Anomaly-based Detection of Denial of Service via Deep Learning Memetic Trained Modular Network

Patrick Ogholuwarami Ejeh [1], Fidelis Oghenevweta Adjogbe [2], David Nwanze [3], Amaka Patience Binitie [4,*]
[1,2,3] Department of Computer Science, College of Computing and Telecommunications, Novena University, Ogume, Nigeria
[4] Department of Computer, Federal College of Education (Technical) Asaba, Nigeria
Email: [1] patrick.ejeh@dou.edu.ng, [2] fidelisinfotech@gmail.com, [3] dnwanze2015@gmail.com,
[4] amaka.binitie@fcetasaba.edu.ng

***Abstract*—Internet's popularity for dissemination of data – has birthed the proliferation of attacks that exploit networks for personal gain. Attackers via social-engineering attacks, gain unauthorized access to a compromised device via subterfuge mode and deny users of network resources. Denial of service (DoS) attack is carefully crafted to exploit high levels of network infrastructures. Our study presents a deep learning scheme to effectively classify between genuine and malicious packets. With benchmark XGBoost, Random Forest, and Decision Tree – our resultant model yields an accuracy 0.9984 and F1 0.9945 to outperform the benchmark XGBoost, RF and DT (with F1 of 0.9925, 0.9881 and 0.9805 – and Accuracy of 0.9981, 0.9964 and 0.9815) respectively. Proposed model correctly classified 13,418 cases with a 0.9984 accuracy and has only 283 cases incorrectly classified. Proposed memetic ensemble effectively differentiates malicious from genuine packets using anomaly-based detection.**

Keywords*—*Anomaly Detection, Machine Learning, Memetic Algorithm, DDoS Attacks, Subterfuge Insider Threats

I. 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 organizations. Information has also become both an integral fundamental requirement cum basis for today's complex culture [2]. The field of informatics is continually advanced with the constant evolution vis-à-vis fusion of information and communication technology (ICT) tools [3]. This integration is attributed to its ubiquitous nature, low cost, usage ease, mobility, portability, and user trust [4][5] – all of which advance the popularity and ease of ICTs. This growth has also attracted intrusive actions from adversaries whom for personal gains, seek to exploit unsuspecting user devices. 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 [6][7].

Capacity development promotes productivity, and the digital revolution today, its impact (positive and negative) on both human-machine connectivity via the adoption of ICT – has also evolved businesses over time; These evolutions, have also experienced both internal or external threats from adversaries [8][9]. Such compromise of user 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. Socially-engineered intrusions include data stealing and corruption, denial of service, buffer overflow, etc [10]. a concerted effort is required to win this war against intrusion with procedures/tools to advance consistent probe of network resources, as studies have proven that intrusion threats and attacks can never be over-emphasized [11][12].

The rise in the rate of these breaches is broad in the range of innovative technology – leading to denial of services attacks, etc [13]. It is necessary to stop as fast and as close to the source – a DDoS breach, because they are carefully crafted against the target user system via a number of compromised systems [14]–[16]. DDoS threatens network infrastructure since by design, they are crafted to target a large cluster of user devices; And in turn, compromised at various levels [17]–[19]. The ease in the spread of these attacks is become of great concern even with available tools and measures that will dissuade adversaries. New studies utilize machine learning (ML) modes to classify genuine from malicious packets [20]–[22]. Intrusion as achieved by an adversary, seeks to exploit vulnerability traces to compromise a user device [3],[23][24] masquerading as a genuine user. The spread of such attacks is losing money for businesses as private files, and network infrastructure are often lost to such breaches. With evolved techs, adversaries often exploit malware as a means to wreak havoc. It has become crucial and imperative to compile counter-intrusions via measures that remain resilient to cyberattacks. This has also become a primary focus for most businesses and organizations, to adopt intelligent models that can deter and dissuade adversaries [25][26].

A. The Distributed Denial of Service (DoS) Attacks

These are carefully crafted attacks and socially engineered threats 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 an entry (pivot cum pilot) point to access a network infrastructure [27]–[29]. On entry to a vulnerable unit – an adversary seizes up resources including CPU time, memory, network bandwidth, and memory [30][31] – denying authorized users access as it further exploits a network's weakness. Many adversaries achieve this feat via code insertion [32]–[34], which overwhelms the network with user requests. This well-crafted DDoS often ensures its success as the botnet size relates to attack severity [35]–[37]. The breach exhausts targeted resources, denies authorized user access, and exploits a compromised network of its resources. DDoS is fixed by

disconnecting affected units – if detected. Thus, firewalls and utilized detection approaches must aim to stop as fast as it is detected, and as close to its source as possible as it can [38] [39]. DDoS is grouped into 2 modes:

1. Floods the network/server with requests that eventually overwhelm a server so that once access is gained, they exhaust/seize up CPU time, power, bandwidth, etc, and make it difficult for all authorized users to access these resources [40][41], and
2. Initiate a large volume of malicious data requests via the use of the protocol design attack that spoofs all user requests; And in turn, denies services to users [42]. The success of DDoS is attributed to its skills for evading detection as the adversary can spoof their source IP address to mask data origin – making it difficult to differentiate genuine data packets from malicious packets [43]–[45].

Detection schemes must spot these based on their locality of deployment as [46] via the following techniques:

a. A source device can explore security mediums to aid in the identification of malicious data with its outgoing packet and filter 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 [47]–[49].
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 user device and dissuades from bandwidth saturation [50].
c. Core-end detection is when a router may attempt to identify 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 it aggregates all traffic flow via rate-limit since both attack and genuine packets arrive at the router at the same time [51]–[53].

Anomaly is best viewed as an outlier data that does not follow or observe the norm. The function is an offset from the norm operation of a system. Its detection is classified into statistical [54], deviation [55], distance [56], profile [57], density [58] and cluster [59] approach. Detection explores machine learning approaches [60] to identify unusual norms in a domain dataset – to resolve tasks such as feature selection mode, poor generalization, imbalance nature of dataset, and prediction performance [61] with the objective of identifying outliers that congest data traffic as attacks [62].

B. Machine Learning Anomaly Detection Approaches

Detection with machine learning approach can be largely accomplished either as a classification or regression task via the methods of vote, stack, bagging and boosting modes. In general, these have been identified to fall into three (3) broad views of Deep learning (DL) [63], Machine Learning (ML) [64], and Ensemble Learning (EL) [65]. ML heuristic models are known to successfully learned intrinsic patterns inherent a dataset via training to help them effectively identify evidence to support ground truth in complex tasks with un(structured) datasets [24]. Its robustness, adaptability and flexibility allow them identify patterns via learning changes in the features to unveil crucial predictors utilized in model construction. And in turn, ease the detection of outliers from behavioral norms of the dataset [66]–[68]. Known MLs are Logistic Regression [69][70], Support Vector [71][72], K-Nearest Neighbors [73][74], and Fuzzy [75].

Deep Learning (DL) here, refers to neural network-based heuristics, and are tailored to learn high-dimensional features in time-series. It is used in non-linear, chaotic, dynamic, and complex traffic data and medical health records [76]. Its poor generalization is due to the vanishing gradients problem. To curb this, studies adopt its variant LSTM, which easily adapts to learned changes experienced as predictor dependency [77]. However, its inability to handle large categorical data and its requirement of longer train time are its demerits. To rescue this, ensemble learning effectively fuse DL and ML [78] to yield optimal fit solution – efficiently achieved via the actions of voting, bagging, stacked, and boost approaches [79].

C. Review of Related Literatures

Network resources are streams of data events checked on predefined attack rules. Managers often formulate a view for known attacks so that the system can easily identify related occurrences of attacks either as signature or anomaly-based analysis using self-organized maps or transition analysis. The rise in DDoS breaches, continues to raise concerns, making its detection an urgent task for businesses. With billions of dollars lost – the cost associated with such attack has become staggering and still on the rise, annually. Businesses and users must remain vigilant with continued evolution in detection schemes. Despite the efforts, adversaries re-invent new mode to evade security and avoid detection; Making this, a constant war [80].

Emordi *et al*. [81] 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 breaches via a disproportional difference in each data's rate in/out of a network – and set up at locations that equip each device to either fail to monitor or detect bandwidth attacks. Haque *et al*. [82] Adversaries evade detection by randomizing source IP. They investigated DDoS via NetBouncer, distinguishing genuine from malicious users, and updated 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, he is added to the legitimacy list, and ceded access to resources till such a window expires; And the list of users are re-validated [83].

Machine learning (ML) schemes have been used to efficiently classify DDoS with ensembles that are tolerant to noise, and ambiguities, and have imprecise data at its input – to yield low-cost, effective optimal solutions. MLs explore traffic (historic) datasets to yield a model design that seeks to group new cases based on class features. Cases that do not conform to the trained heuristic are classified as an anomaly. Thus, Nguyen [84] 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*. [85] used decision trees to detect DDoS with 15 features selected to help it monitor data and flag data rates in/out using traffic patterns. It detects anomalies via a

matching scheme that identifies traffic packets similar to an attack, and traces its origin based on similarity [86][87].

Otorokpo *et al*. [88] used a signature memetic ensemble to detect DDoS breaches using 7-feats to monitor data traffic patterns. It uses a match that identifies traffic flow(s) into classes and traces them back to an attack's origin via the similarity. Emordi *et al*. [89] used a Radial Basis Function to test for packet anomalies on network routers. It used 7-feats to train an RBF network, classifying data into genuine and attack classes. If an incoming traffic is detected as an attack, its source packets are forwarded to a filter and alerts a routine measure of actions. Otherwise, if free of attacks, they are forwarded to their destination(s) [90][91].

D. *Study Motivation and Rationale*

The study wishes to address the problem thus [92][93]:

1. The alarming rise in DDoS attacks compromises user units to exploit resources. This has resulted in loss of finance, reduced user-trust levels, and reduced adoption and technophobia. DDoS can be resolved with targeted schemes [94][95] that have been successfully used on malicious data. This DDoS war is a continuous task that is hindered by the adopted features during selection and data balancing technique explored [96][97].
2. Finding the proper format dataset is crucial to ML tasks as this is needed for model construction, train and test – as there is often, limited available data that in turn, yields high rate false positive valuess [98]. A crucial challenge with imbalanced datasets with cases of DDoS attacks lagging behind genuine ones. New studies must seek to explore intricate sampling techniques or harness the robust power of ensemble(s) tailored explicitly to mitigate the issues of imbalanced datasets.
3. As DDoS prevents authorized clients from access to network resources; thereby consuming or causing the seizure of available resources as it overwhelms the network with user requests until countermeasures are explored. There has become an urgent need to identify its source and manage its existence as fast and as close to its origin. This will imply effectively differentiating between legitimate and malicious acts via the use of statistical heuristics. Many such ensembles that explore hill-climbing approaches – often get trapped at the heuristic's local maxima [99]–[101].
4. Formulating 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 character size limit, non-availability of the 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 proposed model [102][103].
5. With increased multi-channel transactions – new models must integrate data channels to enhance overall accuracy as traditional detection modes are limited in adopting new patterns nor can they keep up with novel tactics.

Thus, we propose a modular memetic ensemble that seeks to effectively classify malware intrusion from genuine traffic flow data packets.

II. Materials and Methods

Our proposed methodology leverages a stacked learning approach with 3-blocks as in [33]: (a) knowledge-base as decision support, (b) supervised cultural genetic algorithm, and (c) unsupervised modular neural network as in Fig. 1:

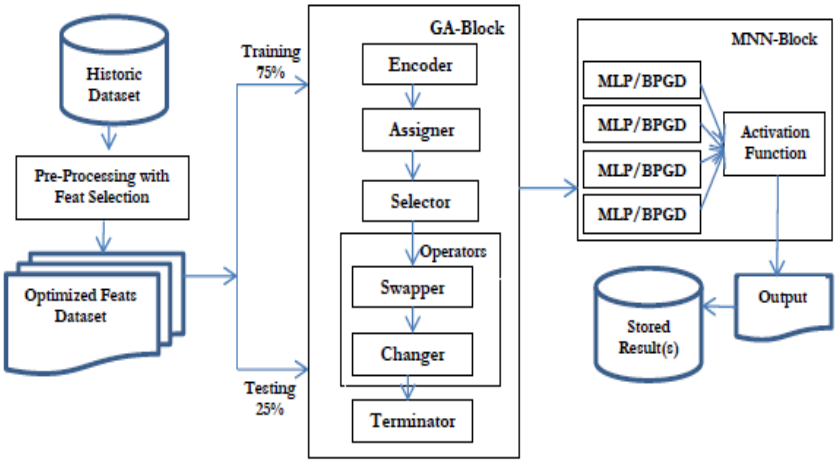

Fig. 1. Proposed Stacking Ensemble Approach with XGBoost as Meta-heuristics

1. **Step-1 – Data Collection:** DDoS dataset is available on [web]: kaggle.com/datasets/DDoS-dataset. It consists of 54804-records divided into 35698-genuine and 19106-attack (for major and minor classes).
2. **Step 2 – Preprocessing** deletes missing labels to ensure quality, and deletes duplicate data to avoid redundancy in dataset. Next, we encode the dataset using principal component analysis (PCA) to converts all categorial data on to their numeric equivalence.
3. **Step 3 – Fitness Function** extracts and select data-labels that yields the input (X), and the corresponding label for which the ensemble will predict as output (Y). It achieves this by removing all docile/irrelevant feats with less significance to the target class. This, dimensionality reduction of the chosen predictors will fasten ensemble construction for improved performance [104], especially for scenarios of cost as critical factor [105]. Its efficiency is evaluated by how well the ensemble fits about ground truth or target class. With a threshold of 11.321 – a total of 7 features was used in lieu of the target class 1 (i.e., anomaly) to aid insights into the contribution of different features to the classification process.

4. **Step-4 Data Balancing** redistributes data and ensures an almost equal class distribution. Here, we explore the SMOTE approach as thus:
5. **SMOTE**: the synthetic over-sample technique is done as thus: (a) identify the minor-class and adjusts labels to those of its closest neighbors, (b) then, interpolate these labels to generate synthetic labels, and (c) repopulate the original dataset with the generated synthetic data to yield a dataset with balanced class distribution as in Fig. 2.

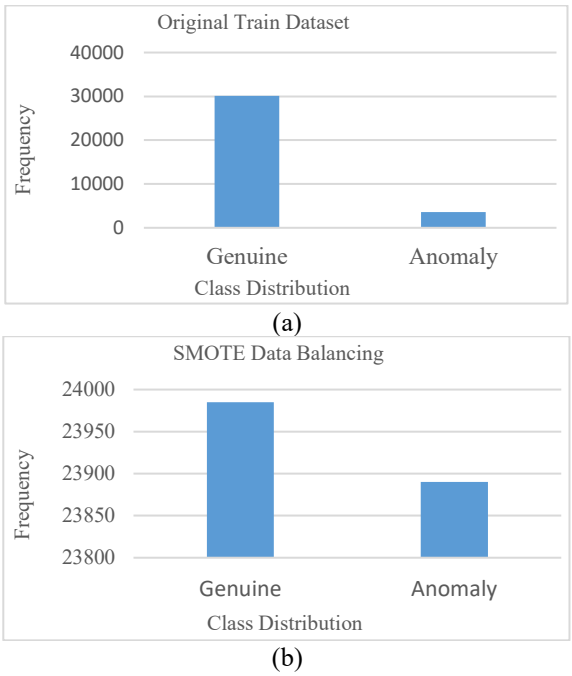

Fig. 2. (a) Original data plot and (b) Data balancing with SMOTE applied

SMOTE-Tomek links approach seek to balance the class distribution extending the SMOTE mode. It uses the Tomek-links to under-sample the major class, and thus, generate overlapping labels in the class [106] as in Fig. 3. For this study, we utilize the SMOTE-Tomek links mode to provision a good-fit for both classes.

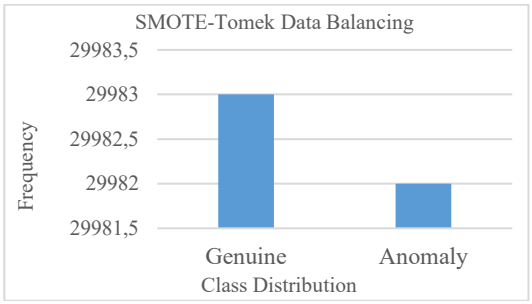

Fig. 3. Data Balancing via SMOTE-Tomek

6. **Step-5 – Normalization and Splitting** utilizes variable transform to act and ensure class distribution nearness, resulting in a more balanced distributed classes using the standard normalizer that reverts data features utilizing a mean of 0 and standard deviation of 1 for the class distribution(s) as in Equation (1):

$$z = \frac{(x - \mu)}{\sigma} \quad (1) \qquad (1)$$

x is the original value, μ is mean, σ is the standard deviation, and z is our normalization process. Afterward, the dataset is split into 75% for training and 25% for testing (validation) subsets.

A. The Genetic Algorithm Trained Modular Neural Net

The modular, stacked nature of this ensemble combines the predictive output of 2-base learners to achieve greater prediction accuracy. Its merits includes: (a) diversification of models via utilization of many schemes [107], (b) enhanced generalization, and (c) reduced risk of model overfit. These must assist the model to optimize the summed outcome and minimize errors at training via out-of-fold prediction. This, improves its accuracy, robustness, and flexibility to harness the processing prowess of the good-fit, multi-base leaners cum classifier models [108]. Thus, we explain the stacked model approach as consisting:

1. The Supervised Genetic Algorithm: Gas by design explores 4 operators/sections 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 thus: (a) ***norm*** specifies the upper/lower range that bounds a gene, (b) ***domain*** specifies data about the task to the model, (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 number of potential candidates that the CGA generates until it reaches the optimum [109].
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 noticed, are 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.

B. Tree-based Training Phase

Here, trees are iteratively constructed using the bootstrap mode to yield the required enhancements. This also improves the trees' collective knowledge so as to assist the ensemble to quickly identify intricate patterns inherent in the dataset. Thus, at training – ensemble can effectively fuse the synthetic generated data-labels with the original labels; And in turn – it guarantees that the classifier yields comprehensive learning, which will improve the heuristics flexibility and adaptability for reuse in other domain tasks.

Table 2 are labeled attacks: ***ICMP PING*** – Internet Control Protocol Packet Internet Groper, ***NP*** – Ping, PS – Port Scan, ***PAS***–Packet Sniffer, ***PA*** – Protocol Analyzer, ***PG*** – Password Guess, ***PC*** – Password Cracking, ***SH*** – Session Hijack, ***SR*** – Session Replay, ***IPS*** – IP Spoof, ***DN*** – Domain Name attack, ***RA*** – Reroute Attack, ***ARS*** – Address Resolution Spoof, ***FA*** – Flood Attack, ***PODA*** – Ping of Death, etc [110].

The net weights (i.e. w1 and w2) were recorded as 0.2 and 0.8. Our first rule from Table 1 is explained thus:
if (duration="-1:0:23", protocol ="telnet" and source-port=-1 dest-port=23, source IP="192.168.1.30", destination IP ="192.168.0.20) ***then*** {log network connection as an **Intrusion**}.

10% training data used in cross-validation with stratified k-fold arranged so that each fold yields a good representation.

Table 1. Fitness Ranking of Features Selected for the 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
0,0,5	-1	-1	-1	192.168.1.30	192.168.0.20	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
-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	192.168.0.20	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

III. Result Findings and Discussion

A. Results Findings and Discussion

Training allows an ensemble to adjust its weights and biases. We tune the hyper-parameters via a trial-n-error mode as in Table 2 with learning_rate, n_estimators, and max_depth, respectively to yield an optimal fit as thus:

Table 2. Hyper-Parameter Tuning

Iteration	Transaction	Confusion Matrix	Attack
Max-Depths	Max. depth	[1, 2, 4, 5, 6, 8, 10]	5
Learning Rate	Step weights	[0.1, 0.2, 0.3, 0.5, 0.75]	0.25
N_Estimators	Number of nodes	[100, 200, 300, 400, 500]	250

We classify DDoS attacks with results as in Table 3.

Table 3. Base Learner Performance Metrics Details

Schemes	F1	Accuracy	Precision	Recall
DT	0.9805	0.9815	0.9805	0.9745
RF	0.9881	0,9968	0.9318	0.9848
XGBoost	0.9925	0.9981	0.9541	0.9881
Our Ensemble	0.9945	0.9984	0.9616	0.9890

Table 3 shows proposed ensemble yields F1 of 0.9945, and outperforms XGBoost, RF, and DT with F1 of 0.9925, 0.9881, and 0.9805 respectively. The proposed model has an accuracy of 0.9984 to outperform RF, XGBoost, and DT with 0.9981, 0.9964, and 0.9815 respectively. Precision and Recall as in Table 3. The ensemble yields insights into which features have a greater influence on performance to identify important feats that influence a model's predictions [111].

Fig. 4 is the confusion matrix, which implies proposed experimental ensemble can correctly classify the test dataset with a 99.84% accuracy – showing that it correctly classified all 13.418 records with only 283 cases incorrectly classified. Thus, SMOTE-Tomek outperformed both SMOTE(EN) with a greater impact to ground truth (i.e. overall performance) by identifying predictors of importance that influences model prediction with enhanced efficiency to differentiate all the various scores of true/false-positives/negatives [112].

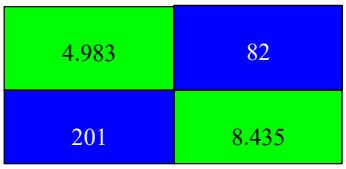

Fig. 4. Confusion Matrix for the Memetic Ensemble

B. Comparison

We benchmark our ensemble against similar constructs and datasets for various domain tasks as seen in Table 4.

Table 4. Benchmark / Comparative Testing of Method

Methods	Accuracy	Precision	Recall	F1	Spec.
Ref [106]	1.0000	1.0000	0.9999	1.0000	1.0000
Ref [113]	0.8728	0.8500	0.8120	0.8925	0.9300
Ref [114]	0,9968	0.9318	0.9848	0.9881	0.8902
Ref [115]	0.9981	0.9541	0.9881	0.9925	0.7829
Our Method	0.9984	0.9616	0.9890	0.9945	0.9998

Whilst some tasks have proven much easier to classify [90]; Others, have are more painstaking such as task(s) with image and medical data, which requires the chosen model to explore metrics such as specificity – with strong impacts on the consequence of a diagnostic error. Thus, specificity is a critical feat that must be evaluated as it directly relates to a patient's clinical output [116]. Furthermore, in dealing with stacked ensemble – we must satisfactorily resolve conflicts

such as: (a) data encoding from one model to another, and (b) structural dependencies as imposed by base heuristics adopted. To resolve the data-encoding conflict – we utilize a one-hot encoding technique which successfully converts all categorical data into their binary equivalence and proper format for use by the proposed ML heuristics.

IV. CONCLUSION

Finding a perfect balance with recall and specificity is a crucial task especially with noise rippled across the dataset. Models must yield tradeoff as accuracy equates to reliability (with less insight due to data imbalance) that yields distorted performance. Also, F1 assess performance on criteria such as data imbalance – as it has been found to provide an altruist insight into a technique's effectiveness in classifying positive cases without the overprediction of false positives. The chaotic nature of breaches vis-à-vis noisy datasets with their many features, will continue to yield studies into the use of deep ensemble learning heuristics as the suitable mode for addressing many cyber-attacks. The variance and bias in the ML task – make for the possibility of an optimized training sample if greater performance must be achieved. We used the deep ensemble (Genetic Algorithm Modular fused learning Neural Network) to detect packet behavior and anomaly-based detection of malicious packets. We explored GA due to its flexibility as an elitist model; While the MNN is used as a learning paradigm for the components; our model validation returns a confusion matrix.

REFERENCES

[1] 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. 2a, pp. 80–94, 2024, https://doi.org/10.4314/dujopas.v10i2a.8.

[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, https://doi.org/10.14569/IJACSA.2021.0120166.

[3] A. Basit, M. Zafar, A. R. Javed and Z. Jalil, "A Novel Ensemble Machine Learning Method to Detect Phishing Attack," *2020 IEEE 23rd International Multitopic Conference (INMIC)*, pp. 1-5, 2020, https://doi.org/10.1109/INMIC50486.2020.9318210.

[4] A. A. Ojugo and O. D. 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, 2018, https://doi.org/10.5539/nct.v3n1p33.

[5] D. R. I. M. Setiadi, A. Susanto, K. Nugroho, A. R. Muslikh, A. A. Ojugo, and H. Gan, "Rice yield forecasting using hybrid quantum deep learning model," *MDPI Comput.*, vol. 13, no. 191, pp. 1–18, 2024, https://doi.org/10.3390/computers13080191.

[6] 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, 2023, https://doi.org/10.11591/ijere.v12i3.24086.

[7] A. A. Ojugo and O. D. Otakore, "Intelligent cluster connectionist recommender system using implicit graph friendship algorithm for social networks," *IAES Int. J. Artif. Intell.*, vol. 9, no. 3, p. 497~506, 2020, https://doi.org/10.11591/ijai.v9.i3.pp497-506.

[8] 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, https://doi.org/10.38124/IJISRT20AUG526.

[9] [9] B. O. Malasowe, M. I. Akazue, A. E. 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 https://doi.org/10.14569/IJACSA.2023.0140816.

[10] 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, https://doi.org/10.14569/IJACSA.2023.0140610.

[11] 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, https://doi.org/10.2139/ssrn.4061818.

[12] 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, https://doi.org/10.14569/IJACSA.2024.0150354.

[13] 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, https://doi.org/10.5120/ijca2018916586.

[14] 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, https://doi.org/10.35877/454RI.asci2192.

[15] 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, https://www.inase.org/library/2015/.

[16] B. Habib and F. Khursheed, "Performance evaluation of machine learning models for distributed denial of service attack detection using improved feature selection and hyper-parameter optimization techniques," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 26, p. e7299, 2022, https://doi.org/10.1002/cpe.7299.

[17] P. Sharma and N. Hasteer, "Analysis of linear sequential and extreme programming development methodology for a gaming application," 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 1916-1920, 2016, https://doi.org/10.1109/ICCSP.2016.7754505.

[18] 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, https://doi.org/10.11591/ijeecs.v21.i3.pp1673-1682.

[19] L. F. Rahman, M. Marufuzzaman, L. Alam, M. A. Bari, U. R. Sumaila, and L. M. Sidek, "Developing an ensembled machine learning prediction model for marine fish and aquaculture production," *Sustainability*, vol. 13, no. 16, p. 9124, 2021, https://doi.org/10.3390/su13169124.

[20] 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, 2021, https://doi.org/10.1016/j.jjimei.2021.100048.

[21] K. G. Arachchige, P. Branch, and J. But, "An Analysis of Blockchain-Based IoT Sensor Network Distributed Denial of Service Attacks," *Sensors*, vol. 24, no. 10, p. 3083, 2024, https://doi.org/10.3390/s24103083.

[22] 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, https://doi.org/10.1007/978-3-031-33743-7_48.

[23] [23] 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, https://doi.org/10.4018/JCIT.318703.

[24] T. Muralidharan and N. Nissim, "Improving malicious email detection through novel designated deep-learning architectures utilizing entire email," *Neural Networks*, vol. 157, pp. 257-279, 2023, https://doi.org/10.1016/j.neunet.2022.09.002.

[25] 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, https://doi.org/10.33633/jcta.v1i2.9462.

[26] 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, https://doi.org/10.35877/454RI.qems139.

[27] 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, https://doi.org/10.7494/csci.2023.24.1.4551.

[28] 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, https://doi.org/10.11591/ijict.v8i3.pp128-138.

[29] S. Pande and A. Khamparia, "Explainable Deep Neural network-based analysis on intrusion detection systems," *Comput. Sci.*, vol. 24, no. 1, pp. 5–30, 2023, https://doi.org/10.7494/csci.2023.24.1.4551.

[30] 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, https://doi.org/10.1109/ACCESS.2020.3037359.

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

[32] E. Bandara, S. Shetty, R. Mukkamala, A. Rahaman and X. Liang, "LUUNU — Blockchain, MISP, Model Cards and Federated Learning Enabled Cyber Threat Intelligence Sharing Platform," *2022 Annual Modeling and Simulation Conference (ANNSIM)*, pp. 235-245, 2022, https://doi.org/10.23919/ANNSIM55834.2022.9859355.

[33] 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, 2021, https://doi.org/10.30534/ijatcse/2021/851032021.

[34] 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, https://journal.fupre.edu.ng/index.php/fjsir/article/view/225.

[35] 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, https://doi.org/10.5815/ijitcs.2018.10.07.

[36] 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, https://doi.org/10.11591/ijict.v9i3.pp185-194.

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

[38] 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, https://doi.org/10.5815/ijmecs.2014.08.04.

[39] 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, https://doi.org/10.33633/jcta.v1i2.9259.

[40] D. A. Obasuyi *et al.*, "NiCuSBlockIoT: Sensor-based Cargo Assets Management and Traceability Blockchain Support for Nigerian Custom Services," *Adv. Multidiscip. Sci. Res. J. Publ.*, vol. 15, no. 2, pp. 45–64, 2024, https://doi.org/10.22624/AIMS/CISDI/V15N2P4.

[41] 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, https://doi.org/10.22624/AIMS/BIHIV10N1P6.

[42] S. K. Majhi, M. Sahoo, and R. Pradhan, "A space transformational crow search algorithm for optimization problems," *Evolutionary Intelligence*, vol. 13, no. 3, pp. 345-364, 2020, https://doi.org/10.1007/s12065-019-00294-7.

[43] V. O. Geteloma *et al.*, "Enhanced data augmentation for predicting consumer churn rate with monetization and retention strategies: a pilot study," *Appl. Eng. Technol.*, vol. 3, no. 1, pp. 35–51, 2024, https://doi.org/10.31763/aet.v3i1.1408.

[44] 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, https://doi.org/10.14569/IJACSA.2023.01404101.

[45] 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, https://doi.org/10.11591/eei.v12i4.4459.

[46] A. A. Ojugo and D. A. Oyemade, "Boyer moore string-match framework for a hybrid short message service spam filtering technique," *IAES Int. J. Artif. Intell.*, vol. 10, no. 3, pp. 519–527, 2021, https://doi.org/10.11591/ijai.v10.i3.pp519-527.

[47] S. E. Brizimor *et al.*, "WiSeCart: Sensor-based Smart-Cart with Self-Payment Mode to Improve Shopping Experience and Inventory Management," *Adv. Multidiscip. Sci. Res. J. Publ.*, vol. 10, no. 1, pp. 53–74, 2024, https://doi.org/10.22624/AIMS/SIJ/V10N1P7.

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

[49] 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. Publ.*, vol. 12, no. 2, pp. 25–44, 2024, https://doi.org/10.22624/AIMS/MATHS/V12N2P3.

[50] B. O. Malasowe, A. E. Okpako, M. D. Okpor, P. O. Ejeh, A. A. Ojugo, and R. E. Ako, "FePARM: The Frequency-Patterned Associative Rule Mining Framework on Consumer Purchasing-Pattern for Online Shops," *Adv. Multidiscip. Sci. Res. J. Publ.*, vol. 15, no. 2, pp. 15–28, 2024, https://doi.org/10.22624/AIMS/CISDI/V15N2P2-1.

[51] R. E. Ako *et al.*, "Effects of Data Resampling on Predicting Customer Churn via a Comparative Tree-based Random Forest and XGBoost," *J. Comput. Theor. Appl.*, vol. 2, no. 1, pp. 86–101, Jun. 2024, https://doi.org/10.62411/jcta.10562.

[52] M. D. Okpor *et al.*, "Comparative Data Resample to Predict Subscription Services Attrition Using Tree-based Ensembles," *J. Fuzzy Syst. Control*, vol. 2, no. 2, pp. 117–128, 2024, https://doi.org/10.59247/jfsc.v2i2.213.

[53] F. O. Aghware *et al.*, "BloFoPASS: A blockchain food palliatives tracer support system for resolving welfare distribution crisis in Nigeria," *Int. J. Informatics Commun. Technol.*, vol. 13, no. 2, p. 178, 2024, https://doi.org/10.11591/ijict.v13i2.pp178-187.

[54] M. Huang, W. Liu, T. Wang, H. Song, X. Li, and A. Liu, "A queuing delay utilization scheme for on-path service aggregation in services-oriented computing networks," *IEEE Access*, vol. 7, pp. 23816–23833, 2019, https://doi.org/10.1109/ACCESS.2019.2899402.

[55] C. Zoremsanga and J. Hussain, "Particle Swarm Optimized Deep Learning Models for Rainfall Prediction: A Case Study in Aizawl, Mizoram," in *IEEE Access*, vol. 12, pp. 57172-57184, 2024, https://doi.org/10.1109/ACCESS.2024.3390781.

[56] X. Tang, K. An, K. Guo, Y. Huang, and S. Wang, "Outage analysis of non-orthogonal multiple access-based integrated satellite-terrestrial relay networks with hardware impairments," *IEEE Access*, vol. 7, no. September, pp. 141258–141267, 2019, https://doi.org/10.1109/ACCESS.2019.2944406.

[57] B. Medina-Salgado, E. Sánchez-DelaCruz, P. Pozos-Parra, and J. E. Sierra, "Urban traffic flow prediction techniques: A review," *Sustain. Comput. Informatics Syst.*, vol. 35, p. 100739, 2022, https://doi.org/10.1016/j.suscom.2022.100739.

[58] A. A. Ojugo and O. Nwankwo, "Multi-Agent Bayesian Framework For Parametric Selection In The Detection And Diagnosis of Tuberculosis Contagion In Nigeria," *JINAV J. Inf. Vis.*, vol. 2, no. 2, pp. 69–76, Mar. 2021, https://doi.org/10.35877/454RI.jinav375.

[59] A. A. Ojugo and R. E. Yoro, "Migration Pattern As Threshold Parameter In The Propagation of The Covid-19 Epidemic Using An Actor-Based Model for SI-Social Graph," *JINAV J. Inf. Vis.*, vol. 2, no. 2, pp. 93–105, 2021, https://doi.org/10.35877/454RI.jinav379.

[60] A. A. Ojugo and O. Nwankwo, "Modeling Mobility Pattern for the Corona-Virus Epidemic Spread Propagation and Death Rate in Nigeria using the Movement-Interaction-Return Model," *Int. J. Emerg. Trends Eng. Res.*, vol. 9, no. 6, pp. 821–826, 2021, https://doi.org/10.30534/ijeter/2021/30962021.

[61] Y. Bouchlaghem, Y. Akhiat, and S. Amjad, "Feature Selection: A Review and Comparative Study," *E3S Web Conf.*, vol. 351, pp. 1–6, 2022, https://doi.org/10.1051/e3sconf/202235101046.

[62] S. Wang, J. Cao, and P. S. Yu, "Deep Learning for Spatio-Temporal Data Mining: A Survey," *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 8, pp. 3681–3700, 2022, https://doi.org/10.1109/TKDE.2020.3025580.

[63] J. Yao, C. Wang, C. Hu, and X. Huang, "Chinese Spam Detection Using a Hybrid BiGRU-CNN Network with Joint Textual and Phonetic Embedding," *Electronics*, vol. 11, no. 15, p. 2418, 2022, https://doi.org/10.3390/electronics11152418.

[64] C. H. Lee, H. C. Yang, Y. C. Wei, and W. K. Hsu, "Enabling blockchain based scm systems with a real time event monitoring function for preemptive risk management," *Appl. Sci.*, vol. 11, no. 11, 2021, https://doi.org/10.3390/app11114811.

[65] D. A. Oyemade and A. A. Ojugo, "A property oriented pandemic surviving trading model," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 5, pp. 7397–7404, 2020, https://doi.org/10.30534/ijatcse/2020/71952020.

[66] S. Basterrech and M. Wozniak, "Tracking changes using Kullback-Leibler divergence for the continual learning," in *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 3279–3285, 2022, https://doi.org/10.1109/SMC53654.2022.9945547.

[67] 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, 2021, https://doi.org/10.35877/jetech613.

[68] A. A. Ojugo, C. O. Obruche, and A. O. Eboka, "Empirical Evaluation for Intelligent Predictive Models in Prediction of Potential Cancer Problematic Cases In Nigeria," *ARRUS J. Math. Appl. Sci.*, vol. 1, no. 2, pp. 110–120, 2021, https://doi.org/10.35877/mathscience614.

[69] 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, 2022, https://doi.org/10.1186/s40537-022-00573-8.

[70] 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, https://doi.org/10.52436/1.jutif.2023.4.6.1529.

[71] A. P. Binitie and O. J. Babatunde, "Evaluating the privacy issues, potential risks, and security measures associated with using social media platforms," *Int. J. African Res. Sustain. Stud.*, vol. 3, no. 2, pp. 167–179, 2024, https://cambridgeresearchpub.com/ijarss/article/view/139.

[72] J. Herdiansyah, F. Ariefka, S. Putra, and D. Septiyanto, "Implementation of Zhang' s Camera Calibration Algorithm on a Single Camera for Accurate Pose Estimation Using ArUco Markers," *J. Fuzzy Syst. Control*, vol. 2, no. 3, pp. 176–188, 2024, https://doi.org/10.59247/jfsc.v2i3.256.

[73] 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, 2023, https://doi.org/10.7717/peerj-cs.1278.

[74] E. Blancaflor, H. K. S. Billo, B. Y. P. Saunar, J. M. P. Dignadice and P. T. Domondon, "Penetration assessment and ways to combat attack on Android devices through StormBreaker - a social engineering tool," *2023 6th International Conference on Information and Computer Technologies (ICICT)*, pp. 220-225, 2023, https://doi.org/10.1109/ICICT58900.2023.00043.

[75] A. S. Ali, E. H. Ali, S. W. Shneen, and L. H. Abood, "Adaptive Fuzzy Filter Technique for Mixed Noise Removing from Sonar Images Underwater," *J. Fuzzy Syst. Control*, vol. 2, no. 2, pp. 45–49, 2024, https://doi.org/10.59247/jfsc.v2i2.176.

[76] A. A. Ojugo and O. Nwankwo, "Tree-classification Algorithm to Ease User Detection of Predatory Hijacked Journals: Empirical Analysis of Journal Metrics Rankings," *Int. J. Eng. Manuf.*, vol. 11, no. 4, pp. 1–9, 2021, https://doi.org/10.5815/ijem.2021.04.01.

[77] H. Huang, Y. Song, Z. Fan, G. Xu, R. Yuan, and J. Zhao, "Estimation of walnut crop evapotranspiration under different micro-irrigation techniques in arid zones based on deep learning sequence models," *Results Appl. Math.*, vol. 20, no. September, p. 100412, 2023, https://doi.org/10.1016/j.rinam.2023.100412.

[78] M. I. Akazue *et al.*, "FiMoDeAL: pilot study on shortest path heuristics in wireless sensor network for fire detection and alert ensemble," *Bull. Electr. Eng. Informatics*, vol. 13, no. 5, pp. 3534–3543, 2024, https://doi.org/10.11591/eei.v13i5.8084.

[79] 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, p. 108, 2024, https://doi.org/10.11591/ijict.v13i1.pp108-115.

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

[81] 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, https://doi.org/10.17977/um018v6i22023p145-156.

[82] M. A. Haque *et al.*, "Cybersecurity in Universities: An Evaluation Model," *SN Comput. Sci.*, vol. 4, no. 5, 2023, https://doi.org/10.1007/s42979-023-01984-x.

[83] C. C. Odiakaose *et al.*, "Hypertension Detection via Tree-Based Stack Ensemble with SMOTE-Tomek Data Balance and XGBoost Meta-Learner," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 3, pp. 269–283, 2024, https://doi.org/10.62411/faith.3048-3719-43.

[84] E. U. Omede, A. E. 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. 1, no. 3, pp. 273–283, Feb. 2024, https://doi.org/10.62411/jcta.9541.

[85] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," *Comput. Secur.*, vol. 104, 2021, https://doi.org/10.1016/j.cose.2021.102221.

[86] K. A. Egbe, A. Ike, and F. Egbe, "Knowledge and burden of hepatitis B virus in Nasarawa State, Nigeria," *Scientific African*, vol. 22, p. e01938, 2023, https://doi.org/10.1016/j.sciaf.2023.e01938.

[87] J. K. Oladele *et al.*, "BEHeDaS: A Blockchain Electronic Health Data System for Secure Medical Records Exchange," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 231–242, 2024, https://doi.org/10.62411/jcta.9509.

[88] 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. Publ.*, vol. 12, no. 2, pp. 45–66, 2024, https://doi.org/10.22624/AIMS/MATHS/V12N2P4.

[89] 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, https://doi.org/10.22624/AIMS/DIGITAL/V11N4P3.

[90] B. O. Malasowe *et al.*, "Quest for Empirical Solution to Runoff Prediction in Nigeria via Random Forest Ensemble: Pilot Study," *Adv. Multidiscip. Sci. Res. J. Publ.*, vol. 10, no. 1, pp. 73–90, 2024, https://doi.org/10.22624/AIMS/BHI/V10N1P8.

[91] S. N. Okofu *et al.*, "Pilot Study on Consumer Preference, Intentions and Trust on Purchasing-Pattern for Online Virtual Shops," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 7, pp. 804–811, 2024, https://doi.org/10.14569/IJACSA.2024.0150780.

[92] M. Dewis and T. Viana, "Phish responder: A hybrid machine learning approach to detect phishing and spam emails," *Applied System Innovation*, vol. 5, no. 4, p. 73, 2022, https://doi.org/10.3390/asi5040073.

[93] 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, https://doi.org/10.12785/ijcds/100119.

[94] 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, https://doi.org/10.33633/jcta.v1i2.9355.

[95] 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, https://doi.org/10.14569/IJACSA.2023.0140424.

[96] M. D. Okpor *et al.*, "Pilot Study on Enhanced Detection of Cues over Malicious Sites Using Data Balancing on the Random Forest Ensemble," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 2, pp. 109–123, 2024, https://doi.org/10.62411/faith.2024-14.

[97] K. Muhamada, D. R. Ignatius, M. Setiadi, U. Sudibyo, B. Widjajanto, and A. A. Ojugo, "Exploring Machine Learning and Deep Learning Techniques for Occluded Face Recognition: A Comprehensive Survey and Comparative Analysis," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 2, pp. 160–173, 2024, https://doi.org/10.62411/faith.2024-30.

[98] V. O. Geteloma *et al.*, "AQuaMoAS: unmasking a wireless sensor-based ensemble for air quality monitor and alert system," *Appl. Eng. Technol.*, vol. 3, no. 2, pp. 86–101, 2024, https://doi.org/10.31763/aet.v3i2.1536.

[99] 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, https://doi.org/10.11648/j.net.20150302.11.

[100] 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. 1, no. 4, pp. 407–420, 2024, https://doi.org/10.62411/jcta.10323.

[101] D. R. I. M. Setiadi, A. R. Muslikh, S. W. Iriananda, W. Warto, J. Gondohanindijo, and A. A. Ojugo, "Outlier Detection Using Gaussian Mixture Model Clustering to Optimize XGBoost for Credit Approval Prediction," *J. Comput. Theor. Appl.*, vol. 2, no. 2, pp. 244–255, 2024, https://doi.org/10.62411/jcta.11638.

[102] 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, 2021, https://doi.org/10.35877/454RI.asci2163.

[103] 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, 2021, https://doi.org/10.11591/ijai.v10.i3.pp623-635.

[104] A. A. Ojugo *et al.*, "Forging a learner-centric blended-learning framework via an adaptive content-based architecture," *Sci. Inf. Technol. Lett.*, vol. 4, no. 1, pp. 40–53, 2023, https://doi.org/10.31763/sitech.v4i1.1186.

[105] O. V. Lee *et al.*, "A malicious URLs detection system using optimization and machine learning classifiers," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 17, no. 3, p. 1210, 2020, https://doi.org/10.11591/ijeecs.v17.i3.pp1210-1214.

[106] D. R. I. M. Setiadi, K. Nugroho, A. R. Muslikh, S. W. Iriananda, 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, https://doi.org/10.62411/faith.2024-11.

[107] A. A. Ojugo and A. O. Eboka, "Empirical Evidence of Socially-Engineered Attack Menace Among Undergraduate Smartphone Users in Selected Universities in Nigeria," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 10, no. 3, pp. 2103–2108, 2021, https://doi.org/10.30534/ijatcse/2021/861032021.

[108] D. Nguyen *et al.*, "Adaptive Evaluation of LQR Control using Particle Swarm Optimization for Pendubot," *J. Fuzzy Syst. Control*, vol. 2, no. 2, pp. 58–66, 2024, https://doi.org/10.59247/jfsc.v2i2.203.

[109] S. Pavithra and K. Venkata Vikas, "Detecting Unbalanced Network Traffic Intrusions With Deep Learning," in *IEEE Access*, vol. 12, pp. 74096-74107, 2024, https://doi.org/10.1109/ACCESS.2024.3405187.

[110] 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, 2023, https://doi.org/10.11591/ijict.v12i3.pp205-213.

[111] A. A. Ojugo and O. D. Otakore, "Intelligent Peer-To-Peer Banking Framework: Advancing The Frontiers of Agent Banking For Financial Inclusion In Nigeria Via Smartphones," *Quant. Econ. Manag. Stud.*, vol. 1, no. 5, pp. 300–311, 2020, https://doi.org/10.35877/454RI.qems140.

[112] Narayanan and Jayashree, "Implementation of Efficient Machine Learning Techniques for Prediction of Cardiac Disease using SMOTE," *Procedia Comput. Sci.*, vol. 233, no. 2023, pp. 558–569, 2024, https://doi.org/10.1016/j.procs.2024.03.245.

[113] A. P. Binitie *et al.*, "Stacked Learning Anomaly Detection Scheme with Data Augmentation for Spatiotemporal Traffic Flow," *J. Fuzzy Syst. Control*, vol. 2, no. 3, pp. 203–214, 2024, https://doi.org/10.59247/jfsc.v2i3.267.

[114] A. N. Safriandono, D. R. I. M. Setiadi, A. Dahlan, F. Z. Rahmanti, I. S. Wibisono, and A. A. Ojugo, "Analyzing Quantum Feature Engineering and Balancing Strategies Effect on Liver Disease Classification," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 1, pp. 51–63, 2024, https://doi.org/10.62411/faith.2024-12.

[115] 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. 1, no. 3, pp. 346–357, 2024, https://doi.org/10.62411/jcta.9539.

[116] S. Khaki, L. Wang, and S. V. Archontoulis, "A CNN-RNN Framework for Crop Yield Prediction," *Front. Plant Sci.*, vol. 10, 2020, https://doi.org/10.3389/fpls.2019.01750.