SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM
TMLAI TRANSACTIONS ON MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE
VOLUME 3, ISSUE 6
ISSN 2054-7390

Telecommunications Subscription Fraud Detection using Artificial Neural Networks

[1]Ledisi G. Kabari, [2]Domaka N. Nanwin and [3]Edikan Uduak Nquoh
[1]School of Applied Sciences, Ken Saro-Wiwa Polytechnic, Bori, Nigeria;
[2,3]Faculty of Natural and Applied Sciences, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Nigeria;
ledisigiokkabari@yahoo.com; kakusman@yahoo.com; nquedt@gmail.com

ABSTRACT

Telecommunications Companies are facing a lot of problems due to fraud; hence the need for an effective fraud detection system for the telecommunications companies. This paper presents a design and implements of a subscription fraud detection system using Artificial Neural Networks. Neurosolutions for Excel was used to implement the Artificial Neural Network. The system was tested and found to be user friendly, effective and 85.7% success rate achieved.

Keywords: Telecommunications; Subscription; Artificial Neural Networks; Neurosolutions; Fraud; detection; Subscription Fraud.

1 Introduction

Telecommunications is fast turning the world into a global village. Globally, the development of telecommunications industry is rapidly increasing with one innovation replacing another in a matter of years, months, and even weeks. Without doubt telecommunication is a key driver of any nation's economy. Telecommunication is the communication of information by electronic means usually over some distance [1]. It involves the transmission and receipt of information, messages, graphics, images, voice, video and data between or among telephones, internet, satellites and radio.

The telecommunications sector is a wide sector with millions of users. This sector is broadly categorized into two categories based on its users; Domestic users and Commercial users.

The domestic users are provided with connections at an affordable rate while the commercial users are provided with connections at a comparatively higher rate as their usage scale is higher. But it has been discovered that there are cases where the subscription at the commercial level is fraudulently brought under the domestic level hence causing a significant loss to the sector. This kind of subscriptions if brought under the right category would have yielded a greater income to the sector. Fraud is defined as the deliberate and premeditated act perpetrated to achieve gain on false ground [2]. Fraud is also seen as any transmission of voice data across a telecommunications network, where the intent of the sender is to avoid or reduce legitimate call charges [3]. Telecommunication fraud is the theft of services or deliberate abuse of voice or data networks [4]. Telecommunications fraud can be broken down into several generic

DOI: 10.14738/tmlai.36.1695
Publication Date: 14th December, 2015
URL: http://dx.doi.org/10.14738/tmlai.36.1695

classes which describe the mode operators are defrauded but this paper focuses on **"SUBSCRIPTION FRAUD"**.

Subscription fraud is a contractual fraud. In these kinds of fraud revenue is generated through the normal use of a service without having to pay. In this scenario, the fraudster operates at level of phone numbers where all transactions from this number is fraudulent and all activities in such cases are further abnormal throughout the active period of the account. Subscription fraud can be divided into two categories:-

- Subscription fraud for the purpose of personal usage by the fraudster.
- Subscription fraud for profit. In this category the fraudster opens a small outfit where he starts up a call center. The fraudster has no intensions of paying his bills but he sells the airtime to people who intend to make cheap long distance calls for cash.

Fraud detection problems are found in many sectors of lives endeavor and the telecoms sector is not an exception. Hence fraud detection is referred to as the attempt engaged in discovering illegitimate usage of a communication network by identifying fraud as quickly as possible once it has been perpetrated [5].

A Neural Network consists of hardware or software that attempts to emulate the processing patterns of the biological brain [1]. It is a type of artificial intelligence system modeled after the neurons (nerve cells) in the biological nervous system and intended to simulate the way a brain processes information, learns and remembers. A neural network is designed as an interconnected system of processing elements, each with a limited number of inputs and outputs. These processing elements are able to "learn" by receiving weighted inputs that with adjustment, time and repetition can be made to produce appropriate outputs. Neural Networks are used in areas such as fraud detection, pattern recognition, speech analysis and speech synthesis.

The radical changes in the terrain of the telecommunications sector have made it difficult to control and detect fraudulent activities. Thus, to achieve positive results the problem of fraud requires to be handled with rapt and effective attention. Artificial Neural Networks has been found to be very useful in fraud detection, hence our usage.

The aim of this paper is to present a design and implement of a subscription fraud detection system via artificial neural networks. To achieve it aim the paper is set out to:-

I. Identify the different subscription services provided by the telecommunications sector.
II. Identify the different ways telecommunications fraud is perpetrated.
III. Utilize the artificial neural network model to detect subscription fraud in the telecommunications sector.

In terms of significance, the paper will benefit the private telecoms sector because they will be able to detect subscription fraud and hence reduce the losses incurred. The paper brought to limelight a novel means of combating telecommunications subscription fraud with the utilization of the intelligent agent like artificial neural networks. The paper will also benefit other researchers who intend to go into this area as this is the birthing of innovative ways of solving the problem of subscription fraud in the telecoms sector.

2 Telecommunication Services and Frauds

2.1 Telecommunications Mobile Subscription Services

Telecommunication companies in Nigeria provide different services to win the heart of their subscribers because of the market competition. However, some of these mobile subscription services are common to all the mobile operators in Nigeria, these includes: Prepaid Services and Postpaid Services.

2.1.1 Prepaid Services

This is the most popular of the services provided by mobile operators. As the name implies 'Pre-paid', all transaction in this service is pay-as-you-go. This service is easy for the mobile operator to maintain in the event of fraud and it is less susceptible to fraud as compared to postpaid services.

2.1.2 Postpaid Services

This is the most conventional service offered by mobile operators all over the world. As the name implies 'Post-paid', credit facilities is given for services used for some period of time, usually between 1- 6 months. Though, this service is not common in Nigeria because there is no proper means of identification in case a subscriber defaults, yet, all mobile operators in Nigeria still render the service as a result of the stiff competition in the industry.

Other services provided by Nigeria's mobile telecommunication companies that are susceptible to fraud includes: Roaming Services, Value Added Features and Service (VAS), Premium Rate Services (PRS).

2.2 Telecommunication Fraud

Telecommunication industry has expanded dramatically in the last few years with the development of affordable mobile phone technology [6]. With the increasing number of mobile phone subscribers, global mobile phone fraud is also set to rise. It is a worldwide problem with substantial annual revenue losses of many companies. Telecommunication fraud which is the focus is appealing particularly to fraudsters as calling from the mobile terminal is not bound to a physical location and it is easy to get a subscription. This provides a means for illegal high profit business for fraudsters requiring minimal investment and relatively low risk of getting caught. Telecommunication fraud is defined as the unauthorized use, tampering or manipulation of a mobile phone or service.

Telecommunication fraud can be simply described as any activity by which telecommunications service is obtained without intention of paying. This kind of fraud has certain characteristics that make it particularly attractive to fraudsters. The main one is that the danger of localization is small. This is because all actions are performed from a distance which in conjunction with the mesh topology and the size of network makes the process of localization time consuming and expensive. Additionally no particularly sophisticated equipment is needed if one is needed at all. The simple knowledge of an access code, which can be acquired even with methods of social engineering, makes the implementation of fraud feasible. Finally, in the product of telecommunication fraud, a phone call is directly convertible to money.

2.3 Types of Telecommunication Fraud

The telecom industry suffers major losses due to fraud [7]and [8]. There are many different types of telecommunications fraud and these can occur at various levels. The two most common types of fraud are subscription fraud and superimposed fraud.

2.3.1 Subscription Fraud

In subscription fraud, fraudsters obtain an account without intention to pay the bill. Thus at the level of a phone number, all transactions from this number will be fraudulent. In such cases abnormal usage occurs throughout the active period of the account. The account is usually used for call selling or intensive self-usage.

2.3.2 Superimposed Fraud

In Superimposed fraud, fraudsters take over a legitimate account. In such cases the abnormal usage is superimposed upon the normal usage of the legitimate customers. There are several ways to carry out superimposed fraud, including mobile phone cloning and obtaining calling card authorization details. Examples of such cases include cellular cloning, calling card theft and cellular handset theft. Superimposed fraud will generally occur at the level of individual calls; the fraudulent calls will be mixed with the justified ones.

2.3.3 Intrusion fraud

This occurs when an existing, otherwise legitimate account, typically a business, is compromised in some way by an intruder, who subsequently makes or sells calls on this account. In contrast to subscription calls, the legitimate calls may be interspersed with fraudulent calls, calling for an anomaly detection algorithm.

2.3.4 Fraud based on loopholes in technology

Consider voice mail systems as an example. Voice mail can be configured in such a way that calls can be made out of the voice mail system (e.g., to return a call after listening to a message), as a convenience for the user. However, if inadequate passwords are used to secure the mailboxes, it creates vulnerability. The fraudster looks for a way into a corporate voice mail system, compromises a mailbox (perhaps by guessing a weak password), and then uses the system to make outgoing calls. Legally, the owner of the voice mail system is liable for the fraudulent calls; after all, it is the owner that sets the security policy for the voice mail system.

2.3.5 Social engineering

Instead of exploiting technological loopholes, social engineering exploits human interaction with the system. In this case the fraudster pretends to be someone he or she is not, such as the account holder, or a phone repair person, to access a customer's account. Recently, this technique has been used by "pre-texters" in some high-profile cases of accessing phone records to spy on fellow board members and reporters [9].

2.3.6 Fraud based on new technology

New technology, such as Voice over Internet Protocol (VoIP), enables international telephony at very low cost and allows users to carry their US-based phone number to other countries. Fraudsters realized that they could purchase the service at a low price and then resell it illegally at a higher price to consumers who were unaware of the new service, unable to get it themselves, or technologically unsophisticated. Detecting this requires monitoring and correlating telephony usage, IP traffic and ordering systems.

2.3.7 Fraud based on new regulation

Occasionally, regulations intended to promote fairness end up spawning new types of fraud. In 1996, the Federal Communications Commission (FCC) modified payphone compensation rules, requiring payphone operators to be compensated by the telecommunication providers. This allowed these operators to help cover the cost of providing access to phone lines, such as toll-free numbers, which do not generate revenue for the payphone operator. This spawned a new type of fraud—payphone owners or their associates placing spurious calls from payphones to toll-free numbers simply to bring in compensation income from the carriers.

2.3.8 Masquerading as another user

Credit card numbers can be stolen by various means (e.g., "shoulder surfing" looking over someone's shoulder at a bank of payphones) and used to place calls masquerading as the cardholder. There are many more fraud techniques, some of which are quite sophisticated and combine more than one known method.

Telecommunications fraud is not static; new techniques evolve as the telecom companies put up defenses against existing ones. The fraudsters are smart opponents, continually looking for exploitable weaknesses in the telecom infrastructure. Part of their motivation is accounted for by the fact that once an exploit is defined, there are thousands (or millions) of potential targets. New types of fraud appear regularly, and these schemes evolve and adapt to attempts to stop them.

2.4 Telecommunication Fraud Detection

Fraud is a multi-billions problem around the globe. The problem with telecommunication fraud is the huge loss of revenue and it can affect the credibility and performance of telecommunication companies. The most difficult problem that faces the industry is the fact that fraud is dynamic. This means that whenever fraudster's feel that they will be detected they find other ways to circumvent security measures. Telecommunication fraud also involves the theft of services and deliberate abuse of voice and data networks. In such cases the perpetrator's intention is to completely avoid or at least reduce the charges for using the services. Over the years, fraud has increased to the extent that losses to telephone companies are measured in terms of billions of American dollars. Fraud negatively impacts on the telephone company in 4 ways such as financially, marketing, customer relations and shareholder perceptions.

There are various **techniques** available for managing and detecting telephone fraud these include:

2.4.1 Manual review of data

The problem with this technique is the fact that there are too many data records for a team to filter the fraudulent data. Typically a telecom company will have in order of 1 million or more records of telephone calls generated by their customers for a single month within a specific region. As a result this is a time consuming and laborious technique for detecting fraud.

2.4.2 Conventional analysis

This is the fixed rule based expert system together with statistical analysis. A rule based system is a set of rules that take into account the normal calling hours, the called destinations as well as the normal duration of the call.

2.4.3 Adaptive flexible techniques

This is using advanced data analysis like artificial neural networks (ANNs). Fed with raw data, a neural network can quickly learn to pick up patterns of unusual variations that may suggest instances of fraud on a particular account [10].

2.5 Approaches to Face Fraud

Dealing with the fraud is a very complex task mainly due to its transversal nature to the operator's structure [11]. Traditional fraud techniques are evolving and adapting to the new network infrastructure. The fraud techniques are considered because basic ideas remain despite the underlying technology. Deceptions in telecommunications include subscription frauds where the cheater accesses the services without being subscribed. User can also suffer line or identity theft being charged for services used by others. Telecommunication operators can oversee users that exceed their download quote and rate performing illegal service redistribution, sometimes for an economic profit. Finally cloning or unauthorized access to services may lead to compromising privacy.

Anyway the most common types of fraud on telecommunications are subscription fraud and identity theft. After that voice mail fraud and calling card fraud prevail. The analysis of different fraud techniques points out that the tendency is a convergence of the fraud which increases the complexity of its detection.

Fraud management systems have proved to be a suitable tool to detect fraud in different networks with diverse techniques such as self-organizing maps (SOM), general data mining, rule based systems profiling through Artificial intelligence techniques like neural networks or decision trees based on the hierarchical regime switching models, Bayesian networks, fuzzy rules or other data mining techniques. There also exist works on how to discover new rules to detect fraud in telecommunications and on the privacy concerns of applying detection techniques to user's data.

Fraud detection can also be done at 2 levels call or behavior and with two different approaches user profile or signature based [12]. Most of the techniques use the CDR data to create a user profile and to detect anomalies based on these profiles. The mined large amounts of CDR have in order to find patterns and scenarios of normal usage and typical fraud situations. These scenarios were then used to configure monitors that observe the user behavior with relation to that type of fraud. These monitors are then combined in a neural network which raises an alarm when sufficient support of fraud exists. This type of system can be classified in a rule based approach since it relies in the triggering of certain rules due to abnormal usage. The rule based system has the drawback of requiring expensive management of rules. Rules need to be precise (avoid false positive alarms) and constantly evolving (detect new scenarios) which result in very time consuming programming.

The most common and best succeeded methods for fraud analysis are signature based. These methods detect the fraud based on deviation detection by comparing the recent activity with the user behavior data which is expressed through the user signature. The work can be adapted and extended by reformulating the notion of signature and by introducing the notion of statistical based distances to detect anomalies. Furthermore the Computational cost can be reduced by using simple statistical functions avoiding processing costly histograms. A clear problem with a histogram approach is that discretization intervals or bucket must be clean and what is right for one customer may be wrong for another. Other

approaches have also been widely applied to fraud analysis like neural networks. Another applied technique is link analysis. Here the client links are updates over time establishing a graph of called communities of interest that can easily reveal networks of fraudster's. These methods are based on the observation that fraudsters seldom change their calling habits but are often linked to other fraudsters.

3 Methodology

The proposed system is a system based on the artificial neural network technology. This system is supposed to handle the challenges encountered by the rule based system of detecting fraud. Artificial Neural Networks is a more efficient mechanism when it comes to telecommunications fraud detection because it can accommodate large amounts of data, analyze it and possibly prompt the network of the fraud to be perpetrated.

The inputs are the data of a subscriber such as the name, age, sex, registration duration, subscription bundle and amount of data used. The data is processed so as to ascertain if the subscriber is fraudulent or non-fraudulent. It outputs the state of a particular subscriber. That is "fraudulent" or "non-fraudulent".

3.1 Design of the Proposed System

We took five basic steps during the design process: Collecting data, preprocessing data, Building the network, Train, and Test performance of the model.

Collecting and preparing sample data is the first step in designing ANN models. The data is gotten from historical data of fraudulent and non-fraudulent subscriptions.

After data collection, three data preprocessing procedures are conducted to train the ANNs more efficiently. These procedures are: (1) solve the problem of missing data, (2) normalize data and (3) randomize data. The missing data are replaced by the average of neighboring values during the same week. Normalization procedure before presenting the input data to the network is generally a good practice, since mixing variables with large magnitudes and small magnitudes will confuse the learning algorithm on the importance of each variable and may force it to finally reject the variable with the smaller magnitude.

We then decided on the number of hidden layers, neurons in each layer, transfer function in each layer, training function, weight/bias learning function, and performance function. In this work, multilayer perceptron (MLP) and radial basis function (RBF) networks are used.

During the training process, the weights are adjusted in order to make the actual outputs (predicated) close to the target (measured) outputs of the network**.**

3.2 Knowledge Base

We used Microsoft excel to design our database because it is simple to access and use. It contains the data in the form of fields, records and attributes. It contains all that is needed to train the network so that it can be able to detect the fraud intuitively. It is seen as the store of all the domain and fraud specific knowledge that is required by the system.

3.3 Knowledge Base of Rules

Knowledge base of rules was constructed. This could also be referred as the inference engine. They are the rules that will be used to train the network so that when a record is to be tested to ascertain if it is

fraudulent or not it can do that effectively. This is where the actual fraud detection methods and techniques are stored. This is done in the form of "if-then-else" rules that reason over the knowledge contained in the knowledge base. The rules for detection and the knowledge base are interrelated as the representation of the rules depends on the contents of the knowledge base.

3.4 Store of Nature of Fraud

This is a store of all the types of fraudulent outputs gotten. This store will be fed into the self-learning system.

3.5 Self-Learning System

This provides the overall system with the capabilities to learn new rules about fraud from the submission of fraudulent and non-fraudulent domain specific data and to automatically detect irregular observations in the data thus providing a feedback mechanism for enriching and updating the knowledge base of rules.

3.6 Architecture of the Proposed System

The architectural design of the proposed system is as shown in figure 1.

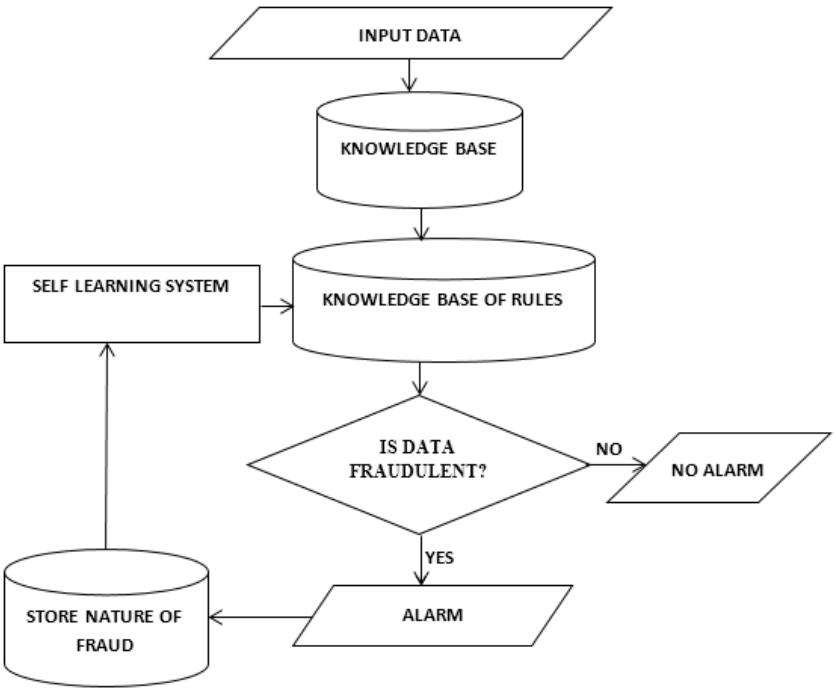


Figure 1: Architectural Design of the System

4 Experiments and Analysis

To implement the proposed system, an Artificial Neural Network (ANN) software called NeuroSolutions was used which is considered one of the leading software available for implementing neural networks. Neural networks are long, complicated mathematical equations and NeuroSolutions is designed to make the technology easy and accessible to both novice and advanced neural network developers. There are three basic phases in neural network analysis: training the network on your data, testing the network for

accuracy and making predictions/classifications from new data. Only the Express Builder in the NeuroSolutions Excel interface can accomplish all of this automatically in one simple step. With the NeuroSolutions for Excel interface, it has never been easier to get started quickly in solving your problem. It provides an easy-to-use and intuitive interface for users to easily setup a simulation that automatically builds, trains and tests multiple neural network topologies and generates an easy-to-read report of the results including the best-performing model.

Neurosolutions is a numerical computing environment and also a programming language. It allows easy matrix manipulation, plotting of functions and data, implementation of algorithms, creating user interfaces and interfacing with programs in other languages. The Neural Network Toolbox contains the Neurosolutions tools for designing, implementing, visualizing and simulating neural networks. It also provides comprehensive support for many proven network paradigms, as well as graphical user interfaces (GUIs) that enable the user to design and manage neural networks in a very simple way. NeuroSolutions provides an easy-to-use and intuitive user interface for Microsoft Excel. It simplifies and enhances the process of getting data into and out of a NeuroSolutions neural network. It also benefits both novice and advanced neural network developers by offering an easy-to-use, yet extremely powerful features (Neurosolutions, 2014).

The collected dataset is divided into three data subsets: first data subset (60% of the whole dataset) was used as inputs for the ANN training phase, and second data subset (15% of the dataset) was used as inputs for the ANN cross validation. The last data subset (25% of the dataset) was used as inputs for the ANN Testing. The system uses the training dataset to predict cases that are fraudulent or not. If there is a big gap (deviation) between the output *parameters* actual values and the predicted values, there is a high probability of fraud in the fraud report, otherwise there is none.

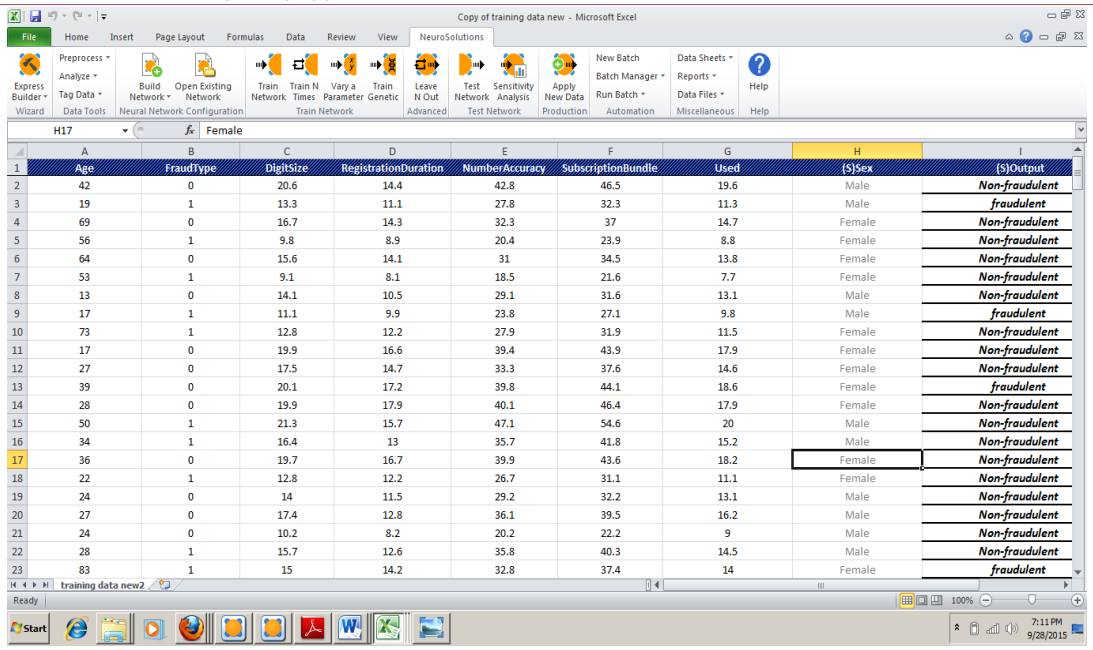
4.1 System Requirement

All computer software needs certain hardware components or other software resources to be present on a computer. These prerequisites are known as system requirements and are often used as a guideline.

For an effective operation, the system can be implemented provided the following hardware and software components are at least met. Processor: Pentium 4, Intel Core Duo or higher, RAM: 3 GB, HDD: 650 MB and above, Keyboard: Enhanced keyboard, Mouse: Enhanced serial or parallel mouse, CRT: 15” colored monitor, Printer: Optimal (Colored/black and white), Operating System: Windows XP, VISTA, 7, 8.1 either 32-bits or 64-bits, Microsoft Excel: 97, 2000, 2002, 2003, 2005, 2007, 2010 and 2013, Neurosolutions 7.0.

4.2 Launching of the Network and Results

We choose the default setup for "Classification PNN (< 10,000 Rows)" since our data has less than 1,000 total samples. A sample for training data is shown in figure 2. Specifying Training, Cross Validation and Testing Data Segments is shown in figure 3. Building the network and result after building are shown in figure 4 and figure 5 respectively. After training and Network testing are shown in figure 6 and figure 7 respectively. The output is as shown in figure 8.



	A	B	C	D	E	F	G	H	I
1	Age	FraudType	DigitSize	RegistrationDuration	NumberAccuracy	SubscriptionBundle	Used	(S)Sex	(S)Output
2	42	0	20.6	14.4	42.8	46.5	19.6	Male	Non-fraudulent
3	19	1	13.3	11.1	27.8	32.3	11.3	Male	fraudulent
4	69	0	16.7	14.3	32.3	37	14.7	Female	Non-fraudulent
5	56	1	9.8	8.9	20.4	23.9	8.8	Female	Non-fraudulent
6	64	0	15.6	14.1	31	34.5	13.8	Female	Non-fraudulent
7	53	1	9.1	8.1	18.5	21.6	7.7	Female	Non-fraudulent
8	13	0	14.1	10.5	29.1	31.6	13.1	Male	Non-fraudulent
9	17	1	11.1	9.9	23.8	27.1	9.8	Male	fraudulent
10	73	1	12.8	12.2	27.9	31.9	11.5	Female	Non-fraudulent
11	17	0	19.9	16.6	39.4	43.9	17.9	Female	Non-fraudulent
12	27	0	17.5	14.7	33.3	37.6	14.6	Female	Non-fraudulent
13	39	0	20.1	17.2	39.8	44.1	18.6	Female	fraudulent
14	28	0	19.9	17.9	40.1	46.4	17.9	Female	Non-fraudulent
15	50	1	21.3	15.7	47.1	54.6	20	Male	Non-fraudulent
16	34	1	16.4	13	35.7	41.8	15.2	Male	Non-fraudulent
17	36	0	19.7	16.7	39.9	43.6	18.2	Female	Non-fraudulent
18	22	1	12.8	12.2	26.7	31.1	11.1	Female	Non-fraudulent
19	24	0	14	11.5	29.2	32.2	13.1	Male	Non-fraudulent
20	27	0	17.4	12.8	36.1	39.5	16.2	Male	Non-fraudulent
21	24	0	10.2	8.2	20.2	22.2	9	Male	Non-fraudulent
22	28	1	15.7	12.6	35.8	40.3	14.5	Male	Non-fraudulent
23	83	1	15	14.2	32.8	37.4	14	Female	fraudulent

Figure 2: Sample of training data from excel

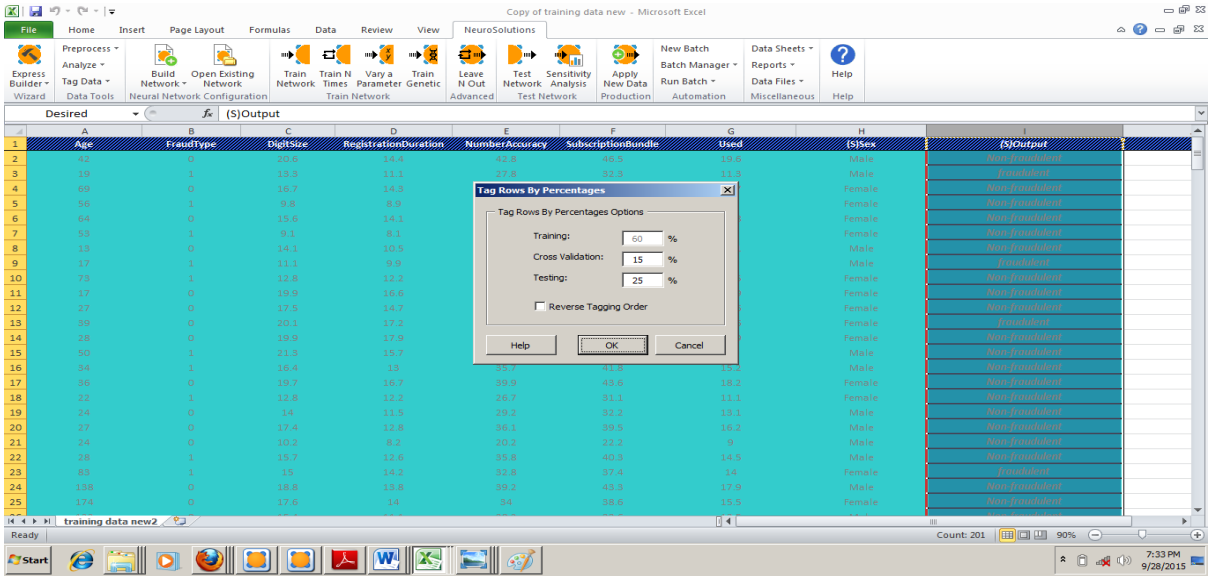


Figure 3: Specifying Training, Cross Validation and Testing Data Segments

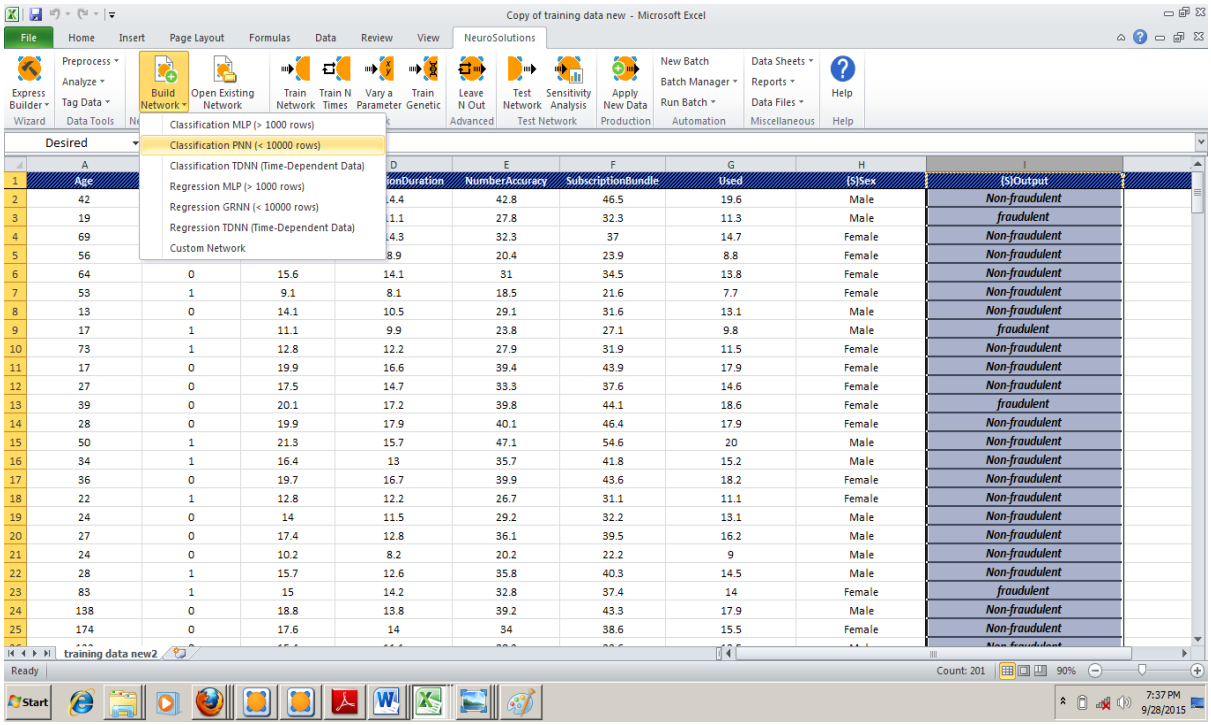


Figure 4: Building the Network

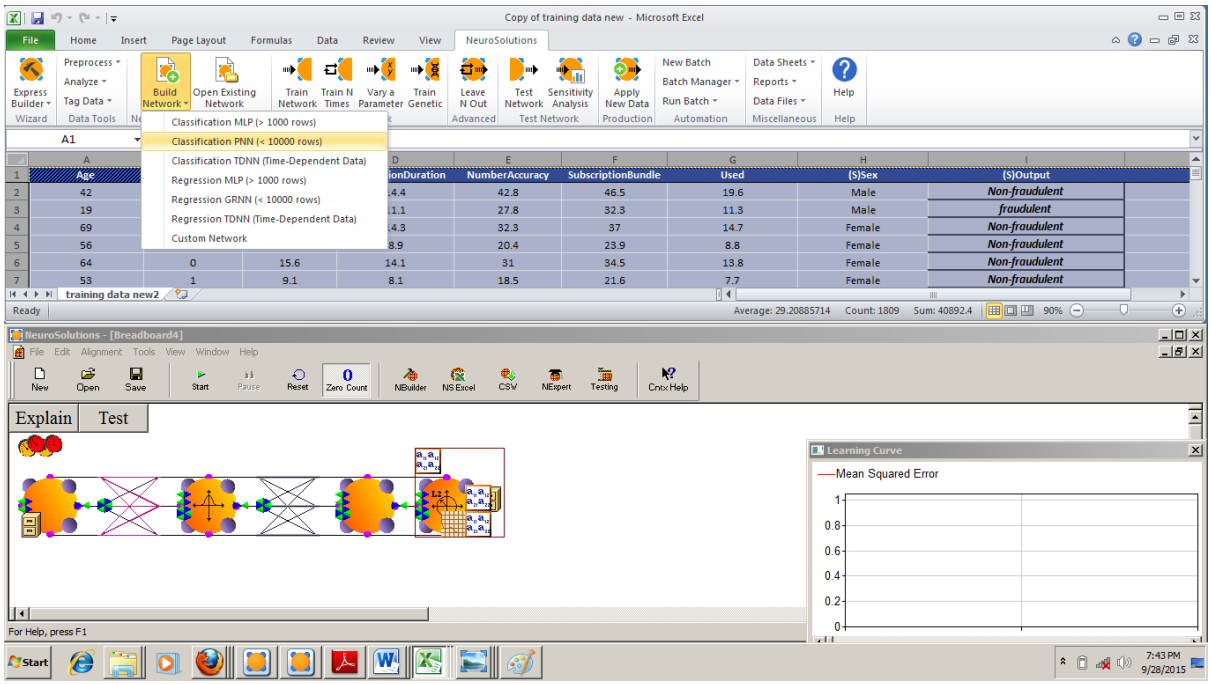


Figure 5: Result after Building Network

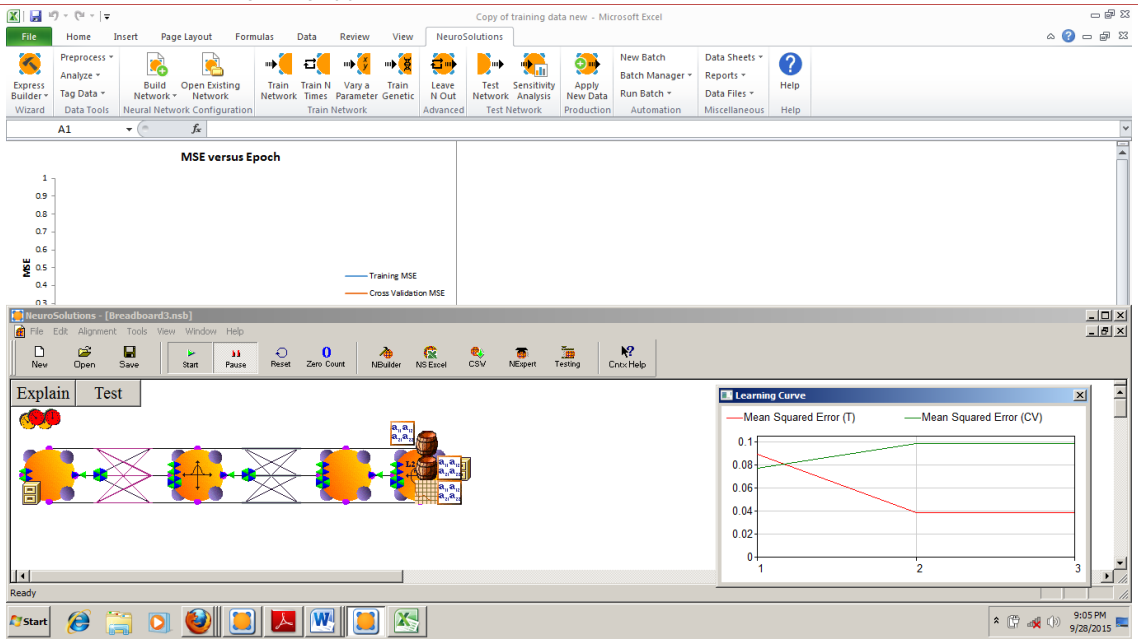


Figure 6: After Training

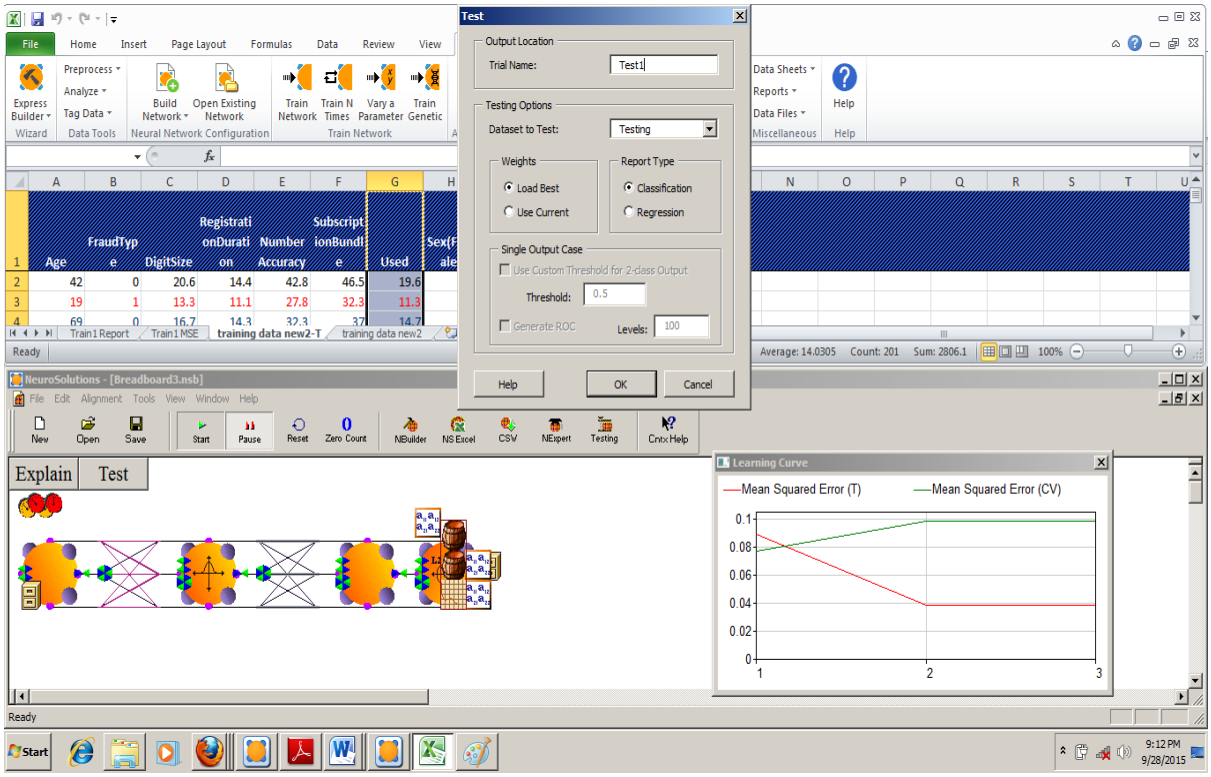
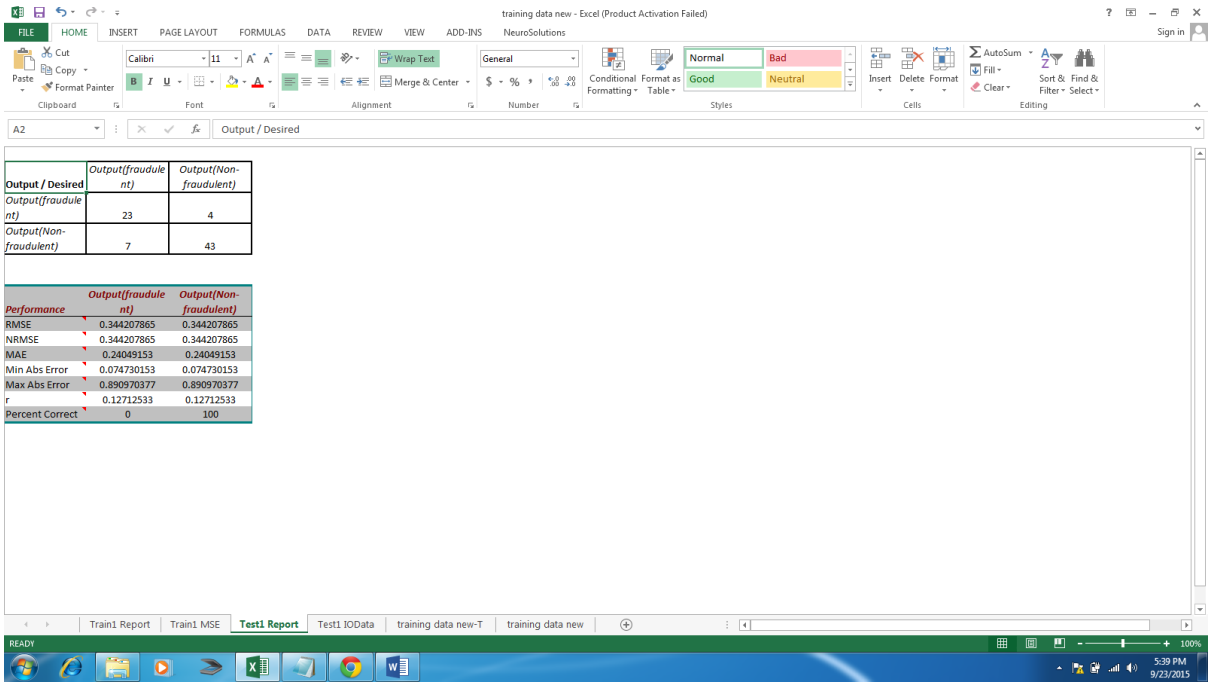


Figure 7: Neural Network Testing



Output / Desired	Output(fraudulent)	Output(Non-fraudulent)
Output(fraudulent)	23	4
Output(Non-fraudulent)	7	43

Performance	Output(fraudulent)	Output(Non-fraudulent)
RMSE	0.344207865	0.344207865
NRMSE	0.344207865	0.344207865
MAE	0.24049153	0.24049153
Min Abs Error	0.074730153	0.074730153
Max Abs Error	0.890970377	0.890970377
r	0.12712533	0.12712533
Percent Correct	0	100

Figure 8: Desired Output Report

The end result is an easy to understand report displaying a confusion matrix of the results as well as some general statistics about the performance of the model on the output of the sample data. The confusion matrix is read from the top left and goes diagonally to the right displaying the correct predictions. So for this particular training run we classified 23 Fraudulent and 43 Non-Fraudulent correctly with 7 Fraudulent and 4 Non-Fraudulent misclassified. Total number of sample data detected is 77, number classified correctly is 66 and 11 was misclassified. Hence, the percentage of success is $66/77 * 100 = 85.7\%$, and the failure rate is $11/77 * 100 = 14.3\%$. This makes a total of 100%.

5 Conclusion

Fraud detection problems are found in many sectors of lives endeavor and the telecoms sector is not an exception. Hence fraud detection is referred to as the attempt engaged in discovering illegitimate usage of a communication network by identifying fraud as quickly as possible once it has been perpetrated.

The radical changes in the terrain of the telecommunications sector have made it difficult to control and detect fraudulent activities. Thus, to achieve positive results the problem of fraud requires to be handled with rapt and effective attention. Artificial Neural Networks has been found to be very useful in fraud detection, hence its usage.

The work thus identified different subscription services provided by the telecommunications sector, identify the different ways telecommunications fraud is perpetrated and utilized the artificial neural network model to design and implement a subscription fraud detection system for the telecommunications sector.

A lot of telecommunications companies are not ready to give reports as it concerns their existing fraud detection system as they deem it confidential, hence analysis of their system was not possible. Thus, we

generate the possible data and simulate the process of fraud detection since we were unable to access real data sets.

REFERENCES

[1]. Laudon K. C., Laudon, J. P. Brabston, M. E, *Management Information System*: Managing the Digital Firm: Pearson Education Canada Inc; Toronto, Ontario, 2002.

[2]. Alexopoulos, P. and Kafentzis, K., *Towards a Generic Fraud Ontology in E Government,* ICE-B*,* 2007*.* p. 269-276.

[3]. Hollmen, J., *User Profiling and Classification for Fraud Detection in Mobile Communication Networks*, PhD thesis, Helsinki University of Technology, Department of Cognitive and Computer Science and Engineering. Espoo, Finland. 2000.

[4]. Hiyam, A. E. Tawashi, *Detecting Fraud in Cellular Telephone Networks Jawwal Case Study*. MBA thesis Islamic University, Faculty of Commerce, Department of Business Administration, Gaza. 2010.

[5]. Bolton, R. J. and Hand, D. J., *Statistical Fraud Detection, A review*, Institute of Mathematical Statistics*,* 2002. 17(3), p. 235–255.

[6]. Pieprzyk, J., Ghodosi, H. and Dawson, E., *Information Security and Privacy, 12th Australasian Conference*, ACISP 2007, Townsville, Australia, July 2-4, 2007: Proceedings, Springer, Germany, p. 446-447.

[7]. Prasad, S. K., Routray, S. and Khurana, R., *Information Systems, Technology and Management*. *Third International Conference, ICISTM 2009, Ghaziabad, India, March 12-13, 2009*, Proceedings, Springer, Germany, p. 259-260

[8]. Żytkow, J. M. and Rauch, J., *Principles of Data Mining and Knowledge Discovery*: *Third European Conference, PKDD'99, Prague, Czech Republic, September 15-18, 1999: Proceedings*, Springer, USA, p. 251.

[9]. Kaplan, D. A., *Intrigue in High Places*, *To Catch a Leaker*, Hewlett– Packard's Chairwoman Spied on the Home–Phone Records of Its Board of Directors, *Newsweek* (September), 2006.

[10]. Liatsis, P., *Recent Trends in Multimedia Information Processing*, Proceedings of the 9th International Workshop on Systems, Signals and Image Processing, *World Scientific Publishing*, London, 2002. P. 474-475.

[11]. Samarati, P., *Information Security Theory and Practices*: *Security and Privacy of Pervasive Systems and Smart Devices*: *4th IFIP WG 11.2 International Workshop, WISTP 2010*, Passau, Germany, April 12-14, 2010, Proceedings, Springer, USA, p. 201.

[12]. Perner, P., *Advances in Data Mining, Applications in Medicine, Web Mining, Marketing, Image and Signal Mining*: *6th Industrial Conference on Data Mining, ICDM 2006, Leipzig, Germany, July 14-15, 2006:* Proceedings, Springer, Germany, p. 535.

[13]. Neurosolutions for Excel. *http://www.neurosolutions.com/documentation/NeuroSolutionsforExcel.pdf* Retrieved, September 28, 2015.