The International Journal of Engineering and Science (IJES)
|| Volume || 7 || Issue || 12 Ver.II || Pages || PP 23-30|| 2018 ||
ISSN (e): 2319 – 1813 ISSN (p): 23-19 – 1805

Soft Computing Approach to Anomaly Detection in Subscribers Call Profiles

*[1]Ismaila W. Oladimeji , [2]Ismaila Folasade. M, [1]Falohun Adeleye S. [2]Oladoye S. Femi
[1]Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[2]Department of Computer Science, Osun State Polytechnic, Iree

---***ABSTRACT:*** ---

Telecommunication frauds have been a problem affecting all operators and customers, and is an important factor in their annual revenue losses. Aside from financial impact, it also constrains new service employment and may contribute to adverse costumer perception. detection and prevention of these frauds were focused by academic and proprietary researchers to make the telecommunication industry viable and customer friendly. This paper employed Counter Propagation Neural Network (CPNN) classifier to detect anomaly in subscribers' call records in telecommunication industry. Eighty users dataset were gotten from a renowned telecommunication industry. The dataset were re-processed to adapt to the neural network processing terrain, and then classified the data into normal and abnormal in an offline processing.

The results of performance metrics of the two neural networks showed that (i) for international calls, CPNN produced averages of fraud catching rate and false alarm rate of 0.46 and 0.91 while BPNN 0.54 and 0.84 respectively, (ii) for national calls, CP produced averages of fraud catching rate and false alarm rate of 0.76 and 0.998 while BP produced 0.64 and 0.998 (for both daytime and night) respectively. CPNN produced 69% precision rate better that BPNN which produced precision of 64%. Also, CPNN produced accuracy of 94.2% better than BPNN accuracy of 81.7%.

Keywords: *Soft Computing, CPNN, False-Positive, True-Positive, Telecommunication fraud, BPNN*

Date of Submission: 28-12-2018 Date of acceptance: 12-01-2019

I. INTRODUCTION

Communications have been an evolving activity right from time past and still in existence till date. In the Stone Age human used different mechanisms in communicating with each other and these have been through various ways which they found out from trial and error. Intelligent bodies stood up during the 19th Century to uphold and make better the communication system of the world by hosting brilliant technology of passing information. During this time, land telephone lines were approximately flooding the western world and this side of the world had the golden opportunity of communicating through this handy technique of passing information. [1].Telecommunication 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 or months. Without doubt telecommunication is a key driver of any nation's economy. The Nigerian economy is not left out in the race for rapid developments induce by innovations in telecommunications. The Nigeria Communication Commission has issued licenses to several private telecommunication operators viz- MTN Nigeria, Airtel, and MTEL, GLOBACOM, and 9-mobile. [2]

Fraud can be defined as "the crime of obtaining money by deceiving people", or a "criminal deception; the use of false representations to gain an unjust advantage." Nowadays, due to the development of new technologies, traditional fraudulent activities, such as money laundering, have been joined by new kinds of fraud like telecommunications fraud and computer intrusion. According to [3] the telecommunication fraud correspond to the abusive usage of an operator infrastructure, this means, a third party is using the resources of a carrier (telecommunications company) without the intention of paying them, of simply or "***the misuse of airtime by fraudsters who have no intention of paying any bill but rather shift the payment burden on the original subscriber.***". 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.[4]

The various types of telecommunication frauds can be classified into two categories: subscription fraud and superimposed fraud.

(i)Subscription Fraud occurs from obtaining a subscription to a service, often with false identity details, with no intention of paying. Or is a type of telecommunication fraud where the fraudsters obtain a mobile account with the intention to never pay any bill. The variants of Subscription Fraud includes**:*Cramming*** is the addition of charges to a subscriber's telephone bill for services which were neither ordered nor desired by the client, or for fees for calls or services that were not properly disclosed to the consumer. ***False answer supervision*** is a mis-configuration of telecommunication equipment, by negligence or design, which causes billing to start as soon as the distant telephone begins ringing, even if a call is busy or no answer; ***Freephone Fraud*** occurs when a person uses a calling card service to dial onwards; ***Roaming Fraud*** is when a fraudster makes use of the delays in the transfer of Toll Tickets through roaming on a foreign network.
(ii) Superimposed Fraud - In this type of telecommunication fraud, the fraudster takes charge of legitimate mobile account(s), and all the illegal use of the account(s) is superimposed on the legitimate customers. Examples of such cases include: ***Handset Theft*** is when many subscribers using their phone only intermittently or for emergencies, a stolen phone may go unnoticed whilst heavy fraudulent usage occurs; ***Call forwarding scam*** occurs where a fraudster tricks a subscriber into call forwarding their number to either a long-distance number or a number at which the fraudster or an accomplice is accepting collect calls; ***Cloning*** has been used as a means of copying both the electronic serial number and the telephone number of another subscriber's phone to a second (cloned) phone. Airtime charges for outbound calls are then mis-billed to the victim's cellular phone account instead of the perpetrator's; ***Caller ID spoofing*** can be used to fraudulently impersonate a trusted vendor (such as a bank or credit union), a law enforcement agency or another subscriber. [6][4][7][8][9]

Soft computing (sometimes referred to as computational intelligence, CI, though CI does not have an agreed definition) is the use of inexact solutions to computationally hard tasks such as the solution of NP-complete problems, for which there is no known algorithm that can compute an exact solution in polynomial time. Soft computing differs from conventional (hard) computing in that, unlike hard computing, it is tolerant of imprecision, uncertainty, partial truth, and approximation. In effect, the role model for soft computing is the human mind. The principal constituents of Soft Computing (SC) are include: Machine learning, including: Neural networks (NN) and its variants; Support Vector Machines (SVM); Fuzzy logic (FL); Evolutionary computation (EC), including: Genetic algorithms, Differential evolution; Metaheuristic and Swarm Intelligence including Ant colony optimization and Particle swarm optimization.[5]
However, neural network technology has been applied to many studies involving sequence data analysis. Back-propagation neural networks currently represent the most popular learning paradigm, and have been used to predict protein secondary and tertiary structures, to distinguish encoding regions from non-coding sequences, to predict bacterial promoter sequences, and to classify molecular sequences. Counter-propagation neural networks, CPNN, also a supervised learning algorithm, is closely related to the nearest-neighbour classifier. The network essentially functions as a nearest-match lookup table. CPNN network has an interesting capability to extract the statistical properties of the input data, and can usually be trained very rapidly.
This paper proceeds as follows: In the next section the various related researches done on telecommunication frauds are presented while section three explains the neural networks variants employed in this work. Section four entails the methodology employed in developing the system. The implementation of the developed system cum analysis of the results were discussed in the fifth Section. In the last section the conclusion is presented.

II. RELATED WORKS

In the last decade modern intelligent systems have been applied to fraud detection. The authors in [10] developed a model that detects fraud in telecommunication sector in which a random rough subspace based neural network ensemble method was employed in the development of the model to detect subscription fraud in mobile telecoms. The authors in [11] present 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. The researchers in [12] in their paper, a method for telecommunications fraud detection is proposed. The method is based on the user profiling utilizing the Latent Dirichlet Allocation (LDA). Fraudulent behavior is detected with use of a threshold-type classification algorithm, allocating the telecommunication accounts into one of two classes: fraudulent account and non-fraudulent account.

The problem of subscriber churning in mobile telecommunications, i.e. the movement of subscriber from one provider to another, has been investigated using Neural Networks. The researchers in [13] employed techniques from statistical machine learning to evaluate the benefits of predicting churn while [14] built a model that churning from subscriber contractual information and call patterns changes extracted CDRs. Additionally, [15] researchers explained that as GSM mobile phones acquire their personality from a smart card known as the Subscriber Identity Module (SIM). All the access rights (including identification for billing) are based on the SIM, rather than the mobile phone itself. GSM cloning refers to a process in which an attacker obtains sufficient information to clone the SIM of a GSM mobile phone. The authors of [16] used fuzzy rules in implementing classification rules which was applied to a database of about a thousand subscribers of a telecommunication company in Chile, 2.2% of subscription fraud prevalence was found. Barson et al. [19] use feed-forward neural networks based on supervised learning to detect mobile phone fraud in their simulated database of call records. They simulate six types of users ranging from low use local users to high use international business users. They report their neural network classifier to correctly classify 92.5% of the calling data. Their work does not include any comment on the false alarm probability and also is not comparable with our work as it is based on simulated data. Moreau et al. [20] report fraud detection in a real mobile communication networks. Their approach is based on feed-forward neural networks with supervised learning. They use different user-profiles and also consider comparisons between past and present behavior. They conclude that although their work is in a prototype phase, they have demonstrated a great potential with their approach.

III. THEORY OF NEURAL NETWORKS

Artificial neural networks were initially developed according to the elementary principle of the operation of the (human) neural system. Since then, a very large variety of networks have been constructed. All are composed of units (neurons), and connections between them, which together determine the behaviour of the network. The choice of the network type depends on the problem to be solved. The earliest neural network variant used was backpropagation. This network consists of three or more neuron layers: one input layer, one output layer and at least one hidden layer. In most cases, a network with only one hidden layer is used to restrict calculation time, especially when the results obtained are satisfactory. All the neurons of each layer (except the neurons of the last one) are connected by an axon to each neuron of the next layer. (for more information on backpropagation network see [21])

Counter Propagation Neural Network

The counter-propagation network in figure 1. is a variant of artificial neural network which is a combination of a portion of the Kohonen self-organizing map [17] and Grossberg outstar structure [18]. During learning, pairs of the input vector ***X*** and output vector ***Y*** were presented to the input and interpolation layers, respectively. These vectors propagate through the network in a counter flow manner to yield the competition weight vectors and interpolation weight vectors. Once these weight vectors become stable, the learning process is completed. The output vector ***Y***' of the network corresponding to the input vector ***X*** is then computed. The vector ***Y***' is intended to be an approximation of the output vector ***Y***' i.e. $Y \approx Y = f(X)$ (1)

The equations of the network are described briefly as follows. $U_j = [U_{ji}]$ (2)

Equation 2. is the arbitrary initial competition weight vector for the *j*-th neuron in the competition layer where u_{ji} is the weight connecting the *j*-th neuron in the competition layer to the *i*-th neuron in the input layer. The Euclidean distance between the input vector ***X*** and the competition weight vector $\boldsymbol{U_j}$ of the *j*-th neuron is calculated, i.e.:

$$d_j = \|X - U_j\| \sqrt{\sum_{t=1}^{m} (x_t - u_{jt})^2} \quad (3)$$

Once the distance d_j for each neuron has been calculated, the neuron with the shortest Euclidean distance to ***X*** is selected to represent the winning neuron. As a result of the competition, the output of the winning neuron is set to unity and the outputs of the other neurons are set to zero. Thus, the output of the *j*-th neuron in the competition layer can be expressed as:

$$z_j = \begin{cases} 1.0 & if\ d_j < d_t\ for\ all\ i \\ 0.0 & otherwise \end{cases} \quad (4)$$

The weight *uji* connecting the *j*-th neuron in the competition layer to the *i*-th neuron in the input layer is adjusted based on the Kohonen learning rule, i.e.:

$$u_{ij}(p+1) = u_{ji} + \beta \left(x_i - u_{ji}(p)\right) z_i \quad (5)$$

Where β is the learning coefficient and *p* is the iteration number.

After the competition weight vector $\boldsymbol{U}_j$ stabilizes, the interpolation layer starts to learn the desired output vector $\boldsymbol{Y}$ by adjusting the interpolation weight vector. Let

$$V_j = [v_{ji}] \quad (6)$$

Equation 6 is the arbitrary initial interpolation weight vector for the j-th neuron in the interpolation layer where v_{ji} is the weight connecting the j-th neuron in the interpolation layer to the i-th neuron in the competition layer. The weight v_{ji} is adjusted based on the Grossberg learning rule, i.e.

$$v_{ij}(p+1) = v_{ji} + \gamma\left(y_i - v_{ji}(p)\right) z_i \quad (7)$$

Where β is the learning coefficient. This is repeated until the interpolation weight vector $\boldsymbol{V}_j$ converges to a preset value. The output vector $\boldsymbol{Y}$' of the network corresponding to the input vector $\boldsymbol{X}$ can be calculated using a weighted summation function. The j-th component y'_j of the output vector $\boldsymbol{Y}$' can be expressed as:

$$y'_j = \sum V_{ji} Z_t \quad (8)$$

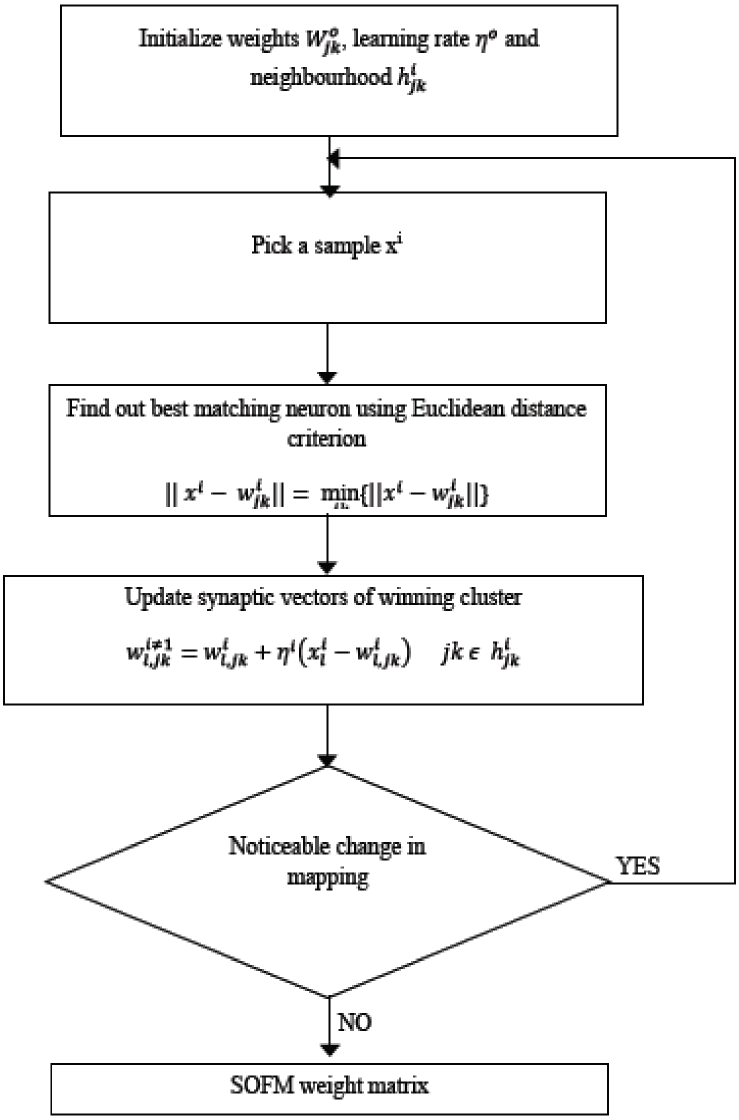

Initialize weights W^{o}_{jk}, learning rate η^{o} and neighbourhood h^{i}_{jk}
Pick a sample x^{i}
Find out best matching neuron using Euclidean distance criterion
$\| x^{i} - w^{i}_{jk} \| = \min_{jk}\{\|x^{i} - w^{i}_{jk}\|\}$
Update synaptic vectors of winning cluster
$w^{i+1}_{i,jk} = w^{i}_{i,jk} + \eta^{i}\left(x^{i}_{i} - w^{i}_{i,jk}\right) \quad jk \in h^{i}_{jk}$
Noticeable change in mapping
YES
NO
SOFM weight matrix

Figure 1: Components of Self-Organizing Map

IV. MATERIALS AND METHOD

The methodology employed involves the design of workflow process as shown in figure 2, for the fraud system which includes data collection, transformation of data, classification stage and evaluation.

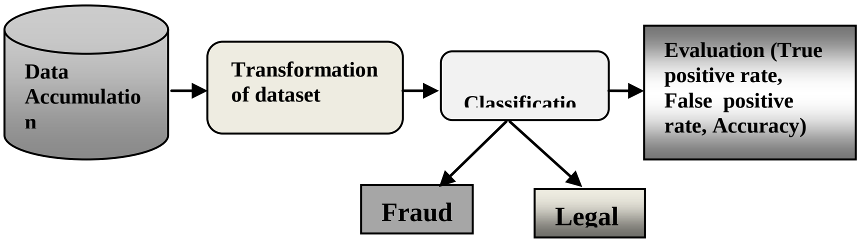

Data Accumulatio n
Transformation of dataset
Classificatio
Evaluation (True positive rate, False positive rate, Accuracy)
Fraud
Legal

Fig.2 System Work flow process

Data Collection / Description

Telecommunication operators store large amounts of data related with the activity of their clients. In these records exists both normal and fraudulent activity records. It is expected for the abnormal/fraudulent activity records to be substantially smaller than the normal activity. The data is called user profile record which is contained in the Call Detail Record (CDR) of any Private Branch Exchange (PBX) or any VoIP switch. Data used were collected from some Nigerian Telecommunication operators for different subscribers. All subscribers are on prepaid platform. The CDR consists of the following variables: National Identification Number,, Address, Local Government Area (number), State of origin, Nationality, Age, Phone Number (Customer number given by the network provider), Sex, Marital status, EmploymentType (private, public), Number of days with unpaid bills, Line account balance, Debt/payment ratio (in Percent).

Transformation of Data Set

The main idea behind user profiling is that the past behaviour of a user can be accumulated which is a vector that contains single numerical summaries of some aspect of behaviour or some kind of multivariate behavioural pattern. A profile may also contain categorical, censored, or other non-numeric data. Thus, a detailed daily behaviour of a user is constructed by separating the number of calls per day and their corresponding duration per day according to the called destination, i.e., national (N) and international (I) calls, and the time of the day, i.e., daytime (d) and night (n).The data is transformed into numerical representation can be easily trained by the classifier. Some of the CDR variables were not available for this work because of security reasons but subscribers' calls records were gotten. Below is a list of features derived from subscribers' calls records that are used when generating a summary description of customers' derived attributes based on the calls they originate over a period of time.

• average calls duration per day • average calls duration per week • average calls duration per month • Distribution of call duration (seconds, minutes, hours) • %age calls to different area code• Distribution of weekday calls (Monday – Friday) • Distribution of weekends calls (Saturday and Sunday) • Distribution of day time calls (6am – 7pm) • Distribution of night time calls (7pm – 6am) • Distribution of mode of call (analogue; Internet; digital)

• Regions of the world called (national or international) • Most frequent phone numbers called

Classification: Neural Networks

The neural networks employed is Counter-propagation neural networks (CPNN) and Back-propagation feed-forward neural networks (BPNN) is used for comparison. CPNN has three layers: an input layer, a Kohonen layer and a Grossberg outstar conditioning layer. The Kohonen layer starts with zero nodes, then nodes are added dynamically when any given training pattern fails to be assigned to the Kohonen units that represent its class. The weight vector of a newly added node is initialized to be the input vector of the wrong (untrainable) pattern. A supervised learning that selects two winners with punishment mechanism is used for weight update: if the first winner is correct, update with positive weights, if incorrect, punish the winner with negative weights and find the second winner; if the second winner is correct, update with positive weights, if incorrect, allocate a new unit. The Kohonen learning rate for weight adjustment is 0.2.

The BPNN used in this work are three-layered, feed-forward networks. The size of the input layer (i.e., number of input units) is dictated by the sequence encoding schema chosen. The output layer size is determined by the number of classes represented in the network, with each output unit representing one phylogenetic class. The hidden size is determined heuristically, usually a number between input and output sizes. Several preliminary studies were conducted to determine the optimum values for various network parameters. In this study, a hidden size of 200 is chosen, and the networks are trained using weight matrices initialized with random weights ranging from -0.5 to 0.5. Other network parameters include the learning factor of 0.5, momentum term of 0.2, a constant bias term of -1.0, and error threshold of 0.03.

Evaluation

One of the most interesting aspects of the problem is the evaluation of different user representations (profiles) and their effect towards the proper discrimination between legitimate and fraudulent activity. In this work, the metrics employed are (i) fraud catching (that is true positive rate) and false alarm rate (that is false positive rate) prediction rate, and overall accuracy as metrics.

$$\textbf{Fraud Catching} = \frac{TP}{TP+FN}$$

$$\textbf{False Alarm rate} = \frac{FP}{TN+FP}$$

$$\textit{Precision rate} = \frac{TP}{TP+FP}$$

$$\text{Accuracy} = \frac{\text{Number of detected fraud customers}}{\text{Number of customers classified fraud}}$$

V. IMPLEMENTATION AND RESULTS

The specifications of computer employed for this work are Intel-based microprocessor of 1.6 GHz, 2 GB of RAM, 10GB of ROM and 8 GB of a Compact Flash memory, a 15.0" touch screen. This configuration provides a compact and fully functional environment for Windows based x86 applications. The system software has three components: a pre-processor to create from input sequence files the training and prediction patterns, a neural network program to classify input patterns, and a postprocessor to summarize classification results. Two separate neural network programs are used for BPNN and CPNN algorithms, respectively. All programs have been coded in C language.

The data used was based on eighty customers' calls detail records gotten from four major Telecommunication providers. The record spanned between the period of July 2014 and November 2015, that is a duration of seventeen months which includes 15,187 individual call records. Some of the assumptions for predicting a fraudulent subscription are; applicant's identification number is similar to that of a fraudster, applicant's contact phone number is similar to a fraudster and applicant's address, age, gender and marital are similar to a fraudster. The distributions of both the normal and fraud calls are shown in table 1 and table 2.

Table 1 Distribution of Normal Calls

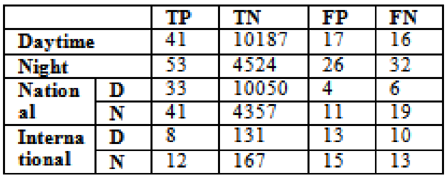
	National	International	
Daytime	10093	168	10261
Night	4428	207	4635

Table 2. Distribution of Abnormal Calls

Fraud	National	International	
Daytime	74	62	136
Night	71	84	155

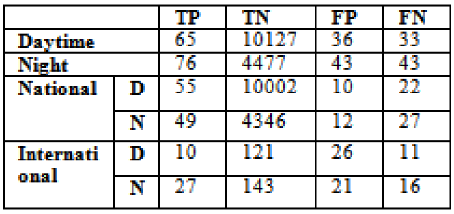
The algorithms, CPNNN and BPN, detection systems are tested with a different 40 percent of data samples that are not part of the 60 percent training set used to create the model. Out of the testing samples, 1.9 percent samples are fraudulent applications while 98.1 percent samples are normal applications. The model is used to simulate the inputs to the predict type of application (Fraud=1; Normal=0). The results of classifications produced by CPNN and BPNN are shown in table 3 and table 4.

Table 3: Results of classification by CPNN



		TP	TN	FP	FN
Daytime		41	10187	17	16
Night		53	4524	26	32
National	D	33	10050	4	6
	N	41	4357	11	19
International	D	8	131	13	10
	N	12	167	15	13

Table 4: Results of classification by BPNN



		TP	TN	FP	FN
Daytime		65	10127	36	33
Night		76	4477	43	43
National	D	55	10002	10	22
	N	49	4346	12	27
International	D	10	121	26	11
	N	27	143	21	16

The results of estimated performance metrics (as estimated from tables 4 and 5) of the two neural networks are presented as follows. The CPNN produced averages of fraud catching rate and false alarm rate as 0.67 and 0.003 (for both daytime and night) respectively while BPNN produced averages of fraud catching rate and false alarm rate as 0.61 and 0.006 (for both daytime and night) respectively. For international calls, CPNN produced averages of fraud catching rate and false alarm rate of 0.46 and 0.91 (for both daytime and night) respectively while BPNN produced averages of fraud catching rate and false alarm rate as 0.54 and 0.84 (for both daytime and night) respectively. While For national calls, CPNN produced averages of fraud catching rate and false alarm rate of 0.76 and 0.998 (for both daytime and night) respectively while BPNN produced averages of fraud catching rate and false alarm rate as 0.64 and 0.998 (for both daytime and night) respectively. CPNN produced 69% precision rate better that BPNN which produced precision of 64%. Also, CPNN produced accuracy of 94.2% (for both daytime and night) while BPNN produced accuracy of 81.7% (for both daytime and night).

Table 4: Results of performance metrics by CPNN

		TP	TN	FP
Daytime		0.67	0.19	0.81
Night		0.64	0.30	0.46
National	D	0.71	0.12	0.89
	N	0.65	0.17	0.83
International	D	0.48	0.43	0.58
	N	0.52	0.47	0.53

Table 5: Results of performance metrics by BPNN

		TP	TN	FP
Daytime		0.62	0.22	0.78
Night		0.60	0.22	0.78
National	D	0.64	0.17	0.83
	N	0.64	0.15	0.85
International	D	0.55	0.32	0.70
	N	0.52	0.36	0.64

VI. CONCLUSION

The theft of telecommunication services has been one of the most enduring types of telecommunications crime which has been evident since the beginning of telephone systems. Each technological development designed to thwart criminal endeavours has been quickly followed by the creation of a new form of crime designed to exploit new security. In particular, fraud detection is important to the telecommunications industry because subscribers, companies and suppliers of telecommunications services lose a significant proportion of their subscriptions or revenues as a result. Moreover, the modelling and characterization of users' behavior in telecommunications can be used to improve network security, improve services, provide personalized applications, and optimize the operation of electronic equipment and/or communication protocols. Thus, neural network variants has become an increasing presence in major aspects of telecommunication networks improving efficiency, adapting to changing calling patterns, and providing better information about the use of networks.

ACKNOWLEDGEMENT

I acknowledge the participation and assistance of my project students and their cohorts for their commitments towards the successive completion of this paper.

REFERENCES

[1]. Qayyum S., Mansoor S., Khalid A., Halim Z. and Baig A.R.(2010). "Fraudulent Call Detection for Mobile Networks", IEEE 2010.

[2]. Ogundile O.O (2013).Fraud Analysis in Nigeria's Mobile Telecommunication Industry , International Journal of Scientific and Research Publications, Volume 3, Issue 2, ISSN 2250- 3153.

[3]. Constantinos S. Hilas, Paris A. Mastorocostas and Ioannis T. Rekanos (2015).Clustering of Telecommunications User Profiles for Fraud Detection and Security Enhancement in Large Corporate Networks: A case Study, Appl. Math. Inf. Sci. 9, No. 4, 1709-1718 (2015).

[4]. *CFCA*. "CFCA's 2011 Worldwide Telecom Fraud Survey" *(PDF)*. *CFCA*. Retrieved 5 December 2014.

[5]. R. Basnet, S. Mukkamala, and Andrew H. Sung (2009).Detection of Phishing Attacks: A Machine Learning Approach, New Mexico Tech, New Mexico 87801, USA.

[6]. Desai A., Deshmukh R. (2013). Data mining techniques for Fraud Detection, Anita B. Desai et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 1 – 4.

[7]. http://freerouteserver.com/wordpress/2012/10/call-fraud-scenarios.html

[8]. R. Bolton and D. J Hand, (2002) "Statistical fraud detection: a review," Statistical Science, vol. 17, no. 3, pp. 235–255.

[9]. H. I, Volkmar and Padraig (2011) "Telecom fraud 101:Fraud types, Fraud methods & Fraud Technology".

[10]. Fayemiwo M. A. and Olasoji B.O. (2014). Fraud Detection In Mobile Telecommunication. International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 4.

[11]. Richard, Volinsky, And Wilks (2010); Fraud Detection In Telecommunications: History and Lessons Learned, Technometrics, February 2010, Vol. 52, No. 1

[12]. Olszewski D. (2012). A probabilistic approach to fraud detection in telecommunications, Knowledge-Based Systems 26 (2012) 246–258.

[13]. Antonio Rosa, Luis Cortesao, Filipe Martins & Pedro Carvalho(2004). Fraud Management Systems in Telecommunication: A practical approach.

[14]. Estevez P., Held C. and PerezA. (2005). Subscription Fraud prevention in telecommunication using Fuzzy rule and Neural Network. Department of Electrical Engineering, University of Chile, Casilla 412-3.

[15]. Kohonen T., (1995). Self-Organizing Map. 2nd edition, Berlin: Springer-Verlag. pp. 1-12.

[16]. Grossberg S. (1982). Studies of Mind and Brain. Boston: Reidel Publishing. Hans-Ulrich Bauer and Klaus R. Pawelzik. (1992). Quantifying the neighborhood preservation of Self-Organizing Feature Maps. IEEE Transactions on Neural Networks, 3(4), pp.570–579.

[17]. P. Barson, S. Field, N. Davey, G. McAskie, and R. Frank. The detection of fraud in mobile phone networks. *Neural Network World*, 6(4):477–484, 1996.

[18]. Y. Moreau, H. Verrelst, and J. Vandewalle. Detection of mobile phone fraud using supervised neural networks: A first prototype. In *International Conference on Artificial Neural Networks Proceedings (ICANN'97)*, pages 1065–1070, October 1997.

[19]. D. Reby, S. Lekb, I. Dimopoulos, J. Joachim, J. Lauga and S. Aulagnier (1997). Artificial neural networks as a classification method in the behavioural sciences, Behavioural Processes 40 (1997) 35–43.

Ismaila W. Oladimeji. Othman" Soft Computing Approach to Anomaly Detection in Subscribers Call Profiles" The International Journal of Engineering and Science (IJES), 7.12 (2018): 23-30