JINAV: Journal of Information and Visualization *ISSN: 2746-1440 (online)*
Vol. 2 No. 1 (2021)
https://doi.org/10.35877/454RI.jinav274

Spectral-Cluster Framework For Credit-Card Fraud Detection Using A Genetic Algorithm Trained Modular Deep Learning Neural Network

Arnold Adimabua Ojugo[a,*], Obinna Nwankwo[b]

[a]*Department of Computer Science, Federal University of Petroleum Resources Effurun, Delta State 32001, Nigeria*
[b]*Department of Computer Science, Novena University Ogume, Delta State 32001, Nigeria*

Abstract

Adversaries achieved such intrusion via carefully crafted attacks of large magnitude that seek to wreak havoc on network infrastructures with a focus on personal gains and rewards. Study proposes a spectral-clustering hybrid of genetic algorithm trained modular neural network to detect fraud in credit card transactions. The hybrid ensemble seeks to equip credit-card users with a system and algorithm whose knowledge will altruistically detect fraud on credit cards. Results show that the hybrid model effectively differentiates between benign and genuine credit card transactions with a model accuracy of 74%.

Keywords: Fraud detection; deep learning; modular neural network; credit card fraud; multi-agent modeling; transaction rules.

1. Introduction

The increasing need for e-commerce, online marketing and the ineffective vigilance of sellers/buyers often constitutes the facts that criminals are steps ahead of biz owners and users of these products – at all times. Pre-empting fraud prior to its occurrence is quite possible in traditional non-automated tasks cum transactions owing to the natural intelligence of a seller/buyer. Advances in computing with improved methods and intelligence – are yet to proffer techniques to completely curb fraud. Use of intelligent systems however, are on the rise for fraud detection – though, it is still proving abortive (Ojugo and Yoro, 2020). Thus, the need to design predictive intelligent system to monitor, detect and prevent fraudulent activities – especially in regards to credit/smart card transactions (Bolton and Hand, 2002).

The advent of credit cards and their increased functionality has not only given more personal comfort, but also attracted malicious characters interested in the handsome rewards. Credit cards are easily targeted as crime therein perpetrated are only discovered few weeks afterwards (Ojugo and Eboka, 2020a; Ojugo et al, 2015a; 2015b). Successful card fraud techniques includes: (a) copying a credit card and in acquiring user's secret data (if needed), and (b) vendors deducting more money than agreed without holder's consent or awareness (Ojugo and Ekurume, 2020; Delamaire and Abdou, 2009; Dheepa and Dhanapal, 2009). When banks lose money due to credit card fraud, card holders partially (possibly entirely) pay for the losses through higher interest rates, higher membership fees, and reduced benefits. Hence, it is both the banks and holders' interest to reduce illegitimate use of credit cards and that is the reason why financial institutions started to do fraud detection (Stolfo et al, 2000; 1997; 1999; Marane, 2011).

1.1. Fraud Detection: An Overview

Fraud is an illegal act that involves obtaining an asset of value via targeted misrepresentation. Fraud can also be in the context of criminal charges such as theft, embezzlement, and larceny. It refers to a state where an unsuspecting

* Corresponding author.
E-mail address: ojugo.arnold@fupre.edu.ng (First Author)

victims relies heavily on the false claims of a material statement made by a criminal for benefits. Fraud has been notably recognized to be perpetuated by either persons inside an organization, or an external body to it (Okobah and Ojugo, 2018). Studies on fraud have shown that people do not originally set out to commit fraud. They exploited an opportunity, which in many cases, the first was by accident. Then realizing it had gone unnoticed (by the business, of which he/her who is the perpetrator was meant to be the one to notice) – then went at various other times. Investigators often note the 10-out-of-80-out-of-10 law. It states that 10percent of people will never commit fraud; 80percent of people will commit fraud under the right circumstances; and 10percent actively seek out opportunities for fraud (Duman and Ozcelik, 2011; Fawcett, 1997; Ghosh and Reiley, 1994). So, there is the constant need for vigilance for the 10percent who are out to get unsuspecting customers. There is also a need to try to protect the 80percent from making a mistake that could ruin their lives (Hand et al, 2000).

Fraud has always occurred as a combination of opportunity, pressure and rationalization (Bolton and Hand, 2002). Opportunities rippled across a task, can ensure the perpetrator feels less guilty of the act – and is likely pressured to commit the fraud. An opportunity is likely to occur when there are weaknesses in the internal control framework or when a person abuses a position of trust. For example, downsizing within a biz implies that there are fewer people to work and accomplish a task – and separation of duties no longer existed. Thus, the biz must re-engineer to bring about new application systems that changed the control framework, removing some of the key checks and balances. The pressures are usually financial in nature, but this is not always true. Unrealistic corporate targets can encourage a sales-person to commit fraud. The desire for revenge – to get back at the organization for some perceived wrong; or poor self-esteem - the need to be seen as the top salesman, at any cost; are also examples of non-financial pressures that can lead to fraud. Rationalization in the criminal's mind usually includes the belief that the activity is not criminal (Khin, 2019; Kim and Kim, 2002; Maes et al, 2019; Malek et al, 2008).

Interestingly, studies have shown that the removal of the pressure is not sufficient to stop an ongoing fraud. Also, the first act of fraud requires more rationalization than the second act, and so on. But, as it becomes easier to justify, the acts occur more often and the amounts involved increase in value. This means that, left alone, fraud will continue and the losses will only increase. Over time, people have had the notions that there is no such thing as a fraud that has reached maturity. Fraud, ultimately, is fed by greed, and greed is never satisfied (Ojugo and Eboka, 2018a; 2019; 2020b; Tohiyama et al, 2016) .

1.2. Motivation of The Study

Our study is motivated thus (Ojugo and Ekurume, 2020; Ojugo and Eboka, 2019; Stolfo et al, 2015):

1. Display of data on fraud detection is often limited as it is unwise to describe in great details over public domain – the adopted fraud detection technique as this will further equip adversaries with adequate data to evade detection.
2. Unavailability of datasets and censored results – makes fraud detection studies difficult to assess. Also, its dataset have been found to consist of ambiguities, impartial truth and noise that must be resolved via robust search in the bid to classify observations and expected values effectively.
3. Using another model to confirm the results of Ojugo and Ekurume (2020).
4. The non-reliability in performance with selecting network parameters, mismatched feats and anomalies has been attributed cum trigger by non-optimized data and lack of dataset. These have resulted in various network breaches and hacks that seek to evade detection. Eliminating noisy feats via an accurately optimized classifier will thus, foster a more efficient network fraud prediction.
5. Fraud persist even with the adoption of several classifiers available. Thus, we need to explore parameter selection. The significance of a unified model capable of addressing optimization problems and machine learning has not been explored, thus the need to explore such model unification.

To overcome these pitfalls, we implement a genetic algorithm trained modular neural network deep learning approach to detect fraud on credit card network using the KDD dataset.

2. Materials and Methods

These are explained under the following headings namely:

2.1. Data Gathering and Population Sampling

Dataset contains 33,000 records of credit card transactions. Each record has 23-fields and our nondisclosure agreement prohibits us from revealing database schema details and its data contents. But, we note that it is a common schema used by banks in Africa and Nigeria. It contains data that the banks deem important for identifying fraudulent transactions. The data was already classified into fraudulent or non-fraudulent classes, from which, 38.2% are fraud transactions (as in fig. 1). The sampled data is for a 24-month period. Note that the number of fraud records for each month varies, and the fraud percentages for each month are different from the actual real-world distribution.

2.2. Hybrid Memetic Algorithm Trained Modular Neural Network Ensemble

Our Modular Neural Network (MNN) as detailed in (Ghazale, 2018) is an improved deep learning neural network with learning that features an independent series of intermediary components – forming a module operating under certain architecture. These intermediary acts as bridge to receive individual network module output as input that helps compute the final output, which is resolved via a tangent activation function. MNN seeks to reduce large network into potentially, smaller, more managerial network (Aleskerov et al, 1997). It enhances efficiency via connected units that exponentially increases, as independent networks are added. While, this complicates the network structure, it improves computational efficiency with reduced computational time on individual task assigned to segmented modules, and tasks are executed in parallel with module re-organization to improve flexibility and network adaptability (Bolton and Hand, 2001).

The network enhances intelligence and increases time efficiency by reducing the network's learning time – achieved via an independent training algorithms applied at each module with training dataset implemented independently and more quickly. This makes the model more flexible, adaptable and robust as rules can be re-used independently at various networks. Re-usability of rules has been a tedious experienced with such large and complex networks. With appropriate data encoding and carefully selected feats – the network experiences improved performance, compartmentalization via removal of partitions of interfaces, greater flexibility and eliminates redundancy (Brause et al, 1999). Thus, our MNN architecture is one comprised of smaller network(s) – whose modularization allows for easy learning and understanding of data feats, grants model greater flexibility via task execution parallelism via compartmentalization, eases code reuse, flexibility and adaptability (Burge and Shawe-Taylor, 2001). MNN passes data via task decomposition and training modules via a multi-objective, multi-agent and multi-region support module that aids effective classification. MNN can be implemented using the multi-layered perceptron, adaptive resonance theory and self-organizing maps. The network is trained via either the supervised, unsupervised or reinforcement learning (Chiu and Tsai, 2004).

Our hybrid is divided into 3-components: (a) a supervised cultural genetic algorithm, (b) an unsupervised Kohenen neural network, and (c) the knowledgebase – as seen in figure 1.

The Supervised Cultural Genetic Algorithm (CGA): GA is inspired by Darwinian evolution of survival of fittest, it consists of a chosen population with potential solutions to specific task. Each potential optimal solution is found via four operators as in (Nigrini, 2011). Individuals with genes close to optimal, is said to be fit. Fitness function determines how close an individual is to optimal solution. Basic operators for GA includes (Ojugo et al, 2012; 2014):

a. Initialize takes input, encodes it for selection and computes fitness function to evaluate how close a solution is to its optimal. If solution is found, the solution is selected for crossover. Fitness function is the only part with knowledge of task.
b. Selection – Best fit solutions are selected to mate. The larger the number of selected, the better the chances of yielding fitter individuals. It continues until one is chosen as parents to new offspring. Selection ensures the fittest

individuals are chosen for mating but also allows for less fit individuals from the pool and the fittest to be selected. A selection that only mates the fittest is elitist and often leads to converging at local optima.

c. Crossover ensures the best fit genes are exchanged to yield a new, fitter pool. There are 2-crossover encoding types: (a) simple is used in binary coded pool with single- or multi-point crosses, and (b) arithmetic allows creation of new pools by adding individual's percentage to another.
d. Mutation alters chromosomes by changing its genes or its sequence, to ensure new pool converges to global minima. Model stops if optimal is found, or after a few runs – with new pools created (though computationally expensive), or if no better solution is found. Genes may change based on probability of mutation rate. Mutation improves the much needed diversity in reproduction.

Cultural GA as a variant, has some belief spaces defined as thus: (a) ***normative*** belief (has specific value ranges to a rule is bound), (b) ***domain*** belief (has data about task domain), (c) ***temporal*** belief (has data about events' space is available), and (d) ***spatial*** belief (has topographical data). In addition, an influence function mediates between belief space and the pool – to ensure and alter individuals in the pool to conform to belief space. CGA is chosen to yield a pool that does not violate its belief space and helps reduce number of possible individuals GA generates till an optimum is found (Ojugo and Otakore, 2018; Ojugo and Eboka, 2018b).

Unsupervised Kohonen Self-Organizing Neural Network is a grid-like feed-forward 2-layer network. Its first layer receives the initial input and transmits it unbound to second layer – which then provides competitive computation via the activation of its transfer function. Also, similarities among patterns are mapped into relations on the competitive layer. After training, the pattern relations are observed from this layer which are used as the result determination (Bolton and Hand, 2001; Brause et al, 1999; Murad and Pinkas, 1999; Feizi et al, 2019).

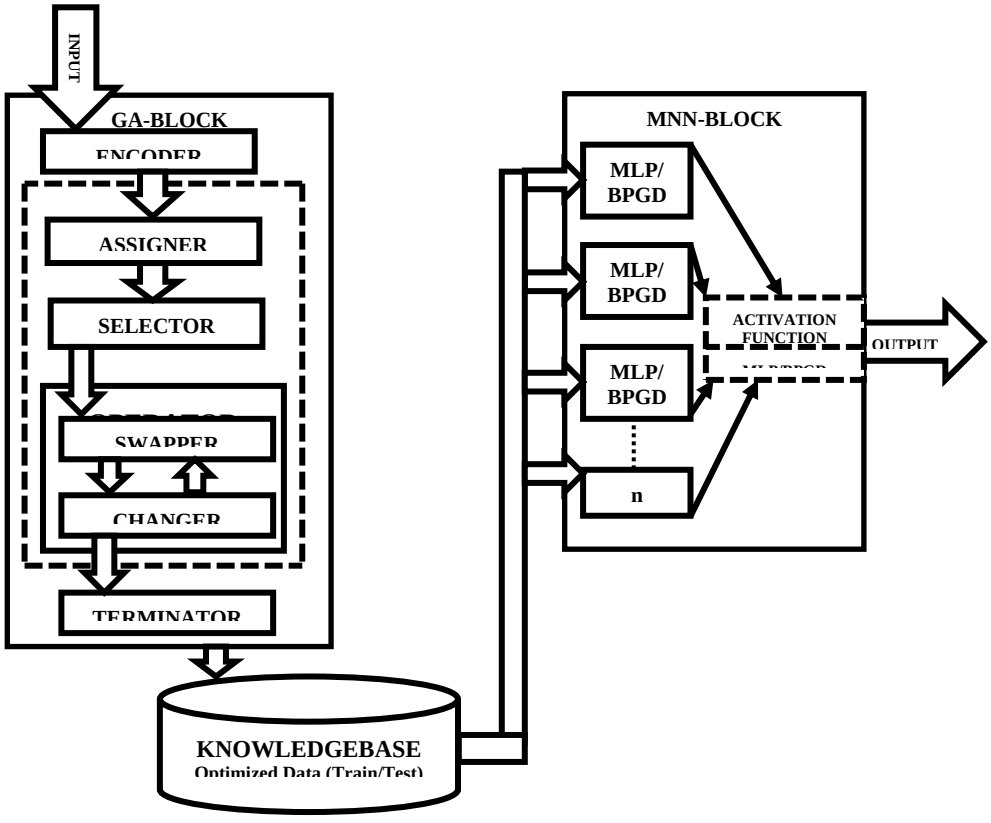

Fig. 1. Hybrid Learning Ensemble

2.3. Hybrid Memetic Algorithm Trained Modular Neural Network Ensemble

The experimental model is trained as thus:

a. The modular design as in figure 1 shows input is received and passed via GA-block (consisting of encoder, selector, swapper recombiner, swapper mutator, and lastly, belief terminator for CGA. Each phase performs and integral GA fundamental operator process to have the dataset trained. Upon completion of the optimization, the dataset feats are held within the knowledgebase as a special holding place for operational data during machine learning process (Ojugo and Yoro, 2021; Ojugo and Eboka, 2020).
b. The MNN block receives optimized rule dataset, grouped as successive labeled/unlabeled transactions instances as in fig 1 (Ojugo and Otakore, 2021; Aleksey and Alexander, 2016; Phua et al, 2004; 2007; Stolfo et al, 1997; 2000). With this, our classifier propagates IF-THEN transaction rule values of selected, predefined variables into the varying classes for detection. Rules are modeled as a production system with 4-components: (i) ***rule set*** containing in each rule, the pattern of how rule(s) and operation(s) are applied, (b) ***knowledgebase*** of transaction rule-set of (genuine and fraud classes) IF-THEN rules as selected data feats, (c) ***control*** strategy to specify the order in which the rules are compared to those in the knowledgebase to find a match and it seeks also a way to resolve conflicts that arise when several rules are matched at the same time, and (d) a rule ***applier***. The MNN provides a self-learning ability and acts as the principal component analyzer with rules optimized by CGA's crossover and mutation so that the trained model or network can effectively, autonomously classify transaction into both class types.
c. Last stage of the network acts as a decision support and recognition system, with predicted values (output) and the automatic update of rules-knowledgebase, as transactions are encountered with new data, and thus, classified.

The model is initialized with IF-THEN rules, whose fitness is computed. 30-rules are selected via ***tournament*** method. Model uses a 2-point crossover that helps it to learn the dynamic and non-linear feats in dataset. 1-to-30 rules randomly generated via Gaussian distribution and correspond to these crossover points are selected (all genes of a single parent). As new parents contribute to yield a new pool of rules with genes of various parents (applied via mutation) – the model selects 3-random genes. These are then allocated new random values (between 0 and 1) – which still conforms to model belief space. The random values yield a score, generated for each time-stamped transaction performed by an account holder as they perform prerequisite transactions on their credit-cards. Selection via MNN ensures that first 3-beliefs are met; mutation ensures the fourth belief is met. Its influence function determines how the number of mutations, how close a solution is and its impact on how algorithm is processed. Model stops when best rule has fitness that equals the suspicion score or is higher than computed fitness function of transactions by each cardholder (Stolfo and Prodromidis, 1999; Syeda et al, 2002; Vasta et al, 2005; Wheeler and Aitken, 2019; Minahan, 2013; Xu et al, 2007).

3. Result Findings and Discussion

3.1. Result Findings

Dataset is divided into a ratio of 40% for training and 60% for testing. The predictive capability of the model is identified via fifteen-sign abnormalities labelled among GA-optimized (fraud and normal) dataset. Fig. 2 shows fitness score as the encoder partitions dataset; While, Fig. 3 shows the graph of the swapper mutated genes.

The training phase uses a feedforward training algorithm and approach with an epoch training cycle for each phase until a finite epoch is obtained or an equilibrium is reached. We obtained an equilibrium at 40-epochs as in the training phase interface with the dots. Fig. 4 shows training phase interface; while Fig. 5 shows the test phase.

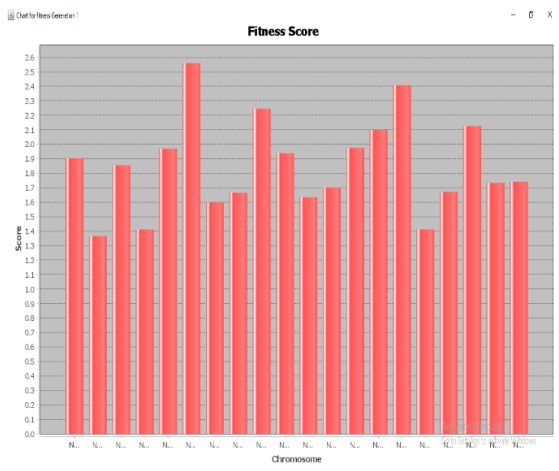

Fig. 2. Fitness Score graph of the GA-MNN model

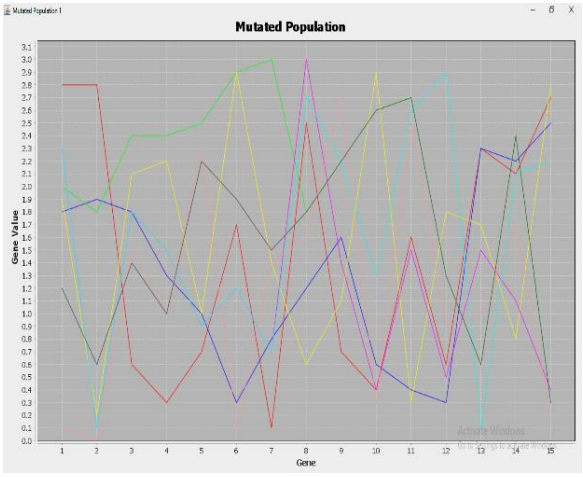

Fig. 3. Graph of Model's Swapper Mutated Genes

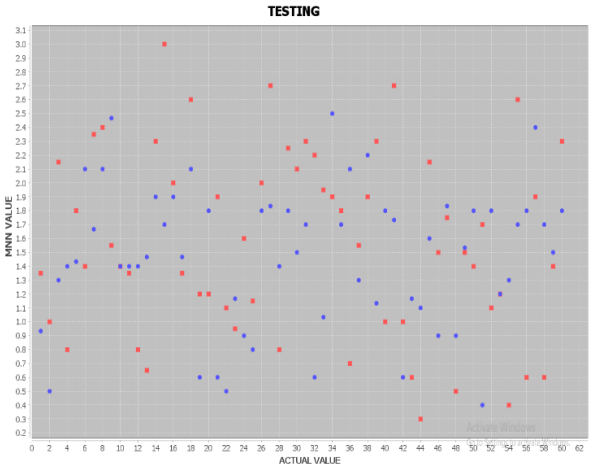

Fig. 4. Training Phase Result

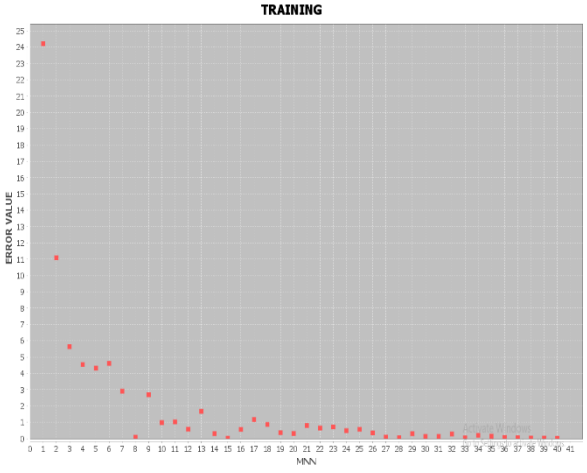

Fig. 5. Testing Phase Result

From our confusion matrix, we compute: (a) sensitivity is the measure of how likely the model will predict the presence of all fraudulent transaction attacks on the credit card when it is present, (b) specificity measures how likely model will detect the absence of fraud transactions when it is not present and not exhibited in the dataset, and (c) accuracy measures the proportion of true results seen as the degree of truth of a prediction. And given by Equations (1) – (3) respectively.

$$\text{Sensitivity} = TP / (TP + FN) \text{ – where } TP = 43, \text{ and } FN = 5 \quad (1)$$
$$\text{Thus, we have } [43 / (43 + 5) * 100] \rightarrow [\ 0.895 * 100] = 90\%.$$

$$\text{Specificity} = [TN / (TN + FP) * 100] \quad (2)$$
$$\text{We have that } [3 / (11 + 5) * 100] = 19\%.$$

$$\text{Accuracy} = [(TP+TN) / (TP+TN+FP+FN) * 100] \quad (3)$$
$$\text{We also have } [(43 + 3) / (43 + 3 + 11 + 5)] * 100 = 74\%$$

The model is found to have a sensitivity of 90%, specificity value of 19% and prediction accuracy of 74% (0.74) with a rate of improvement of 12-percent for data inclusion that were not originally used to train the model as in figure 8.

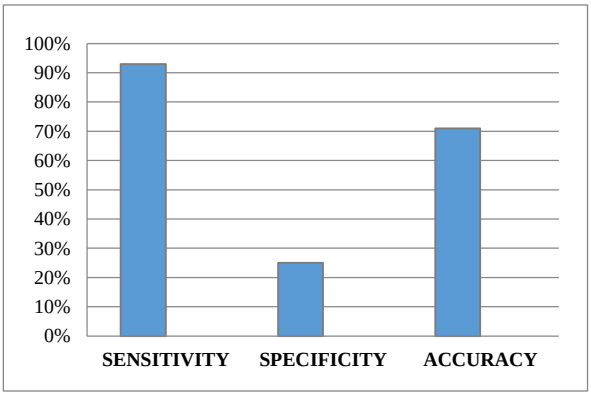

Fig. 8. Graph of Statistical Analyses for the Model

3.2. Discussion of Findings

The impact of fraud – have always required a concerted effort to detect such attack. Many of the detection techniques and schemes adopted filters the transaction request, analyzes them to decide compromised versus uncompromised – and, ultimately met out safety measures for further actions. Their performance is often hindered by the errors in classification of incorrectly from unidentified data-points that each of the resulting model generates. An ideal model correctly classifies all request packets with almost zero rates of false positive and true-negative errors (Ojugo et al, 2015a; Ojugo and Yoro, 2020; Tobiyama et al, 2016; Voosoghi et al, 2019).

Fraud schemes and techniques usually filters a credit card transaction request, analyses it to decide uncompromised and compromised packets, and met out safety measures for further actions. This performance can be hindered by the error rate for incorrectly classified and unidentified rules that the scheme/model generates. An ideal scheme will correctly classify all request and packets with almost zero error rates of false positive cum false negative – through trade-off between the number of false positives and false negatives.

4. Summary and Conclusion

The advent of the Internet as well as the ever-increasing adoption cum usage by users for e-commerce and/or online purchases has further advanced the ineffective vigilance of both seller/buyers seamlessly. Thus, criminals are always steps-ahead. And criminals will continue to leverage on social engineering methods – because human nature by default seeks to improve on their trust-level of technologies amongst other means that seek to improve their daily living. Thus, the need to protect clients via effective implementation of predictive fraud management and prevention systems aimed at keeping at bay techniques such as phishing, vishing, keystroke logging – to mention a few.

Acknowledgements

We acknowledge gratefully Tertiary Education Trust Fund (TetFund) for fully funding this research under the Institution Based Research (IBR) efforts. We, also appreciate our Vice Chancellor Prof. Akpofure Rim-Rukeh, who has continued in the strides of research as a way of life in the Federal University of Petroleum Resources, Effurun. Thank you for the vision. We acknowledge the contributions of Prof. S. Chiemeke for your push and cooperation. We express also our thanks to our colleagues in the Department of Computer Science at the Federal University of Petroleum Resources Effurun, for providing healthy competition, ideas and other materials necessary for this research.

References

Aleksey, A and Alexander, A., (2016). *Kohonen self-organizing map application to representative sample formation in training of MLP*, Available from [web]: http://researchgate.net/publication/303635615_Kohonen_selforganizing_map_application_to_representative_sample_formation_in_training_of_multilayer_perceptron

Aleskerov, E., B. Freisleben, B. Rao, (1997). *Cardwatch: A neural network based database Mining System for Credit Card Fraud Detection*, Proc. IEEE Computational Intelligence for Financial Eng., pp. 220-226

Bolton, R and Hand, D., (2001). *Unsupervised Profiling Methods for Fraud Detection*. Credit Scoring and Credit Control VII, 22, pp149-178

Bolton, R.J and Hand, D.J., (2002). *Statistical fraud detection: a review*, Statistical Science, 17(3), pp235-255, 2002

Brause, R., T. Langsdorf, M. Hepp, (1999). *Neural Data mining for credit card fraud detection*, Proc. IEEE Int. Conf. Tools with Artificial Intelligence, pp. 103-106, 1999.

Burge, P and Shawe-Taylor, J., (2001). *An Unsupervised Neural, Network Approach to Profiling the Behaviour of Mobile Phone, Users for Use in Fraud Detection*. J. of Parallel and Distributed Computing 61: 915–925

Chiu, C and Tsai, C., (2004). *A Web Services-Based Collaborative Scheme for credit card fraud detection*, Proc. IEEE Int. Conf. e-Technology, e-Commerce and e-Service, pp. 177-181

Delamaire, L and Abdou, H., (2009). *Credit card fraud and detection techniques: a review*, Banks and Bank Systems, 4(2), pp57-67

Dheepa, V and Dhanapal, R., (2009). *Analysis of Credit Card Fraud Detection Methods*, International Journal of Recent Trends in Engineering, 2(3), pp126-135.

Duman, E.M and Ozcelik, H., (2011). *Detecting credit card fraud by genetic algorithm and scatter search*. Expert Systems with Applications, 38: pp13057–13063

Fawcett, T., (1997). *AI Approaches to Fraud Detection and Risk Management*, AAAI Workshop. Technical Report WS-97-07, AAAI Press.

Ghazale, B., (2018). *Reasoning Using Modular Neural Network: an Innovative Solution to address question answering AI tasks*, Available from [web] https://towardsdatascience.com/reasoning-using-modular-neural-networks-f003cb6109a2?gi=7dbcd12eb7c, July 18, 2020

Ghosh, S and Reilly, D.L., (1994) *Credit Card Fraud Detection with a Neural-Network*, Proc. 27th Int. Conf. System Sciences: Information Systems: Decision Support and Knowledge-Based Systems, 3, pp.621-630

Hand, D.J., G. Blunt, M.G. Kelly, N.M. Adams, (2000). *Data mining for fun and profit*, Statistical Science, 15(2), pp. 111-131,

Khin, E.M., (2019). *Employing artificial intelligence to minimize internet fraud*. Int. Journal Cyber Society & Education, 2(1), pp.61-72, [web]: academic-journals.org/ojs2/index.php/IJCSE/article/viewFile/753/17

Kim, M.J and Kim, T.S., (2002). *A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection*, Proc. International Conf. Intelligent Data Eng. and Automated Learning, pp. 378-383, 2002

Maes, S., K. Tuyls, B. Vanschoenwinkel, B. Manderick, (2017). *Credit Card Fraud Detection*, Vrije Universiteit Brussel – Department of Computer Sci., Pleinlaan 2, B-1050, Belgium. [web]:personeel.unimaas.nl/k-tuyls/publications/papers/maenf02.pdf

Malek, W.M., K. Mayes, K. Markantonakis, (2008). *Fraud Detection and Prevention in Smart Card Based Environments Using Artificial Intelligence*. Int. Conf. CARDIS 2008, London, UK, September 8-11, 2008.

Marane, A., (2011). *Utilizing Visual Analysis for Fraud Detection, Understanding Link Analysis*, 2011, [web]: linkanalysisnow.com/2011/09/leveraging-visual-analytics-for.html

Minahan, T., (2013). *Fraud detection and prevention*. Available online and retrieved 2020 from [web]: nebhe.org/info/pdf/tdbank_breakfast/Fraud_Prevention_and_Detection.pdf

Murad, U and Pinkas, G. (1999). Unsupervised Profiling for Identifying Superimposed Fraud. Proc. of PKDD99.

Nigrini, M. (2011). Forensic Analytics: Methods and Techniques for Forensic Accounting Investigation. Hoboken, NJ: John Wiley & Sons Inc. ISBN 978-0-470-89046-2. Available from [online]: http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470890460.html

Ojugo, A.A and A.O. Eboka., (2018a). *Comparative evaluation for high intelligent performance adaptive model for spam phishing detection*, Digital Technology, Vol. 3, No.1: pp. 9-15, doi: 10.1269/dt-3-1-1, 2018

Ojugo, A.A and A.O. Eboka., (2018b). *Modeling solution of market basket associative rule mining approaches using deep neural net*, Digital Technology, 3(1), pp.1–8, doi: 10.12691/dt-3-1-1

Ojugo, A.A and A.O. Eboka., (2019). *Signature-based malware detection using approximate Boyer Moore string matching algorithm*, International Journal of Mathematical Sciences and Computing, 3(5): pp49-62, doi: 10.5815/ijmsc.2019.03.05

Ojugo, A.A and A.O. Eboka., (2020). *Memetic algorithm for short messaging service spam filter text normalization and semantic approach*, International Journal of Information & Communication Technology, 9(1), pp. 13 – 27, doi: 10.11591/ijict.v9i1.pp9-18

Ojugo, A.A and Eboka, A.O., (2020). *Empirical evaluation on comparative study of machine learning techniques in detection of DDoS*, Journal of Applied Science, Engineering, Technology & Education, 2(1), pp18–27, doi: 10.35877/454RI.asci2192

Ojugo, A.A and Ekurume, E., (2020). *Towards a more satisfied user framework through a dependable secured hybrid deep learning ensemble for detection of credit-card fraud*, Submitted to WARSE International Journal of Advanced Trends in Computer Science and Engineering

Ojugo, A.A and Otakore, D.O., (2018). *Improved early detection of gestational diabetes via intelligent classification models: a case of Niger Delta*, J. of Computer Science & Application, 6(2), pp. 82-90, doi: 10.12691/jcsa-6-2-5

Ojugo, A.A and Otakore, D.O., (2021). *Forging optimized Bayesian network model with selected parameter for detection of Coronavirus in Delta State Nigeria*, Journal of Applied Science, Engineering, Technology & Education, 3(1): pp37–45, doi: 10.35877/454RI.asci2163

Ojugo, A.A and Yoro, R.E., (2020). *Empirical solution for an optimized machine learning framework for anomaly-based network intrusion detection*, Technology Report of Kansai University, TRKU-13-08-2020-10996, 62(10): pp6353-6364, Available on [web]: https://www.kansaiuniversityreports.com/article/empirical-solution-for-an-optimized-machine-learning-framework-for-anomaly-based-network-intrusion-detection

Ojugo, A.A and Yoro, R.E., (2021). *Forging a deep learning neural network intrusion detection framework to curb distributed denial of service attack*, International Journal of Electronics and Computer Engineering, Vol. 11, No. 2, pp 128-138

Ojugo, A.A., Allenotor, D. D.A. Oyemade., O. Longe., C.N. Anujeonye., (2015a). *Comparative stochastic study for credit-card fraud detection models*, African Journal of Computing and ICT, 8(1-2): pp15 –24, 2015.

Ojugo, A.A., Eboka, A., R.E. Yoro., M.O. Yerokun., F.N. Efozia., (2015b). *Framework design for statistical fraud detection*, Mathematics and Computers in Sciences and Engineering, 50: 176-182, ISBN: 976-1-61804-327-6.

Ojugo, A.A., Ben-Iwhiwhu, E., O.D. Kekeje., M. Yerokun., I. Iyawah., (2014). *Malware propagation on time varying networks: comparative study,* International Journal of Modern Education and Computer Science, 6(8), pp. 25-33, doi: 10.5815/ijmecs.2014.08.04

Okobah, I.P and Ojugo, A.A., (2018). *Evolutionary memetic models for malware intrusion detection: a comparative quest for computational solution and convergence,* IJCAOnline International Journal of Computing Application. 179(39), pp34–43

Phua, C., D. Alahakoon, V. Lee, (2004). *Minority Report in fraud detection: classification of skewed data*, ACM SIGKDD Explorations Newsletter, 6(1), pp. 50-59, 2004

Phua, C., V. Lee, K. Smith, R. Gayler, (2007). *A comprehensive survey of data mining-based fraud detection research*, Available online and retrieved from [web]: www.bsys.monash.edu.au/people/cphua/ .

Stolfo, S. J., Fan, D. W., Lee, W., Prodromidis, A and Chan, P. K. (2000). *Cost-Based Modeling for Fraud and intrusion detection: results from the JAM Project*, In Proc. DARPA Information Survivability Conf. and Exposition, vol. 2, pp. 130-144.

Stolfo, S.J and Prodromidis, A.L, (1999). *Agent-based distributed learning applied to fraud detection*, Technical Report CUCS-014-99, Columbia University, 1999

Stolfo, S.J., Fan, D.W., W. Lee, L.K. Prodromidis, P.K. Chan., (1997). *Credit card fraud detection using meta-learning: issues and initial results,* Proc. AAAI Workshop AI Methods in Fraud and Risk Management, pp. 83-90

Syeda, M., Zhang, Y. Q. and Pan, Y. (2002). *Parallel Granular Networks for Fast Credit Card Fraud Detection*, Proc. IEEE Int'l Conf. Fuzzy Systems, pp. 572-577.

Tobiyama, S., Y. Yamaguchi., et al., (2016). *Malware detection with deep neural network using process behaviour, IEEE 40th Annual Computer Software and Applications Conf.,* Vol. 2, pp. 577-582, 2016

Vatsa, V., Sural, S. and Majumdar, A. K. (2005). *A game-theoretic approach to credit card fraud detection*, In. Proc. of Int. Conf. Information Systems Security, pp. 263-276.

Voosoghi, R.B., Ghaffari, M and Razin, R., (2019). *Evaluation of the Efficiency of Adaptive Neuro Fuzzy Inference System in modeling of the Ionosphere Total Electron Content Time Series Case Study: Tehran Permanent GPS Station*, Journal of Geomatics Science and Tech., Vol. 8, no.4, Pp. 109-119, 2019

Wheeler, R and Aitken, S. (2019). *Multiple Algorithms for Fraud Detection Artificial intelligence Applications*, The University of Edinburg, Scotland, pp. 1-12, [web]: http://home.cc.gatech.edu/ccl/uploads/45/multiple-algorithms-for-fraud.pdf

Xu, J., Sung, A. H. & Liu, Q. (2007). *Behaviour Mining for Fraud Detection*, Journal of Research and Practice in Information Technology. 39(1), pp. 3–18