Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal
Volume 10, No 2, 2024 Series

Enhanced Anomaly-Based Detection of the Distributed Denial of Service Attack using Modular Memetic Behavioral Analysis

[1]Sulu, Gbenga Ayanshola., [2]Akazue, Maureen Ifeanyi., [3]Edje, Abel Efetobore
[1,2,3]Department of Computer Science, Delta State University, Abraka, Nigeria;
E-mails: sulu_gbenga@gmail.com; akazue@delsu.edu.ng; edje.abel@delsu.edu.ng,

ABSTRACT
The Internet's popularity has proven to be an effective mode for data dissemination, and also advance the proliferation of adversaries whose exploits network for personal gain via unauthorized access that compromises a user device. Adversaries have achieved such feats via socially-engineered, subterfuge schemes – some of which deny users of network resources. These distributed denial of service (DDoS) attacks are carefully crafted to impact a large magnitude with the capability to wreak havoc at high levels of network infrastructures. This study posits a deep learning approach to distinguish between benign exchange of data and malicious attacks from data traffic. With benchmark ensemble such as XGBoost, Random Forest and Decision Tree – the results shows our proposed ensemble yields F1 of 0.9945, and outperforms XGBoost, RF and DT (with F1 of 0.9925, 0.9881 and 0.9805 respectively); And with an Accuracy of 0.9984 to outperform XGBoost, RF and DT (with 0.9981, 0.9964 and 0.9815 respectively). The proposed ensemble incorrectly classified only 283-instances with 13,418 correctly classified test instances with a 99.84% accuracy. Result shows our use of the deep learning memetic model effectively differentiate between genuine and malicious packets via anomaly-based detection.

Keywords: Memetic Algorithm, Random Forest, XGBoost, feature selection, imbalanced dataset

Aims Research Journal Reference Format:
Sulu, G.A., Akazue, M.I., Edje, A.E., (2024): Enhancing computer network intrusion detection using the network behaviour analysis technique: a pilot study. Advances in Multidisciplinary and Scientific Research Journal Vol. 10. No. 2. Pp 125-142www.isteams.net/aimsjournal. dx.doi.org/10.22624/AIMS/V10N2P11

1. INTRODUCTION

Information has since been known to be both critical, imperative and crucial to aid effective decision making in businesses [1]. This is so because, it improves performance, and strategies implementation to guide better monetization policies and portfolios for such organization. Information has also become both an integral foundation and fundamental requirement cum basis for today's complex culture [2], [3]. The field of informatics is continually advanced with the constant evolution vis-à-vis the integration of the information and communication technology (ICT) tools. This ease of adoption cum integration can be attributed to its ubiquitous nature, low-cost, ease of use, mobility, portability and user-trust [4]–[6] – all of which does continue to advance the popularity and adoption ease of ICTs. This growth has equally attracted intrusion activities from adversaries [7]–[9] whom for their personal gains, seek to exploit the device of unsuspecting users. They achieve these by exploring unsolicited adverts, phishing techniques and malware distribution to exploit user devices – as its rise today, has become and proven to be a great concern to both businesses. security experts, individuals and organizations [10]–[12].

Human capacity development is poised at promoting greater productivity. Even with digital revolution as experienced today, its impact (positively and negatively) on both human and machine connectivity via the adoption of ICT systems – has also evolved businesses over-time; And these evolutions, have also experienced both internal and external assaults from adversaries often referred to as hackers [13]–[15]. Such compromises of unsuspecting user targeted-devices with adversarial tools designed to evade security measures, obscure data privacy and weaken network infrastructure have become a great concern with negative impacts on the adoption of technology [16]–[18]. Examples of socially-engineered intrusive actions include data stealing, tamper and corruption, service denial and outage, phishing, pharming, spamming, stack and buffer overflow, etc – to mention a few. Reports continue to advance that concerted efforts in this war against intrusion continues to usher in great procedures, tools and modes to fight and stay the course of this war as well as advance that while it is a consistent probe, studies have successfully proven that intrusion threats, breaches and attacks to networks infrastructures, user devices and businesses can never be over-emphasized [19]–[21].

The rise in rate of these breaches are as broad in range of the innovative technology [22] – leading to denial of services attack, etc [23]. It is necessary to stop as close to the source and as fast, any DDoS breach. These breaches on networked resources are careful coordinated and targets user system via a number of compromised systems [24]–[26]. DDoS threatens network infrastructure since by design, they are crafted to target a large cluster of user devices; And in turn, wreaks havoc if compromised at various levels [27]–[29].

The ease in propagation of these attacks, is become of great concern such that, even with available tool/method to act as measures to dissuade adversaries. New studies explore machine learning (ML) approaches as modes to effectively classify genuine from malicious packets that attempts intrusion [30]–[32]. These feats as achieved by an adversary, is accomplished via the vulnerability trace that attempts to compromise a user device [33]–[35] masquerading as genuine user. The spread of such breaches/attacks are losing monies for businesses as private files, and network infrastructure are often lost to such breaches. With evolved techs, adversaries often exploit malware as means to wreak havoc. It has become crucial and imperative to compile counter-intrusions via measures that remains resilient to cyberattacks. This has also become a primary focus for most businesses and organizations, to adopt intelligent model that can deter and dissuade adversaries [36]–[38].

1.1 Distributed Denial of Service (DDoS) Attacks

DDoS are carefully crafted attack, socially-engineered threats, breaches and attacks initiated against network resource(s). it is often targeted as a subterfuge, stealth mode threat aimed to compromise a user device, and use same as entry (pivot cum pilot) point to access a network infrastructure [39]–[41]. So that on access entry to a vulnerable compromised device – an adversary seizes up resources to include CPU time, memory, network bandwidth, memory [2], [42], [43] – denying authorized users access as (s)he further exploits the network's weakness. Many adversaries achieve this feat via the aid of code insertion mechanism [44]–[46], which seeks and eventually overwhelms a network with user requests. The well-coordinated and careful crafting of the DDoS – often ensures its success and the size of the botnet often corresponds to the severity of the attack [47]–[49].

Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal
AIMS Research Journal
Volume 10, No 2, 2024 Series

Thus, such breach tries to exhaust targeted resources, deny authorized user access, and exploits a compromised network of its resources. DDoS can easily be fixed by manually disconnecting affected devices – if/when they are detected. Thus, firewalls and employed detection approaches must aim to stop as fast as it is detected, and as close to its source as possible as it can [50]–[52]. DDoS are basically grouped into: (a) an adversary by design, exploits cum floods a network with user requests to eventually overwhelm a server with requests so that once access is gained – s(he) exhaust/seize up CPU-time, power, bandwidth, etc and makes it difficult for all other genuine/authorized user to access these resources, and (b) an adversary can initiate a large volume of malicious data requests via s(he) usage of the protocol design attack that spoofs all user requests; And in turn, deny services to users [53]–[55]. The success of DDoS is attributed to its skills for evading detection as adversary can spoof their source IP-address to mask data origin – making it difficult to differentiate genuine data packets from malicious data packets [56]–[59].

Thus, detection approaches must be able to spot these based on their locality of deployment as [60], [61] via the following techniques:

a. A source device can explore security medium to aid identification of malicious data with its outgoing packet and filters it. Such detection is launched at the attack's source and prevents other network users from generating a DDoS. This detection mode stops such an attack breach so fast and so close as possible to the attack source (a best practice) and minimizes havoc the attack ought to accomplish on the network packets cum traffic [62], [63].
b. A victim-end detection is when a compromised device can detect/distinguish incoming malicious data from genuine data via its misuse of intrusion, or anomaly intrusion detection scheme – such that the data packet is denied entry or granted degraded services as it reaches a victim device so as to dissuade it from bandwidth saturation [64], [65].
c. Core-end detection is when a router may attempt to identify a malicious data via traffic flow rate-limit so as to balance between its detection accuracy and bandwidth consumption of a request (attack). Thus, it traces back such detection with ease as its aggregates all traffic flow via rate-limit since both attack and genuine packets arrive at the router at same time [66], [67].

1.2. Study Motivations

Despite its widespread adoption – the inherent gaps and persistent challenges that often degrades the performance and efficacy of collaborative filtering heuristics in practical applications are as below [54], [68]–[71]. These include (but not limited to):

a. The alarming growth rate of DDoS breaches, attacks and threats portends to compromise unsuspecting user devices and exploit resources. This rise has triggered loss of finance, caused reduced user-trust, and reduced care towards integration cum adoption of technology. DDoS can be resolved with targeted IDS schemes [41], [72]–[74], knowledge-driven heuristic models [75]–[77], and statistical dynamic models [78]–[82]. All these have successfully been implemented on malicious data. Thus, to combat DDoS is a continuous task even when many such classification heuristics' performances are degraded cum hindered by the adopted feature selection scheme that often yield model overfit and over-train.
b. Finding the right-format dataset – is crucial to machine learning task. Access to high-quality datasets is needed in training and performance evaluation [83] – as there is limited data, which often yield significant false positives [84]. A crucial hurdle is challenge with imbalanced datasets

with cases of DDoS attack lagging behind genuine ones. New studies must seek explore intricate sampling techniques, or harness the robust power of ensemble(s) tailored explicitly to mitigating the issues of imbalanced dataset [85], [86].

c. As DDoS prevents authorized clients from access to network resources; thereby consuming or causing the seizure of available resources as it overwhelms/overloads a network with requests, until countermeasures are explored. There is become the urgent need to identify its source, manage their existence as fast and as close to its origin. This will imply to effectively differentiate between legitimate and malicious acts via use of statistical heuristics. Many of such ensemble that explores hill-climbing approach – often gets trapped at the heuristic's local maxima.
d. To formulate an effective detection approach also yields a variety of drawbacks as malicious packets by design – seek to evade filter detection. These filters are by design also hampered by the character size limit, non-availability of dataset, feature selection and extraction in the quest for ground truth, heuristic construction, and training. These, can lead to both poor generalization and poor test dataset classification for the proposed heuristics.
e. With increased use of multiple channels for transactions [87]–[89] – new models must integrate various channel data to enhance the overall accuracy [90]–[92] as traditional detection modes are limited in adapting then emergent attack patterns as well as keeping up with novel tactics.

To overcome these, we propose cum adapt a modular memetic consisting of a cultural genetic algorithm fused neural network learning algorithm that seeks to effectively classify malware intrusion from genuine traffic flow data packets.

2. MATERIAL AND METHOD

Network resources are best viewed as a stream of data events, checked on the backdrop of predefined threat rules and patterns. Managers often formulate a general view for known attacks so that the system can easily improvise and identify related occurrence as attacks, based on either a signature and/or anomaly analysis, self-organized maps, and transition analysis. The rise in DDoS breaches today, continues to raise concerns, making its detection an urgent task for businesses. The loss in cost associated with DDoS has since become staggering, incurring losses in billions of dollars annually. Thus, businesses and users must remain committed to and vigilant towards continued improvements and detection systems. Despite these efforts, adversaries continue to invent new techniques to evade and circumvent security measures to avoid detection, making it a constant battle [93].

Today also, machine learning models have been successfully trained to effectively recognize breaches patterns. They learn via features classification of the normal behavior in traffic flow, or a quick detect of the unusual activity as pattern indicative of a breach/threat profile. A variety of machine learning (ML) schemes successfully implemented includes: Logistic Regression [94]–[96], Deep Learning [97]–[99], Bayesian model [100], Naive Bayes [101], Support Vector Machine [102], [103], K-Nearest Neighbors [104], Random Forest [26], [105], and other models [106], [107] that have been effectively used to detect credit-card fraud. Many of these, have drawbacks with their flexibility in feature selection, importance, and accuracy. Our ensemble should be able to reduce overfitting, to address imbalanced datasets, and yield a vigorous prediction accuracy [108]–[110].

Emordi et al. [111] used a multi-level tree for packet statistics to monitor data traffic(s) on devices, and to detect as well as eliminate DDoS. They aggregated and rated each packet statistics to successfully detect ongoing breach via a disproportional difference between each data's rate in/out a network – and set-up at locations that equips each device to either fails to monitor or detect bandwidth attacks. Haque et al. [112] Adversaries evade detection by randomizing source-IP. They investigated DDoS via NetBouncer, distinguishing the vulnerable from non-vulnerable users, and update the client list that allowed access to resources. As a user forwards a packet, the NetBouncer compares for legitimacy of the user. Once the user passes the test, s(he) is added to the legitimacy list and therein, granted access to network resources till such a window for legitimacy expires at expiration of the list and users are thus, re-validated.

Machine learning (ML) schemes have been used to efficiently classify DDoS with ensembles that are tolerant to noise, ambiguities, and have imprecise data at its input – to yield low-cost, effective optimal solution. MLs explores traffic (historic) dataset to yield a model design that seeks to group new cases based on class features. Instances that do not conform to the trained heuristic are classified as an anomaly. Thus, Nguyen [113] Proactively classified network status into phases that seek to investigate packets based on selected features using the KNN model to classify packets of DDoS attack. Yuan et al [114] used decision trees to detect DDoS with 15-features selected to help it monitor data and flag data rates in/out using traffic flow pattern. It detects traffic anomalies via a matching scheme that identifies traffic similar to an attack, and trace to its origin based on similarity via DARPA 2000 dataset.

Otorokpo et al [115] used a signature memetic ensemble to detect DDoS breach using 7-features to monitor data rate and packet traffic pattern. It uses a match method to identify traffic flow(s) into classes and trace them back to an attack's origin via the similarity. Odiakaose et al. [116] investigated DDoS attacks using the Radial Basis Function to test data packets for anomalies as applied to an edge-routers on a victim networks. It uses 7-feats to train a RBF-network, and classified data into genuine and attack class(es) such that if heuristics detects an incoming traffic as attack, its source packets is forwarded to a filter and alarm routine for further measures of actions. Otherwise, if clear and free of attacks, they are forwarded to their respective destination(s) [117]–[119].

2.1. Data Gathering

Dataset used was obtained from [web]: www.kaggle.com/datasets/DDoS/attacks.htm". It consists of 54,807 DDoS attacks recorded classifications. Input is transformed using the principal component analysis (PCA) [120]–[122]. A more detailed description can be seen in [123], [124].

2.2. Experimental Neural Network with Fused Genetic Algorithm Trained Learning Ensemble

Studies have proven that reinforcement (hybrid) ensemble always outperforms single classifiers. Their fundamental issues include their challenges to resolve conflicts arising from: (a) data encoding and transcription from one heuristic to another, and (b) structural dependencies as imposed by the base heuristics used/adopted. These must be effectively/adequately resolved. Our proposed experimental hybrid deep learning ensemble is constructed with 3-blocks as adapted from [125] and [126] which is detailed thus: (a) deep learning, unsupervised modular Kohonen neural network, (b) the supervised cultural genetic algorithm, and (c) the knowledgebase – as in figure 3.

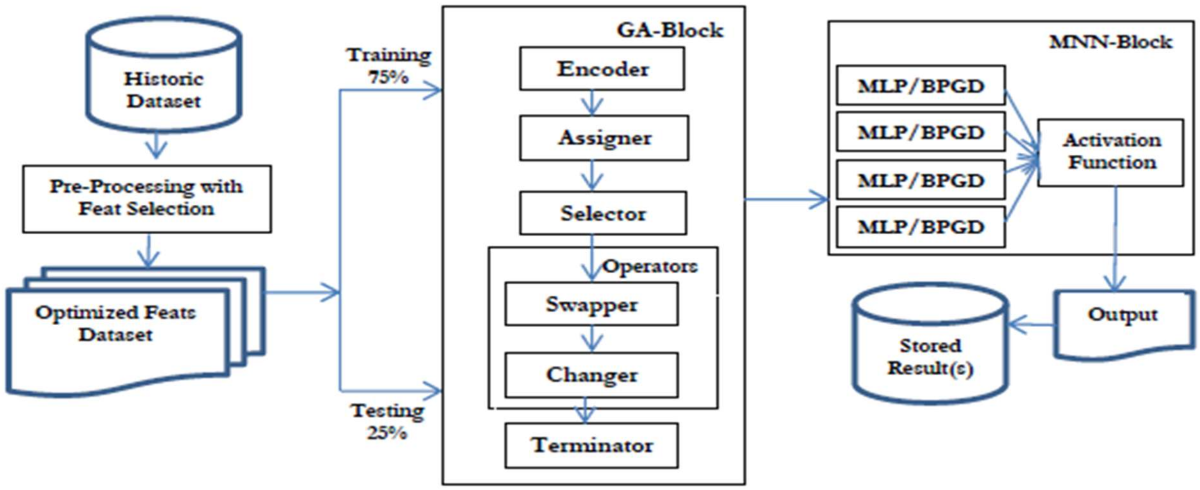

Figure 1. Modular Neural Network with Fused Genetic Algorithm Trained Learning Algorithm

1. The Supervised Genetic Algorithm: Gas by design explores 4-operators/section namely initialize unit, fitness function and select unit, retrain/crossover unit, and mutation/diversity unit – so as to reach optimality. A fit gene yields a value close to the optimal. The Cultural GA (CGA) is a variant that uses 4-belief spaces to yield a solution. They include: (a) ***norm*** specifies the upper/lower range that bounds a gene, (b) ***domain*** specifies data about the task, (c) ***temporal*** specifies knowledge about the available problem space, and (d) ***spatial*** specifies the coverage topography of the task. In addition, it exploits an influence function to bridge gaps between its gene pool and these belief spaces – to ensure that modified genes do not exist outside the lower/upper bounds and they still conform to the belief space(s). Thus, its result pool does not violate the belief space(s) to reduce the amount of potential candidate that the CGA generates until it reaches optimum [127]–[129].
2. Unsupervised Modular Kohonen Neural Network (MNN) is a feed-forward, grid network – whose input layer accepts data, and forwards them as unbound to its hidden layer. This layer activates the transfer function to yield the desired computation by mapping its similarity patterns into relations. These pattern cum relations when/if noticed, is then employed to determine its training result. To create the deep learning impact of the MNN – we carefully modify its features through the 2-stages namely pre-trained, and fine-tuned processes as described in [130].

2.3. Training Phase

Table 1 lists the generated top 22-rules during training with fitness values between 0.80-to-0.8065. With these top-rules yielding 80percent and above – they are good enough to be used to detect intrusion of the test-dataset. For example, rule 14 (in bold) states that any connection with any infinity hours, 0 minutes, infinity seconds – using any protocol from a source-port 1023, and headed for any destination port with source-IP 192.168.1.30, and destination-IP 192.168.0.-1 (as the last octet can range from 0 to 255) – will be regarded as intrusion. We thus, infer from other rules that 10-of-22 rules with the destination port of -1 (infinity amount) yields an intrusion – since most destination rules search for traffic flow pattern and connections from any destination port -1. This increases its chances of detecting an intrusion on any port in the network as well as improves generality of rules.

Table 1. Fitness function for selected features with top-22 generated rules

Time	Protocol	Source Port	Destination Port	Source IP	Destination IP	Attack	Fitness
-1,0,23	telnet	-1	23	192.168.1.30	192.168.0.20	PG	0.8063
-1,0,23	-1	-1	-1	192.168.1.30	192.-1.0.20	PC	0.8063
0,0,5	-1	-1	-1	192.168.1.30	192.168.0.20	PS	0.8063
0,0,5	-1	-1	-1	192.168.1.30	192.-1.0.20	PS	0.8063
-1,0,23	telnet	-1	23	192.-1.1.30	192.168.0.20	PC	0.8063
0,0,5	-1	-1	-1	192.168.1.30	192.168.0.20	ARS	0.8063
-1,0,23	telnet	-1	23	192.168.1.30	192.168.0.20	ICMP	0.8063
0,0,5	-1	-1	-1	192.168.1.30	192.168.0.20	NP	0.8063
0,0,23	telnet	-1	-1	192.168.1.30	192.168.0.20	PA	0.8063
-1,0,23	telnet	-1	23	192.168.1.30	192.168.0.20	FA	0.8063
0,0,5	-1	-1	-1	192.168.1.30	192.-1.0.20	FA	0.8063
-1,0,23	telnet	-1	23	192.168.1.30	192.168.0.20	ARS	0.8063
0,0,-1	-1	1023	1021	192.-1.1.30	-1.168.0.20	PODA	0.8031
-1,0,-1	**-1**	**1023**	**-1**	**192.168.1.30**	**192.168.0.-1**	**PODA**	**0.8031**
0,0,14	-1	-1	513	192.168.1.30	192.168.0.-1	PA	0.8031
0,0,14	-1	-1	513	192.168.1.30	192.168.0.20	SR	0.8031
0,0,14	-1	-1	513	-1.168.1.30	192.168.0.20	SH	0.8031
0,0,14	-1	-1	513	192.168.1.30	192.168.0.-1	RA	0.8031
-1,0,-1	-1	1023	-1	192.168.1.30	192.168.0.-1	DN	0.8031
0,0,5	-1	-1	23	192.168.1.30	192.168.0.20	IPS	0.8031
-1,0,-1	-1	1023	-1	192.168.1.30	192.168.-1.20	PODA	0.8031
0,0,14	-1	-1	513	192.168.1.30	192.168.0.-1	ICMP	0.8031

Table 1 lists training result for our deep learning modular memetic ensemble with labeled attacks: *ICMP PING* – Internet Control Protocol Packet Internet Groper, *NP* – Network Ping, PS – Port Scan, *PAS* – Packet Sniffer, *PA* – Protocol Analyzer, *PG* – Password Guess, *PC* – Password Cracking, *SH* – Session Hijack, *SR* – Session Replay, *IPS* – IP Spoofing, *DN* – Domain Name attack, *RA* – Reroute Attack, *FA* – Flood Attack, *ARS* – Address Resolution Spoof, *PODA* – Ping of Death, etc [131], [132].

Our rule generator uses a population of 400 over 5000-evolutions, with 0.05 probability of a gene to be mutated. The network weights (i.e. w1 and w2) were recorded as 0.2 and 0.8 respectively. So – taking our first rule from the Table 1 as a case study, it is explained as thus [133]–[136]:

> *if* (duration="-1:0:23" and protocol ="telnet" and source-port=-1 and destination-port=23 and source IP="192.168.1.30" and destination IP ="192.168.0.20) *then* {log network connection as an Intrusion}.

3. RESULTS AND DISCUSSION

3.1. Training Performance Evaluation

Training allows the ensemble to adjust its weights and biases. We tune the various hyper-parameters of the heuristic using a trial-n-error approach as in Table 2 as follows: max_depth, learning_rate, and n_estimators respectively with the hybrid ensemble training to yield an optimal solution [137]–[139].

Table 2. Hyper-parameter Values

Hyper-Parameters	Definition	Trial-n-Error	Best Value
Max-Depths	Max. depth of trees	[1, 2, 4, 5, 6, 8, 10]	5
Learning Rate	Step-size learning weights	[0.1, 0.2, 0.3, 0.5, 0.75]	0.25
N_Estimators	Number of Neurons	[100, 200, 300, 400, 500]	250

Using the hyper-parameters as in Table 2, the ensemble yields the metrics to detect and effectively classify DDoS attacks.

Table 3. Performance Evaluation with Benchmark ensembles

ML Schemes	F1	Accuracy	Precision	Recall
Decision Tree (DT)	0.9805	0.9815	0.9805	0.9745
Random Forest (RF)	0.9881	0,9968	0.9318	0.9848
XGBoost	0.9925	0.9981	0.9541	0.9881
Proposed Memetic Ensemble	0.9945	0.9984	0.9616	0.9890

Table 3 shows our proposed ensemble yields F1 of 0.9945, and outperforms XGBoost, RF and DT (with F1 of 0.9925, 0.9881 and 0.9805 respectively). Our hybrid heuristic also yield an Accuracy of 0.9984 to outperform XGBoost, RF and DT (with 0.9981, 0.9964 and 0.9815 respectively). The values for the respective Precision and Recall scores are detailed in Table 3 which agrees with [131], [140], [141].

3.2. Discussion of Findings

It provides insights into which characteristics have a bigger influence on overall performance and aids in identifying the most important aspects influencing the model's predictions [142].

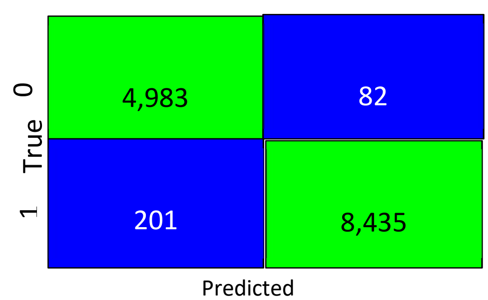

Figure 2. Confusion matrix for Experimental Ensemble

Figure 2 yields the confusion matrix values. This implies that our proposed experimental ensemble can correctly classify the test dataset (instances) with a 99.84% accuracy. It incorrectly classified only 283-instances with 13,418 correctly classified test instances.

4. CONCLUSIONS

The chaotic nature of breaches vis-à-vis noisy dataset with its many features, will continue to yield studies into the use of deep ensemble learning heuristics as suitable mode to addressing many cyber-attacks [143]. The variance and bias associated with ML tasks and its available dataset – also makes for the possibility of optimized training sample if greater performance must be achieved [144]–[146].

We propose a deep ensemble (Genetic Algorithm Modular fused learning Neural Network) to detect packet behaviour and anomaly-based detection of malicious packets. We explored GA was due to its flexibility as an elitist model [147]; While, the MNN is used as a learning paradigm for modular learning components. Model validation return a confusion matrix with these values: TP = 50, TN = 2, FN = 5, FP = 3 [148], [149]..

REFERENCES

[1] B. O. Malasowe, M. I. Akazue, E. A. Okpako, F. O. Aghware, D. V. Ojie, and A. A. Ojugo, "Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 8, pp. 135–142, 2023, doi: 10.14569/IJACSA.2023.0140816.

[2] M. N. Al-Mhiqani, S. N. Isnin, R. Ahmed, and Z. Z. Abidi, "An Integrated Imbalanced Learning and Deep Neural Network Model for Insider Threat Detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 1, pp. 1–5, 2021.

[3] P. Shanmuga Sundari and M. Subaji, "Integrating Sentiment Analysis on Hybrid Collaborative Filtering Method in a Big Data Environment," *Int. J. Inf. Technol. Decis. Mak.*, vol. 19, no. 02, pp. 385–412, Mar. 2020, doi: 10.1142/S0219622020500108.

[4] A. A. Ojugo and D. O. Otakore, "Redesigning Academic Website for Better Visibility and Footprint: A Case of the Federal University of Petroleum Resources Effurun Website," *Netw. Commun. Technol.*, vol. 3, no. 1, p. 33, Jul. 2018, doi: 10.5539/nct.v3n1p33.

[5] A. A. Ojugo, A. Osika, I. J. Iyawa, and M. O. Yerokun, "Information and communication technology integration into science, technology, engineering and mathematic (STEM) in Nigeria," *West African J. Ind. Acad. Res.*, vol. 4, no. 1, pp. 22–30, 2012.

[6] S. Chiemeke and E. Omede, "Mal-typho diagnosis intelligent system (MATDIS): the auto-diagnostic rule generation algorithm," *Comput. Inf. Syst. Dev. Informatics Allied Res. J.*, vol. 5, no. 4, pp. 83–92, 2021.

[7] M. I. Akazue, A. A. Ojugo, R. E. Yoro, B. O. Malasowe, and O. Nwankwo, "Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 28, no. 3, pp. 1756–1765, Dec. 2022, doi: 10.11591/ijeecs.v28.i3.pp1756-1765.

[8] R. E. Yoro, F. O. Aghware, B. O. Malasowe, O. Nwankwo, and A. A. Ojugo, "Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, p. 1922, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1922-1931.

[9] R. E. Yoro, F. O. Aghware, M. I. Akazue, A. E. Ibor, and A. A. Ojugo, "Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, p. 1943, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1943-1953.

[10] F. F. Haryani, S. Sarwanto, and D. Maryono, "Online learning in Indonesian higher education: New indicators during the COVID-19 pandemic," *Int. J. Eval. Res. Educ.*, vol. 12, no. 3, p. 1262, Sep. 2023, doi: 10.11591/ijere.v12i3.24086.

[11] D. A. Oyemade *et al.*, "A Three Tier Learning Model for Universities in Nigeria," *J. Technol. Soc.*, vol. 12, no. 2, pp. 9–20, 2016, doi: 10.18848/2381-9251/CGP/v12i02/9-20.

[12] E. D. Ananga, "Gender Responsive Pedagogy for Teaching and Learning: The Practice in Ghana's Initial Teacher Education Programme," *Creat. Educ.*, vol. 12, no. 04, pp. 848–864, 2021, doi: 10.4236/ce.2021.124061.

[13] T. M. Fagbola, A. A. Adigun, and A. O. Oke, "Computer-Based Test (CBT) System For University Academic Enterprise Examination," *Int. J. Sci. Technol. Res.*, vol. 2, no. 8, pp. 336–342, 2013, [Online]. Available: http://www.ijstr.org/final-print/aug2013/Computer-based-Test-Cbt-System-For-University-Academic-Enterprise-Examination.pdf

[14] O. B. Chibuzo and D. O. Isiaka, "Design and Implementation of Secure Browser for Computer-Based Tests," *Int. J. Innov. Sci. Res. Technol.*, vol. 5, no. 8, pp. 1347–1356, 2020, doi: 10.38124/ijisrt20aug526.

[15] B. O. Malasowe, D. V. Ojie, A. A. Ojugo, and M. D. Okpor, "Co-Infection Prevalence of Covid-19 Underlying Tuberculosis Disease Using a Susceptible Infect Clustering Bayes Network," *DUTSE J. Pure Appl. Sci.*, vol. 10, no. 2, pp. 80–94, 2024, doi: 10.4314/dujopas.v10i2a.8.

[16] S. D. Durojaye, E. O. Okon, and D. D. Samson, "Software Quality and Usability for Computer-Based Test in Tertiary Institution in Nigeria: A Case Study of Kogi State University," *Am. J. Educ. Res.*, vol. 3, no. 10, pp. 1224–1229, 2015, doi: 10.12691/education-3-10-3.

[17] E. O. Okonta, A. A. Ojugo, U. R. Wemembu, and D. Ajani, "Embedding Quality Function Deployment In Software Development: A Novel Approach," *West African J. Ind. Acad. Res.*, vol. 6, no. 1, pp. 50–64, 2013.

[18] U. R. Wemembu, E. O. Okonta, A. A. Ojugo, and I. L. Okonta, "A Framework for Effective Software Monitoring in Project Management," *West African J. Ind. Acad. Res.*, vol. 10, no. 1, pp. 102–115, 2014.

[19] J. A. Abah, O. Honmane, T. J. Age, and S. O. Ogbule, "Design of Single-User-Mode Computer-Based Examination System for Senior Secondary Schools in Onitsha North Local Government Area of Anambra State, Nigeria," *SSRN Electron. J.*, vol. 6, no. January, pp. 12–21, 2022, doi: 10.2139/ssrn.4061818.

[20] H. Danladi and A. K. Dodo, "A comparative Analysis of Joint Admissions and Matriculation Board‟s (JAMB) Performance, Pre and Post Electronic migration," *Int. J. Humanit. Soc. Sci.*, vol. 6, no. 5, pp. 80–85, 2019, doi: 10.14445/23942703/ijhss-v6i5p111.

[21] A. I. Ben, A. M. I, and O. C. O, "Ant Colony Optimization Algorithm Based Vehicle Theft Prediction-Prevention and Recovery System Model (Aco-Vtp 2 rsm)," vol. 7, no. 06, pp. 251–260, 2016.

[22] S. Iskandarov, "Develop a centralized and secure online testing system for a large number of users," *J. Inf. Knowl. Manag.*, vol. 23, no. October, pp. 1–6, 2020.

[23] I. P. Okobah and A. A. Ojugo, "Evolutionary Memetic Models for Malware Intrusion Detection: A Comparative Quest for Computational Solution and Convergence," *Int. J. Comput. Appl.*, vol. 179, no. 39, pp. 34–43, 2018, doi: 10.5120/ijca2018916586.

[24] A. A. Ojugo and A. O. Eboka, "An Empirical Evaluation On Comparative Machine Learning Techniques For Detection of The Distributed Denial of Service (DDoS) Attacks," *J. Appl. Sci. Eng. Technol. Educ.*, vol. 2, no. 1, pp. 18–27, 2020, doi: 10.35877/454ri.asci2192.

[25] A. A. Ojugo, A. O. Eboka, R. E. Yoro, M. O. Yerokun, and F. N. Efozia, "Framework design for statistical fraud detection," *Math. Comput. Sci. Eng. Ser.*, vol. 50, pp. 176–182, 2015.

[26] M. Akazue, C. Asuai, A. Edje, E. Omede, and E. Ufiofio, "Cybershield : Harnessing Ensemble Feature Selection Technique for Robust Distributed Denial of Service Attacks Detection," *Kongzhi yu Juece/Control Decis.*, vol. 38, no. 03, pp. 1211–1224, 2023.

[27] R. O. Bello, M. Olugbebi, A. O. Babatunde, B. O. Bello, and S. I. Bello, "A University Examination Web Application Based on Linear-Sequential Life Cycle Model," *Daffodil Int. Univ. J. Sci. Technol.*, vol. 12, no. 1, p. 25, 2017.
[28] A. A. Ojugo, E. Ugboh, C. C. Onochie, A. O. Eboka, M. O. Yerokun, and I. J. B. Iyawa, "Effects of Formative Test and Attitudinal Types on Students' Achievement in Mathematics in Nigeria," *African Educ. Res. J.*, vol. 1, no. 2, pp. 113–117, 2013, [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1216962&site=ehost-live
[29] R. E. Yoro and A. A. Ojugo, "An Intelligent Model Using Relationship in Weather Conditions to Predict Livestock-Fish Farming Yield and Production in Nigeria," *Am. J. Model. Optim.*, vol. 7, no. 2, pp. 35–41, 2019, doi: 10.12691/ajmo-7-2-1.
[30] O. Thorat, N. Parekh, and R. Mangrulkar, "TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification," *Int. J. Inf. Manag. Data Insights*, vol. 1, no. 2, p. 100048, Nov. 2021, doi: 10.1016/j.jjimei.2021.100048.
[31] K. Godewa, P. Branch, and J. But, "An Analysis of Blockchain-Based IoT Sensor Network Distributed Denial of Service A tt acks," 2024.
[32] C. S. de Almeida *et al.*, "Credit card fraud detection using enhanced Random Forest Classifier for imbalanced data," *Rev. Bras. Linguística Apl.*, vol. 5, no. 1, pp. 1689–1699, 2016.
[33] S. F. Tan and G. C. Chung, "An Evaluation Study of User Authentication in the Malaysian FinTech Industry With uAuth Security Analytics Framework," *J. Cases Inf. Technol.*, vol. 25, no. 1, pp. 1–27, 2023, doi: 10.4018/JCIT.318703.
[34] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "Sentiment analysis in detecting sophistication and degradation cues in malicious web contents," *Kongzhi yu Juece/Control Decis.*, vol. 38, no. 01, p. 653, 2023.
[35] A. A. Ojugo, M. I. Akazue, P. O. Ejeh, C. Odiakaose, and F. U. Emordi, "DeGATraMoNN: Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing," *Kongzhi yu Juece/Control Decis.*, vol. 38, no. 01, pp. 667–678, 2023.
[36] M. I. Akazue, I. A. Debekeme, A. E. Edje, C. Asuai, and U. J. Osame, "UNMASKING FRAUDSTERS : Ensemble Features Selection to Enhance Random Forest Fraud Detection," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 201–212, 2023, doi: 10.33633/jcta.v1i2.9462.
[37] A. A. Ojugo and R. E. Yoro, "Extending the three-tier constructivist learning model for alternative delivery: ahead the COVID-19 pandemic in Nigeria," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, p. 1673, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1673-1682.
[38] A. A. Ojugo and R. E. Yoro, "Predicting Futures Price And Contract Portfolios Using The ARIMA Model: A Case of Nigeria's Bonny Light and Forcados," *Quant. Econ. Manag. Stud.*, vol. 1, no. 4, pp. 237–248, 2020, doi: 10.35877/454ri.qems139.
[39] A. A. Ojugo and A. O. Eboka, "Modeling the Computational Solution of Market Basket Associative Rule Mining Approaches Using Deep Neural Network," *Digit. Technol.*, vol. 3, no. 1, pp. 1–8, 2018, doi: 10.12691/dt-3-1-1.
[40] A. A. Ojugo and A. O. Eboka, "Inventory prediction and management in Nigeria using market basket analysis associative rule mining: memetic algorithm based approach," *Int. J. Informatics Commun. Technol.*, vol. 8, no. 3, p. 128, 2019, doi: 10.11591/ijict.v8i3.pp128-138.
[41] S. Pande and A. Khamparia, "Explainable Deep Neural network-based analysis on intrusion detection systems," *Comput. Sci.*, vol. 24, no. 1, pp. 5–30, Mar. 2023, doi: 10.7494/csci.2023.24.1.4551.

[42] S. Khanam, I. Bin Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, "A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things," *IEEE Access*, vol. 8, pp. 219709–219743, 2020, doi: 10.1109/ACCESS.2020.3037359.

[43] F. K. Nishi *et al.*, "Electronic Healthcare Data Record Security Using Blockchain and Smart Contract," *J. Sensors*, vol. 2022, pp. 1–22, May 2022, doi: 10.1155/2022/7299185.

[44] P. O. Ejeh, E. Adishi, E. Okoro, and A. Jisu, "Hybrid integration of organizational honeypot to aid data integration, protection and organizational resources and dissuade insider threat," *FUPRE J. Sci. Ind. Res.*, vol. 6, no. 3, pp. 80–94, 2022.

[45] B. O. Malasowe, F. O. Aghware, and B. E. Edim, "Pilot Study on Web Server HoneyPot Integration Using Injection Approach for Malware Intrusion Detection," *Comput. Inf. Syst. Dev. Informatics ALlied Res. J.*, vol. 15, no. 1, pp. 13–28, 2024, doi: 10.22624/AIMS/CISDI/V15N1P2.

[46] E. Adishi, P. O. Ejeh, E. Okoro, and A. Jisu, "Reinforcement deep learning memetic algorithm for detection of short messaging services spam using filters to curb insider threats in organizations," *FUPRE J. Sci. Ind. Res.*, vol. 6, no. 3, pp. 80–94, 2022.

[47] A. A. Ojugo and A. O. Eboka, "Assessing Users Satisfaction and Experience on Academic Websites: A Case of Selected Nigerian Universities Websites," *Int. J. Inf. Technol. Comput. Sci.*, vol. 10, no. 10, pp. 53–61, 2018, doi: 10.5815/ijitcs.2018.10.07.

[48] A. A. Ojugo and O. D. Otakore, "Computational solution of networks versus cluster grouping for social network contact recommender system," *Int. J. Informatics Commun. Technol.*, vol. 9, no. 3, p. 185, 2020, doi: 10.11591/ijict.v9i3.pp185-194.

[49] A. A. Ojugo *et al.*, "Dependable Community-Cloud Framework for Smartphones," *Am. J. Networks Commun.*, vol. 4, no. 4, p. 95, 2015, doi: 10.11648/j.ajnc.20150404.13.

[50] A. A. Ojugo and A. O. Eboka, "Memetic algorithm for short messaging service spam filter using text normalization and semantic approach," *Int. J. Informatics Commun. Technol.*, vol. 9, no. 1, p. 9, 2020, doi: 10.11591/ijict.v9i1.pp9-18.

[51] A. A. Ojugo, E. Ben-Iwhiwhu, O. D. Kekeje, M. O. Yerokun, and I. J. Iyawa, "Malware Propagation on Social Time Varying Networks: A Comparative Study of Machine Learning Frameworks," *Int. J. Mod. Educ. Comput. Sci.*, vol. 6, no. 8, pp. 25–33, 2014, doi: 10.5815/ijmecs.2014.08.04.

[52] M. I. Akazue, G. A. Nwokolo, O. A. Ejaita, C. O. Ogeh, and E. Ufiofio, "Machine Learning Survival Analysis Model for Diabetes Mellitus," *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 4, pp. 754–760, 2023, [Online]. Available: www.ijisrt.com754

[53] A. A. Ojugo and E. O. Ekurume, "Predictive Intelligent Decision Support Model in Forecasting of the Diabetes Pandemic Using a Reinforcement Deep Learning Approach," *Int. J. Educ. Manag. Eng.*, vol. 11, no. 2, pp. 40–48, Apr. 2021, doi: 10.5815/ijeme.2021.02.05.

[54] A. A. Ojugo and R. E. Yoro, "Computational Intelligence in Stochastic Solution for Toroidal N-Queen," *Prog. Intell. Comput. Appl.*, vol. 1, no. 2, pp. 46–56, 2013, doi: 10.4156/pica.vol2.issue1.4.

[55] M. I. Akazue, R. E. Yoro, B. O. Malasowe, O. Nwankwo, and A. A. Ojugo, "Improved services traceability and management of a food value chain using block-chain network : a case of Nigeria," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 29, no. 3, pp. 1623–1633, 2023, doi: 10.11591/ijeecs.v29.i3.pp1623-1633.

[56] A. O. Eboka and A. A. Ojugo, "Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: A logical view," *Int. J. Mod. Educ. Comput. Sci.*, vol. 12, no. 6, pp. 29–45, 2020, doi: 10.5815/ijmecs.2020.06.03.

[57] H. Zardi and H. Alrajhi, “Anomaly Discover: A New Community-based Approach for Detecting Anomalies in Social Networks,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, pp. 912–920, 2023, doi: 10.14569/IJACSA.2023.01404101.
[58] S. F. Okumaya, “Analytic Approaches To Detect Insider Threats,” *Softw. Eng. Inst.*, vol. 12, pp. 1–50, 2022, [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=451065
[59] H. A. Abdulmalik and A. A. Yassin, “Secure two-factor mutual authentication scheme using shared image in medical healthcare environment,” *Bull. Electr. Eng. Informatics*, vol. 12, no. 4, pp. 2474–2483, 2023, doi: 10.11591/eei.v12i4.4459.
[60] A. A. Ojugo and A. O. Eboka, “Signature-based malware detection using approximate Boyer Moore string matching algorithm,” *Int. J. Math. Sci. Comput.*, vol. 5, no. 3, pp. 49–62, 2019, doi: 10.5815/ijmsc.2019.03.05.
[61] M. Akazue and A. Augusta, “Identification of Cloned Payment Page in Ecommerce Transaction,” *Int. Manag. Rev.*, vol. 11, no. 2, pp. 70-76,113, 2015, [Online]. Available: http://0-search.proquest.com.pugwash.lib.warwick.ac.uk/docview/1718903209?accountid=14888%0Ahttp://webcat.warwick.ac.uk:4550/resserv??genre=article&issn=15516849&title=International+Management+Review&volume=11&issue=2&date=2015-04-01&atitle=Identification
[62] M. I. Akazue and I. Ben Ajenaghughrure, “Fuzzy Based Enhanced Smart Rest Room Automated Faucet System,” *Int. J. Eng. Manuf.*, vol. 7, no. 3, pp. 20–30, 2017, doi: 10.5815/ijem.2017.03.03.
[63] I. Ben Ajenaghughrure, P. Sujatha, and M. I. Akazue, “Fuzzy Based Multi-Fever Symptom Classifier Diagnosis Model,” *Int. J. Inf. Technol. Comput. Sci.*, vol. 9, no. 10, pp. 13–28, 2017, doi: 10.5815/ijitcs.2017.10.02.
[64] I. D. Ukadike, M. I. Akazue, E. U. Omede, and T. . Akpoyibo, “Development of an iot based air quality monitoring system,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 10 Special Issue, pp. 23–28, 2019, doi: 10.35940/ijitee.J1004.08810S19.
[65] M. I. Akazue, J. I. Onyeacholem, and E. . Omede, “Application of supervised machine learning algorithm with an intrusion detection system for grazing animals’ detection,” *FUPRE J. Sci. Ind. Res.*, vol. 8, no. 1, pp. 69–78, 2024.
[66] E. . Ihama, M. I. Akazue, E. U. Omede, and D. V. Ojie, “A Framework for Smart City Model Enabled by Internet of Things (IoT),” *Int. J. Comput. Appl.*, vol. 185, no. 6, pp. 6–11, 2023, doi: 10.5120/ijca2023922685.

[67] M. I. Akazue, A. Aghaulor, and B. I. Ajenaghughrure, “Customer’s Protection in Ecommerce Transaction Through Identifying Fake Online Stores,” *Int. Conf. e-Learning, e-Bus., EIS, e-Gov. | EEE’15*, pp. 52–54, 2015, [Online]. Available: https://search.proquest.com/openview/ec0d4e6d828f7569f14153067d45646c/1?pq-origsite=gscholar&cbl=1976356
[68] A. A. Ojugo and A. O. Eboka, “Comparative Evaluation for High Intelligent Performance Adaptive Model for Spam Phishing Detection,” *Digit. Technol.*, vol. 3, no. 1, pp. 9–15, 2018, doi: 10.12691/dt-3-1-2.
[69] B. N. Supriya and C. B. Akki, “Sentiment prediction using enhanced xgboost and tailored random forest,” *Int. J. Comput. Digit. Syst.*, vol. 10, no. 1, pp. 191–199, 2021, doi: 10.12785/ijcds/100119.

[70] S. Meghana, B. . Charitha, S. Shashank, V. S. Sulakhe, and V. B. Gowda, "Developing An Application for Identification of Missing Children and Criminal Using Face Recognition.," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 12, no. 6, pp. 272–279, 2023, doi: 10.17148/ijarcce.2023.12648.
[71] Sharmila, R. Sharma, D. Kumar, V. Puranik, and K. Gautham, "Performance Analysis of Human Face Recognition Techniques," *Proc. - 2019 4th Int. Conf. Internet Things Smart Innov. Usages, IoT-SIU 2019*, no. May 2020, pp. 1–4, 2019, doi: 10.1109/IoT-SIU.2019.8777610.
[72] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.
[73] A. A. Ojugo *et al.*, "CoSoGMIR: A Social Graph Contagion Diffusion Framework using the Movement-Interaction-Return Technique," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 37–47, 2023, doi: 10.33633/jcta.v1i2.9355.
[74] A. D. Bhavani and N. Mangla, "A Novel Network Intrusion Detection System Based on Semi-Supervised Approach for IoT," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, pp. 207–216, 2023, doi: 10.14569/IJACSA.2023.0140424.
[75] A. Maureen, O. Oghenefego, A. E. Edje, and C. O. Ogeh, "An Enhanced Model for the Prediction of Cataract Using Bagging Techniques," vol. 8, no. 2, 2023.
[76] M. I. Akazue, "A Survey of E-commerce Transaction Fraud Prevention Models," *Proc. Int. Conf. Digit. Inf. Process. Data Mining, Wirel. Commun.*, pp. 140–146, 2015.
[77] B. O. Ojeme and A. Maureen, "Human Immunodeficiency Virus (HIV) Diagnosis Using Neuro-Fuzzy Expert System," *Orient. J. Comput. Sci. Technol.*, vol. 7, no. 2, pp. 207–218, 2014, [Online]. Available: http://www.computerscijournal.org/?p=1070
[78] A. A. Ojugo, A. O. Eboka, E. O. Okonta, R. E. Yoro, and F. O. Aghware, "Predicting Behavioural Evolution on a Graph-Based Model," *Adv. Networks*, vol. 3, no. 2, p. 8, 2015, doi: 10.11648/j.net.20150302.11.
[79] F. O. Aghware *et al.*, "Enhancing the Random Forest Model via Synthetic Minority Oversampling Technique for Credit-Card Fraud Detection," *J. Comput. Theor. Appl.*, vol. 2, no. 2, pp. 190–203, 2024, doi: 10.62411/jcta.10323.
[80] A. A. Ojugo, C. O. Obruche, and A. O. Eboka, "Quest For Convergence Solution Using Hybrid Genetic Algorithm Trained Neural Network Model For Metamorphic Malware Detection," *ARRUS J. Eng. Technol.*, vol. 2, no. 1, pp. 12–23, Nov. 2021, doi: 10.35877/jetech613.
[81] F. U. Emordi, C. C. Odiakaose, P. O. Ejeh, O. Attoh, and N. C. Ashioba, "Student's Perception and Assessment of the Dennis Osadebay University Asaba Website for Academic Information Retrieval, Improved Web Presence, Footprints and Usability," *FUPRE J. Sci. Ind. Res.*, vol. 7, no. 3, pp. 49–60, 2023.
[82] C. C. Odiakaose *et al.*, "DeLEMPaD: Pilot Study on a Deep Learning Ensemble for Energy Market Prediction of Price Volatility and Direction," *Comput. Inf. Syst. Dev. Informatics Allied Res. J.*, vol. 15, no. 1, pp. 47–62, 2024, doi: 10.22624/AIMS/CISDI/V15N1P4.
[83] E. Omede, J. Anenechukwu, and C. Hampo, "Use of Adaptive Boosting Algorithm to Estimate User's Trust in the Utilization of Virtual Assistant Systems," *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 1, pp. 502–509, 2023.
[84] M. K. G. Roshan, "Multiclass Medical X-ray Image Classification using Deep Learning with Explainable AI," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 6, pp. 4518–4526, Jun. 2022, doi: 10.22214/ijraset.2022.44541.

[85] A. A. Ojugo and O. D. Otakore, "Forging An Optimized Bayesian Network Model With Selected Parameters For Detection of The Coronavirus In Delta State of Nigeria," *J. Appl. Sci. Eng. Technol. Educ.*, vol. 3, no. 1, pp. 37–45, Apr. 2021, doi: 10.35877/454RI.asci2163.

[86] A. A. Ojugo and A. O. Eboka, "Empirical Bayesian network to improve service delivery and performance dependability on a campus network," *IAES Int. J. Artif. Intell.*, vol. 10, no. 3, p. 623, Sep. 2021, doi: 10.11591/ijai.v10.i3.pp623-635.

[87] L. De Kimpe, M. Walrave, W. Hardyns, L. Pauwels, and K. Ponnet, "You've got mail! Explaining individual differences in becoming a phishing target," *Telemat. Informatics*, vol. 35, no. 5, pp. 1277–1287, Aug. 2018, doi: 10.1016/j.tele.2018.02.009.

[88] K. Deepika, M. P. S. Nagenddra, M. V. Ganesh, and N. Naresh, "Implementation of Credit Card Fraud Detection Using Random Forest Algorithm," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 3, pp. 797–804, Mar. 2022, doi: 10.22214/ijraset.2022.40702.

[89] J. R. Amalraj and R. Lourdusamy, "A Novel distributed token-based algorithm using secret sharing scheme for secure data access control," *Int. J. Comput. Networks Appl.*, vol. 9, no. 4, p. 374, Aug. 2022, doi: 10.22247/ijcna/2022/214501.

[90] P. Boulieris, J. Pavlopoulos, A. Xenos, and V. Vassalos, "Fraud detection with natural language processing," *Mach. Learn.*, Jul. 2023, doi: 10.1007/s10994-023-06354-5.

[91] I. A. Anderson and W. Wood, "Habits and the electronic herd: The psychology behind social media's successes and failures," *Consum. Psychol. Rev.*, vol. 4, no. 1, pp. 83–99, Jan. 2021, doi: 10.1002/arcp.1063.

[92] Y. Kang, M. Ozdogan, X. Zhu, Z. Ye, C. Hain, and M. Anderson, "Comparative assessment of environmental variables and machine learning algorithms for maize yield prediction in the US Midwest," *Environ. Res. Lett.*, vol. 15, no. 6, p. 064005, Jun. 2020, doi: 10.1088/1748-9326/ab7df9.

[93] T. Sahmoud and D. M. Mikki, "Spam Detection Using BERT," *Front. Soc. Sci. Technol.*, vol. 14, no. 2, pp. 23–35, Jun. 2022, doi: 10.48550/arXiv.2206.02443.

[94] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using GA algorithm for feature selection," *J. Big Data*, vol. 9, no. 1, p. 24, Dec. 2022, doi: 10.1186/s40537-022-00573-8.

[95] S. V. S. . Lakshimi and S. D. Kavila, "Machine Learning for Credit Card Fraud Detection System," *Int. J. Appl. Eng. Res.*, vol. 15, no. 24, pp. 16819–16824, 2018, doi: 10.1007/978-981-33-6893-4_20.

[96] C. Li, N. Ding, H. Dong, and Y. Zhai, "Application of Credit Card Fraud Detection Based on CS-SVM," *Int. J. Mach. Learn. Comput.*, vol. 11, no. 1, pp. 34–39, 2021, doi: 10.18178/ijmlc.2021.11.1.1011.

[97] I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, "Enhanced credit card fraud detection based on attention mechanism and LSTM deep model," *J. Big Data*, vol. 8, no. 1, p. 151, Dec. 2021, doi: 10.1186/s40537-021-00541-8.

[98] U. K. Okpeki, S. Adegoke, and E. U. Omede, "Application of Artificial Intelligence for Facial Accreditation of Officials and," *FUPRE J. Sci. Ind. Res.*, vol. 6, no. 3, pp. 1–11, 2022.

[99] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, pp. 94–100, 2023, doi: 10.14569/IJACSA.2023.0140610.

[100] L. E. Mukhanov, "Using bayesian belief networks for credit card fraud detection," *Proc. IASTED Int. Conf. Artif. Intell. Appl. AIA 2008*, no. February 2008, pp. 221–225, 2008.

[101] V. Filippov, L. Mukhanov, and B. Shchukin, “Credit card fraud detection system,” in *2008 7th IEEE International Conference on Cybernetic Intelligent Systems*, IEEE, Sep. 2008, pp. 1–6. doi: 10.1109/UKRICIS.2008.4798919.
[102] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, “Credit Card Fraud Detection - Machine Learning methods,” in *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, IEEE, Mar. 2019, pp. 1–5. doi: 10.1109/INFOTEH.2019.8717766.
[103] E. R. Altman, “Synthesizing Credit Card Transactions,” *PeerJ Comput. Sci.*, vol. 14, Oct. 2019.
[104] E. A. L. Marazqah Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, “A systematic review of literature on credit card cyber fraud detection using machine and deep learning,” *PeerJ Comput. Sci.*, vol. 9, p. e1278, Apr. 2023, doi: 10.7717/peerj-cs.1278.
[105] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, “Random forest for credit card fraud detection,” in *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, IEEE, Mar. 2018, pp. 1–6. doi: 10.1109/ICNSC.2018.8361343.
[106] Y. Abakarim, M. Lahby, and A. Attioui, “An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning,” in *International Conference on Intelligent Systems*, New York, NY, USA: ACM, Oct. 2018, pp. 1–7. doi: 10.1145/3289402.3289530.
[107] M. Zareapoor and P. Shamsolmoali, “Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier,” *Procedia Comput. Sci.*, vol. 48, pp. 679–685, 2015, doi: 10.1016/j.procs.2015.04.201.
[108] B. Gaye and A. Wulamu, “Sentimental Analysis for Online Reviews using Machine learning Algorithms,” pp. 1270–1275, 2019.
[109] Maya Gopal P S and Bhargavi R, “Selection of Important Features for Optimizing Crop Yield Prediction,” *Int. J. Agric. Environ. Inf. Syst.*, vol. 10, no. 3, pp. 54–71, Jul. 2019, doi: 10.4018/IJAEIS.2019070104.
[110] D. O. Oyewola, E. G. Dada, N. J. Ngozi, A. U. Terang, and S. A. Akinwumi, “COVID-19 Risk Factors, Economic Factors, and Epidemiological Factors nexus on Economic Impact: Machine Learning and Structural Equation Modelling Approaches,” *J. Niger. Soc. Phys. Sci.*, vol. 3, no. 4, pp. 395–405, 2021, doi: 10.46481/jnsps.2021.173.
[111] A. A. Ojugo *et al.*, “Evidence of Students’ Academic Performance at the Federal College of Education Asaba Nigeria: Mining Education Data,” *Knowl. Eng. Data Sci.*, vol. 6, no. 2, pp. 145–156, 2023, doi: 10.17977/um018v6i22023p145-156.
[112] M. A. Haque *et al.*, “Cybersecurity in Universities: An Evaluation Model,” *SN Comput. Sci.*, vol. 4, no. 5, 2023, doi: 10.1007/s42979-023-01984-x.
[113] G. Nguyen *et al.*, “Machine Learning and Deep Learning frameworks and libraries for large-scale data mining: a survey,” *Artif. Intell. Rev.*, vol. 52, no. 1, pp. 77–124, 2019, doi: 10.1007/s10462-018-09679-z.
[114] S. Yuan and X. Wu, “Deep learning for insider threat detection: Review, challenges and opportunities,” *Comput. Secur.*, vol. 104, 2021, doi: 10.1016/j.cose.2021.102221.
[115] E. A. Otorokpo *et al.*, “DaBO-BoostE: Enhanced Data Balancing via Oversampling Technique for a Boosting Ensemble in Card-Fraud Detection,” *Adv. Multidiscip. Sci. Res. J.*, vol. 12, no. 2, pp. 45–66, 2024, doi: 10.22624/AIMS/MATHS/V12N2P4.
[116] F. U. Emordi *et al.*, “TiSPHiMME: Time Series Profile Hidden Markov Ensemble in Resolving Item Location on Shelf Placement in Basket Analysis,” *Digit. Innov. Contemp. Res. Sci.*, vol. 12, no. 1, pp. 33–48, 2024, doi: 10.22624/AIMS/DIGITAL/v11N4P3.
[117] B. Ojeme, M. Akazue, E. Nwelih, S. Africa, and C. Science, “Automatic Diagnosis of Depressive Disorders using Ensemble Techniques 1,” vol. 8, no. 3, pp. 31–38, 2016.

[118] O. D. Voke, M. I. Akazue, E. U. Omede, E. . Oboh, and A. . Imianvan, "Survival Prediction of Cervical Cancer Patients using Genetic Algorithm-Based Data Value Metric and Recurrent Neural Network," *Int. J. Soft Comput. Eng.*, vol. 13, no. 2, pp. 29–41, May 2023, doi: 10.35940/ijsce.B3608.0513223.
[119] O. D. Voke, A. Maureen, and I. Anthony, "A Framework for Feature Selection using Data Value Metric and Genetic Algorithm," vol. 184, no. 43, pp. 14–21, 2023.
[120] F. Mustofa, A. N. Safriandono, A. R. Muslikh, and D. R. I. M. Setiadi, "Dataset and Feature Analysis for Diabetes Mellitus Classification using Random Forest," *J. Comput. Theor. Appl.*, vol. 1, no. 1, pp. 41–48, 2023, doi: 10.33633/jcta.v1i1.9190.
[121] A. R. Muslikh, D. R. I. M. Setiadi, and A. A. Ojugo, "Rice disease recognition using transfer xception convolution neural network," *J. Tek. Inform.*, vol. 4, no. 6, pp. 1541–1547, 2023, doi: 10.52436/1.jutif.2023.4.6.1529.
[122] D. R. I. M. Setiadi, K. Nugroho, A. R. Muslikh, S. Wahyu, and A. A. Ojugo, "Integrating SMOTE-Tomek and Fusion Learning with XGBoost Meta-Learner for Robust Diabetes Recognition," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 1, pp. 23–38, 2024, doi: 10.62411/faith.2024-11.
[123] A. A. Ojugo *et al.*, "Forging a User-Trust Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 1–11, Oct. 2023, doi: 10.33633/jcta.v1i2.9259.
[124] A. A. Ojugo and E. O. Ekurume, "Deep Learning Network Anomaly-Based Intrusion Detection Ensemble For Predictive Intelligence To Curb Malicious Connections: An Empirical Evidence," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 10, no. 3, pp. 2090–2102, Jun. 2021, doi: 10.30534/ijatcse/2021/851032021.
[125] G. Behboud, "Reasoning using Modular Neural Network," *Towar. Data Sci.*, vol. 34, no. 2, pp. 12–34, 2020.
[126] A. A. Ojugo and O. Nwankwo, "Spectral-Cluster Solution For Credit-Card Fraud Detection Using A Genetic Algorithm Trained Modular Deep Learning Neural Network," *JINAV J. Inf. Vis.*, vol. 2, no. 1, pp. 15–24, Jan. 2021, doi: 10.35877/454RI.jinav274.
[127] X. Lin, P. R. Spence, and K. A. Lachlan, "Social media and credibility indicators: The effect of influence cues," *Comput. Human Behav.*, vol. 63, pp. 264–271, Oct. 2016, doi: 10.1016/j.chb.2016.05.002.
[128] S. M. Albladi and G. R. S. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," *Human-centric Comput. Inf. Sci.*, vol. 8, no. 1, p. 5, Dec. 2018, doi: 10.1186/s13673-018-0128-7.
[129] A. A. Ojugo and R. E. Yoro, "Empirical Solution For An Optimized Machine Learning Framework For Anomaly-Based Network Intrusion Detection," *Technol. Rep. Kansai Univ.*, vol. 62, no. 08, pp. 6353–6364, 2020.
[130] R. J. Urbanowicz, M. Meeker, W. La Cava, R. S. Olson, and J. H. Moore, "Relief-based feature selection: Introduction and review," *J. Biomed. Inform.*, vol. 85, pp. 189–203, Sep. 2018, doi: 10.1016/j.jbi.2018.07.014.
[131] A. A. Ojugo, P. O. Ejeh, C. C. Odiakaose, A. O. Eboka, and F. U. Emordi, "Improved distribution and food safety for beef processing and management using a blockchain-tracer support framework," *Int. J. Informatics Commun. Technol.*, vol. 12, no. 3, p. 205, Dec. 2023, doi: 10.11591/ijict.v12i3.pp205-213.
[132] A. A. Ojugo, P. O. Ejeh, C. C. Odiakaose, A. O. Eboka, and F. U. Emordi, "Predicting rainfall runoff in Southern Nigeria using a fused hybrid deep learning ensemble," *Int. J. Informatics Commun. Technol.*, vol. 13, no. 1, pp. 108–115, Apr. 2024, doi: 10.11591/ijict.v13i1.pp108-115.

[133] F. Omoruwou, A. A. Ojugo, and S. E. Ilodigwe, "Strategic Feature Selection for Enhanced Scorch Prediction in Flexible Polyurethane Form Manufacturing," *J. Comput. Theor. Appl.*, vol. 2, no. 1, pp. 126–137, 2024, doi: 10.62411/jcta.9539.

[134] A. N. Safriandono *et al.*, "Analyzing Quantum Feature Engineering and Balancing Strategies Effect on Liver Disease Classification," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 1, pp. 50–63, 2024, doi: 10.62411/faith.2024-12.

[135] D. C. Le, N. Zincir-Heywood, and M. I. Heywood, "Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 30–44, Mar. 2020, doi: 10.1109/TNSM.2020.2967721.

[136] S. Gokarn and A. Choudhary, "Modeling the key factors influencing the reduction of food loss and waste in fresh produce supply chains," *J. Environ. Manage.*, vol. 294, p. 113063, Sep. 2021, doi: 10.1016/j.jenvman.2021.113063.

[137] C. Joshi, J. R. Aliaga, and D. R. Insua, "Insider Threat Modeling: An Adversarial Risk Analysis Approach," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1131–1142, 2021, doi: 10.1109/TIFS.2020.3029898.

[138] F. L. Greitzer, J. D. Lee, J. Purl, and A. K. Zaidi, "Design and Implementation of a Comprehensive Insider Threat Ontology," *Procedia Comput. Sci.*, vol. 153, pp. 361–369, 2019, doi: 10.1016/j.procs.2019.05.090.

[139] P. A. Zawislak, F. M. Reichert, D. Barbieux, A. M. S. Avila, and N. Pufal, "The dynamic chain of innovation: bounded capabilities and complementarity in agribusiness," *J. Agribus. Dev. Emerg. Econ.*, vol. 23, pp. 1–113, Apr. 2022, doi: 10.1108/JADEE-04-2021-0096.

[140] J. Li *et al.*, "Feature selection: A data perspective," *ACM Comput. Surv.*, vol. 50, no. 6, 2017, doi: 10.1145/3136625.

[141] C. C. Aggarwal, "Educational and software resources for data classification," *Data Classif. Algorithms Appl.*, pp. 657–665, 2014, doi: 10.1201/b17320.

[142] M. Armstrong and J. Vickers, "Patterns of Price Competition and the Structure of Consumer Choice," *MPRA Pap.*, vol. 1, no. 98346, pp. 1–40, 2020.

[143] M. I. Akazue *et al.*, "Handling Transactional Data Features via Associative Rule Mining for Mobile Online Shopping Platforms," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 3, pp. 530–538, 2024, doi: 10.14569/IJACSA.2024.0150354.

[144] R. R. Ataduhor *et al.*, "StreamBoostE: A Hybrid Boosting-Collaborative Filter Scheme for Adaptive User-Item Recommender for Streaming Services," *Adv. Multidiscip. Sci. Res. J.*, vol. 10, no. 2, pp. 89–106, 2024, doi: 10.22624/AIMS/V10N2P8.

[145] P. O. Ejeh *et al.*, "Counterfeit Drugs Detection in the Nigeria Pharma-Chain via Enhanced Blockchain-based Mobile Authentication Service," *Adv. Multidiscip. Sci. Res. J.*, vol. 12, no. 2, pp. 25–44, 2024, doi: 10.22624/AIMS/MATHS/V12N2P3.

[146] A. M. Ifioko *et al.*, "CoDuBoTeSS: A Pilot Study to Eradicate Counterfeit Drugs via a Blockchain Tracer Support System on the Nigerian Frontier," *J. Behav. Informatics, Digit. Humanit. Dev. Res.*, vol. 10, no. 2, pp. 53–74, 2024, doi: 10.22624/AIMS/BHI/V10N2P6.

[147] R. A. Alsowai and T. Al-Shehari, "A multi-tiered framework for insider threat prevention," *Electron.*, vol. 10, no. 9, 2021, doi: 10.3390/electronics10091005.

[148] E. U. Omede, A. Edje, M. I. Akazue, H. Utomwen, and A. A. Ojugo, "IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defense System," *J. Comput. Theor. Appl.*, vol. 2, no. 1, pp. 43–53, 2024, doi: 10.33633/jcta.v2i1.9541.

[149] E. Omede and U. K. Okpeki, "Design and implementation of autotech resource sharing system for secondary schools in Delta State," *J. Niger. Assoc. Math. Phys.*, vol. 51, no. 5, pp. 325–337, 2023.