DEVELOPMENT OF AN EFFECTIVE SYSTEM FOR DETECTING CYBERCRIMES USING MODIFIED RIPPLE DOWN RULE SYSTEM AND NEURAL NETWORK.

D.G. Amusan[1*], A.S. Falohun[2], O.T. Arulogun [3]

[1]Department Of Computer Science Open And Distance Learning, Ladoke Akintola University Of Technology, Ogbomoso, Email: dgamusan@lautech.edu.ng, Tel.: +2348032081412*
[2]Department Of Computer Engineering, Ladoke Akintola University Of Technology, Ogbomoso. Email:asfalohun@lautech.edu.ng
[3]Department Of Computer Engineering, Ladoke Akintola University Of Technology, Ogbomoso. Email:otarulogun@lautech.edu.ng

[*]***Corresponding Author:***
dgamusan@lautech.edu.ng

Abstract:

Cybercrime is an unlawful act in which computer is the tools to commit an offense; cyber criminals perform operation in cyber space with the help of the internet. Most existing techniques used in detecting cybercrimes could detect individual attacks but failed in terms of coordinated and distributed attacks. Also, most of the detection system used to curb cybercrimes on web application generates a large number of false alarms. Hence, this research developed an enhanced system which could not only detect individual, coordinated and distributed attacks but also reduce the number of false alarms. The research data for this work which consists of six cards (labeled A, B, C, D, E and F) were sourced from an online shopping store. The six cards contain four attributes with associated two thousand seven hundred (2700) transactions. The number of transactions carried out through each card were 200, 300, 400, 500, 600 and 700 respectively. Sixty percent of transactions carried out on each card were used to train the system while the remaining forty percent were used to test the system. The acquired attributes through each card were used as inputs in developing the system. Radial basis function was used for features extraction and the extracted features were moved to the Modified Ripple Down Rule engine that compared the profiling of the cardholder transaction information. The developed system was implemented on Matrix laboratory environment. The performance of the developed system was evaluated at 0.80 threshold using Sensitivity, Specificity, False Alarm Rate, Accuracy and Computational Time.

Keywords—*Cybercrime, Modified Ripple Down Rule, Radial basis Function, Credit Card, (key words)*

I INTRODUCTION

Information and Communication Technology (ICT) is an enabler of change, an essential element of new developments and a major contributor to successes in daily life. The impact of ICT is extensive, affecting individuals, businesses, industries, communities and governments. It changes the way daily activities are accomplished and also impacts social and economic development globally. The spread of ICT promotes the development of information society where economic success and social development became more dependent on the availability and accessibility of ICT. The trend in ICT altered fundamental methodologies of doing business and gave rise to electronic services in communication, trade, employment, education, government, and health. Recently, there is increase in social media and mobile devices usage as they facilitate the interaction between individual and their participation in decision-making processes [1].

Today, our society is increasingly relying on ICT and the internet to conduct businesses, manage industrial activities and engage in personal communication among numerous benefits. These technologies allow enormous gain in efficiency, productivity and communication. They also create a vulnerability to those who choose to take an advantage of new situations or new development in the usage of ICT [2]. The rapid growth of the internet and its global acceptance is producing increasing security threats. The cyber space creates unlimited opportunities for commercial, social and educational activities. Criminals perform operation in cyber space with the help of internet. Cybercrime is defined as a crime in which a computer is the object (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercrime is increasing astronomically each day as the internet continues to reach every nook and crannies of our society and none can predict accurately the next dimension. It has caused a lot of harm to the society and to individual's lives. [3] informed that Nigeria's loss to cybercrimes was about N127 billion yearly and has become a source of challenge to the Federal Government of Nigeria.

More Nigerians embrace ICTs lately compared to other African countries [4]. Some years ago, limited number of countries had local internet access but today the story has changed positively. Internet usage is on the increase in Nigeria with most of the citizens who cannot afford the private internet facilities, depending on the public and commercial internet access points such as cybercafes for rudimentary internet access. All these cybercafes make use of this advantage to charge individual, group or companies exorbitant fees for their services. Despite the growth in ICT adoption, fundamental problem of erratic power supply also rears its ugly head. The inadequate telecommunication infrastructures also continue to hinder the nation from uninterrupted access to innovative information technology applications such as e-government, e-commerce, telemedicine and teleconferencing [5].

The purpose of this research is to develop a modified ripple down rule system for detecting cybercrimes. The effect of cybercrime on Nigerian socio-economy has been an active area of research because of its adverse effect on Nigerian due to hacking, theft, cyber stalking, identity theft, malicious software and abuse. There is need to investigate the effect of cybercrime on the society and design a system capable of detecting the action of cybercrime perpetrator and their location. This article reckons with the theoretical presentation (investigation), design of a system for detecting and preventing internet fraudulent activities using Ripple Down Rule system technique and Neural Networks.

II RELATED WORK

Different researches have been carried out in the field of cybercrime detection. Strategic reliability approach to anomaly detection recommends different techniques, depending on the type of the network. Markov analysis was used for the strategic defense of a system, which has been targeted by multiple attackers. [6] took into account the essential dissimilarities of the network elements and considered several parallels and complicated series of defensive techniques. [7] proposed an extension of Anomaly detection model for computer system security to ambient intelligence domain. The extended model can provide perceptual functions and detection capabilities with device intelligence such as multimedia sensor system interpretation. The author also studied the benefits of AI in general for improving Intrusion detection system by investigating different IDS designs based on Artificial intelligent. The results showed how Artificial intelligent approach to IDS design can be fruitful for future applications. The work was limited to the use of sensing devices to secure the system from intrusion. The researchers in [8] proposed a technique for telecommunications fraud detection. The method proposed 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. [9] analyzed various Artificial Immune System (AIS) models used in Intrusion detection system (IDSs) and introduced Danger Theory in AIS as a method for danger response in wireless mesh networks. For classification of network dangers, they used Self-Organizing Maps (SOMs) as classifiers. The experiments validated their proposal of applying Danger Theory to security of wireless mesh networks. It is deduced that the model works only on the test or fraud attack. [10] proposed Hidden Markov Model (HMM) to verify fraudulent transactions which initially trained with the normal behavior of a cardholder therefore if an incoming credit card transaction is not accepted by the HMM with sufficiently high probability, it is considered to be fraudulent and K Mean Clustering algorithm was used to identify spending behavior of a customer. [11] developed financial fraud Detection technique based on three approaches combined: Rule based filtering, Dempster–Shafer theory and Bayesian learning in which Dempster rule was used to match customer current behavior compared with the previous behavior, to determine the suspicious level of each incoming transaction. Rule based filtering approach was used and Bayesian learning approach to update the suspicious score of transaction using history database of both genuine cardholder as well as fraudster.

[12], evaluated genetic algorithm and scatter search technique to score each transaction and based on these scores the transaction may be classified as either fraudulent or genuine and these approaches are based on the classification problem. [13] proposed a detector framework to detect fraud by telecommunication subscribers using different techniques: data cleaning, dimension reduction, clustering and classification. The main challenges in the proposed framework is that it

requires the historic data to identify whether the customer is fraudster or genuine to perform the transaction. [14] proposed two methods in detecting fraudulent acts based on the finite fixture model to detect fraudulent items automatically without the requirement of labeled items and modeled the dependency between the description and the price of an item by considering the possible combinations of the item description and price clusters according to item clusters and a real-world dataset to evaluate the effectiveness of the proposed models and compared them to existing outlier detection methods so the proposed model significantly identified the fraudulent transactions. The model proposed by Kim is limited to the numbers of trained dataset. Lee [15] adopted an algorithm called online Oversampling Principal Component Analysis Algorithm (OSPCA) to solve real world applications problem such as intrusion detection or credit card fraud detection and the aim of the author was to detect the presence of outliers from a large amount of data via an online updating technique. [16], proposed two practical techniques for outlier detection named ITB-SS and ITB-SP to solve problem that is real such as Intrusion Detection, Criminal activity detection in E-Commerce etc. and these methods does not require user defined parameter to decide whether an object is outlier and author also proposed a new concept called "Holoentropy" that takes data and total correlation together into consideration. Sahin [17], the security mechanism such as CHIP and PIN were developed for credit card system that does not prevent from fraudulent credit card usages over online fraud and the author have developed and implemented a cost sensitive decision tree approach to detect fraudulent transactions and this approach is compared with the traditional classification models on a real-world credit card data set. [18] proposed SGDIDS a new hierarchical Distributed Intrusion Detection System for improving cyber security of the Smart Grid. The system consists of an intelligent module (among other modules) which uses AIS to detect and classify malicious data and possible cyber-attacks. Simulation results showed that the system is applicable to identification of malicious network traffic and improving system security also enhanced the anomaly detection based on AIS and showed how the model improves AIS performance in applications such as anomaly detection, ensuring security, detecting errors and performing datamining in mobile ad hoc networks. The limitation of the proposed SGDIDS is that it identifies malicious network traffic rather than detecting the anomaly behaviours posed. [19] worked on a method of solving business problems in banking sectors which are done best by contribution of Data Mining. Better targeting, acquiring new customers and fraud detection in credit cards, the researcher ascertains those transactions that are fraudulent can be achieve by Data mining techniques. [20] presented the necessary theory to detect fraud in credit card transaction processing using a Hidden Markov Model. If an incoming credit card transaction is not accepted by the Hidden Markov Model with sufficiently high probability, it is considered to be fraudulent. At the same time, author tried to ensure that genuine transactions are not rejected. Author showed how HMM helped to obtain high fraud coverage combined with a low false alarm rate. This research aimed at the case of customers' default payments in Taiwan and compared the predictive accuracy of probability of default among six data mining methods. From the perspective of risk management, the result of predictive accuracy of the estimated probability of default will be more valuable than the binary result of classification - credible or not credible clients. Because the real probability of default is unknown, the study presented the novel ''Sorting Smoothing Method" to estimate the real probability of default. With the real probability of default as the response variable (Y), and the predictive probability of default as the independent variable (X), the simple linear regression result (Y = A + BX) shows that the forecasting model produced by Artificial Neural Network has the highest coefficient of determination; its regression intercept (A) is close to zero, and regression coefficient (B) to one. Therefore, among the six data mining techniques, artificial neural network is the only one that can accurately estimate the real probability of default [21].

III METHODOLOGY

The developed cybercrime detector system aims to identify and detect fraudulent online activities using modified ripple down rule and neural network; In developing the detection and prevention system, a database of financial transactions was created; which was used to train the developed system. The implementation of the program is developed on MATLAB R2020a environment. The following are the stages involved during implementation of the system:

- Data Acquisition
- Modified Ripple Down Rule
- Machine Learning
- Classification stage

Cyber-crime Data Acquisition (Financial Transaction)

The dataset used for this work contains six (6) cards. The card comprised four attributes and consisted of Two thousand Seven Hundreds (2700) transactions where One thousand six hundred and twenty were used for training and one thousand and eighty were used for the testing. Using cross-validation method, 60% transactions of each card were used to train the system and 40% transactions were used to test the system. These were subjected to Modified Ripple Down Rule (MRDR) and benchmarked Ripple Down Rule (RDR). In this work, real time data and synthetic data were used. The real time data used was collected from an online shopping store. Gaussian distribution was used to generate synthetic data. The input to the developed system was the data collected from online shopping store and the synthetic data generated by Gaussian distribution.

The Modification of RDR

The operation of Ripple Down Rules (RDR) is that, after a case is processed a corresponding conclusion or result was returned. In the modification of RDR after a case is processed, a model was returned instead of a conclusion or a class. The model was called Situated Profile (SP). This SP contains profiles describing each of the attributes matching the current case. Figure 1 and Figure 2 depict the basic RDR operation and the Modified RDR operation respectively.

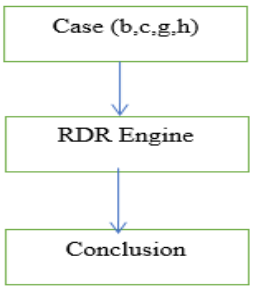

Figure 1: Basic Ripple Down Rules operation

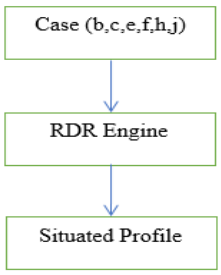

Figure 2: Modified Ripple Down Rules operation

The modification of RDR (MRDR) was an improved RDR with the added capability to handle multiple classifications. The inability of Rule Based System to provide multiple classifications was seen as a limitation to its applicability in many domains. MRDR was developed to be applicable for domains where a single case may lead to multiple conclusions while still retaining the advantages of RDR. In fact, MRDR should be shown to cover a domain quicker than its single class counterpart and it should be able to produce a more compact Knowledge Base with fewer redundancies than single class RDR. An MRDR parent node can have any number of exception branches and each branch will be followed when the parent node condition is true for a given case. Inferencing in MRDR is generally similar to RDR except that if a condition is false at a parent node, then no child nodes should be evaluated. Inferencing in MRDR is such that the root node is evaluated first, and then all nodes connected to the root are tested next. The nodes that evaluate to true have their child nodes tested and the ripple continues until a terminating node is reached or until all children are false. The effective conclusions for the case were a collation of the firing terminal rules in each branch. Figure 3 illustrates the inferencing process in an MRDR structure. Diagram in figure 3, it is assumed the structure has the following inputs:

- the spending behaviour
- the location of the transaction
- the time variance
- the devices used/ IP address

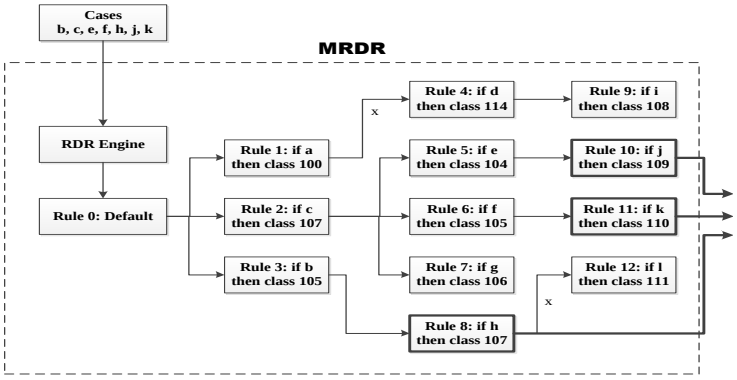

Figure 3: Modified Ripple Down Rule Structure

Radial Basis Function (RBR) Networks

Radial basis function (RBF) networks was used in this research as classifier; Classifying Suspicious/ Fraudulent Online Transaction. RBR neural networks is easy to design, it has good generalization, strong tolerance to input noise, and have online learning ability. The properties of RBF networks make it very suitable to design flexible control systems. Neural Networks has been utilized to resolve a variety of problems that are very hard to resolve by ordinary programming which is based upon certain rules. Figure 4 give a detail of three-layered RBNN. The sigmoid function provides enough information about the output to earlier nodes (hidden and input) so that the weights can be adjusted accordingly to reduce the difference between the NN's calculated output and the desired target output.

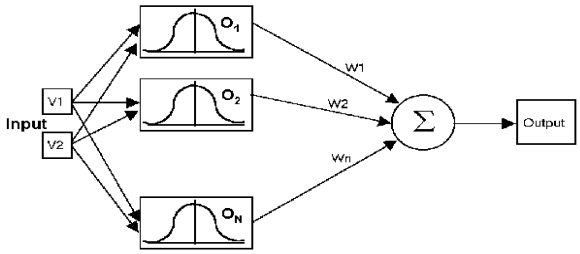

Figure 4: Radia Basis Function Neural Network Architecture

Equation 1 represents sigmoid function.

$$f(net) = \frac{1}{(1+e\ -knet)} \quad (1)$$

From this equation, k is the positive constant and it controls the breadth of the function. RBFNN was used as a secondary classifier where MRDR outputs was indexed and passed to the Radial Basis Function (RBF) NN and the output was used to substantiate the MRDR result.

Implementation of the Designed System

The developed cybercrime detection system was implemented using MATLAB R2020a software on Windows 10 64-bit operating system. The results gotten were examined at different threshold values using some selected performance metrics which are Sensitivity, Specificity, False Alarm Rate (FAR), Accuracy and Computational Time (CT). The dataset used for this work contains Six credit cards. The card comprised four attributes and consisted of Two thousand Seven Hundreds (2700) with fraudulent type and non-fraudulent type where One thousand six hundred and twenty were used for training and one thousand and eighty were used for the testing. Figure 5 represents the flow chart of the developed system. The flow diagram in Figure 5 starts by inputting the acquired data from financial institute then locate the machine address if the transaction is done via mobile phone or laptop then the address is the IP address which is unique to each of the devices used in transaction. The system prompted to ascertain if there is any machine address then traces the IP address and if the system cannot ascertain the IP address returned back to the acquired data. Another measure is to compare the current geographical location and the spending behavior of the present transaction with the previous transactions and decide if the transaction is suspicious or genue.

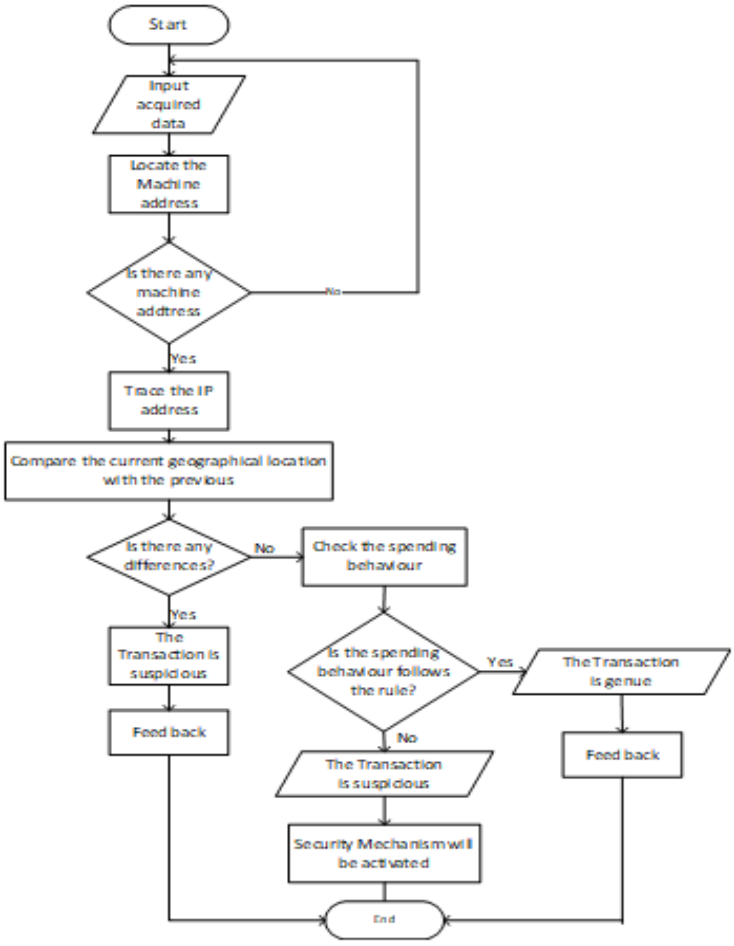

Figure 5: Flow chart of the developed system

IV RESULTS AND DISCUSSION

The developed detection system has an efficiency of about 98% in term of sensitivity, specificity, and Accuracy. False alarm rate has reduced drastically to the value of 1.08%. The system studied the financial transaction pattern and detect fraudulent online activities. Table 1 shows the simulation results of the developed cybercrime detector system.

TABLE 1: RESULT OF THE MRDR SIMULATION
Result of MRDR at 700 transactions

Threshold	Sensitivity (%)	Specificity (%)	False Alarm Rate(%)	Accuracy (%)	CT(sec)
0.2	97.30	89.16	10.84	91.67	206.06
0.4	98.93	93.55	6.45	97.14	138.28
0.6	98.40	96.77	3.23	97.86	149.36
0.8	97.86	98.92	1.08	98.21	140.91

TABLE 2: RESULT OF THE RDR SIMULATION
Result of RDR at 700 transactions

Threshold	Sensitivity (%)	Specificity (%)	False Alarm Rate(%)	Accuracy (%)	CT (sec)
0.2	97.85	88.30	11.70	94.64	130.57
0.4	97.31	90.43	9.57	95.00	131.40
0.6	96.77	92.55	7.45	95.36	130.08
0.8	96.24	95.74	4.26	96.07	131.11

The outcome, from table 1 showed that accuracy for the detection of cybercrime is 98.21%, 97.86% for sensitivity and 98.92% for specificity considering 700 transactions. MRDR was able to detect outliers as the system learnt the network behavior with the least false alarm rate as displayed in table. The results generated with MRDR produced more efficient results in terms of prediction accuracy compared with RDR shown in table 2.

V CONCLUSION AND FUTURE SCOPE

In this research, a system has been developed to detect cybercrimes in an online transaction to reduce the rate of fraudulent act with low false alarm rate. Four important attributes are involved in cybercrime detection system. The cybercrime detection system is critically important for security and economic operation in banking system. This work developed a Modified Ripple Down Rule that can used to detect and prevent financial cybercrimes. The combination of Radial Basis Function (RBF) and RDR established powerful problem-solving ability called MRDR. It contains the dynamic rule which is generally based on human knowledge. The MRDR technique reported a reasonably and effective results in terms of accuracy, sensitivity, specificity and false alarm rate in comparison with RDR. Financial data for research is a big challenge because of the fraudulent acts and non-fraudulent acts involved. Future work can be carried out by comparing the effect of other artificial neural network algorithms with RDR.

References

[1]. J. O. Odumesi, "A socio-technological analysis of cybercrime and cyber security in Nigeria"., International Journal of Sociology and Anthropology, Vol.**6, Issue** 3, pp.**116-125. 2014**

[2]. D. Sumanjit, and N. Tapaswini, "Impact of Cyber Crime: Issues and Challenges". International Journal of Engineering Sciences & Emerging Technologies, Vol. **6, Issue 2**, pp. **142-153, 2013**

[3]. P. Adeyemi, and A. Nkechi, "Research on Intrusion Detection and Response: A Survey". International Journal of Network Security, Vol.**2**, pp. **84-102**, **2016**

[4]. U. B. Steve, O. Diepreye and D. A. Uduak, "Information Communication Technologies in the Management of Education for Sustainable Development in Africa." An International Multi-Disciplinary Journal, Ethiopia, Vol. **3,** Issue **3,** pp**. 414-428, 2009**

[5]. O. Maitanmi, S. Ogunlere, S. Ayinde and Y. Adekunle. "Impact of Cyber Crimes on Nigerian Economy". The International Journal Of Engineering And Science (IJES) Vol.**2**, Issue. **4**, pp. **45-51, 2013**

[6]. A. Patcha and J .M. Park . "An overview of anomaly detection techniques: Existing solutions and latest technological trends". Computer Networks,Vol. **51**, pp. **3448-3470, 2007**

[7]. G. Gianini, M. Anisetti, V. Azzini, V. Bellandi, E. Damiani and S. Marrara. " An Artificial Immune System approach to Anomaly Detection in Multimedia Ambient Intelligence". 3rd IEEE International Conference on Digital Ecosystems and Technologies. Pp**. 502 – 506, 2009**

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

[9]. M. A. Lebbe, J. I. Agbinya, Z. Chaczko and F. Chiang, "Self-Organized Classification of Dangers for Secure Wireless Mesh Networks", Australasian Telecommunication Networks and Applications Conference. pp. **322 – 327**, **2007**

[10]. A. Srivastava, Kundu.A, Sural.S and Maju-mdar. A.K, "Credit Card Fraud Detection Using Hidden Markov Model", IEEE Transactions on Dependable & Secure Computing Vol. **5**, **2008.**

[11]. S. Panigrahi, A. Kundun, S. Sural and A.K. Majum-dar, "Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning" Science Direct, pp. **354-363**, **2009**.
[12]. E. Duman and H.M. Ozcelik., "Detecting credit card fraud by genetic algorithm and scatter search", Science Direct, Expert System with Applications. Vol.**38** , pp **13057- 13063**, **2011**
[13]. H. Farvaresh and M.M. Sepehri, "A data mining framework for detecting subscription fraud in telecommunication", Science Direct, Engineering Applications of Artificial Intelligence. Vol.**24**, pp. **182-194**, **2010.**
[14]. K. Kim, Y. Choi and J. Park. "Pricing fraud detection in online shopping malls using a finite mixture model". Science Direct Electronic Commerce Research and Applications, pp. **195-207, 2013**
[15]. M. A. Lebbe, J. I. Agbinya, Z. Chaczko, and F. Chiang . "Self-Organized Classification of Dangers for Secure Wireless Mesh Networks", Australasian Telecommunication Networks and Applications Conference. Ppp. **322 – 327, 2007**
[16]. S. Wu and S. Wang, "Information-Theoretic Outlier Detection for Large-Scale Categorical Data", IEEE Vol. **25** Issue..**3**, **2013**
[17]. Y. Sahin, S. Bulkan.and E. Duman., "A cost-sensitive decision tree approach for fraud detection", Science Direct, Expert System with Applications. Vol. **40**, pp-**5916- 5923**, **2013.**
[18]. A. Zhang, C. Chen and H. Karimi. "A new adaptive LSSVR with on-line multikernel RBF tuning to evaluate analog circuit performance". Abstract and Applied Analysis.Vol. **20**, pp. **1-7**. Article ID **231735**, **2013**
[19]. V.Mareeswari, Dr G. Gunasekaran, "Prevention of Credit Card Fraud Detection based on HSVM", International Conference on Information Communication and Embedded System **2016.**
[20]. S. M. Jaba, P. Soumyashree, and K. M. Ashis, "A Novel Approach for Credit Card Fraud Detection Targeting the Indian Market", IJCSI International Journal of Computer Science Issues, Vol. **10**, Issue **3**, **No 2, 2013.**
[21]. IC. Yeh, and C. Lien, "The comparisons of data mining techniques for the predictive accuracy of probability of defualt of credit card client," Expert Syetem with Applications Vol. **36**, pp.**2473-2480**, **2008**

Authors Profile

Amusan D. G. is an E-Tutor in the Department of Computer Science Open and Distance Learning Centre of Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria. He graduated with B. Tech Computer Engineering from Ladoke Akintola University of Technology, Ogbomoso, Nigeria the year 2010. He obtained M.Tech Computer Science from Ladoke Akintola University of Technology (2016) and obtain his Ph.D Computer Engineering from Ladoke Akintola University of Technology. His research interests includes Intelligent security Systems, Character &Pattern Recognition, Data and Information Security. He belongs to the following professional bodies: Full member, The Nigerian Society of Engineers (NSE); International Association of Engineer (IAE); Registered Engineer, Council for the Regulation of Engineering in Nigeria (COREN. R.50782). He has 7 years of teaching experience and 5 years of Research Experience. He can be reached through this email: dgamusan@lautech.edu.ng .

Arulogun O. T. is a Professor in the Department of Computer Science and Engineering, LadokeAkintola University of Technology, Ogbomoso, Nigeria and he is the current Director of LAUTECH Open and Distance Learning Center, Ogbomoso. He graduated with B.Tech. Computer Engineering (1998) from LadokeAkintola University of Technology, Ogbomoso, Nigeria. He obtained M.Sc. Microprocessor and Control Engineering from University of Ibadan, Nigeria (2004) and Ph.D Computer Science from Ladoke Akintola University of Technology (2008). As an erudite scholar, he has published reputable journals and scholarlistic articles in referred journals and learned conferences. His research interests include: Intelligent systems and their applications. Typical application areas include intelligent sensors for fault diagnosis (electronic noses), security and computer vision. He belongs to the following professional bodies: Full member, Computer Professionals (Registration) Council of Nigeria (MCPN); Registered Engineer, Council for the Regulation of Engineering in Nigeria (COREN). He can be reached through this email: otarulogun@lautech.edu.ng

Falohun A. S. is a Professor in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He graduated with B.Tech. Computer Engineering from LadokeAkintola University of Technology, Ogbomoso, Nigeria. He obtained M.Tech Computer Science from Ladoke Akintola University of Technology and Ph.D Computer Science from Ladoke Akintola University of Technology. As an erudite scholar, he has published reputable journals and scholarlistic articles in referred journals and learned conferences. His research interests includes Intelligent security Systems, Character &Pattern Recognition, Data and Information Security. He belongs to the following professional bodies: Full member, The Nigerian Society of Engineers (NSE); International Association of Engineer (IAE); Registered Engineer, Council for the Regulation of Engineering in Nigeria (COREN. He can be reached through this email: asfalohun@lautech.edu.ng .