Australian Journal of Basic and Applied Sciences, 4(8): 3025-3037, 2010
ISSN 1991-8178

A Comparative Analysis of Different Neural Networks Performances in the Prediction of Superimposed Fraud in Mobile Phone Usage

Oluwagbemi O.O.

Covenant University College of Science & Technology, Department of Computer & Information Sciences Ota, Ogun State Nigeria.

Abstract: Neural Networks is an essential information-processing paradigm,that is inspired by a way of biological nervous systems, which can be used in predicting fraud occurrence in mobile phone usage. Superimposed fraud occurrence could occur as a result of overlapping calls and irregularities in the time pattern spent in calling. The power of neural network-based technology is a potent mechanism in combating the menace of superimposed fraud in mobile technology. The methodology employed in this research work included data collection by survey from a telecommunication industry in Africa, data testing and analysis by making use of a Neural Network Software known as NeuroSolutions. Performance comparative analysis was carried out by using six different neural network models. The final deductions from the results of the experiments carried out, showed that the Fuzzy network model outperformed the other five neural networks in terms of the least error difference generated between the predicted output and the final output generated. This showed that Fuzzy network model is more efficient in its performance in comparison with the other five models.

Key words: Neural Networks, superimposed fraud, comparative analysis, mobile phone usage, Fuzzy network model.

INTRODUCTION

The rapid growth of wireless communication and access, together with the success of the internet, has brought a new era of mobile multimedia applications and services.

However, mobile technology has certain problems associated with it. Fraud is prevalent in both fixed and mobile networks of all technologies. Fraud means deception deliberately practiced in order to secure unfair or unlawful gain. Fraud could also mean intentional perversion of the truth in order to induce another to part with something of value or to surrender a legal right. Thus, the problem of the fraudulent use of mobile phones is not an uncommon thing in wireless communication .The most prevalent of them being the Superimposed fraud, where fraudsters can take over a legitimated account without being the rightful owner. The outcome of this process is that the, the account of the legitimate user becomes more debited than the normal amount consumed. The legitimate user becomes inhibited and restricted to the proper, effective and efficient usage of such mobile phones, the ratings in the bill record of the legitimate user becomes irregular and the overall security of all the legitimate subscribers in such communication industry is not guaranteed.

Fraudsters are not only motivated by money, but also by the need for anonymity to mask other crimes or the challenge of beating a security system .Fraudsters are cleverly contrived and determined and frequently find a way to misuse services and compromise security.

As a result, fraud counter-measures are essential and there is need for corporate policy supported by a suitable implementation strategy not only in combating mobile technology crimes, but also in carrying out performance analysis and evaluation of different neural nets in the prediction of fraud occurrence in mobile phone usage

The power of neural network-based technology is a potent mechanism in combating the menace of fraud in mobile technology. Thus, the importance of neural networks cannot be overemphasized in dealing with fraud related issue in mobile technology.

The aims and objectives of this research work is to apply various neural network models in predicting the occurrence of fraud in the real life data of phone usage, applying certain factors in determining any trace of

Corresponding Author: Oluwagbemi, O.O., Covenant University College of Science & Technology, Department of Computer & Information Sciences Ota, Ogun State Nigeria.
E-mail: gbemiseun@yahoo.com

fraud in such usage, and then performing a comparative analysis in terms of comparative performances between the six different neural networks models that will be used for this fraud predicting purpose. The final goal is to obtain a moderate result which will help in determining the most efficient model that will be useful in predicting fraud based on the minimum error difference generated for the prediction purpose.

2.Relevant Materials and Previous Work Done:

2.1 Artificial Neural Network Models for Predicting Patterns in Auditing Monthly Balances:

Artificial neural networks (ANNs) are a computing paradigm that can be used as a basis for building intelligent information systems. The purpose of the work done in this research paper as presented by Eija Koskivaara was to provide additional evidence as to the ability of an ANN model to forecast and recognize patterns when auditing financial accounts.

The study examined the predictive ability of an ANN by building models using monthly balances of a manufacturing firm. The study also used the backpropagation algorithm as learning algorithm. The monthly balances were considered a time-series and the target was to observe the non-linear dynamics and the relationships between accounts. Furthermore, the certain seeded material errors with signals from the ANN model were investigated. The results achieved indicated that neural networks seemed promising for analyzing patterns that resulted in a need for additional investigations of un-audited financial data.The relevance of the work done by Eija Koskivaara to this present research work is the application of neural network for predictive purpose (Eija Koskivaara, 1996).

2.2 Robust and Adaptive Travel Time Prediction with Neural Networks:

In this work carried out by S.P. Hoogendoorn in 2000, an overview of the state -of-the art in travel time prediction using neural networks was presented (Hoogendoorn, S.P. and Ir. J.W.C. van Lintin, 2000).

However, prediction of travel times based on past and current traffic information is not straightforward due to the high complexity and ill -predictability of the traffic process, incorrect or missing observations, and different data sources. Given the properties of the travel time prediction problem, neural networks were used as a tool for travel time prediction, as shown by a number of past studies including this reviewed work.

In this work, two methods for predicting traffic conditions and times were presented. The indirect method dealt with the prediction of traffic conditions, while the direct method dealt with the prediction of travel times. This work presented an overview of applications of ANN (Artificial Neural Networks) for travel time prediction. The applications showed very promising results.

2.3 Neural Network Detection of Management Fraud Using Published Financial Data:

This paper made used of Artificial Neural Networks to develop a model for detecting management fraud. Although similar to the more widely investigated area of bankruptcy prediction, the research had been minimal. To increase the body of knowledge on this subject, an in-depth examination of important publicly available predictors of fraudulent financial statements was carried out. The values of these suggested variables was tested for detection of fraudulent financial statements within a matched pairs sample. A self organizing Artificial Neural Network (ANN) AutoNet was used for this purpose 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. The study also 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 (Fanning, K., K. Cogger, 1998).

2.4 Fraud Detection In Communications Networks Using Neural And Probabilistic: Methods:

In this review, three methods to detect fraud were presented. Firstly, a feed-forward neural network based on supervised learning was used to learn a discriminative function to classify subscribers using summary statistics. Secondly, a Gaussian mixture model was used to model the probability density of subscribers' past behavior so that the probability of current behavior can be calculated to detect any abnormalities from the past behavior.

Lastly, the Bayesian network was used to describe the statistics of a particular user and the statistics of different fraud scenarios. The Bayesian network was now used to infer the probability of fraud given the subscribers' behavior. The data features were derived from toll tickets. The experiments showed that the methods detected over 85 % of the fraudsters in the research carried out by Michiaki Taniguchi and others in 1998.

The main difference between this reviewed work and this research work is the probabilistic methods employed. The reviewed work is related to this research work because it employed the Feed forward Neural Network based on supervised learning to classify the phone subscribers and the Bayesian Neural Network to infer the probability of fraud, hence detecting fraudulent practices in the use of mobile phones

2.5 Distributed Management in the Security Area for Cloned Mobile Phones:

This work presented the development of a distributed application in the security management area for telecommunication networks. The application consists of a system that intends to avoid the use of cloned telephones. The main focus of this work was the classification of the telephone users into seven classes according to their usage logs. Such logs contained three relevant characteristics for every call made by the user. The classification made use of pattern recognition techniques. The users include:

> those that made few local calls, those with many local calls, those with few long distance calls, those with many long-distance calls, those with few short international calls, those with few long international calls, those with many long international calls.

It was possible to identify more easily if a call does not correspond to the patterns of a specific user, and thus identify, whether a fraudulent person made the call.

In order to conduct the classification from the existing data base, an artificial neural network was used, built from a Radial Base Function (Gaussian), known in the literature as RBF with the use of a clustering algorithm (k-means), which proved to be very efficient. Mirela Sechi Moretti Annoni Notare carried out this work in 1998.

The relevance of this revised work to ours is about the use of the Radial Basis Function Neural Network model, as a means of detecting fraudulent practices in the use of mobile phone usage.

The work contributed towards the reduction of losses or damages, for clients as well as for telecommunication carriers, through the implementation of an anti-fraud system, which avoided the cloning of mobile phones. Beyond this, the work also employed a classification algorithm of high reliability. The method used for the classification of users, which included the K-means, P-Nearest Neighbour and Gauss algorithms and the purelin function, proved to be efficient and reliable with the use of the Mat Lab software.

2.6 Detection of Management Fraud: a Neural Network Approach:

In the research work carried out by Fanning *et. al*, (1995) neural network approach was applied to the detection of management fraud. This work is a relevant material to this current research work, as it applies to the detection of fraud using neural network approach.

2.7 A Comparison of Feed Forward Neural Network Architectures for Piano Music Transcription:

The work carried out by Matija Marolt in 1999 showed the application of the feed forward neural networks in recognizing piano chords and polyphonic piano music transcription. (Matija, M., 1999). The work presented results obtained by using several feed forward neural network architectures for transcription, namely multilayer perceptrons, RBF networks, support vector machines and time-delay networks**.**

2.8 Pattern Recognition: Radial Basis Function Network:

The International School on Gas Sensors originally carried out this work in conjunction with the 3rd European School of the Nose Network in 2001. The main work done here, centered on gas and odour concentration prediction, using the radial basis network (Caesarea, T.L., 2001).

In gas and odour analysis, it was necessary to perform not only classification of substances but also quantification of the concentration level of individual components.

This was an important problem in environmental pollution monitoring and in cosmetics, food and industries.

The Radial Basis Function Network was made use of and the results obtained showed that the research work was successful.

2.9 Applications of Neural Networks to Communication Systems:

This particular research work gave an overview of a project involving the application of neural networks to Telecommunication systems. Five application areas were discussed , including cloned software identification and the detection of fraudulent use of cellular phones. The systems were summarized and the general results were presented (Davey, N., 1996).

2.9.1 Mobile Phone Fraud:

Fraud is the deliberate changing of financial statements or other records by either a member of the public or someone who works for the council, done to hide theft or use of equipment, money or services for personal gain.

Fraud can also be defined as "an intentional perversion of truth" or a "false misrepresentation of a matter of fact" which induces another person to "part with some valuable thing belonging to him or to surrender a legal right".

There are various types of mobile phone fraud,which can be classified into two categories namely:

(i) Subscription fraud
(ii) Superimposed fraud
(i) Subscription fraud: In this kind of fraud, fraudsters obtain a phone account without having any intention to pay the bill. In such cases, abnormal usage occurs throughout the active period of the account. Such account is usually used for call selling or intensive self-usage. Also, into this category falls the case of bad debt, where customers who do not necessarily have fraudulent intentions but never pay a single bill.
(ii) Superimposed fraud: Here, fraudsters “take over” a legitimate account. In such a case, the abnormal usage is superimposed upon the normal usage of the legitimate customers. Examples of such include cellular cloning, call card theft, and cellular handset theft. Usage volume (total number, duration or rated value of calls over a certain period) is crucial in establishing a fraud case.

The focus of this scientific research work is to analyze and evaluate the performances of six different neural network models in predicting fraud occurrence in mobile phone usage. The kind of fraud being treated in this research work is that of the superimposed fraud (Olugbenga, O.O., 2004).

2.9.2 Identification of Factors That Can Be Useful in Fraud Detection:

Certain factors could be very useful in determining and predicting the occurrence of fraud patterns in a mobile phone usage data.

These factors are:

1. The call collision detection factor which identified overlapping calls.
2. Irregularity or inconsistency in phone no-location relation
3. The call duration factor, which monitored individual and aggregate calls for specific conditions such as calls which are unusually long.
4. The content factor, which helps to monitor and note the occurrence of fraudulent context of words spoken during phone conversation.

All these factors helped in establishing fraud patterns in phone usage data. Based on these factors, the same data sample was fed into about nine different neural network models in order to analyze the predicting capability of each network model

MATERIALS AND METHODS

Methodology:

The methodology employed in this research work included, data collection by survey from the telecommunication industry ,data entry, data training and data testing, using three different neural network models.

Data Collection (Description of Data and Significance of Choice of Data):

The data used for the purpose of this experiment was obtained by survey from the telecommunication industry. The significance of the choice of this data can bee seen in the important features it contains which helped to facilitate the discovery and detection of fraud occurrence in its usage patterns.

Data Entry and Analysis:

Data Preprocessing (Scaling Techniques):

The data collected by survey was scaled for it to properly fit into the neural network software used for this research work. The major factors discussed in the previous section was applied.

Table 1: Sample data from an African Telecommunication industry (2003)

Time Of Call	Duration of Call (Mins)	Destination Called	Destination No	Rate
0.3493055556	1	China	986532579033	99
0.3611111111	5	South Africa	927117880335	67.5
0.3631944444	5	United Kingdom	9442087408050	99
0.3756944444	1	Sierria Leone	9232222241039	67.5
0.3847222222	2	United Kingdom	9447950364015	99
0.3972222222	1	Italy	9393339145272	99
0.4069444444	10	United Kingdom	9442083100189	99
0.4076388889	5	United Kingdom	9442083100189	99
0.4180555556	2	Benin	9229941278	67.5
10.08	3	Canada	913182471323	67.5
0.4375	4	Australia	91297711764	99
0.4645833333	2	Togo	92289493998	99
0.4673611111	5	United Kingdom	9442073576822	99
0.4770833333	7	Sierra Leone	92322222241350	67.5
0.4826388889	9	Benin	9229335538	67.5
0.4902777778	5	USA	912122819185	99
0.4944444444	1	Canada	912142325592	99
0.4951388889	3	USA	92149046400	99
0.5013888889	1	United Kingdom	9442087650981	99
0.5180555556	1	United Kingdom	9442085338257	99

Table 2: Preprocessed data of Sample data from Table 1

Time Of Call	Duration of Call (Mins)	Destination Called	Destination No	Fraud Occurrence Value (FOV)
0.349305556	1	China	986532579033	115
0.361111111	5	South Africa	927117880335	230
0.363194444	5	United Kingdom	9442087408050	115
0.375694444	1	Sierria Leone	9232222241039	230
0.384722222	2	United Kingdom	9447950364015	100
0.397222222	1	Italy	9393339145272	100
0.406944444	10	United Kingdom	9442083100189	230
0.407638889	5	United Kingdom	9442083100189	220
0.418055556	2	Benin	9229941278	110
10.08	3	Canada	913182471323	120
0.4375	4	Australia	91297711764	130
0.464583333	2	Togo	92289493998	125
0.467361111	5	United Kingdom	9442073576822	220
0.477083333	7	Sierra Leone	92322222241350	225
0.482638889	9	Benin	9229335538	220
0.490277778	5	USA	912122819185	120
0.494444444	1	Canada	912142325592	125
0.495138889	3	USA	92149046400	225
0.501388889	1	United Kingdom	9442087650981	230
0.518055556	1	United Kingdom	9442085338257	228

Regions of fraud occurrence take values btw 200-230 at random
Regions of Non-fraud occurrence take values btw 100-130 at random

Implementation:

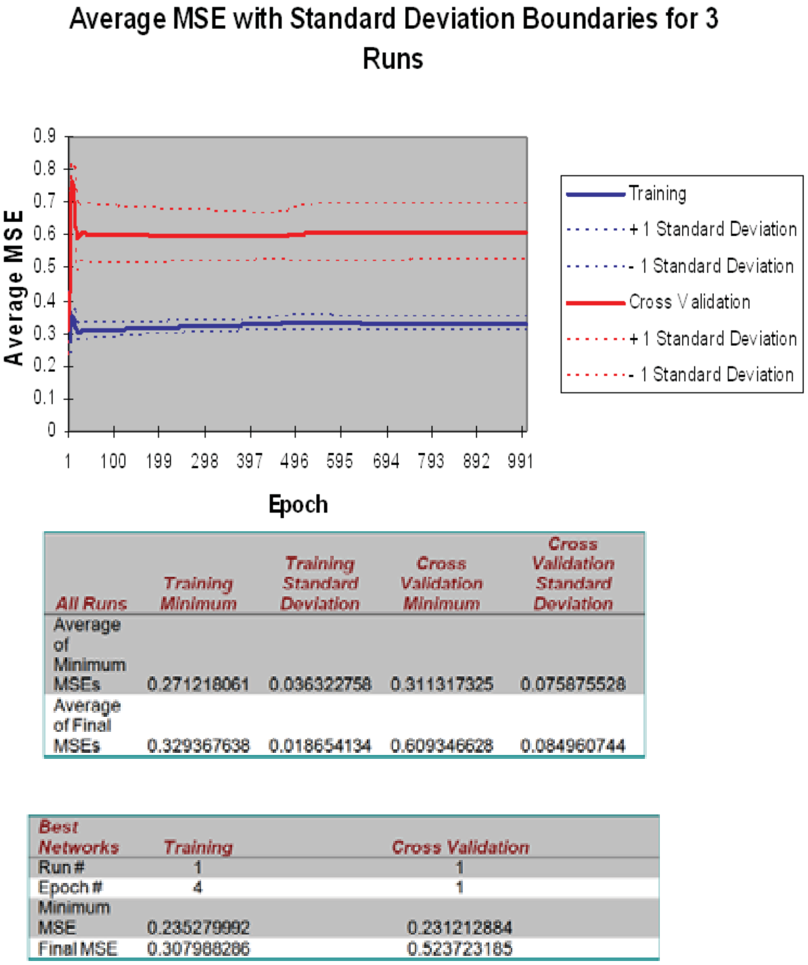
This research work was implemented by using a Neural network software called NeuroSolutions. This software has all the six different neural networks used for the purpose of this analysis. The phone data was keyed into six different neural network models.

These data were fed into six different neural network models for prediction purpose.

RESULTS AND DISCUSSIONS

Report on the experimental results obtained and the display of relevant graphs are shown in the next section.

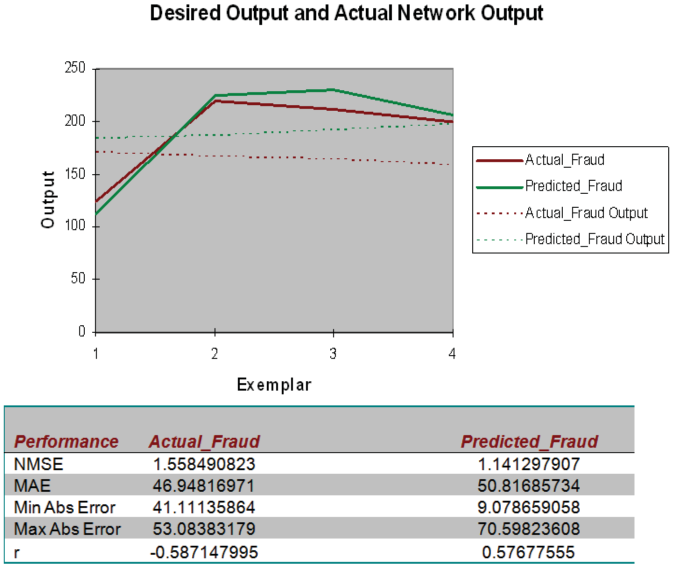
Experimental Results and Performance Analysis of the Six Different Models:



All Runs	*Training Minimum*	*Training Standard Deviation*	*Cross Validation Minimum*	*Cross Validation Standard Deviation*
Average of Minimum MSEs	0.271218061	0.036322758	0.311317325	0.075875528
Average of Final MSEs	0.329367638	0.018654134	0.609346628	0.084960744

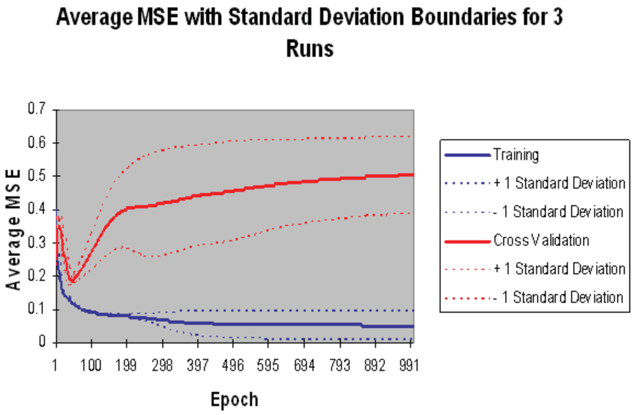
Best Networks	*Training*	*Cross Validation*
Run #	1	1
Epoch #	4	1
Minimum MSE	0.235279992	0.231212884
Final MSE	0.307988286	0.523723185

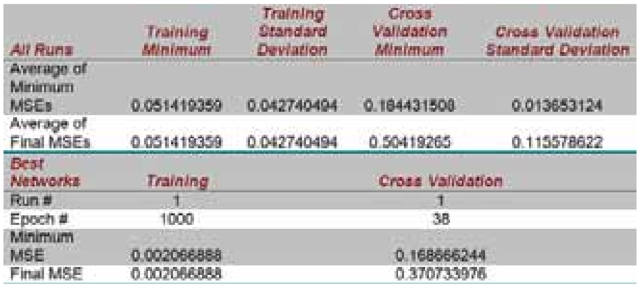
Fig. 1a: Recurrent Model Performance Evaluation & Predictability



Performance	*Actual_Fraud*	*Predicted_Fraud*
NMSE	1.558490823	1.141297907
MAE	46.94816971	50.81685734
Min Abs Error	41.11135864	9.078659058
Max Abs Error	53.08383179	70.59823608
r	-0.587147995	0.57677555

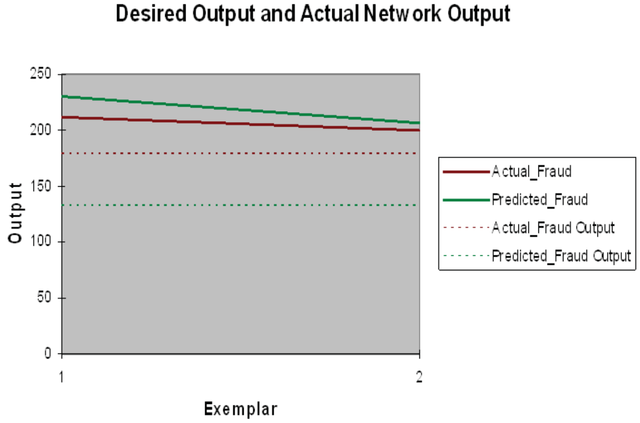
Fig. 1b:

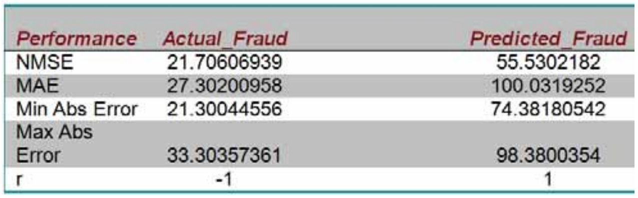




All Runs	Training Minimum	Training Standard Deviation	Cross Validation Minimum	Cross Validation Standard Deviation
Average of Minimum MSEs	0.051419359	0.042740494	0.184431508	0.013653124
Average of Final MSEs	0.051419359	0.042740494	0.50419265	0.115578622
Best Networks	Training		Cross Validation	
Run #	1		1	
Epoch #	1000		38	
Minimum MSE	0.002066888		0.168666244	
Final MSE	0.002066888		0.370733976	

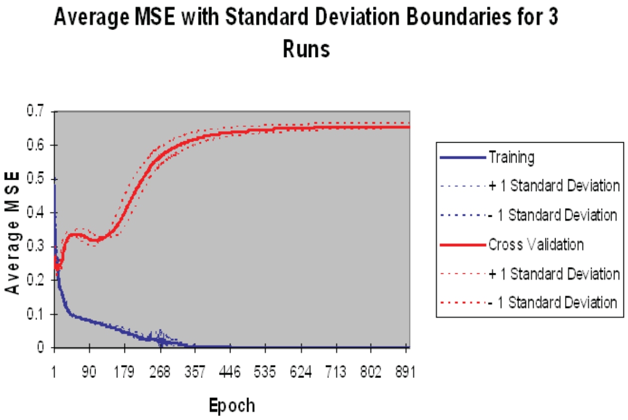
Fig. 2a: Multilayer Perceptron Model Performance Evaluation & Predictability

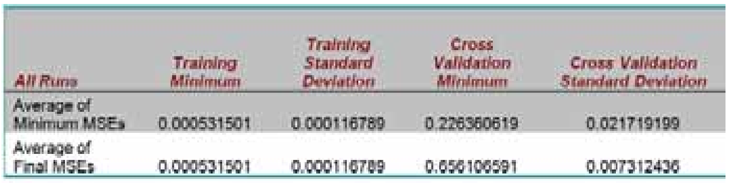




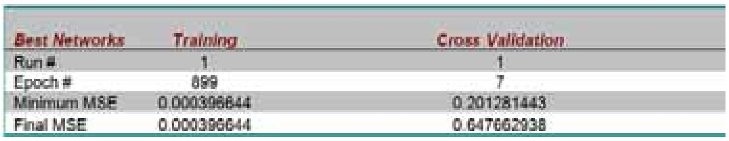
Performance	Actual_Fraud	Predicted_Fraud
NMSE	21.70606939	55.5302182
MAE	27.30200958	100.0319252
Min Abs Error	21.30044556	74.38180542
Max Abs Error	33.30357361	98.3800354
r	-1	1

Fig. 2b:



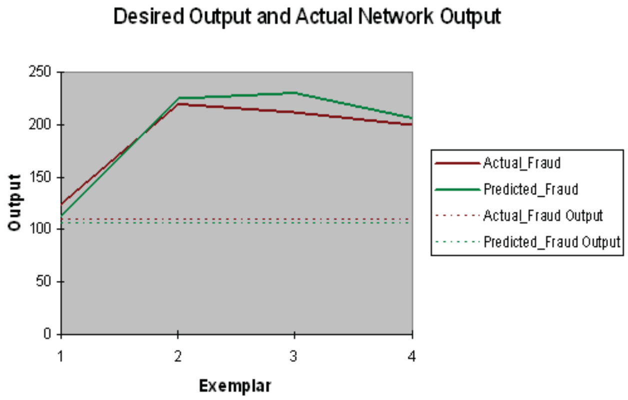


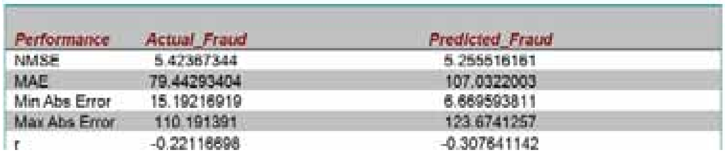
All Runs	Training Minimum	Training Standard Deviation	Cross Validation Minimum	Cross Validation Standard Deviation
Average of Minimum MSEs	0.000531501	0.000116789	0.226360619	0.021719199
Average of Final MSEs	0.000531501	0.000116789	0.656106591	0.007312436



Best Networks	Training	Cross Validation
Run #	1	1
Epoch #	899	7
Minimum MSE	0.000396644	0.201281443
Final MSE	0.000396644	0.647662938

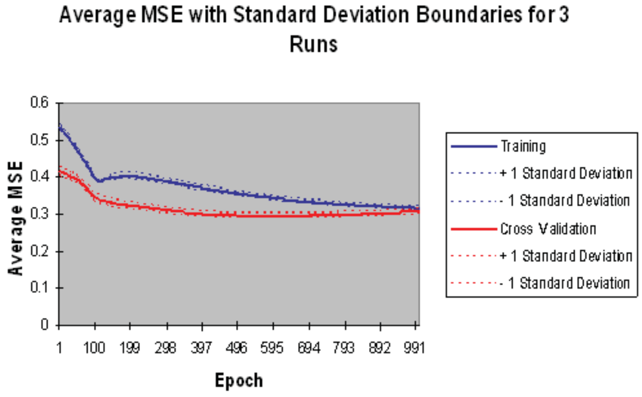
Fig. 3a: Self -Organizing Feature Model Performance Evaluation & Predictability

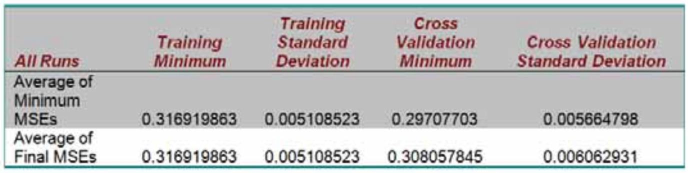




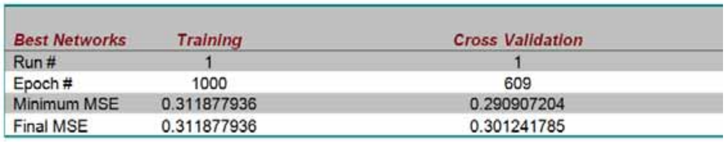
Performance	Actual_Fraud	Predicted_Fraud
NMSE	5.42367344	5.255516161
MAE	79.44293404	107.0322003
Min Abs Error	15.19216919	6.669593811
Max Abs Error	110.191391	123.6741257
r	-0.22116698	-0.307641142

Fig. 3b:



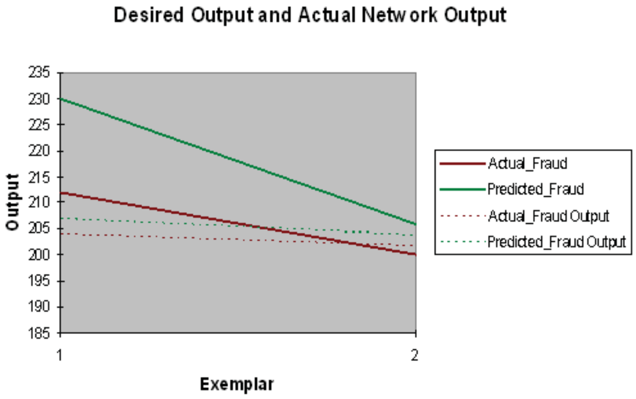


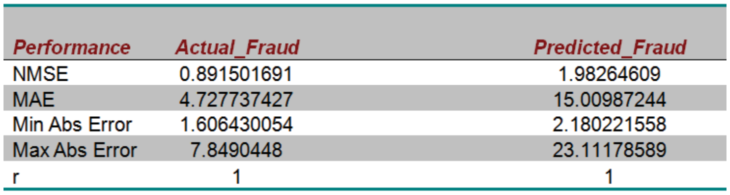
All Runs	Training Minimum	Training Standard Deviation	Cross Validation Minimum	Cross Validation Standard Deviation
Average of Minimum MSEs	0.316919863	0.005108523	0.29707703	0.005664798
Average of Final MSEs	0.316919863	0.005108523	0.308057845	0.006062931



Best Networks	Training	Cross Validation
Run #	1	1
Epoch #	1000	609
Minimum MSE	0.311877936	0.290907204
Final MSE	0.311877936	0.301241785

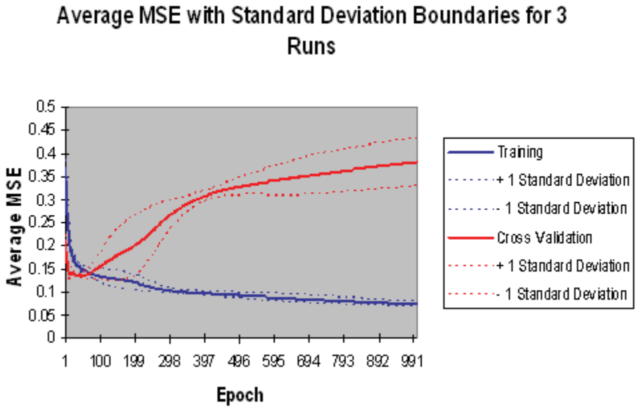
Fig. 4a: Fuzzy Network Model Performance Evaluation & Predictability





Performance	Actual_Fraud	Predicted_Fraud
NMSE	0.891501691	1.98264609
MAE	4.727737427	15.00987244
Min Abs Error	1.606430054	2.180221558
Max Abs Error	7.8490448	23.11178589
r	1	1

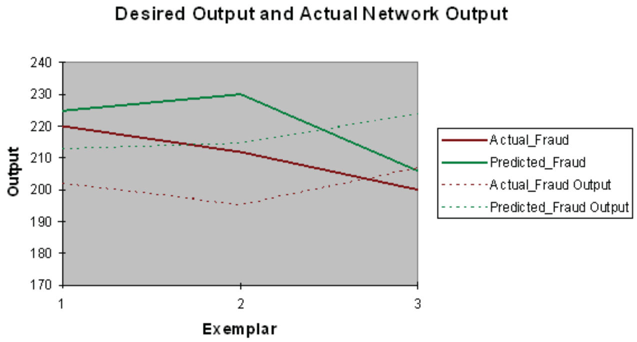
Fig. 4b:



All Runs	Training Minimum	Training Standard Deviation	Cross Validation Minimum	Cross Validation Standard Deviation
Average of Minimum MSEs	0.073837444	0.005849992	0.130082786	0.001430886
Average of Final MSEs	0.073837444	0.005849992	0.381579846	0.051584337

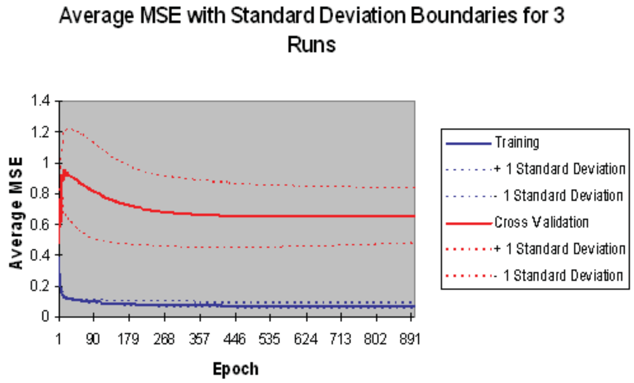
Best Networks	Training	Cross Validation
Run #	3	2
Epoch #	1000	12
Minimum MSE	0.068558045	0.12856859
Final MSE	0.068558045	0.351533055

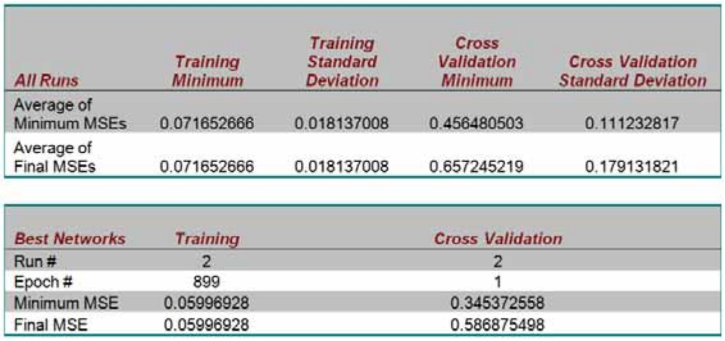
Fig. 5a: FeedForward Network Model Performance Evaluation & Predictability



Performance	Actual_Fraud	Predicted_Fraud
NMSE	3.226233252	2.887962542
MAE	13.87532552	19.82550218
Min Abs Error	6.791488647	12.27384949
Max Abs Error	18.12606812	17.69332886
r	-0.527090207	-0.943488246

Fig. 5b:

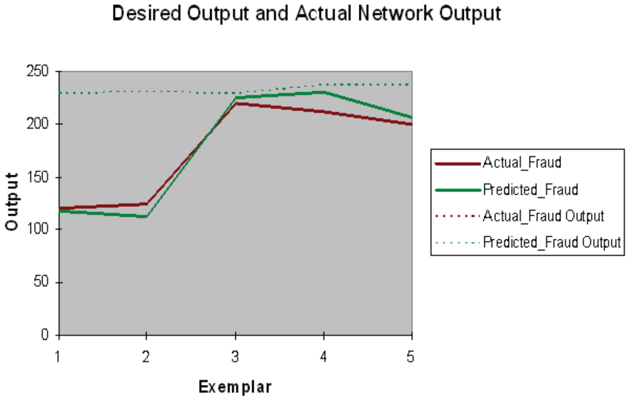


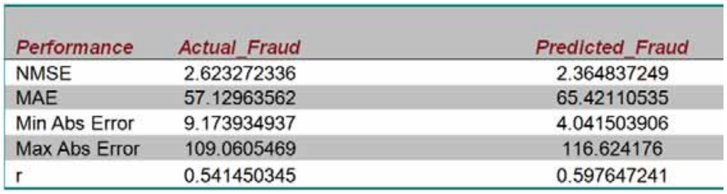


All Runs	*Training Minimum*	*Training Standard Deviation*	*Cross Validation Minimum*	*Cross Validation Standard Deviation*
Average of Minimum MSEs	0.071652666	0.018137008	0.456480503	0.111232817
Average of Final MSEs	0.071652666	0.018137008	0.657245219	0.179131821

Best Networks	*Training*	*Cross Validation*
Run #	2	2
Epoch #	899	1
Minimum MSE	0.05996928	0.345372558
Final MSE	0.05996928	0.586875498

Fig. 6a: Radial Basis Function Model Performance Evaluation & Predictability





Performance	*Actual_Fraud*	*Predicted_Fraud*
NMSE	2.623272336	2.364837249
MAE	57.12963562	65.42110535
Min Abs Error	9.173934937	4.041503906
Max Abs Error	109.0605469	116.624176
r	0.541450345	0.597647241

Fig. 6b:

5. Discussions of Experimental Results:

From the analysis and model predictability experiment carried out in this scientific research work, for these six neural networks, it was discovered that for the Recurrent model, the following experimental result was also obtained:

Performance	Actual_Fraud	Predicted_Fraud
NMSE	1.558490823	1.141297907
MAE	46.94816971	50.81685734
Min Abs Error	41.11135864	9.078659058
Max Abs Error	53.08383179	70.59823608
R	-0.587148	0.57677555

For the Multilayer Perceptron Model, the following experimental result was obtained:

Performance	Actual_Fraud	Predicted_Fraud
NMSE	21.70606939	55.5302182
MAE	27.30200958	100.0319252
Min Abs Error	21.30044556	74.38180542
Max Abs Error	33.30357361	98.3800354
R	-1	1

Finally, for the Self-Organizing Feature Model, the following result was also obtained:

Performance	Actual_Fraud	Predicted_Fraud
NMSE	5.42367344	5.255516161
MAE	79.44293404	107.0322003
Min Abs Error	15.19216919	6.669593811
Max Abs Error	110.191391	123.6741257
R	-0.22116698	-0.307641142

For the Fuzzy network model , the following was generated:

Performance	Actual_Fraud	Predicted_Fraud
NMSE	0.891501691	1.98264609
MAE	4.727737427	15.00987244
Min Abs Error	1.606430054	2.180221558
Max Abs Error	7.8490448	23.11178589
r	1	1

Thus, its performance in terms of the error generated in this fraud prediction experiment showed that its NMSE (Normalized mean squared error) for the fraud predicted was 1.98264609.

The mean absolute error (MAE = 15.00987244) for its fraud prediction was also the least; this showed that the fuzzy model fraud predictability was much better than the other five models.

Furthermore, the experiment showed that the Fuzzy neural network model had the least Minimum absolute error and the least Maximum absolute error in its fraud predicting performance.

All these experimental analysis showed that the fuzzy model was more effective and efficient in its fraud prediction capability than the other five models (Feed forward model, Radial Basis model, Multilayer Perceptron, Recurrent Model, Self-Organizing Map Feature,). Thus, the fuzzy network model outperformed these other models in terms of the least errors generated in their fraud predicting capability. Hence, the fuzzy network is more faster than the others from this experimental results.

For Radial Basis Function, we have the following experimental values generated:

June 16, 2010Performance	Actual_Fraud	Predicted_Fraud
NMSE	2.623272336	2.364837249
MAE	57.12963562	65.42110535
Min Abs Error	9.173934937	4.041503906
Max Abs Error	109.0605469	116.624176
R	0.541450345	0.597647241

For the Feedforward model, the following experimental result was produced:

Performance	Actual_Fraud	Predicted_Fraud
NMSE	3.226233252	2.887962542
MAE	13.87532552	19.82550218
Min Abs Error	6.791488647	12.27384949
Max Abs Error	18.12606812	17.69332886
R	-0.52709021	-0.943488246

6. Conclusion:

In conclusion, based on the comprehensive comparative analysis of the six neural networks used in this performance analysis experiment, it was finally concluded that the Fuzzy Neural network had the least errors generated and the least error difference generated between the actual fraud and the predicted fraud for the experimental results in the prediction of fraud in mobile phone usage. This implies that the Fuzzy neural network is more efficient than the other five neural networks, based on the minimal error generated in its prediction. Moreover, the more the errors generated, the less efficient the model, while the less the error generated, the more efficient the model. Since, more errors consumes more time and less errors consumes less time. Thus, it can be finally concluded based on this research work, that the Fuzzy neural network is more efficient than the other five neural network in predicting superimposed fraud in mobile phone usage.

REFERENCES

Eija Koskivaara, 1996. Artificial Neural Network Models for Predicting Patterns in Auditing Monthly Balances, Turku Centre for Computer Science TUCS Technical Report No 67, November 1996,ISBN 951-650-893-6, ISSN 1239-1891.

Hoogendoorn, S.P. and Ir. J.W.C. van Lintin, 2000. Robust and Adaptive Travel Time Prediction with Neural Networks, TRAIL Research School, Delft University of Technology.

Fanning, K., K. Cogger, 1998. "Neural network detection of management fraud using published financial data", International Journal of Intelligent Systems in Accounting, Finance & Management, 7(1): 21-41.

Michiaki, T., H. Michael, H. Jaakko and T. Volker, 1998. Fraud detection in communication networks using neural and probabilistic methods. In Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'98) 2 1241-1244. IEEE Computer Society Press, Silver Spring, MD.

Mirela Sechi Moretti A.N., *et al*., 1998. Distributed Management in the Security Area For Cloned Mobile Phones, Federal University of Santa Catarina, Brazil.

Fanning, K.M., K.O. Cogger and R. Srivastava, Detection of management fraud: A neural network approach. International Journal of Intelligent Systems in Accounting, Finance and Management, 4(2): 113-126.

Matija, M., 1999. A comparison of feed forward neural network architectures for piano music transcription, Faculty of Computer and Information Science University of Ljubljana, Slovenia.

Caesarea, T.L., 2001. Pattern Recognition-Radial Basis Function Networks, International School On Gas Sensors in conjunction with the 3rd European School of the Nose Network.

Davey, N., S.D.H. Field, R. Frank, P. Barson and G. McAsley, 1996. The Detection of Fraud in Mobile Phone Networks, Neural Network World, 6(4): 477-484.

Olugbenga, O.O., 2004. Using Neural Network To Predict Fraud in Mobile Phone Usage, M.Sc Thesis (2004), University of Ibadan, Department of Computer Science, Oyo State, Nigeria, West Africa.