Empirical Evaluation of Hybrid Cultural Genetic Algorithm Trained Modular Neural Network Ensemble for Credit-Card Fraud Detection

Article · March 2023

DOI: 10.35629/5252-050315161524

2 authors:

Fidelis Aghware
University of Delta, Agbor, Delta State, Nigeria
23 PUBLICATIONS **287** CITATIONS
SEE PROFILE

Bridget Malasowe
University of Delta Agbor
12 PUBLICATIONS **161** CITATIONS
SEE PROFILE

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 1516-1524 www.ijaem.net ISSN: 2395-5252

Empirical Evaluation of Hybrid Cultural Genetic Algorithm Trained Modular Neural Network Ensemble for Credit-Card Fraud Detection

Fidelis Obukohwo Aghware[a,*], Bridget Ogheneovo Malasowe[b]

Department of Computer Science, University of Delta, Agbor, Delta State 32001, Nigeria,
[b]Department of Computer Science, University of Delta, Agbor, Delta State 32001, Nigeria,

Date of Submission: 20-03-2023 Date of Acceptance: 30-03-2023

ABSTRACT
The increasing need for e-commerce, online marketing, and the ineffective vigilance of sellers/buyers often constitutes the fact that criminals are steps ahead of biz owners and users of these products – at all times. Pre-empting fraud before 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 procedures to whollyrestraint fraud. The routine of smart systems,though, is on the upsurge for fraud recognition – nevertheless, it is still demonstratingfutile. Thus, the need to design a predictive intelligent system to monitor, detect and prevent fraudulent activities – especially in regards to credit/smart card transactions. The study suggests a spectral-clustering amalgam of aninherentalgorithm-trainedintegrated neural system to perceive fraud in credit card businesses. The hybrid collaborative seeks to equip credit-card operators with a scheme and procedure whose information will selflesslyspot frauds on credit cards. Consequently, the model excellentlydistinguishesbetween benign and genuine credit card dealings with a prototypical accuracy of 74%.

Keywords: Genetic Algorithm, Trained Neural Network, Credit card, Fraud detection, Hybrid Culture.

I. INTRODUCTION

Fraud is criminal conduct that includes getting a valuable asset via deliberate deception. Fraud can also refer to criminal crimes including embezzlement, larceny, and theft. It denotes where agulliblevictim relies profoundly on the false claims of a material statement made by a criminal for benefits. Information security is the act of preventing unwanted access to your data. It covers data privacy and includes operations such as preserving data against unlawful disclosure, destruction, disturbance, or change (Aghware and Egbuna, 2012). The number of individuals utilising the network and the internet to exchange information is rapidly increasing; this has resulted in a decrease in the strength of their transactions through electronic networks. Information security is a major issue that simply cannot be disregarded at this time, thus a model for successful information transfer and exchange through electronic networks must be developed (Aghware & Egbuna, 2012).According to fraud studies, people do not intentionally commit fraud. They took advantage of an opportunity that, in many cases, arose by chance. Then realizing it had gone unnoticed (by the business, of which he/her whom the perpetrator was meant to be the one to notice) went at various other times. Investigators often note the 10-out-of-80-out-of-10 law. It states that 10 percent of people will never commit fraud; 80 percent of people will commit fraud under the right circumstances; and 10 percent actively seek out opportunities for fraud (Duman and Ozcelik, 2011). So, there is a constant need for vigilance for the 10 percentthat targetgulliblecliente le. There is also a need to try to keep the other 80% from making the wrong decision that will wreck their lives.

There is a no bigger concern than a lack of safety in a specific infrastructure interdependency that was initially implemented to increase efficiency and performance. This can result in material damage, information loss, unauthorised access to information, and so

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 1516-1524 www.ijaem.net ISSN: 2395-5252

forth,Obukohwo(2011). 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 where there are flaws in the inside control architecture or when someone compromises a position of trust, is more likely to happen. Downsizing inside a business, for example, suggests the existence of fewer individuals to work with and achieve a task - and division of roles no longer exists.Consequently, the businessessentially muststrategize to introduce newerapplications that could change the control mechanism of eradicatingmajorbalances of power. It is an opinion that theburdens are typicallymonetary, but this is not always true. Impracticable corporate aimsat encouragingsalespeople to oblige fraud. The craving for retribution – to recuperatefromsociety 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 felon'scognizancetypicallyconsists of the credence that the actionsare non-criminal (Khin, 2019; Maes et al, 2019; Malek et al, 2008) as seen in figures 1 and 2 respectively.

Fraud Detection: An Overview

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. Since crimes are sometimes not found until many weeks later, credit cards are frequently targeted. (Ojugo and Eboka, 2020a; Ojugo et al, 2015a; 2015b; Aghware and Egbuna, 2012). Effective card fraud schemes include (a) duplicating a credit card and (if necessary) obtaining the user's confidential information, and (b) having merchants deduct more money than agreed upon without the cardholder's knowledge or approval (Aghware and Egbuna, 2012; Dheepa and Dhanapal, 2009; Delamaire and Abdou, 2009; Ojugo and Ekurume, 2020). As nothing more than a consequence of credit card theft, financial institutions may be required to cover part (perhaps all) of the expenses using higher interest rates, increased dues, and fewer privileges. As a result, minimising illegal credit card usage benefits both of the institution and the cardholder, which is the reason banking institutions began to utilise fraud detection software (Aghware and Egbuna, 2012; Marane, 2011).

It's interesting to be mindful that relieving pressure alone is insufficient to halt an ongoing scam. Additionally, the first deception requires more justification than the second, and so forth. However, while the activities are simpler to defend, they happen more frequently and involve larger sums of money. This indicates that if fraud is allowed to continue, the losses will only grow. People have come to believe that there is no such thing as a mature scam throughout time. Ultimately, greed is what fuels fraud since it can never be satiated (Ojugo and Eboka, 2018a; 2019; 2020b; Tohiyama et al, 2016; Aghware and Egbuna, 2012).

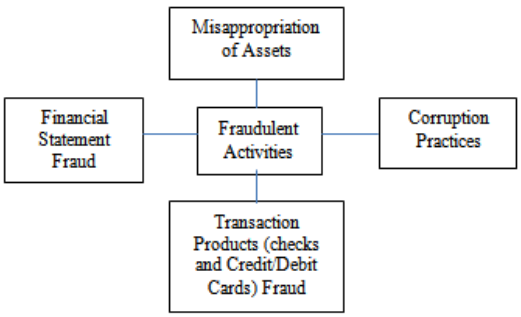


Fig. 1: Types of Fraud and Fraudulent Activities

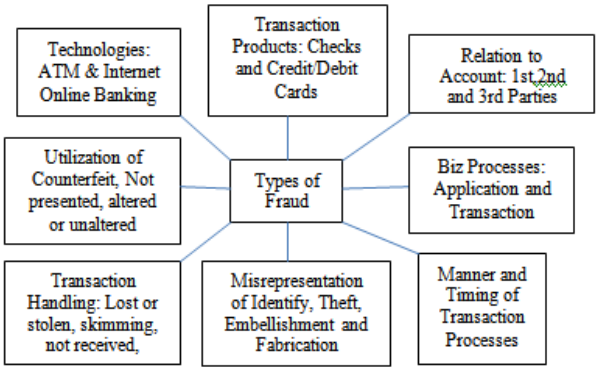


Fig. 2: Forms of Transaction Product Fraud (Delamaire et al, 2009)

Motivation of The Study

The following are the problem statements:

1. Since it is dangerous to disclose in the public domain, the exchange of ideas in fraud detection is frequently limited (fraud detection techniques in great detail). Additionally, it will provide invaders with the necessary knowledge to avoid discovery. As a result, we use the same heuristics and statistical fraud detection technique as in Section II.
2. It is crucial and necessary for the early and accurate identification of fraud due to the complex-chaotic nature of fraud via malware and the variety of problems to a network, including backdoors for other crimes. As well-monitored and managed network diagnosis

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 1516-1524 www.ijaem.net ISSN: 2395-5252

frequently produces equivocal answers for unknown inputs, increasing the likelihood of false-positive and false-negative results, it is somewhat redundant and time-wasting. The understudied statistical models have been successfully applied and discovered to successfully categorize transactions by unsupervised predictive calculation of suspicion scores, accomplished through various methods as in Section III.

3. It is challenging to evaluate fraud detection systems and research due to the lack of fraud datasets and their filtered results. To properly categorize observations and predicted values as in Sections II and III, the dataset also contains ambiguities, imprecision, noise, and impartial truth that must be addressed using a robust search.
4. The proposed techniques employ hill-climbing methods, which are often limited by speed that traps their solution at local maxima. This is resolved via hybridization of the statistical methods as in Sections II and III. Also, the search for optima via evolutionary heuristics is often cumbersome and no one techniqueproducesimproved optima than hybrids. How will the proposed models resolve the statistical dependency imposed on them via hybridization? This is resolved via discretization and data encoding as in Section II/IIIto avoid overtraining and over-fitting of the model. The model resolves these as it seeks to find the underlying probability of the data accomplishment(s) of concern via proper parameter selection in preprocessing and data encoding to avoid model over-parameterization (decided in section III).
5. A few versions intention at a single suspicion score to globally classify statistical fraud. studies display, however, that a few cases may be a result of authentic-negatives and fake-positives scores as resolved in section III. To triumph over these pitfalls, we implement a genetic algorithm trained modular neural network deep learning approach to locate fraud on credit score card networks through the use of the KDD dataset.

II. MATERIALS AND METHODS

Data Gathering and Population Sampling

The 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 fraudulent transactions. The sampled data is for 24 months. 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.

Trained Hybrid Memetic Algorithm Ensemble of Modular Neural Communities

The Modular Neural Network (MNN), as specified (Ghazale, 2018), is a step advance in deep learning of neural networks learning that functions as unbiased collection of intermediary components - constituting a module operating beneath the specific structure, which are intermediaries that act as a bridge to obtain character community module output as input that allows calculating the final result, which is resolved via tangent activation MNN's goal is to break down big networks into smaller and more manageable networks. It improves efficiency through connected devices that grow rapidly as impartial networks are built. Whereas this impedes the network structure, it greatly enhances algorithmic productivity by minimizing processor complexity at the man or woman struggle assigned to segmented modules. Additionally, expectations are conducted contemporaneously with component re-corporation to increase flexibility and neighbourhood ability to adapt (Bolton and Hand, 2001). The network enhances intelligence and time efficiency by reducing the network's learning time, which is accomplished by independent training algorithms used at every component with the training examples implemented autonomously and more rapidly. Because rules may be reused independently across networks, the model becomes more flexible, adaptive, and resilient. With such big and intricate networks, reusing procedures has been a laborious experience. With adequate data coding and carefully chosen achievements, the network enjoys significant enhancement, sequestration via the elimination of partitions at gateways, more flexibility, and redundancy elimination.For this reason, our MNN structure is one produced from the smaller network(s) – whose modularization allows for easily getting to know and know-how of records feats, grants the model greater flexibility thru mission execution parallelism through compartmentalization, eases code reuse, flexibility, and flexibility. MNN passes information thru venture decomposition and education modules through a multi-goal, multi-agent, and multi-region help module that aids

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 1516-1524 www.ijaem.net ISSN: 2395-5252

powerful class. MNN may be carried out with the use of the multi-layered perceptron, adaptive resonance principle, and self-organizing maps. The community is skilled via both supervised and unsupervised mastering, as well as reinforced accomplishing (Chiu and Tsai, 2004).
Our hybrid is made up of three parts: A guided cultural genetic algorithm, an unsupervised Kohonen neural community, as well as a knowledgebase – as visible in figure 3.

The Supervised Cultural Genetic Algorithm (CGA): GA is inspired by Darwinian evolution and comprises of a selected population with viable answers to a certain objective. Four operators are used to find each probable optimum solution (Nigrini, 2011). Fit people have genes that are near to optimum. The applicability of a solution governs how near a someone is to finding the best answer. Basic GA operators are as follows (Ojugo et al., 2014; 2012):

a. Initiate receives information, encrypts it for selecting, and evaluates an objective function to determine how near to optimum a solution is. If a solution is discovered, it is chosen for crossing. The fitness function is aware of the job.

b. Selection: Just the finest suit solutions are paired.
The greater the number of possibilities, the greater the likelihood of producing more fit individuals. It will persist until a figure is picked to represent fresh progenies. Choice ensures the fittest individuals are selected for mating but additionally allows for fewer healthy people from the pool and the fittest to be decided on. a spread that only pals the fittest is elitist and regularly results in converging at neighborhood's optima.

c. Crossover guarantees that pleasant healthy genes are swapped to create a new organism - healthier pool. There are 2-crossover encoding kinds: (a) easy is used in binary coded swimming pools with single- or multi-factor crosses, and (b) arithmetic permits the advent of recent swimming pools with the aid of adding a man or woman's percentage to some other.

d. Mutation modifies chromosomes by altering their genes or sequence in order for the new pool to converge to the minimization problem. If the ideal solution is found after a few iterations, with new pools generated (albeit computationally costly), or if no superior solution is found, the model quits. Genes can alter depending on the likelihood of mutation rates. Mutation increases the much-needed variation in reproduction.

Enlightening GA as a variation has some perception spaces described as consequences: (a) normative notion (has unique cost tiers to a statute is certain), (b) area notion (has facts about task area), (c) temporal belief (has information about potential activity locations) and (d) spatially awareness (has topographical information). Consequently, an influence function acts as a go-between between the idea area and the pool, assuring and controlling that persons inside the pool comply to the concept space. CGA is selected to develop a pool that does not contradict its idea area and to help reduce the number of feasible persons created by GA till the best is discovered (Ojugo and Eboka, 2018b).

Kohonen, unsupervised personality neural network is a two-layer, grid-like network. Its first layer takes the input image and sends it unrestrained to the two layers, which performs competitive computing by activating its transfer function. Similarly, similarities between patterns are translated into competitive layer interactions. Following training, the sampling relations are calculated using this layer, which is employed due to the result devotion (Feizi et al., 2019).

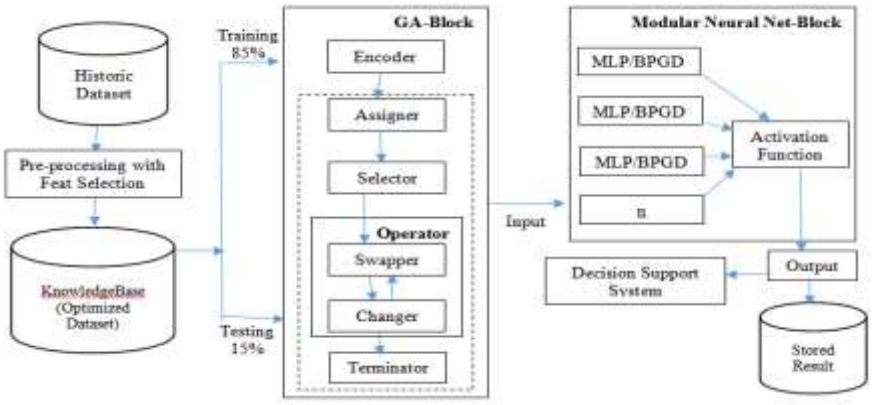


Figure 3.Hybrid Learning Ensemble

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 1461-1467www.ijaem.net ISSN: 2395-5252

Hybridized Ensemble Memetic Algorithm of Trained Modular Neural Networks

This is how the experimental modelis trained:

a. According to the modular architecture depicted in Figure 1, input is received and sent via a GA-block, which consists of an encoder, selectors, swapper recombiner, swapper dynamic amplification, and, lastly, a belief finisher for CGA. Each stage in training the dataset performs a crucial GA fundamental operator process. During machine learning process, the dataset feats are retained in the centralized repository as a specific reservoir for operational data until the improvement is accomplished (Ojugo and Eboka, 2020).

b. The MNN block gets an optimised rule dataset, which is organised as a series of labeled/unlabeled transaction instances. as in fig 1 (Ojugo and Otakore, 2021; Aleksey and Alexander, 2016). With this, our classifier propagates IF-THEN transaction rule values of selected, predefined variables into varying classes for detection. Rules are modeled as a 4-component production system: the order in which each rule and its associated operations are applied I (b) transaction rule-set knowledge base (genuine and fraud classes) As chosen data feats, IF-THEN rules (c) control strategy aims to resolve conflicts that occur when several rules are matched simultaneously and specifies the order in which the rules are compared to those in the knowledgebase to establish a match,and (d) a rule applier. The trained model or network may efficiently and independently categorize transactions into both class types using its self-learning capabilities as a principal component analyzer and rules optimized by crossover and mutation in CGA.

c. The network's final step operates as a decision-support and recognition system, with anticipated values (output) and the automated updating of the rules-knowledgebase when transactions are met with fresh data and subsequently categorized.

IF-THEN occasionsparameters for the model, and their fitness is evaluated. The tournament technique is used to choose the 30 rules. The model employs a 2-point crossover to aid in learning the dataset's dynamic and non-linear achievements. One to thirty rules are chosen at random using a Gaussian distribution and correspond to these crossover places (all genes of a single parent). The model chooses three random genes as new parents contribute to producing a fresh pool of rules with genes from different parents (applied via mutation). Then, fresh random values (between 0 and 1) are assigned to them, keeping adhering to the model belief space.For each time-stamped transaction made by an account holder as they make required purchases on their credit cards, the random values produce a score. The first three beliefs are ensured through selection via MNN, while the fourth belief is ensured by mutation. Its effect function defines how many mutations there will be, how near a solution will be, and how it will affect how the algorithm is run. When the best rule's fitness matches the suspicion score or exceeds the calculated fitness function of each cardholder's transactions, the model pauses (Wheeler and Aitken, 2019; Minahan, 2013)

III. RESULTS, FINDINGS, AND DISCUSSION

Result Findings

40% of the dataset is used for training, while 60% is used for testing. Through the labeling of fifteen-sign anomalies in GA-optimized (fraud and normal) datasets, the model's predictive power is discovered. Figure 4 and Figure 5 depict the fitness score as the encoder splits the dataset and the swapper-mutated gene network, respectively.

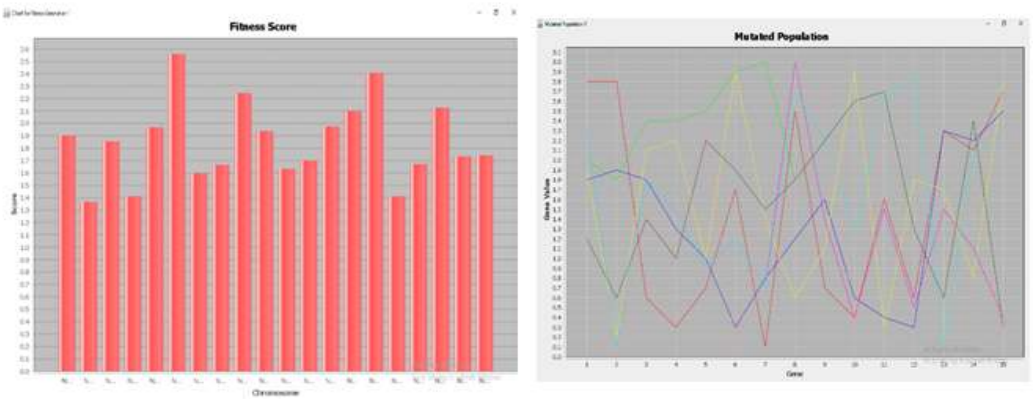
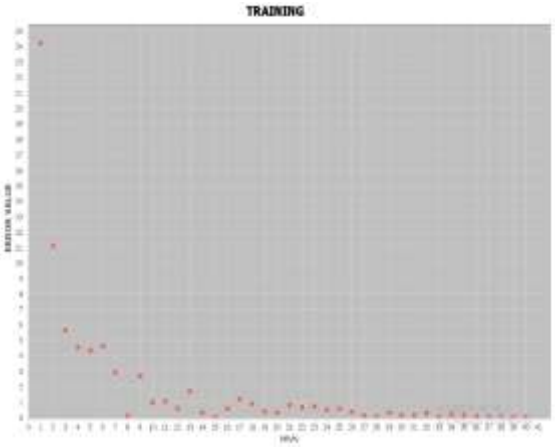


Figure 4. Fitness Score graph of the GA-MNN model Figure 5. Graph of Model's Swapper Mutated Genes

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 1461-1467www.ijaem.net ISSN: 2395-5252

Until a limited epoch is achieved or equilibrium is reached, the training phase employs a feedforward training method and approach with an epoch training cycle for each phase. At 40 epochs, as in the training phase contact with the dots, we achieved an equilibrium. Figures 6 and 7 depict the interface for the training phase and the test phase, respectively.



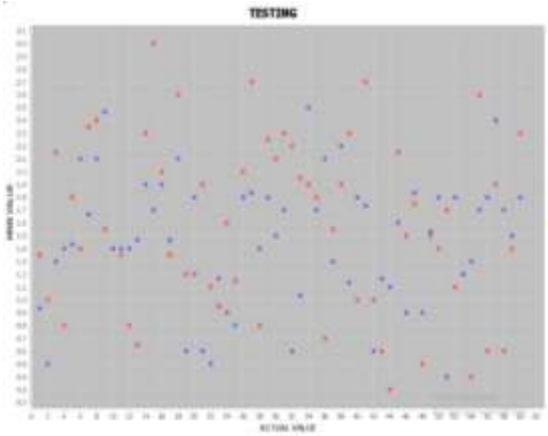


Figure 6. Training Phase Result Figure 7. Testing Phase Result

We evaluate the following from our confusion matrix: (a) sensitivity, which is a measure of how likely the model is to predict the presence of all credit card fraud attacks when they occur; (b) specificity, which is a measure of how likely the model is to detect the absence of credit card fraud attacks when they occur and are not exhibited in the dataset; and (c) accuracy, which is a measure of the percentage of true results viewed as the degree of truth of a prediction. and as shown by Equations (1) through (3).

$$\text{Sensitivity} = \frac{(\text{TP} + \text{FN})}{\text{TP}} (1)$$

$$\text{Thus, we have TP} = 43, \text{and FN} = 5$$

Thus, we have [43 / (43 + 5) * 100] → [0.895 * 100] = 90%.

Specificity = [TN / (TN + FP) * 100] (2)

We have that [3 / (11 + 5) * 100] = 19%.

Accuracy = [(TP+TN) / (TP+TN+FP+FN) * 100] (3)

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 was not originally used to train the model as in figure 8.

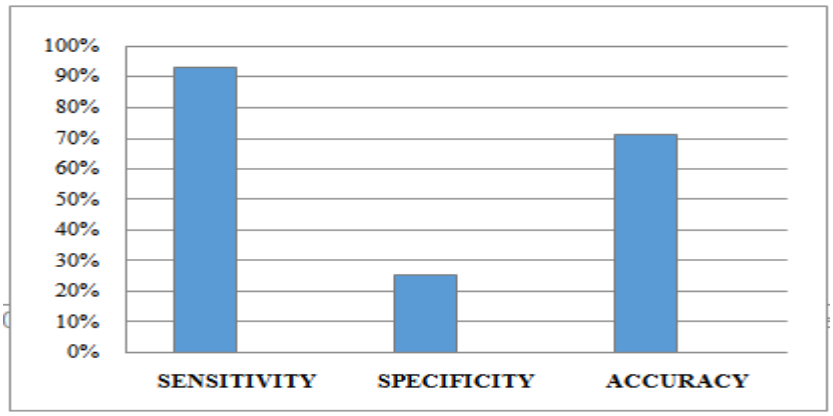


Figure 8. Graph of Statistical Analyses for the Model

IV. DISCUSSION OF FINDINGS

The impact of fraud – has always required a concerted effort to detect such attacks. Many of the detection techniques and schemes adopted to filter the transaction request, analyze them to decide compromised versus uncompromised – and, ultimately met safety measures for further actions. Their performance is often hindered by the errors in the classification of incorrectly unidentified data points that each of the resulting models generates. An ideal model correctly classifies all request packets with almost zero rates of false positive and true-negative errors (Ojugo et al, 2015a; Tobiyama et al, 2016; Voosoghi et al, 2019; Aghware and Egbuna, 2012).

Fraud schemes and techniques usually filter a credit card transaction request, analyze it to decide on uncompromised and compromised packets, and met 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 requestsDelivering packets with near nil false positive/false negative error rates by a trade-off between the number of false positives and false negatives.

V. SUMMARY AND CONCLUSION

The proliferation of the Internet, along with users' escalating acceptance and utilization of e-shopping and/or e-commerce, has furthered the ineffectual vigilance of both sellers and purchasers. Criminals are thus perpetually one step ahead. Criminals will also keep using social engineering techniques since, by nature, people want to have more confidence in technology and other means of improving their everyday lives. Thus, it is important to safeguard clients by putting into place predictive fraud management and prevention systems that are successful in thwarting methods like phishing, vishing, and keystroke tracking, to name a few.

REFERENCES

[1]. Aghware, Fidelis O, & Egbuna, Emeka O. (2012). People Centred Information Security Model for Corporate Nigeria. Paper presented at the Proceedings of the World Congress on Engineering and Computer Science.

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

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

[4]. 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

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

[6]. 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

[7]. 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,

[8]. 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

[9]. 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

[10]. 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.

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

[12]. 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

[13]. 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

[14]. Obukohwo, A. F. (2011). Computer-Based Infrastructure Sector Interdependencies and Security Implications. Int.J.Communications,NetworkandSystemSciences,2011,4,735-738

[15]. doi:10.4236/ijcns.2011.411090PublishedOnlineNovember2011(http://www.SciRP.org/journal/ijcns)

[16]. Ojugo, A.A and A.O. Eboka., (2018a). Comparative evaluation for highly 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

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

[18]. 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

[19]. Ojugo, A.A and A.O. Eboka., (2020). A 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

[20]. Ojugo, A.A and Eboka, A.O., (2020). Empirical evaluation on a 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

[21]. Ojugo, A.A and Eboka, A.O., (2021). Empirical Bayesian network to improve service delivery and performance dependability on a campus network, International Journal of Artificial Intelligence, 10(3), pp623-635

[22]. Ojugo, A.A and Oyemade, D.A., (2021) Boyer Moore string-match framework for a hybrid short messaging service spam filtering technique, IAES International Journal Artificial Intelligence, 10(3): pp519-527

[23]. 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

[24]. Ojugo, A.A and Otakore, D.O., (2021). Forging optimized Bayesian network model with a 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

[25]. 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.

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

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

[28]. 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

[29]. 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

[30]. 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.

[31]. 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.

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

[33]. 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.

[34]. 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

[35]. 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

[36]. 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