tanwaadegbola [@]yahoo.com

Reference Format: Adeyiga,, J.A, Ezike, J.O.J & Adegbola, O.M. (2012). An Intelligent System for Detecting Irregularities in Electronic Banking TransactionsComputing, Information Systems & Development Informatics Journal. Vol 3, No .2. pp 57-66

cisdi Journal Computing, Information Systems & Development Informatics Journal Vol 3. No. 2, May , 2012

An Intelligent System for Detecting Irregularities in Electronic Banking Transactions

Adeyiga,, J.A, Ezike, J.O.J & Adegbola, O.M.

ABSTRACT
Frauds have historically been the major cause of bank losses. It has led to failures of some banks in the pasts, contributing to shareholders losing their investments in the banks. Information technology is a critical component in creating value in the banking sectors, it provides decision makers with an efficient means to store, calculate, report and predict bank frauds and security failures. Information system security views this challenge as a prediction problem that attempts to detect irregular transactions in the banking sector operations scenario. This study applies neural network techniques to the bank fraud prediction problem. Using Nigerian banks as a point of reference, we design a Neural Network-Based Model that employs multilayered Feed Forward Artificial Neural Network on database system for collecting training data for the Artificial Neural Network. The Intelligence of the system is being tested on data extracted from statements of accounts from three different banks in Nigeria and the results were discussed.

Keywords: Artificial neural network, transactions, bank fraud, financial institutions & cyber security

1. INTRODUCTION

The Concise Oxford Dictionary defines fraud as 'criminal deception; the use of false representations to gain an unjust advantage'. Economic growth has been the major objective of any successive governments and it is the engine of growth in any economy, given its function of financial intermediation. Banks as financial intermediaries are expected to provide avenue for people to save incomes not expended on consumption however most of these banks failed as a result; they were unable to contribute to the growth of their economy. Banking flaws are caused by several reasons and one of the most common and persistent reason is the issue of security. In order to reduce the stress caused as a result of conventional banking practise, banking sector came up with electronic banking so as to avail customers the opportunity of doing their transaction without having to walk into the bank but as good as their arrangement is, it came up with a lot of security issues. Through its function, banks facilitate capital formation and promote economic growth. However, bank's ability to render economic growth and development depends on the health, soundness and stability of the system [2]. It is, therefore, not surprising that the banking industry is one of the most regulated sectors in any economy. It is against this background that the Central Bank of Nigeria outlined as part of the first phase of its banking sector reforms, the assurance of a diversified, strong and reliable banking industry [15]

The main objective of the reforms is to guarantee an efficient and sound financial system. The reforms are designed to enable the banking system develop the required resilience to support the economic development of the nation by efficiently performing its functions as the fulcrum of financial intermediation [11]. The objective is to ensure the safety of depositors' money, position banks to play active developmental roles in the Nigerian economy, and become major players in the sub-regional, regional and global financial markets. But banking industry started given their staff untenable targets for mobilizing profits, mobilizing deposits and in the process they threw caution to the winds and got very careless. [19].

As more financial institutions in Nigeria moves towards information technology driven services, security issues need to be addressed before banks and customers can confidently take advantage of these platforms. Banks are afraid of losing their cash to fraudsters who can manipulate their system and get undue advantage, while customers are still not convinced that banking is totally secured. There is need for customers' transactions to be monitored so as to notice and alert the bank officials of irregular and suspicious transactions on customer accounts.

Currently, transactions are usually manually monitored by bank personnel who look through the customers' statement of accounts when unusual transactions are noticed. The process is often very tedious and inefficient mainly because of the number of transactions and customer base.
With the advent of computers and Information systems there is a possibility of an automated approach to the analysis of the customers' statement of account for detecting irregularities in banking activities. However, considering the fast pace at which mainstream business rules changes, the definition of fraudulent transaction changes rapidly thereby making the design and development of such a system a rather complex process [1]. A solution paradigm is to explore automated approaches to irregularity detection using algorithmic approach and artificial Intelligent System.

This paper is aimed to create a Neural Network-Based System to detect irregular transactions based on certain parameters for the banking industry in Nigeria. The system should provide a means of automatically alerting relevant officers as soon as irregular transactions are detected. The officers will then investigate further and make a decision. A multilayered Feed Forward Artificial Neural Network will be created and a reliable database system of collecting training data for the Artificial Neural Network. The system was tested using real life customer's statement of account which was collected from three commercial banks in Nigeria

2. RELATED WORKS

It is evident from our investigations that one of the causes of frauds in the financial institutions was a combination of too much money in the possession of banks. The too much money in their hands was as a result of Banking consolidation by the former CBN governor, Prof Soludo which made them go from N2 billion of shareholders fund to N25 billion and then on to N100 billion of share capital. Moreover, there was a candy held that any one that got to N100 billion will be able to manage the Nigeria's external reserve.

The drive to meet the target made banks grow tremendously in terms of capital base and assets without a corresponding growth in their risk management and compliance IT system; People were given untenable targets for mobilizing profits, mobilizing deposits and in the process they threw Caution to the winds and got very careless. [19].

In [7][12] an approach to fraud detection that is based on tracking calling behaviour on an account over time and scoring calls according to the extent that they deviate from patterns that resemble fraud are described. Account summaries are compared to threshold each period and an account whose summary exceeds a threshold can be queued to be analyzed for fraud. Thresholding has several disadvantages; it may vary with time of day, type of account and types of call to be sensitive to fraud investigation without setting off too many false alarms for legitimate traffic [12].

Fawcett and Provost [7] developed an innovative method for choosing account-specific threshold rather than universals threshold that apply to all accounts or all accounts in a segment. In the experiment, fraud detection is based on tracking account behaviour. Fraud detection was event driven and not time driven, so that fraud can be detected as it is happening. Second, fraud detection must be able to learn the calling pattern on an account and adapt to legitimate changes in calling behaviour. Lastly, fraud detection must be self-initializing so that it can be applied to new accounts that do not have enough data for training. The approach adopted probability distribution functions to track legitimate calling behaviour.

Other models that have been developed in research settings that have promising potential for real world applications include the Customer Relationship Model, Bankruptcy Prediction Model, Inventory Management Model, and Financial Market Model. In [4] it was stated that many financial institutions see the value of ANNs as a supporting mechanism for financial analysts and are actively investing in this arena. The models described provide the needed knowledge to choose the type of neural network to be used. The use of techniques of decision trees, in conjunction with the management model CRISP-DM, to help in the prevention of bank fraud was evaluated in {5}. The study recognized the fact that it is almost impossible to eradicate bank fraud and focused on what can be done to minimize frauds and prevent them. The research offered a study on decision trees, an important concept in the field of artificial intelligence.

The study focused on discussing how these trees are able to assist in the decision making process of identifying frauds by the analysis of information regarding bank transactions. This information is captured with the use of techniques and the CRISP-DM management model of data mining in large operational databases logged from internet bank. The Cross Industry Standard Process for Data-Mining – CRISP-DM is a model of a data mining process used to solve problems by experts. The model identifies the different stages in implementing a data mining project while, A decision tree is both a data representing structure and a method used for data mining and machine learning. [3] Describes the Use of neural networks in analyzing the great increase in credit card transactions; credit card fraud has become increasingly rampant in recent years. This study investigates the efficacy of applying classification models to credit card fraud detection problems.

To increase the body of knowledge on this subject, an in-depth examination of important publicly available predictors of fraudulent financial statements was offered. They tested the value of these suggested variables for detection of fraudulent financial statements within a matched pair's sample. Self-organizing Artificial Neural Network (ANN) AutoNet was used in conjunction with standard statistical tools to investigate the usefulness of these publicly available predictors.

The study resulted in a model with a high probability of detecting fraudulent financial statements on one sample [1][6]. The study reinforced the validity and efficiency of AutoNet as a research tool and provides additional empirical evidence regarding the merits of suggested red flags for fraudulent financial statements. [10] Reviews the various factors that lead to fraud in the Nigerian Banking industry. The problem of fraud in our banking system may have some attachment. Therefore, there must be some factors that may have led to this fraudulent act. [17] Discuses the approaches used by fraudsters, and identify phishing have the most common forms for stealing account details for authentication from the customers.

Social engineering is the most common method used in phishing. Social engineering usually comes in the form of e-mails trying to convince users to open attachments or by directing them to some fraudulent site**,** and most of the time it is so well designed that many customers are led to informing their account details**.** [17] Also, present a framework, and the corresponding system, for online banking fraud detection in real time. It uses two complementary approaches for fraud detection. In the differential analysis approach, the account usage patterns are monitored and compared with the history of its usage, which represent the user's normal behavior. Any significant deviation from the normal behavior indicates a potential fraud

In this paper, we present a model for detecting irregularities in e-banking transactions to address the above challenges in Nigeria. The proposed System, a continuation of our work in [18], would assist bank personnel the opportunity to notice irregularities in transactions which will normally be successfully carried out oblivious of abnormal patterns. The system is convenient and easy to use and increase the integrity of the bank. It also gives customer some level of trust transacting with the bank.

3. METHODOLOGY

We perceive neural networks as tools that can recall and learn patterns of behaviour, detect changes in patterns, and detect fraud in a payment card environment. We research to do the following:

- Generate/ create a unique network for each account in the bank
- Generate patterns for the network using the client history.
- Train the network at user defined epoch value or till there error value is approximately 0.
- Once the network has learned, feeds the current transaction into the network to know if it is a fraud or not.

Components of The Irregularity Detection System

i. Neural network based detector
ii. Database
iii. Computer System

3.1.1 Neural Network Based Detector

The neural network based detector is a mathematical model or computational model based on biological neural networks, in other words, it is an emulation of biological neural system. A neural network is a massively parallel distributed processor that has a natural propensity for storing experiential knowledge and making it available for use. It resembles the brain in two respects [8].

1. Knowledge is acquired by the network through a learning process.

2. Interconnection strengths known as synaptic Weights are used to store the knowledge.

3.1.2 Database

The data are typically organized to model relevant aspects of reality. Structured query language will be used for the data store. This is the region where the account statements will be lodged and details of all transactions that take place in each account are stored in the database.

All transactions carried out in a customer's account are stored in the database and can be retrieved when needed. The database serves as the knowledge base to the neural network, the network trains and generates results based on the information in the knowledge base.

3.1.3 Computer System

The Computer system consists of the platform in which the irregularity detection system will operate, neural network cannot exist on its own. It is usually implemented in computer systems and related devices. The computer also serves as the interface between the neural network based detector and the system user. The computer presents the input data (user query) to the neural network.

3.2 Layout of the Irregularity Detection System

The simplified activities that take place in the irregularity detection system

1. The input data (customer credit/debit transaction) is presented by the interface (computer) to the database (knowledge base).
2. The network is fed by the knowledge base.
3. The network trains based on the data in the knowledge base
4. If the network based detector detects any irregularity, the transaction is disallowed else the transaction is allowed. Whatever decision the network based detector arrives at is stored at the knowledge base (database)

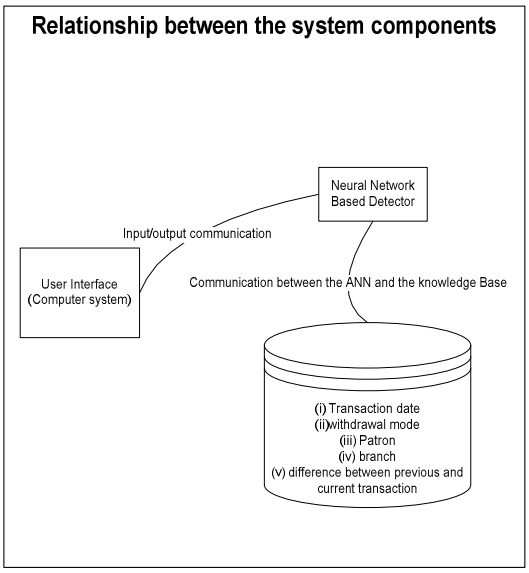


Fig 1. Proposed System components

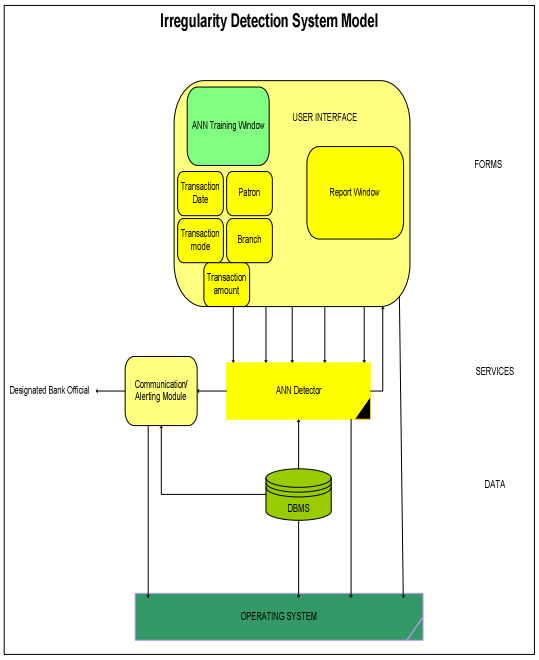


Fig 2. Proposed System Model

3.3 The Network Training Model

Modeling was done using the unified modeling language (UML). The system is modeled to be able to look through a client's transaction history and generate an intelligent pattern which will be used as standard for testing the next transaction.

For example consider

i. A client that has made withdrawals about 1000 times from a particular branch of a bank is suddenly withdrawing from a farther (another) branch.
ii. A client transaction history can denote his maximum withdrawal/Deposit to be 5000 naira, and suddenly he/she withdraws/deposits 5,000,000 naira.
iii. A client withdrawal/deposit mode and transaction date difference can also be used as a pointer in identifying irregularities.

In training the multilayer perceptron network (MLP), five different entries will be inputted which are as follows;

Entry 1 :difference between the current and last transaction based on the number of days.

Entry 2: percentage of last withdrawal/deposit to current transaction

Entry 3: the branch the transaction is taking place (location)

Entry 4: patron that is; self or different person?

Entry 5: transaction date.

The network produces reasonable outputs for inputs it has not been taught how to deal with. The various entries are presented to the network in form of numeric values. Transaction mode for withdrawal can only be either cheque/slip, ATM, Credit Card. These values can only be presented with numeric values in order to generate a pattern. Fixed numbers are chosen at random with the condition of being centralized around zero. The numbers are chosen in order to have distinctive output when presented to the network. These random values assist in reducing the learning time of the MLP else the network might take a longer time to learn (training a Neural Network involves trial an error till the result generated matches the target output).

The same process is followed for branches though each branch a bank is uniquely identified by codes. Random values between -1 and +1 are used to represent the parameters. MLP learns well with values cantered on zero. The amount involved in the transaction is represented as the percent of the last transaction amount to the current transaction amount; the date is captured by the system based on the system's calendar and clock.

The training process and algorithm is thus described below:

3.4 The Training Algorithm

Supervised Back propagation training algorithm was used to train the neural network because of its effectiveness towards pattern recognition. Training set is a collection of training samples gathered. A training sample is a pair of input vector plus a desired output value (0.8 or -0.8). The network was provided with the training set and allowing it to learn by adjusting weights of its synapses by back propagating the error calculated as the disparity between the output neuron to the expected/target value.

3.5 The Actual Algorithm

1. Identify number of input neurons (same as number of elements in the input vector)
2. Identify number of hidden layers and number of neurons on each layer. (Minimum required for back propagation is one hidden layer but for faster training we used two hidden layers each with 10 neurons each).
3. Identify number of output neurons. We used one neuron on the output layer because we have one target value.
4. Initialize random weight values for the synapses connecting each neurons of preceding layer to the next layer. With back propagation, weight values should be restricted to between -0.5 and +0.5.
5. Choose a random training set from the training sample and assign input vector to the input neurons.
6. Propagate all neurons in the forward direction to obtain output at the output layer.
    a) The output of each neuron is a function of its inputs. In particular, the output of the **j**th neuron in any layer is described by two sets of equations on the right: Uj = ∑ (Xi . wij)……(1)
    b) For every neuron, **j**, in a layer, each of the **i** inputs, $\mathbf{X}_i$, to that Yj = Fth (Uj + tj) layer is multiplied by a previously established weight, $\mathbf{w}_{ij}$. These are all summed together, resulting in the internal value of this operation, $\mathbf{U}_j$. This value is then biased by a previously established threshold value, $\mathbf{t}_j$, and sent through an activation function, $\mathbf{F}_{th}$(tanh function).
    c) The resulting output, $\mathbf{Y}_j$, is an input to the next layer or it is a response to the neural network if it is the last layer.
7. Evaluate error values at the output neuron as the difference between obtained output and the desired output of the training set chosen.
8. Backpropagate the error, all the way up to the input layer.
    a. Back propagation starts from the output layer with the following equation.

$$Ơij = wij + LR \cdot ej \cdot Xi \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

b. For the input of neuron in the output layer, the weight **w** is adjusted by adding to the previous weight value, $\mathbf{w'}_{ij}$, a term determined by the product of a learning rate, **LR**, an error term, $\mathbf{e}_j$, and the value of the input, $\mathbf{X}_i$. The error term, $\mathbf{e}_j$, for the output neuron is determined by the product of the actual output, $\mathbf{Y}_j$, its complement, $\mathbf{1 - Y}_j$, and the difference between the desired output, $\mathbf{d}_j$, and the actual output.

$$Ej = Yj \,.\, (1 - Yj) \,.\, (dj - Yj) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

9. Calculate and update weight values for all synapses such that the sum squared value of the error are minimized.
   a. Once the error term is computed and weights are adjusted for the output layer, the value is recorded and the next layer back is adjusted. A **revised weight adjustment process** was adopted for updating the weights following the Equation below.

$$Wij = w'ij + (1 - M) \cdot LR \cdot ej \cdot Xj + M \cdot (w'ij - w''ij) \ldots . (4)$$

Momentum (M) basically allows a change to the weights to persist for a number of adjustment cycles. The magnitude of the persistence is controlled by the momentum factor. If the momentum factor is set to 0, then the equation reduces to that used to adjust the weight of the output layer. If the momentum factor is increased from 0, increasingly greater persistence of previous adjustments is allowed in modifying the current adjustment. This can improve the learning rate in some situations, by helping to smooth out unusual conditions in the training set.

   b. The error term is generated by a slightly modified version of Equation in steps 9 above. This modification is:

$$ej = Yj \cdot (1 - Yj) \cdot \sum (ek \cdot W''jk) \ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

10. Choose another random training set form the training sample and repeat the steps above.
11. Train all training set in the training sample in a random selection order. A cycle through the training sample is called an epoch.
12. Stopping criterion is until the error obtained at the output layer is at an acceptable value. (0.02)

3.6 The Transfer Functions of the Neural Network.
Activation function is used to obtain output from each neuron. Tangential Activation function was adopted.

The equation is Y=tanh(x).

Input nodes shall be presented which are expected to yield a target output.

If the output is not correct, the weights are adjusted according to the formula:

$$w_{new} = w_{old} + \alpha(\text{desired} - \text{output})*\text{input} \ldots\ldots\ldots\ldots\ldots (6)$$

where α is the learning rate (Cheung and Cannons, 2002)
Using tanh activation function on all neurons the network, the output of each neuron ranges between -1 and +1. Some training set in the training sample has a target value of 0.8 and some -0.8. Once the error at the output layer is at an acceptable level, the test data is fed into the network from the input layer and the output value is derived. The sensitivity bar ranges from -0.8 to 0.8 although presented to range from 0 to 100%. The transaction is committed if the output of the test data is greater than the value of the sensitivity bar, otherwise rolled back.

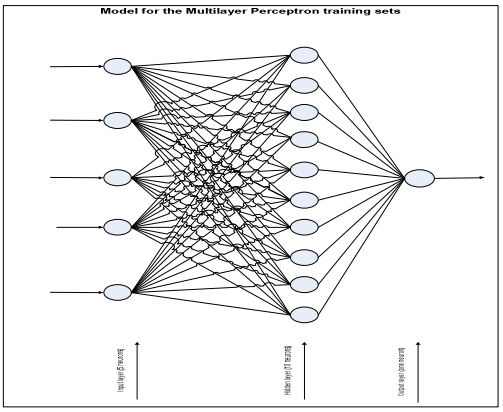


Fig 3. An illustration of the training sets for the multilayer perceptron network.
Source: (Werbos [16]; Rumelhart [14])

3.7 Training and Verification
The training set is not fixed based on all previous transactions with the bank. The training set (initials training set) is 70% of the previous transactions while the testing set (cross validation in the training process) is 30% of the transactions. Cross validation patterns are a fraction of the client history not used for training rather to check if the network has learned, the error ratio (cross validation error) is shown before training.

The function of the current transaction is therefore to test against the neural network to determine its performance.
A sensitivity bar will be included so that transactions with values heading towards accepted level that should be suspicious will not be successful. The training set is the set of all known samples is broken into two orthogonal (independent) sets:

1. **Training set 1**: A group of samples used to train the neural network
2. **Testing set 2**: A group of samples used to test the performance of the neural network. It is also used to estimate the error rate

Verification;
i. Provides an unbiased test of the quality of the network
ii. Common error is to "test" the neural network using the same samples that were used to train the neural network.

Based on the testing set;

1. The network is optimized based on these samples, and will obviously perform well on them.
2. Verification doesn't give any indication as to how well the network will be able to classify inputs that weren't in the training set

Epoch

This is basically the number of times the neural network should train for a particular transaction.

i. One iteration through the process of providing the network with an input and updating the network's weights.
ii. The amount of epochs needed for the neural network is not fixed. Typically many epochs are required to train the neural network.

Irregularities detected by the system based on the training set provided to it will be made known to the bank official, it then becomes the duty of the bank officials to decide if such transactions should continue or be discontinued.

4. SYSTEM IMPLEMENTATION

This section discusses the implementation of the system developed. It describes the functionality of the various interfaces provided and how the interfaces are used to achieve the aim of the system.

Java programming language was used to implement the system due to its strong data manipulation control structures and great support online.

My SQL server will be the relational database management system (RDBMS) since it is a robust RDBMS that provides multi-user access to a number of databases. It can manage the large amount of data generated in an inventory management system and can be integrated with the development platform used for this project**.**

The system is flexible and easy to use by the user. The interface, menu arrangement, the language used ensures ease of operation without the supervision or training. The system interfaces are explained below.

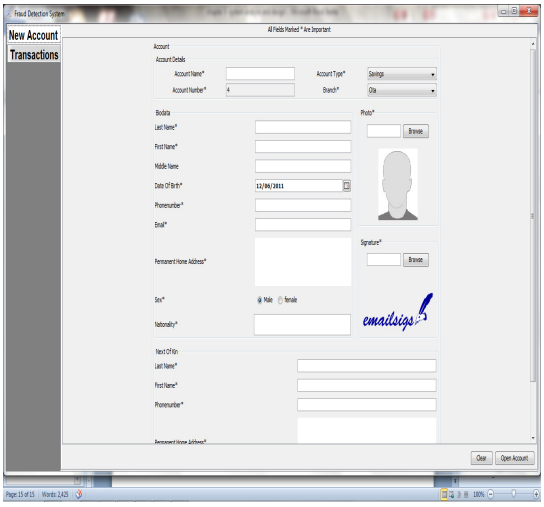


Fig 4.1: Home Page of the System

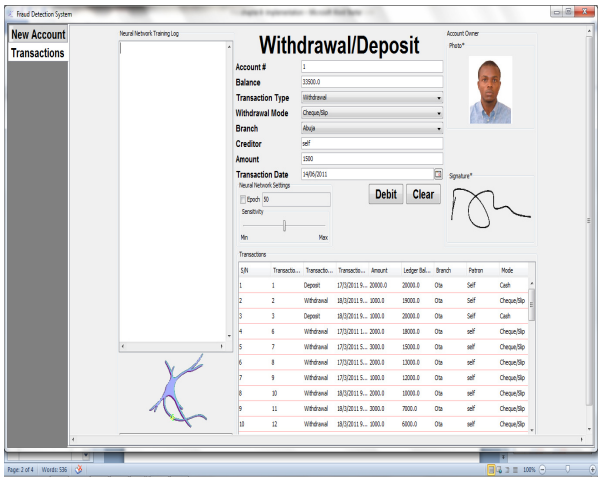


Fig 4.2: The Transactions Page

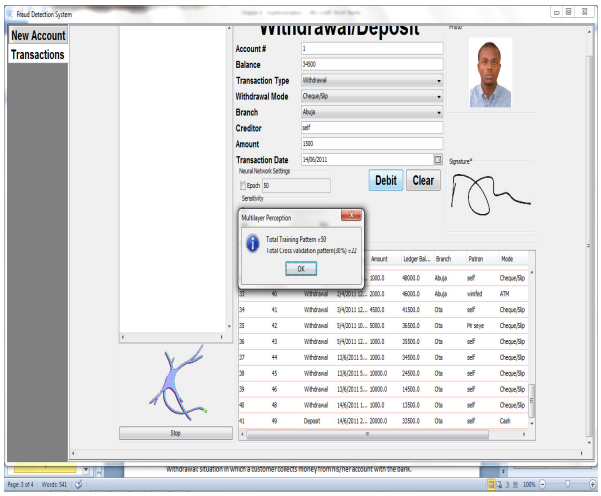


Fig. 4.3: Trainning and Cross Validation Screen

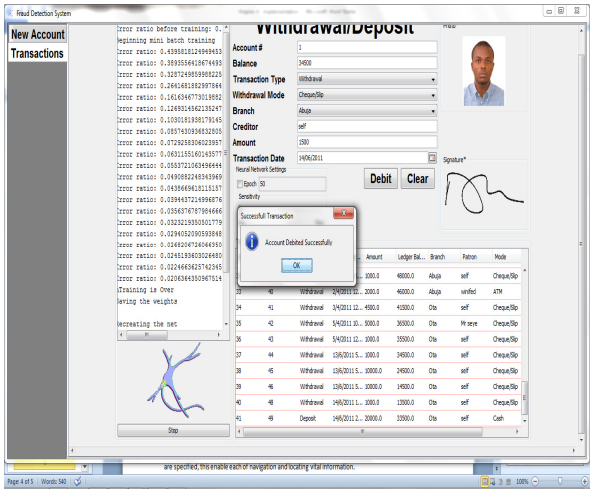
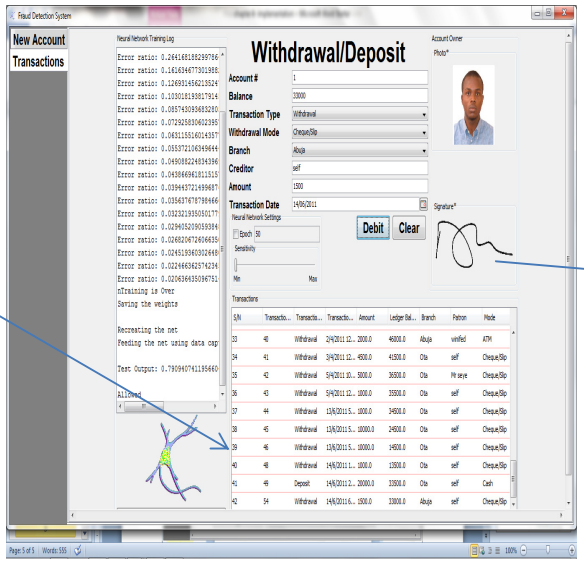


Fig. 4.4: Transaction Screen (Success)



FIig 4.5: Value of a sucessful transaction

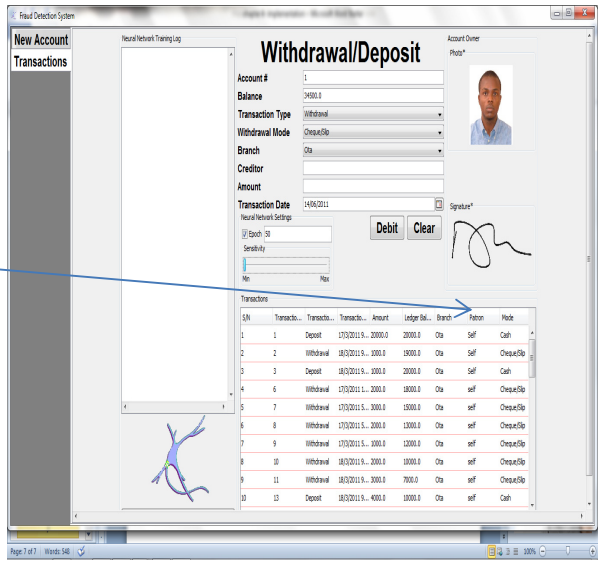


Fig 4.9: Inclusion of epoch value

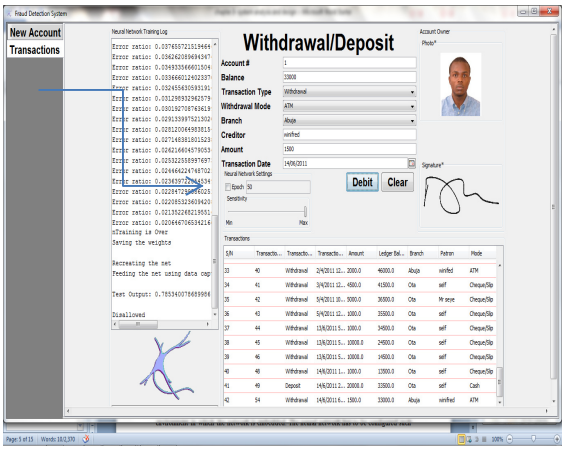


Fig. 4.6: Unsucessful Transaction

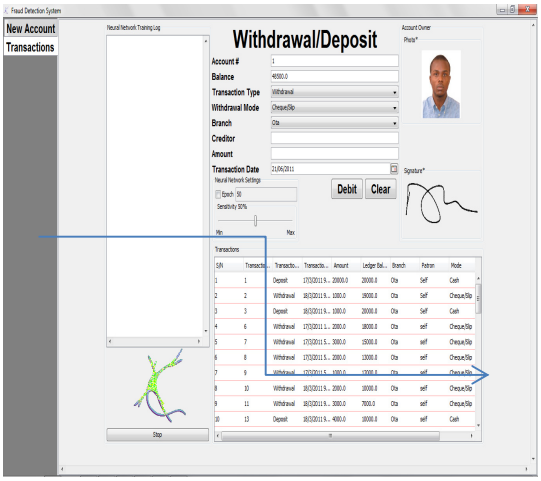


Fig 4.7: Sensitivity bar

5. DISCUSSION OF RESULTS

Figure 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7 and 4.8 shows the result of the tested system. Fig 4.1, The Home Page of the system contains a menu strip which provides navigation to all other interfaces on the system. The menu strip includes New Account and Transactions.
Each menu strip is further explained below

(i) New Account
The New Account menu strip provides navigation to a page containing forms which are filled in the process of creating new bank accounts. This form requires certain bio information about the customer, as well as account types, account number and the branch. The irregularity detection system can only work when there are valuable statements of account that is; the customer most have an account with the bank.

(ii) Transactions
The Transactions menu strip provides navigation to a page containing all the transactions (credit/debit) carried out by the customers with inclusion of the account numbers, transaction dates, amount debited or credited, ledger balance, withdrawal or deposit mode, branch and creditor
Fig 4.3, Show the Percentage for MLP Training and Cross Validation. This is a typical description of the percentage used for the training pattern and that used for the cross validation in the Multi-Layer Perceptron Network during withdrawals.

Out of the 100% training patterns presented to the network, 70% is for the actual network training while 30% is the test pattern used in testing the accuracy of the results generated by the training sets. While figure 4.4, signifies the success of a debit transaction, when the Training and Cross Validation pattern has been specified, the neural network then resumes training based on the information it's been fed and previous experiences to determine the continuity or discontinuity of a transaction.

Fig 4.5 shows the descriptions of a successful transaction. After training, the neural network describes the success or failure of transactions based on numerical values. The screen shows a successful transaction with numerical value heading strong towards +0.8 which is the value specified by the network as successful (very low or complete absence of errors).

Fig. 4.6: show an unsuccessful transaction due to the change in some parameters and inclusion of maximal sensitivity bar. With the inclusion of a maximal sensitivity bar in Fig 4.7 and a change in some parameters, the same amount debited successfully in fig 4.5 will not be successful. Reason been that after training, the network might allow a transaction to go through simply because of its seemingly high level of accuracy (0.7 is very close to +0.8), the sensitivity bar then steps in and notices the change in location, the patron, the withdrawal mode then stops the transaction.

Also Fig 4.9, show the Inclusion of an epoch value which signifies the number of time the ANN should train.
In situations whereby the time required to train the network for a particular transaction is prolonged, number of epoch can be specified. Epoch signifies the number of time a network should train to yield results. The limitation in specifying the number of epoch is that suspicious transactions might be successful because the number of epoch specified might not be enough for the network training process.

6. CONCLUSION

The irregularity Detection system implemented has sought to reduce the amount of irregular transactions that take place in the Nigerian banking industry, thereby aiding in the decrement of bank fraud. The system gives bank personnel the opportunity to notice irregularities in transactions which will normally be successfully carried out oblivious of abnormal patterns. The system is convenient and easy to use and increase the integrity of the bank. In course of implementing this project the current method of detecting irregular transaction (manual method) was reviewed, its flaws shown and ways to improve it by introducing the detection system outlined. Other areas of future research therefore include application of biometrics techniques into the system to handle the authentication problems.

REFERENCES

[1] Idowu, A., "An Assessment of Fraud and its Management in Nigeria Commercial Banks". European Journal of Social Sciences. Vol. 10, No 4.,2009, pp 628-640,

[2] Adeyemi, k,"Banking Sector consolidation in Nigeria: issues and challenges",2005. Retrieved from www.unionbankng.com

[3] Aihua Shen, Rencheng Tong, Yaochen Deng, (2007). "Application of classification Models on Credit Card fraud detection." Service Systems and Service Management, 2007 International Conference on 07/2007; DOI: 10.1109/ICSSSM.2007.4280163

[4] Amit Khajanchi.. "Artificial Neural Networks: The next intelligence",2003,. Available at www.globalriskguard.com/resources/market/NN.pdf

[5] Bruno Carneiro, Rafael Sousa, "Identifying Banks Fraud Using CRISP-DM and Decision Trees." International Journal of Computer Science and Information Technology (IJCSIT) Vol.2, No.5, October 2010.

[6] Fanning. K, Cogger. K. O and Srivastava. R. "Detection of management fraud: A neural network approach" International Journal of Intelligent Systems in Accounting, Finance and Management .1995. 4 113-126.

[7] Fawcett, T. and Provost, F. "Adaptive fraud detection". Data Mining and knowledge Discovery,1997. 1:291-316

[8] Haykin, S , "Neural Networks; A Comprehensive Foundation", 2nd ed. (Englewood Cliffs, NJ: Prentice-Hall). 1999.

[9] Idolor Eseoghene Joseph ."BANK FRAUDS IN NIGERIA"; underlying causes, effects and possible remedies". African Journal of Accounting, Economics, Finance and Banking Research Vol. 6.No. 6. 2010.

[10] Ivor Ogidefa . "Fraud in Banking System in Nigeria", November 19, 2008. Available at http://socyberty.com/law/fraud-in-banking-system-in-nigeria/

[11] Lemo: T ,"Regulatory Oversight and Stakeholder Protection" A paper presented at the BGL Mergers and Acquisition Interactive Seminar, Held at Eko hotels $ Suits. V.I, on June 24.2005.

[12] Micheal, H., Diane L, Jose C.P and Don X. "Detecting fraud in the real World".Available at stat.bell-labs.com/cm/ms/departments/sia/doc/ HMDS.pdf. 2001.pp. 7 – 12

[13] Cheung and Cannon "An Introduction to Neural Networks", Signal and Data Compression Laboratory Group Meeting, University of Manitoba, May 27, 2002.

[14] Rumelhart, D. E., G. E. Hinton, and R. J. Williams: "Learning internal representations by error propagation," in D. E. Rumelhart and J. L. McCleland, eds. (Cambridge, MA: MIT Press), vol. 1, Chapter 8, page 318-62, 1986.

[15] Soludo, C., "Consolidating the Nigerian banking industry to meet the development challenges of the 21st century". Being an address delivered to the Special meeting of bankers committee held on july 6, 2004 at the CBN headquarters Abuja.

[16] Werbos, P.J.,"Beyond Regression: new tools for prediction and analysis in the behavioural sciences, " Ph.D Thesis, Havard University, Cambridge, MA.1974

[17] Stephan Kovach, Wilson Vicente Ruggiero: Online Banking Fraud Detection Based on Local and Global Behavior. 'Fifth international Conference on Digital Society'2011.

[18] J.A Adeyiga, J.O.J Ezike, A. Omotosho & W. Amakulor (2011). A Neural Network Based Model for Detecting Irregularities in e-Banking Transactions. Afr J. of Comp & ICTs. Vol 4, No. 3. Issue 2 pp 14-22

[19] Chioke(2009), Season of Bank logs. Thisday, Vol.14, No 5319. Nov