Research Article / Review Article

FUPRE JOURNAL 10(1):43-58(2026)
https://doi.org//10.60787/FJSIR.v10i1.43-58

FUPRE Journal

of

Scientific and Industrial Research

ISSN: 2579-1184(Print) ISSN: 2578-1129 (Online)

http://fupre.edu.ng/journal

Unmasking High Performance Phishing Detection with Feature Fusion of a Tree-based Transfer Learning Boosted Approach using SMOTE-Tomek Balancing: A Pilot Study

OJUGO. A. A.*[1,*], *AGBOI, J.*[2], *UGBOH, E.*[3], *ASUNOGIE. O. T.*[4], *IGULU, T. K.*[5], *ONOMA, P. A.*[6], *ABERE, R. A.*[7], *AHEROBO, O. V.*[8] *OKPERIGHO, S. U.

[1,6,7,8,9]*College of Computing, Federal University of Petroleum Resources Effurun, Delta 330212,*
[2]*Faculty of Computing, Delta State University Asaba. Delta 331202*
[3]*School of Science, Federal College of Education Technical Asaba*
[4]*Faculty of Computing, Edo State University Iyamho. Edo 312102,*
[5]*Faculty of Computing, Ignatius Ajuru University of Education, Rivers*

ARTICLE INFO

Received: 25/01/2026

Accepted: 01/03/2026

Keywords

Cultural GA
Feature Fusion
Phishing Detection
Tree-based Algorithm
SMOTE-Tomek

ABSTRACT

Daily exchange of data has eased its proliferation, accessibility, availability and interoperability of accompanying devices. This is further eased with widespread proliferation of smartphones, which has also in turn – birthed attacks targeted at network infrastructures to exploit interconnected, shared resources. Its rising success rate and increased susceptibility to these attacks can be traced to user's personality traits and behaviours, which renders them repeatedly vulnerable to such exploits especially those rippled across spoofed websites. Our study posits a stacked approach to classify malicious contents over a spoofed website. It explores 3-base classifiers namely Cultural Genetic Algorithm, Random Forest, and Korhonen Modular Neural Network – whose output is utilized as input for XGBoost meta-learner. Our study resolved dataset imbalance challenge using the SMOTE-Tomek mode; while, the selected predictors was resolved using the relief rank feature selection. Results shows ensemble yields F1 0.95, Accuracy 1.00, Recall 0.98, Precision 1.00, and Specificity 1.00 – to accurately classify all 2,764 cases of its test dataset. Ensemble outperformed benchmarks and was effectively classified phishing (cues and lures) contents on websites.

1. INTRODUCTION

Digital revolution has ushered in a plethora of tools/processes that seek to advance efficient knowledge exchange among users (Hera, 2024; Sinduja, 2021). The devices ease data processing while offering the benefits of flexibility in the shared resource cum enhanced user-connectivity (Allenotor *et al.*, 2015; Allenotor & Ojugo, 2017). With security a major issue, such advances also ignite the interest of attackers (Aghware, Ojugo, *et al.*, 2024; Aghware *et al.*, 2025). Smartphone proliferation has eased itself as invasive target (Agboi, Emordi, *et al.*, 2025; Agboi, Onoma, *et al.*, 2025; Aghware *et al.*, 2023a; Aghware, Okpor, *et al.*, 2024). Adversary use penetrative tools like malware to bolster attacks that explore subterfuge to coordinate its attack at unsuspecting device, and compromise network resources (Atuduhor *et al.*, 2024; Otorokpo *et al.*, 2024). Attack ensures data exchange is targeted to exploit a user's social need (Sudheer *et al.*, 2025), desires and insatiable trait (Umar, 2025). Businesses are reshaped via fusion of informatics (Sasikala *et al.*, 2022) – as a channel to deliver high values to consumers,

*Corresponding author, e-mail: ojugo.arnold@fupre.edu.ng, abere.reuben@fupre.edu.ng, kenbridge14@gmail.com, okperigho.samuel@fupre.edu.ng, ovieaherobo0709@gmail.com, agboijoy0@gmail.com, ugboh1972@gmail.com, asunogie.taibat@edouniversity.edu.ng, igulu.kingsley@iaue.edu.ng.
https://doi.org/10.60787/FJSIR.v10i1.43-58
©Scientific Information, Documentation and Publishing Office at FUPRE Journal

who receive services as rendered. This exchange has become a trillion-dollar war (Baker *et al.*, 2025), as businesses seek new frontiers to curb phishing and other issues (Ojugo & Eboka, 2018a, 2018b, 2018c) as failure to safeguard the data exchange ushers in cross-cutting studies (Geteloma *et al.*, 2024a, 2024b, 2025; Umar, 2025).

The success of the attacks is hinged on user personality traits, which include online presence, emotional seclusion, insatiable wants, and trust issues (Hakonen, 2022). Adversary masks his/her intent as a trusted ally, to exploit an unsuspecting compromised resource – providing the attacker with a pivot access for further exploits on the infrastructure (Ibor *et al.*, 2023; Ifioko *et al.*, 2024). The rise in the adoption of smartphones has further eased these attacks and compromises considerably. Phishing redirects a user's request to a spoofed site, rippled with malicious content that seeks to expose a targeted user without their knowledge (Li, Manickam, *et al.*, 2025). Phishing consists of 3-elements: (a) lure masks an attacker as a genuine user, targeting a user's empathy, fear and curiosity (Nur *et al.*, 2025), (b) a hook is an embedded link in a message (Jáñez-Martino *et al.*, 2022), and (c) a catch obtains an exposed device's private data. Its success is hinged on its frequency and diversity with unrealistic demands that seek to intimidate a user's psyche with gifts (Haque *et al.*, 2023). Scam vulnerability due to gender and age (Ojugo, Akazue, Ejeh, Odiakaose, *et al.*, 2023; Ojugo, Odiakaose, Emordi, Ako, *et al.*, 2023) noted that girls between 24-to-42 years were most phished via social seclusion; There is the issue of education and society approval (Okpor, Aghware, Akazue, Eboka, *et al.*, 2024); and users between 18-to-29years phished more due to behavioural traits (Ejeh *et al.*, 2024; Justice & Dumka, 2021).

To identify malicious contents, we eliminate gaps as follows (Malasowe, Edim, *et al.*, 2024; Malasowe, Okpako, *et al.*, 2024; Mia *et al.*, 2025): (a) identify lures that increases user believability (Malasowe, Aghware, *et al.*, 2024; Malasowe, Ojie, *et al.*, 2024), and (b) assess its detectability and potency of cues to unsuspecting users (Nayak *et al.*, 2025). Learning models are successfully used to identify attacks, and detect cues and lures that leave users as susceptible. They identify data anomalies via learned outliers in a dataset (Setiadi, Muslikh, *et al.*, 2024) as accomplished via vote, bagging, boosting, and stacked models (Binitie *et al.*, 2024, 2025, 2026; Oyemade *et al.*, 2016; Oyemade & Ojugo, 2020, 2021).

MLs are veritable tools to identify attacks. A trained MLs can detect anomalous patterns – even with its dynamic predictors. Learning schemes are grouped into: machine learning (ML) (Onoma, Agboi, Geteloma, *et al.*, 2025), deep learning (DL) (Varun Kumar *et al.*, 2025), and ensemble learning (EL) (Ako *et al.*, 2024, 2025). ML's flexibility and robustness help it to learn intrinsic patterns and decode predictors that fasten model design cum ease outlier groups identification. Its pitfalls are imbalanced dataset and the feature selection mode used. DLs utilize recurrent neural nets to capture high-dimensional, chaotic data (Malasowe, Aghware, *et al.*, 2024). Its poor generalization due to vanishing gradient problem restricts its use. Its variant overcomes this via its gates to control its input (Kumar *et al.*, 2025), and eases adaptability to learned changes as long-term dependency (Kayathri *et al.*, 2024). Its inability to handle larger dataset and longer training time required implies the quest for better alternative. Lastly, EL can fuse both ML with DL into a stronger learner to enhance performance (Eboka, Aghware, *et al.*, 2025; Eboka, Odiakaose, *et al.*, 2025). It must resolve conflicts of structure and data-encode; while, leveraging the merits of both ML and DL to avoid model overfit as birthed by the underlying models (Odiakaose *et al.*, 2024, 2025). Thus, we explore XGB to achieve such abilities, leveraging its base, weak learners to enhance itself (Qasim & Flayh, 2023; Tahir *et al.*, 2025). It improves performance by reducing error of its base learner, and reduce its overall variance and bias in the dataset to improve generalization. It benefits from the comprehensive knowledge of its base learners, to improve its generalization via XGB. With degraded performance due to an imbalanced data (Islam *et al.*, 2021; Ugbotu, Aghaunor, *et al.*, 2025), we explore SMOTE-Tomek balancing. Our study wishes to: (a) identify phishing lures on spoofed site, (b) resolve data imbalance via SMOTE-Tomek, and (c) select predictors about the target class via the relief rank feature selection.

A cursory look at the reviewed works shows the utilization of Phishing Websites dataset from the UCI Machine Learning Repository. It implies there is a consistent baseline to compare various phishing detection

schemes. Studies demonstrate the effectiveness of ML/DL approaches including feature selection flexibility and data imbalance resolution have necessitated the need to explore more advanced architectures such as transfer learning using stacked approach with meta-learners to improve phishing detection. We propose transfer learning with XGB meta-learner as combined with the relief-rank feature selection with SMOTE-Tomek mode. It exploits temporal dependencies in data more effectively with better performance to detect phishing sites compared to existing modes (Brizimor *et al.*, 2024).

Resolving data imbalance via oversampling is imperative in ML, as it accounts for the minor class as crucial (Aghaunor *et al.*, 2026; Aghaunor, Agboi, *et al.*, 2025; Aghaunor, Omede, *et al.*, 2025). It is opposed to under-samplers that often reduces or ignore as meaningless, the minor class in a dataset. Thus, we use synthetic minority oversample technique (SMOTE), and its variants SMOTE-Tomek and SMOTEEN (Akazue *et al.*, 2023, 2024). Study contributes thus: Section 1 introduces the subject with gaps that motivate the study, (b) Section 2 explores the proposed method – and leans on data collection, pre-processing, dataset split-balance-normalize via SMOTE-Tomek, transfer model design, train-and-validate with XGBoost, and (c) Section 3 shows experimental results obtained as evidence in a broader sense cum context for the stacked ensemble on the phishing website dataset as obtained from UCI (Ojugo, Allenotor, *et al.*, 2015; Ojugo, Akazue, Ejeh, Ashioba, *et al.*, 2023; Ojugo, Ejeh, Akazue, Ashioba, *et al.*, 2023).

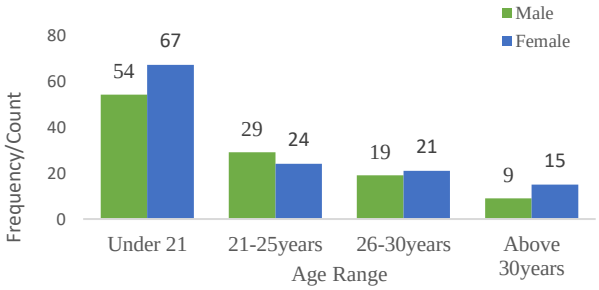


Figure 1. Phishing susceptibility by Age

2. *MATERIALS AND METHODS*

The proposed method is as in Figure 2:

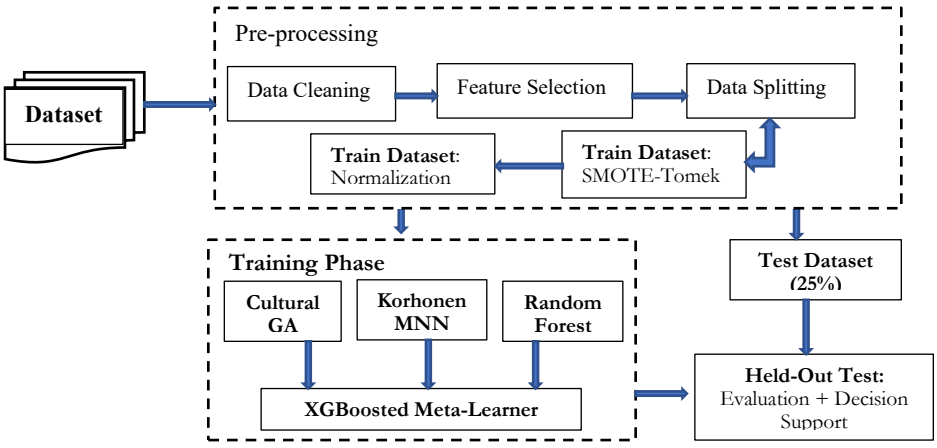


Figure 2. Proposed System Architecture

Step-1 – Data Collection: The UCI phishing dataset consist of 11,055-records distributed into 5,180-cases in genuine class, and 5,875-cases in phishing class (Li, Ul Arfeen Laghari, *et al.*, 2025). The original dataset plot as in Figure 5.

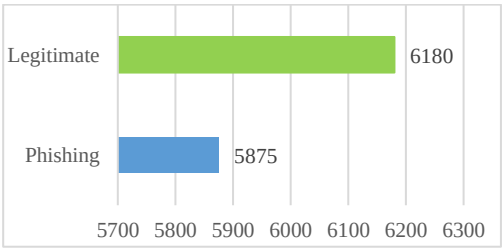


Figure 3. Original Dataset plot

Step-2 – Pre-processing cleans up dataset by expunging redundancies to yield integrity, and removes missing values to yield quality.

Optimized data is then encoded using the one-hot to transform data into its equivalent binary forms (Alsaidi *et al.*, 2025; Komalasari *et al.*, 2025; Ojugo *et al.*, 2024; Ojugo & Nwankwo, 2021b).

Step 3 Relief Rank Feature Selection: We select only the predictors of relevance to expunge all docile feats and reduce dataset dimensionality, to aid fastened model construction (Nakano *et al.*, 2025). The relief rank: (a) assumes all features have same weight and influence on accuracy, (b) identifies the nearest sample from the same class as the nearest hit, and the nearest sample from a varying class as the nearest miss, and (c) uses feature value of nearest neighbour to update its weight(s) (Pratama *et al.*, 2025). It assesses the correlation of all predictors for ground-truth as in Eq. 1 (Okpor, Aghware, Akazue, Ojugo, *et al.*, 2024). With a threshold of 8.321 as computed, algorithm 1 ranked features to choose a total of 20 predictors as in Table 1, from the original UCI dataset with initial 30 features (Ojugo & Eboka, 2019, 2020b, 2020a; Okobah & Ojugo, 2018).

$$Y = 100 * \sum |(x_1^2 - x_2^2)^2 + (1 - x_1^2)^2| \quad (1)$$

Algorithm 1: Relief Ranking Feature Selection Approach

1. load dataset with training samples, predictors, weights and initialize predictor weights
2. for all weights → randomly select target predictor R && compute nearest hit = H && nearest miss = M
3. find W[A] = W[A] – *diff*(A,R,H)/m + *diff*(A,R,M)/m
4. return computed predictorScore for W: end

Table 1: Phishing Dataset with Relief Ranking Feature Selection for Predictors

Parameters	Description	Data Type	Selected
shortening_service	Whether a URL shortening service like bit.ly is used (1=Yes, -1=No)	char	Yes
double_slash_redirect	Presence of "//" in the URL path (1: Yes, -1: No)	char	Yes
having_IP_Address	Whether URL has IP Address instead of a domain name (1=Yes, 1=No)	alphanumeric	No
having_At_Symbol	Presence of "@" symbol in the URL (1: Yes, -1: No)	char	No
having_Sub_Domain	Number of subdomains in the URL (1: More than one, 0: One, -1: None)	char	Yes
URL_lenght	Length of the URL (1=long, 0=medium, -1=short)	integer	Yes
domain_reg_length	Length of time domain has been registered (1: over a year, -1: Less than a year)	integer	Yes
Prefix_Suffix	Presence of "-" in the domain part of the URL (1: Yes, -1: No)	char	No
SSLfinal_State	Whether the website uses HTTPS with a valid SSL certificate (1: Yes, -1: No)	char	Yes
Favicon	Whether the favicon is loaded from the same domain (1: Yes, -1: No)	char	Yes
port	Use of non-standard ports (1: Yes, -1: No)	alphanumeric	No
HTTPS_token	Presence of "HTTPS" token in the URL (1: Yes, -1: No)	char	Yes
Request_URL	Percentage of external links in the source code of the website (1: High, -1: Low)	alphanumeric	No
URL_of_Anchor	Percentage of external anchor links on the website (1: High, -1: Low)	char	Yes
Links_in_tags	Percentage of external links in tags (e.g., meta, script) (1: High, -1: Low)	char	Yes
SFH	Form Handler, where form data is submitted (1: External, 0: Internal, -1: Same)	alphanumeric	Yes
Submitting_to_email	Whether the form submits data to an email address (1: Yes, -1: No)	alphanumeric	Yes
Abnormal_URL	Whether the URL is abnormal (1: Yes, -1: No)	alphanumeric	No
Redirect	Number of redirects (1: More than one, -1: Less than one)	alphanumeric	No
on_mouseover	Whether changing status bar content on mouseover (1: Yes, -1: No)	char	No
RightClick	Whether right-click is turned off on the website (1: Yes, -1: No)	char	Yes
popUpWindow	Whether pop-up windows are present (1: Yes, -1: No)	char	Yes
Iframe	Whether iframe is used on the website (1: Yes, -1: No)	char	No
age_of_domain	Age of the domain (1: More than 6 months, -1: Less than 6 months)	integer	No
DNSRecord	Whether the DNS record exists (1: Yes, -1: No)	boolean	Yes
web_traffic	Web traffic rank (1: High, 0: Medium, -1: Low)	alphanumeric	Yes
Page_Rank	Google PageRank (1: High, -1: Low)	integer	Yes
Google_Index	Whether Google indexes the site (1: Yes, -1: No)	integer	Yes
Links_point_to_page	Number of links pointing to the page (1: High, 0: Medium, -1: Low)	alphanumeric	Yes
Statistical_report	Whether the website is reported as a phishing site (1: Yes, -1: No)	integer	Yes

Step 4 – Data Split and Data Balance: First, dataset is split into train (75% or 8,291-label), and test (25%, or 2,764-label). Balancing resample data, interpolating its nearest neighbour to create synthetic data to repopulate a pool, or removing data from train dataset to create a balanced dataset. Using SMOTE-Tomek (Setiadi, Nugroho, *et al.*, 2024), we fused the SMOTE oversampler with Tomek-links undersampler as in algorithm 2 with Figure 5 as plot via SMOTE-Tomek (Ojugo, Eboka, *et al.*, 2015; Ojugo & Nwankwo, 2021d, 2021a, 2021c; Ojugo & Otakore, 2018a, 2018b; Zuama *et al.*, 2025).

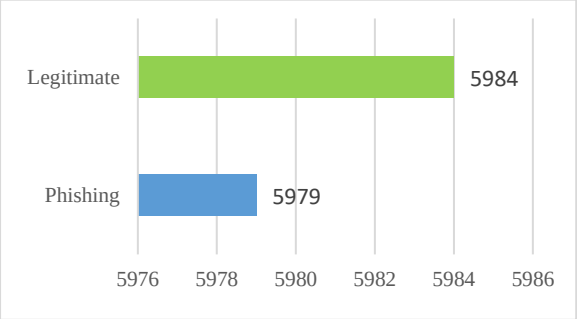


Figure 4. SMOTE-Tomek Data Balancing

The choice of data split depends largely on the trade-off between the need for a more robust model favors 75%:25% train-and-test ratio mode, or it can be poised towards the need for improved performance as guided by model complexity, larger dataset size and other feats so as to favors the 80%:20% mode (Ojugo & Yoro, 2013, 2020). Here, our choice of the 75%:25% ratio leans on the small nature of the explored dataset with 11,055 records so that we can ultimately have a more robust evaluation on diverse test data, address flexibility concerns in feature selection, and proffer a more adaptive assessment with more accurate (Ojugo & Otakore, 2020, 2021) and less bias generalization of the model. In addition – with the train-subset still unbalanced, we performed data normalization using the z-score normalization as in Equation 2.

$$z = \frac{x - \mu}{\sigma} \quad (2)$$

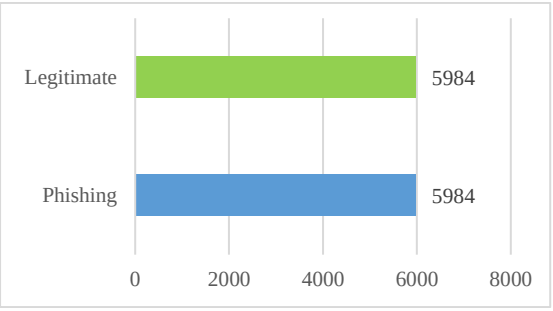


Figure 5. Normalized train sub-dataset

Step-5 – Stacked-Ensemble fuses 3-base learners with XGB meta-learner, explained as:

1. **Korhonen Modular Neural Net KMNN** yields a deep, modular learning model that computes its output using the tan-sigmoid function. It splits a network into smaller units for enhanced dependence and improved efficacy of its units (Yoro *et al.*, 2025). This improves its computational efficiency, reduces time convergence, and lets it handle more tasks effectively in parallel. Its diversity grants each unit independent training to make KMNN more robust and flexible, with improved generalization as in Table 2.

Table 2: KMNN design configuration

Features	Value	Description
evalPerfSet	MSE	Evaluation metrics at training
hiddenLayers	10	Number of hidden layers adopted
trainPercent	50	k-fold dataset used for training
transferHidden	tan-sigmoid	Activation learning function
learnRate	0.25	Step size learning to update
numberLayer	10	Minimal number of samples needed
dataDivision	stratified	k-fold dataset for construction
trainNetAlgo	LMBP	Training mode by a neural network
BPGMomentum	Auto	Backpropagation-in-momentum learn

2. **Cultural Genetic Algorithm** uses these belief spaces as: (a) ***normative*** values to which predictors are bound, (b) ***domain*** equip predictors with knowledge data about task, (c) ***temporal*** ensures each predictor knows the solution, and (d) ***spatial*** ensures each predictor with its topology. It uses an influence function to set its (upper and lower) bounds which lies between (0,1) in its quest for optimal as in Equation 3; And Equation 4 – allows knowledge transfer between its belief space(s) and the pool, and to alter each predictor to conform with its belief space. Each $b_i \in \{1,0\}$ is a chromosome gene (Ojugo & Ekurume, 2021; Olaniyi *et al.*, 2023; Rtayli & Enneya, 2020). Table 3 is the CGA design.

Table 3: CGA design configuration

Features	Value	Description
maxNosGen	120	Maximum number of generations
nosIndividuals	30	Number of solutions in a generation
selectionType	int	1-rank, 2-elitism, 3-steadyState, 4-tourney, 5-stochasticUniversalSampling
offspringCreated	int	Offspring: 1-crossover, 2-mutation
reqFitFunction	10	Minimal number of samples needed
learnRate	0.1	Determines the step size in learning
randomState	25	The seeds for reproduction

3. **Random Forest** successively grows its decision trees independently via a bootstrap sample, in bagging mode. It uses a binary split on its extra layer to extend the randomness on how its trees are constructed, so that its best nodes are selected randomly to capture intricate feats in the dataset. Its inability to handle diversity in categorical data results in its poor performance. Thus, we tune the hyperparameters to reduce model overfitting (Anthony-Akhutie *et al.*, 2025; Oladele *et al.*, 2024; Omede *et al.*, 2024;

Omoruwou *et al.*, 2024; Omosor *et al.*, 2025).

Table 4: RF design configuration

Features	Value	Description
nEstimators	250	Number of trees constructed
learnRate	0.25	Step size learning for update
maxDepth	5	Max depth of each tree
minSampleSplit	10	Minimal samples needed
randomState	25	The seeds for reproduction
evalMetric	error, logloss	Performance evaluation metrics
evalSet	x,val, y_val	Train data for evaluation

4. **Transfer Learning** with XGB meta-classifier – it trains a meta/higher learner to effectively combine the predictive outcome of several learners, allowing its meta-learner to improve as it learns from the errors of its base classifiers. This flexibility ensures stacking yields better outcomes with more iterations. In voting, the learners are applied independently to achieve a more stable performance with reduced overfit via predictive aggregation in its quest for ground truth. Since it seeks to combine only the final output of all learners without recourse to their predictive relations – in some instances, it yields degraded performance due to its dataset complexity and diversity. Bagging trains similar learners with equal voting weight.

   To promote variance, each learner is trained using a randomly drawn subset of the train data. It achieves higher accuracy by averaging all learners' predictions. It can also be configured to use various learners on different populations to reduce the variance error(s) in each learner. Lastly. Boost mode sequentially trains its learners so that each new model corrects the errors of its previous model. It yields a series of learner that focus on difficult tasks that their predecessors failed to correctly predict; And results in higher generalization with improved accuracy. A common boost is adaptive boosting. However, to improve this scheme, an ensemble can be based on a gradient scale such as the eXtreme Gradient Boost (Okonta *et al.*, 2013, 2014; Wemembu *et al.*, 2014).

Table 5: XGBoost design configuration

Features	Value	Description
nEstimators	250	Number of trees constructed
learnRate	5	Max depth of each tree
maxDepth	x,val, y_val	Train data to evaluate performance
minSampleSplit	0.25	Step size learning to update XGB
randomState	error, logloss	Performance evaluation metrics
evalMetric	25	The seeds for reproduction
evalSet	250	Number of trees constructed

XGB leans on predictive output of its base models, expanding its goal function via its regularize term $\Omega(f_t)$ and loss function $l(Y_i^t, \hat{Y}_i^t)$ (Ju *et al.*, 2020) to ensure its resultant solution remains within the upper and lower bounds objective for its improved accuracy via its tuned hyper-parameters (Abakarim *et al.*, 2018; Aghware *et al.*, 2023b; Ugbotu, Ako, *et al.*, 2025).

Step 6 – Train/Cross Validation is initialized with default configuration to tune the hyper-parameters. Each tree is iteratively constructed and trained to ensure the collective knowledge to identify intricate data. Training blends synthetic with original data to guarantee its comprehensive learning with improved adaptability to various configurations (Ghasemieh *et al.*, 2023).

3. RESULT FINDINGS AND DISCUSSION

3.1. Ensemble Performance

For a comprehensive evaluation devoid of overfit, we use a 5-fold training partition on 75% train-subset obtained via SMOTE-Tomek, and a final evaluation carried out via a held-out test (25%) subset as in Table 6. Proposed hybrid yields average accuracy of 99.34% with a Precision of 99.6%, a Recall of 98.64%, an F1 of 99.2%, a Specificity of 99.66%, an MCC of 97.7% and AUC-ROC of 99.6%. Table 6 results in high value for MCC, and implies model accurately and consistently handles the minority class with data balancing performed; while the Specificity value of 99.66% reached indicates that the model effectively recognizes phishing sites. Test data (25%) assesses the model's generalization ability with unseen data. The results showed an accuracy of 99.7%, precision 100%, recall of 99.8%, and F1 of 99.5%. The AUC value of 99.7% implies that the model was able to differentiate between benign and malignant records. Also, Specificity of 100% indicates that no benign record was misclassified (Muhamada *et al.*, 2024).

Table 7. Ensemble Design Configuration

	5-Fold Training with Validation					Test
Models	**Fold-1**	**Fold-2**	**Fold-3**	**Fold-4**	**Fold-5**	**Dataset**
Accuracy	0.991	0.981	0.997	0.998	1.000	0.997
Recall	0.981	1.000	0.975	0.976	1.000	0.998
Precision	1.000	0.984	1.000	0.996	1.000	1.000

F1	0.991	0.989	0.995	0.985	1.000	0.995
MCC	0.982	0.963	0.955	0.985	1.000	0.986
Specificity	1.000	1.000	0.985	0.998	1.000	1.000
AUC-ROC	0.999	0.999	0.986	0.996	1.000	0.997

Figure shows discriminative performance of each model. It achieves the highest AUC of 0.98, with great sensitivity and low false positive rates. XGBoost follows with an AUC of 0.97, showing strong discrimination but slightly less than the ensemble. Random Forest achieves AUC of 0.95, reflecting robustness but reduced precision in borderline cases. Figure 8 is the AUC-ROC with a 99.73%, and shows the model's capability to differentiate the negative and positive classes. The proposed model accurately identified all 2,764 of the test data. With only a misclassified case and no false positives cases – Its specificity of 1.00 implies that no phishing was misclassified. This is critical to avoid misclassification when detecting phishing. Proposed model enhances phishing website detection performance on both the training data and the held-out test set (Setiadi, Susanto, *et al.*, 2024; Setiadi, Ojugo, *et al.*, 2025).

Figure 6 shows ensemble correctly classified all test data with perfect accuracy. Use of feature selection, SMOTE-Tomek, and normalization did not degrade performance (Sun *et al.*, 2021). But, it focuses on critical feats for model construction to successfully detect spoofed websites with reduced errors that will secure user resources and enhance experience (Aghaunor, Omede, *et al.*, 2025; Falconnet *et al.*, 2023; Obasuyi *et al.*, 2024; Ojugo, Yoro, *et al.*, 2015).

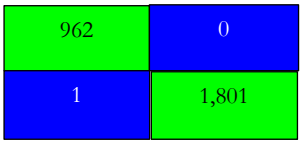


Figure 6. Confusion Matrix

3.2. Ablation Studies

To assess performance of our proposed ensemble, we focus on held-out test which offers a more realistic indication of the model's generalization capabilities. Summarized using the metric, Table 6 shows the ablation studies with performance of the base learners applied. Our hybrid ensemble yielded best result with F1 0.699, Accuracy 0.697, Precision and Recall of 0.685 and 0.684 respectively. Conversely, our benchmark models as in Table 6 yields F1 range [0.619, 0.639], Accuracy range [0.609, 0.637], Precision range [0.611, 0.64] and Recall range [0.614, 0.64] respectively (Okpor *et al.*, 2025; Yoro & Ojugo, 2019b, 2019a).

Table 8. Ensemble Performance

Models	Accuracy	Precision	Recall	F1
Kohonen NN	0.609	0.611	0.614	0.619
CGA	0.619	0.632	0.634	0.611
Random Forest	0.627	0.642	0.653	0.631
XGBoost	0.637	0.640	0.640	0.639
Ensemble	0.697	0.685	0.684	0.699

Table 8 shows proposed model outperforms against all benchmark models (Setiadi, Widiono, *et al.*, 2024) due to its use of feature selection and SMOTE-Tomek across metrics on test dataset – achieving its accuracy (99.7%), precision (100%), recall (99.8%) and specificity (100%) – showing best generalization with low false-positives, which is crucial in phishing detection especially with complex lures used by adversaries (Setiadi, Rustad, *et al.*, 2025; Setiadi, Sutojo, *et al.*, 2025; Ugbotu, Aghaunor, *et al.*, 2025; Ugbotu, Emordi, *et al.*, 2025) in their evolving exploit methods.

Models leverage deep learning capabilities – their performance can be seen to be slightly lower in metrics, and the lack thereof of specificity indicates that they are less robust; whereas, our model can be seen to maintain high sensitivity performance, even with its transfer learning architectures (Setu *et al.*, 2025). We used the SMOTE-Tomek to address class imbalances (Onoma, Agboi, Ugbotu, *et al.*, 2025; Onoma, Ako, Anazia, Oghorodi, *et al.*, 2025; Onoma, Ako, Ojugo, Geteloma, *et al.*, 2025; Onoma, Ugbotu, Aghaunor, Agboi, *et al.*, 2025).

4. CONCLUSION

The study affirms that our proposed stacked learning approach yields a strong learner potential with improved performance generalization by proffering a total of 60-rules using its CGA block with 18-of-such-rules found to yield a classification accuracy of 99.7%. It implies that the rules as generated by stacking ensemble has 99.7% rate to adequately identify phishing websites. Furthermore, the upper/lower bounds of the CGA ensures an

elitist system for ground-truth is averted via the use of other base learners in the stacked ensemble. This increases its early detection rate at its train-and-validation so that model witnesses an increase in accuracy with decreased loss. Results suggest a robust, well-regularized model that effectively fuses balanced dataset, and suitable learning. Ensemble yields F1 0.995, Accuracy 0.997, Recall 0.998, Precision 1.000, AUC 0.997 and Specificity 1.000 respectively (Okofu, Akazue, *et al.*, 2024; Okofu, Anazia, *et al.*, 2024).

In addition, the proposed ensemble achieved high discriminative capability via statistically fused heuristics mode to successfully mitigate class-imbalance with enhanced evaluation scores for F1, Accuracy, Recall, Specificity and AUC respectively. Study advances a lightweight yet effective framework that avoids complex training and validation that results in overfit or over-parameterization, effectively handles larger data complexities; while offering interpretability and high performance.

Conflict of Interest

The authors declare that there is no conflict of interest.

REFERENCES

Abakarim, Y., Lahby, M., & Attioui, A. (2018). An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning. *International Conference on Intelligent Systems*, 1–7. https://doi.org/10.1145/3289402.3289530

Agboi, J., Emordi, F. U., Odiakaose, C. C., Idama, R. O., Jumbo, E. F., Oweimieotu, A. E., Ezzeh, P. O., Eboka, A. O., Odoh, A., Ugbotu, E. V., Onoma, P. A., Ojugo, A. A., Aghaunor, T. C., Binitie, A. P., Onochie, C. C., Nwozor, B., & Ejeh, P. O. (2025). Phishing Website Detection via a Transfer Learning based XGBoost Meta-learner with SMOTE-Tomek. *Journal of Fuzzy Systems and Control*, *3*(3), 181–189. https://doi.org/10.59247/jfsc.v3i3.325

Agboi, J., Onoma, P. A., Ugbotu, E. V., Aghaunor, T. C., Odiakaose, C. C., Ojugo, A. A., Eboka, A. O., Binitie, A. P., Ezzeh, P. O., Ejeh, P. O., Geteloma, V. O., Idama, R. O., Orobor, A. I., Onochie, C. C., & Obruche, C. O. (2025). Lung Cancer Detection using a Hybridized Contrast- based Xception Model on Image Data : A Pilot Study. *MSIS - International Journal of Advanced Computing and Intelligent System*, *4*(1), 1–11. https://msis-press.com/paper/ijacis/4/1/21

Aghaunor, T. C., Agboi, J., Ugbotu, E. V., Onoma, P. A., Ojugo, A. A., Odiakaose, C. C., Eboka, A. O., Ezzeh, P. O., Geteloma, V. O., Binitie, A. P., Orobor, A. I., Nwozor, B., Ejeh, P. O., & Onochie, C. C. (2025). EcoSMEAL: Energy Consumption with Optimization Strategy via a Secured Smart Monitor- Alert Ensemble. *Journal of Fuzzy Systems and Control*, *3*(3), 190–196. https://doi.org/10.59247/jfsc.v3i3.319

Aghaunor, T. C., Omede, E. U., Ugbotu, E. V., Agboi, J., Onochie, C. C., Max-Egba, A. T., Geteloma, V. O., Onoma, P. A., Eboka, A. O., Ojugo, A. A., Odiakaose, C. C., & Binitie, A. P. (2025). Enhanced Scorch Occurrence Prediction in Foam Production via a Fusion SMOTE-Tomek Balanced Deep Learning Scheme. *NIPES - Journal of Science and Technology Research*, *7*(2), 330–339. https://doi.org/10.37933/nipes/7.2.2025.25

Aghaunor, T. C., Ugbotu, E. V., Ugboh, E., Onoma, P. A., Emordi, F. U., Ojugo, A. A., Geteloma, V. O., Idama, R. O., & Ezzeh, P. O. (2026). Investigating Security Enhancement in Hybrid Clouds via a Blockchain-Fused Privacy Preservation Strategy: Pilot Study. *Journal of Computing Theories and Applications*, *3*(4), 428–442. https://doi.org/10.62411/jcta.15508

Aghware, F. O., Akazue, M. I., Okpor, M. D., Malasowe, B. O., Aghaunor, T. C., Ugbotu, E. V., Ojugo, A. A., Ako, R. E., Geteloma, V. O., Odiakaose, C. C., Eboka, A. O., & Onyemenem, S. I. (2025). Effects of Data Balancing in Diabetes Mellitus Detection: A Comparative XGBoost and Random Forest Learning Approach. *NIPES - Journal of Science and Technology Research*, *7*(1), 1–11. https://doi.org/10.37933/nipes/7.1.2025.1

Aghware, F. O., Ojugo, A. A., Adigwe, W., Odiakaose, C. C., Ojei, E. O., Ashioba, N. C., Okpor, M. D., & Geteloma, V. O. (2024). Enhancing the Random Forest Model via Synthetic Minority Oversampling Technique for Credit-Card Fraud Detection. *Journal of Computing Theories and Applications*, *1*(4), 407–420. https://doi.org/10.62411/jcta.10323

Aghware, F. O., Okpor, M. D., Adigwe, W., Odiakaose, C. C., Ojugo, A. A., Eboka, A. O., Ejeh, P. O., Taylor, O. E., Ako, R. E., & Geteloma, V. O. (2024). BloFoPASS: A blockchain food palliatives tracer support system for resolving welfare distribution crisis in Nigeria. *International Journal of Informatics and Communication Technology*, *13*(2), 178–187. https://doi.org/10.11591/ijict.v13i2.pp178-187

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023a). DeLClustE: Protecting Users from Credit-

Card Fraud Transaction via the Deep-Learning Cluster Ensemble. *International Journal of Advanced Computer Science and Applications*, *14*(6), 94–100. doi: 10.14569/IJACSA.2023.0140610

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023b). Sentiment Analysis in Detecting Sophistication and Degradation Cues in Malicious Web Contents. *Kong Zhu Yuece / Control and Decision*, *38*(1), 653.

Akazue, M. I., Edje, A. E., Okpor, M. D., Adigwe, W., Ejeh, P. O., Odiakaose, C. C., Ojugo, A. A., Edim, E. B., Ako, R. E., & Geteloma, V. O. (2024). FiMoDeAL: pilot study on shortest path heuristics in wireless sensor network for fire detection and alert ensemble. *Bulletin of Electrical Engineering and Informatics*, *13*(5), 3534–3543. doi.org/10.11591/eei.v13i5.8084

Akazue, M. I., Yoro, R. E., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Improved services traceability and management of a food value chain using block-chain network: a case of Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(3), 1623–1633. doi: 10.11591/ijeecs.v29.i3.pp1623-1633

Ako, R. E., Aghware, F. O., Okpor, M. D., Akazue, M. I., Yoro, R. E., Ojugo, A. A., Setiadi, D. R. I. M., Odiakaose, C. C., Abere, R. A., Emordi, F. U., Geteloma, V. O., & Ejeh, P. O. (2024). Effects of Data Resampling on Predicting Customer Churn via a Comparative Tree-based Random Forest and XGBoost. *Journal of Computing Theories and Applications*, *2*(1), 86–101. https://doi.org/10.62411/jcta.10562

Ako, R. E., Okpor, M. D., Aghware, F. O., Malasowe, B. O., Nwozor, B., Ojugo, A. A., Geteloma, V. O., Odiakaose, C. C., Ashioba, N. C., Eboka, A. O., Binitie, A. P., Aghaunor, T. C., & Ugbotu, E. V. (2025). Pilot Study on Fibromyalgia Disorder Detection via XGBoosted Stacked-Learning with SMOTE-Tomek Data Balancing Approach. *NIPES - Journal of Science and Technology Research*, *7*(1), 12–22. https://doi.org/10.37933/nipes/7.1.2025.2

Allenotor, D., & Ojugo, A. A. (2017). A Financial Option Based Price and Risk Management Model for Pricing Electrical Energy in Nigeria. *Advances in Multidisciplinary & Scientific Research Journal*, *3*(2), 79–90.

Allenotor, D., Oyemade, D. A., & Ojugo, A. A. (2015). A Financial Option Model for Pricing Cloud Computational Resources Based on Cloud Trace Characterization. *African Journal of Computing & ICT*, *8*(2), 83–92. www.ajocict.net

Alsaidi, S. A. A. A., Mohammed, H. J., Al Ogaili, R. R. N., Dashoor, Z. A., Alsaeedi, A. H., Al-Shammary, D., & Ibaida, A. (2025). HawkPhish-DNN cybersecurity model: adaptive hybrid optimization and deep learning for enhanced multi-objective phishing URL detection. *International Journal of Information Technology (Singapore)*, *17*(7), 3859–3875. https://doi.org/10.1007/s41870-025-02597-8

Anthony-Akhutie, P., Omosor, J. C., Onoma, P. A., Ojugo, A. A., Ako, R. E., Agboi, J., Odiakaose, C. C., Max-Egba, A. T., Geteloma, V. O., Niemogha, S. U., & Abdullahi, M. B. (2025). SEMAEco-IoT: A Secured IoT-based Smart Energy Monitor and Alert for Enhanced Energy Conservation and Optimization. *FUPRE Journal of PetroScience*, *1*(1), 150–166.

Atuduhor, R. R., Okpor, M. D., Yoro, R. E., Odiakaose, C. C., Emordi, F. U., Ojugo, A. A., Ako, R. E., Geteloma, V. O., Ejeh, P. O., Abere, R. A., Ifioko, A. M., & Brizimor, S. E. (2024). StreamBoostE: A Hybrid Boosting-Collaborative Filter Scheme for Adaptive User-Item Recommender for Streaming Services. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *10*(2), 89–106. https://doi.org/10.22624/AIMS/V10N2P8

Baker, M. R., Etem, T., Jihad, K. H., & Buyrukoğlu, S. (2025). *The Role of Hyperparameter Tuning in Phishing Website Classification: A Comparative Analysis of ML Models* (pp. 68–77). https://doi.org/10.1007/978-3-031-78928-1_8

Binitie, A. P., Odiakaose, C. C., Okpor, M. D., Ejeh, P. O., Eboka, A. O., Ojugo, A. A., Setiadi, D. R. I. M., Ako, R. E., Aghaunor, T. C., Geteloma, V. O., & Afotanwo, A. (2024). Stacked Learning Anomaly Detection Scheme with Data Augmentation for Spatiotemporal Traffic Flow. *Journal of Fuzzy Systems and Control*, *2*(3), 203–214. https://doi.org/10.59247/jfsc.v2i3.267

Binitie, A. P., Okofu, S. N., Okpor, M. D., Anazia, K. E., Ojugo, A. A., Egbokhare, F. A., Egwali, A., Ezzeh, P. O., Ako, R. E., Geteloma, V. O., Aghaunor, T. C., Ugbotu, E. V., & Onyemenem, S. I. (2025). MoBiSafe: an obfuscated single factor authentication mode to enhance secured USSD channel transaction in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *40*(1), 426. doi.org/10.11591/ijeecs.v40.i1.pp426-436

Binitie, A. P., Onyemenem, S. I., Anujeonye, N. C., Adimabua, A., Egbokhare, F. A., & Aghaunor, T. C. (2026). A Graph-Augmented Isolation Forest Using Node2Vec and GraphSAGE for Mobile User Behavior Anomaly Detection. *Journal of Computing Theories and*

Applications, *3*(3), 369–383. https://doi.org/10.62411/jcta.15494

Brizimor, S. E., Okpor, M. D., Yoro, R. E., Emordi, F. U., Ifioko, A. M., Odiakaose, C. C., Ojugo, A. A., Ejeh, P. O., Abere, R. A., Ako, R. E., & Geteloma, V. O. (2024). WiSeCart: Sensor-based Smart-Cart with Self-Payment Mode to Improve Shopping Experience and Inventory Management. *Social Informatics, Business, Politics, Law, Environmental Sciences and Technology Journal*, *10*(1), 53–74. https://doi.org/10.22624/aims/sij/v10n1p7

Eboka, A. O., Aghware, F. O., Okpor, M. D., Odiakaose, C. C., Okpako, A. E., Ojugo, A. A., Ako, R. E., Binitie, A. P., Onyemenem, S. I., Ejeh, P. O., & Geteloma, V. O. (2025). Pilot study on deploying a wireless sensor-based virtual-key access and lock system for home and industrial frontiers. *International Journal of Informatics and Communication Technology*, *14*(1), 287–297. https://doi.org/10.11591/ijict.v14i1.pp287-297

Eboka, A. O., Odiakaose, C. C., Agboi, J., Okpor, M. D., Onoma, P. A., Aghaunor, T. C., Ojugo, A. A., Ugbotu, E. V., Max-Egba, A. T., Geteloma, V. O., Binitie, A. P., Onochie, C. C., & Ako, R. E. (2025). Resolving Data Imbalance Using a Bi-Directional Long-Short Term Memory for Enhanced Diabetes Mellitus Detection. *Journal of Future Artificial Intelligence and Technologies*, *2*(1), 95–109. https://doi.org/10.62411/faith.3048-3719-73

Ejeh, P. O., Okpor, M. D., Yoro, R. E., Ifioko, A. M., Onyemenem, S. I., Odiakaose, C. C., Ojugo, A. A., Ako, R. E., Emordi, F. U., & Geteloma, V. O. (2024). Counterfeit Drugs Detection in the Nigeria Pharma-Chain via Enhanced Blockchain-based Mobile Authentication Service. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *12*(2), 25–44. doi.org/10.22624/aims/maths/v12n2p3

Falconnet, A., Coursaris, C. K., Beringer, J., Van Osch, W., Sénécal, S., & Léger, P.-M. (2023). Improving User Experience with Recommender Systems by Informing the Design of Recommendation Messages. *Applied Sciences*, *13*(4), 2706. doi.org/10.3390/app13042706

Geteloma, V. O., Aghware, F. O., Adigwe, W., Odiakaose, C. C., Ashioba, N. C., Okpor, M. D., Ojugo, A. A., Ejeh, P. O., Ako, R. E., & Ojei, E. O. (2024a). AQuamoAS: unmasking a wireless sensor-based ensemble for air quality monitor and alert system. *Applied Engineering and Technology*, *3*(2), 70–85. https://doi.org/10.31763/aet.v3i2.1409

Geteloma, V. O., Aghware, F. O., Adigwe, W., Odiakaose, C. C., Ashioba, N. C., Okpor, M. D., Ojugo, A. A., Ejeh, P. O., Ako, R. E., & Ojei, E. O. (2024b). Enhanced data augmentation for predicting consumer churn rate with monetization and retention strategies: a pilot study. *Applied Engineering and Technology*, *3*(1), 35–51. doi.org/10.31763/aet.v3i1.1408

Geteloma, V. O., Okpor, M. D., Ugboh, E., Anazia, K. E., Odoh, A., Agboi, J., Abere, R. A., Aghaunor, T. C., Ugbotu, E. V., Odiakaose, C. C., & Ojugo, A. A. (2025). Investigating Risk Level in Maternal Mortality via a 3ConFA Feature Fused SMOTE-Tomek Balancing with Attention-Guided BiGRU Scheme : A Pilot Study. *Journal of Behavioral Informatics, Digital Humanities and Development Research*, *11*(3), 59–80. https://doi.org/10.22624/AIMS/BHI/V11N3P5x

Ghasemieh, A., Lloyed, A., Bahrami, P., Vajar, P., & Kashef, R. (2023). A novel machine learning model with Stacking Ensemble Learner for predicting emergency readmission of heart-disease patients. *Decision Analytics Journal*, *7*, 100242. doi.org/10.1016/j.dajour.2023.100242

Hakonen, P. (2022). Detecting Insider Threats Using User and Entity Behavior Analytics. *International Journal of Electrical and Computer Engineering*, *21*(October), 5765–5783.

Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in Universities: An Evaluation Model. *SN Computer Science*, *4*(5). https://doi.org/10.1007/s42979-023-01984-x

Hera, J. (2024). Phishing Defense Mechanisms: Strategies for Effective Measurement and Cyber Threat Mitigation. *ResearchSquare*, *September*. https://doi.org/10.13140/RG.2.2.27576.15364

Ibor, A. E., Edim, E. B., & Ojugo, A. A. (2023). Secure Health Information System with Blockchain Technology. *Journal of the Nigerian Society of Physical Sciences*, *5*(2), 992. https://doi.org/10.46481/jnsps.2023.992

Ifioko, A. M., Yoro, R. E., Okpor, M. D., Brizimor, S. E., Obasuyi, D. A., Emordi, F. U., Odiakaose, C. C., Ojugo, A. A., Atuduhor, R. R., Abere, R. A., Ejeh, P. O., Ako, R. E., & Geteloma, V. O. (2024). CoDuBoTeSS: A Pilot Study to Eradicate Counterfeit Drugs via a Blockchain Tracer Support System on the Nigerian Frontier. *Journal of Behavioral Informatics, Digital Humanities and Development Research*, *10*(2), 53–74. doi.org/10.22624/AIMS/BHI/V10N2P6

Islam, N., Farhin, F., Sultana, I., Kaiser, S., Rahman, S., Mahmud, M., Hosen, S., & Cho, G. H. (2021). Towards Machine Learning Based

Intrusion Detection in IoT Networks. *Computers, Materials and Continua*, *69*(2), 1801–1821. https://doi.org/10.32604/cmc.2021.018466

Jáñez-Martino, F., Alaiz-Rodríguez, R., González-Castro, V., Fidalgo, E., & Alegre, E. (2022). A review of spam email detection: analysis of spammer strategies and the dataset shift problem. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-022-10195-4

Ju, S., Lim, H., & Heo, J. (2020). Machine learning approaches for crop yield prediction with MODIS and weather data. *40th Asian Conference on Remote Sensing, ACRS 2019: Progress of Remote Sensing Technology for Smart Future*, *Acrs*, 1–4.

Justice, P., & Dumka, N. (2021). An Improved Model for Detecting Uniform Resource Locator (URL) using Deep Learning. *International Journal of Advanced Research in Computer and Communication Engineering*, *10*(11). https://doi.org/10.17148/ijarcce.2021.101107

Kayathri, S., Harikrishnan, T., Kb, K., & Kirubanithi, K. (2024). Mechanism for Identifying Appropriate Phishing Websites Utilizing Machine Learning. *International Research Journal of Modernization in Engineering Technology and Science*, *January*. https://doi.org/10.56726/irjmets52165

Komalasari, D., Kurniawan, T. B., Dewi, D. A., Zakaria, M. Z., Abdullah, Z., & Alanda, A. (2025). Phishing Domain Detection Using Machine Learning Algorithms. *International Journal on Advanced Science, Engineering and Information Technology*, *15*(1), 318–327. https://doi.org/10.18517/ijaseit.15.1.12553

Kumar, C. L., Betam, S., Pustokhin, D., Laxmi Lydia, E., Bala, K., Aluvalu, R., & Panigrahi, B. S. (2025). Metaparameter optimized hybrid deep learning model for next generation cybersecurity in software defined networking environment. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-96153-w

Li, W., Manickam, S., Chong, Y., & Karuppayah, S. (2025). *Talking Like a Phisher: LLM-Based Attacks on Voice Phishing Classifiers*. *July*. https://doi.org/10.48550/arXiv.2507.16291

Li, W., Ul Arfeen Laghari, S., Manickam, S., & Chong, Y. W. (2025). Exploration and Evaluation of Human-centric Cloaking Techniques in Phishing Websites. *KSII Transactions on Internet and Information Systems*, *19*(1), 232–258. https://doi.org/10.3837/tiis.2025.01.011

Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., Ako, R. E., & Ojugo, A. A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech). *NIPES - Journal of Science and Technology Research*, *6*(2), 293–311. https://doi.org/10.5281/zenodo.12617068

Malasowe, B. O., Edim, E. B., Adigwe, W., Okpor, M. D., Ako, R. E., Okpako, A. E., Ojugo, A. A., & Ojei, E. O. (2024). Quest for Empirical Solution to Runoff Prediction in Nigeria via Random Forest Ensemble: Pilot Study. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *10*(1), 73–90. https://doi.org/10.22624/aims/bhi/v10n1p8

Malasowe, B. O., Ojie, D. V., Ojugo, A. A., & Okpor, M. D. (2024). Co-Infection Prevalence of Covid-19 Underlying Tuberculosis Disease Using a Susceptible Infect Clustering Bayes Network. *Dutse Journal of Pure and Applied Sciences*, *10*(2), 80–94. https://doi.org/10.4314/dujopas.v10i2a.8

Malasowe, B. O., Okpako, A. E., Okpor, M. D., Ejeh, P. O., Ojugo, A. A., & Ako, R. E. (2024). FePARM: The Frequency-Patterned Associative Rule Mining Framework on Consumer Purchasing-Pattern for Online Shops. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *15*(2), 15–28. https://doi.org/10.22624/aims/cisdi/v15n2p2-1

Mia, M., Derakhshan, D., & Pritom, M. M. A. (2025). Can Features for Phishing URL Detection Be Trusted Across Diverse Datasets? A Case Study with Explainable AI. *Proceedings of the 2024 11th International Conference on Networking, Systems and Security, NSysS 2024*, 137–145. https://doi.org/10.1145/3704522.3704532

Muhamada, K., Setiadi, D. R. I. M., Sudibyo, U., Widjajanto, B., & Ojugo, A. A. (2024). Exploring Machine Learning and Deep Learning Techniques for Occluded Face Recognition: A Comprehensive Survey and Comparative Analysis. *Journal of Future Artificial Intelligence and Technologies*, *1*(2), 160–173. https://doi.org/10.62411/faith.2024-30

Nakano, H., Koide, T., & Chiba, D. (2025). *PhishParrot: LLM-Driven Adaptive Crawling to Unveil Cloaked Phishing Sites*. http://arxiv.org/abs/2508.02035

Nayak, G. S., Muniyal, B., & Belavagi, M. C. (2025). Enhancing Phishing Detection: A Machine Learning Approach With Feature Selection and Deep Learning Models. *IEEE Access*, *13*, 33308–33320. doi: 10.1109/ACCESS.2025.3543738

Nur, M. J., Moses Setiadi, D. R. I., Ojugo, A. A., & Nguyen, M. T. (2025). Improving Customer Churn Prediction Using Domain-Driven Feature Engineering, Resampling, and CatBoost with Explainability Extensions.

2025 International Seminar on Application for Technology of Information and Communication, 493–499. doi: 10.1109/ISemantic67418.2025.11291801

Obasuyi, D. A., Yoro, R. E., Okpor, M. D., Ifioko, A. M., Brizimor, S. E., Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ako, R. E., Geteloma, V. O., Abere, R. A., Atuduhor, R. R., & Akiakeme, E. (2024). NiCuSBlockIoT: Sensor-based Cargo Assets Management and Traceability Blockchain Support for Nigerian Custom Services. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *15*(2), 45–64. doi.org/10.22624/aims/cisdi/v15n2p4

Odiakaose, C. C., Aghware, F. O., Okpor, M. D., Eboka, A. O., Binitie, A. P., Ojugo, A. A., Setiadi, D. R. I. M., Ibor, A. E., Ako, R. E., Geteloma, V. O., Ugbotu, E. V., & Aghaunor, T. C. (2024). Hypertension Detection via Tree-Based Stack Ensemble with SMOTE-Tomek Data Balance and XGBoost Meta-Learner. *Journal of Future Artificial Intelligence and Technologies*, *1*(3), 269–283. doi.org/10.62411/faith.3048-3719-43

Odiakaose, C. C., Omede, E. U., Anazia, K. E., Okpor, M. D., Ako, R. E., Aghaunor, T. C., Ugbotu, E. V., Ojugo, A. A., Moses Setiadi, D. R. I., Eboka, A. O., Max-Egba, A. T., Agboi, J., Onochie, C. C., & Onoma, P. A. (2025). Investigating Data Balancing Effects for Enhanced Behavioural Risk Detection in Cervical Cancer Using BiGRU: A Pilot Study. *NIPES - Journal of Science and Technology Research*, *7*(2), 319–329. https://doi.org/10.37933/nipes/7.2.2025.24

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Ashioba, N. C., Odiakaose, C. C., Ako, R. E., & Emordi, F. U. (2023). Forging a User-Trust Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study. *Journal of Computing Theories and Applications*, *1*(2), 50–60. https://doi.org/10.33633/jcta.v1i2.9259

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Odiakaose, C., & Emordi, F. U. (2023). DeGATraMoNN: Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing. *Kongzhi Yu Juece/Control and Decision*, *38*(01), 667–678.

Ojugo, A. A., Allenotor, D., Oyemade, D. A., Yoro, R. E., & Anujeonye, C. N. (2015). Immunization Model for Ebola Virus in Rural Sierra-Leone. *African Journal of Computing & ICT*, *8*(1), 1–10. www.ajocict.net

Ojugo, A. A., & Eboka, A. O. (2018a). Assessing Users Satisfaction and Experience on Academic Websites: A Case of Selected Nigerian Universities Websites. *International Journal of Information Technology and Computer Science*, *10*(10), 53–61. doi: 10.5815/ijitcs.2018.10.07

Ojugo, A. A., & Eboka, A. O. (2018b). Comparative Evaluation for High Intelligent Performance Adaptive Model for Spam Phishing Detection. *Digital Technologies*, *3*(1), 9–15. https://doi.org/10.12691/dt-3-1-2

Ojugo, A. A., & Eboka, A. O. (2018c). Modeling the Computational Solution of Market Basket Associative Rule Mining Approaches Using Deep Neural Network. *Digital Technologies*, *3*(1), 1–8. https://doi.org/10.12691/dt-3-1-1

Ojugo, A. A., & Eboka, A. O. (2019). Inventory prediction and management in Nigeria using market basket analysis associative rule mining: memetic algorithm based approach. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *8*(3), 128. https://doi.org/10.11591/ijict.v8i3.pp128-138

Ojugo, A. A., & Eboka, A. O. (2020a). An Empirical Evaluation On Comparative Machine Learning Techniques For Detection Of The Distributed Denial Of Service (DDoS) Attacks. *Journal of Applied Science, Engineering, Technology, and Education*, *2*(1), 18–27. https://doi.org/10.35877/454RI.asci2192

Ojugo, A. A., & Eboka, A. O. (2020b). Cluster prediction model for market basket analysis: quest for better alternatives to associative rule mining approach. *IAES International Journal of Artificial Intelligence*, *9*(3), 429–439. https://doi.org/10.11591/ijai.v9.i3.pp429-439

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015). Framework design for statistical fraud detection. *Mathematics and Computers in Science and Engineering Series*, *50*, 176–182.

Ojugo, A. A., Ejeh, P. O., Akazue, M. I., Ashioba, N. C., Odiakaose, C. C., Ako, R. E., Nwozor, B., & Emordi, F. U. (2023). CoSoGMIR: A Social Graph Contagion Diffusion Framework using the Movement-Interaction-Return Technique. *Journal of Computing Theories and Applications*, *1*(2), 163–173. https://doi.org/10.33633/jcta.v1i2.9355

Ojugo, A. A., Ejeh, P. O., Odiakaose, C. C., Eboka, A. O., & Emordi, F. U. (2024). Predicting rainfall runoff in Southern Nigeria using a fused hybrid deep learning ensemble. *International Journal of Informatics and Communication Technology*, *13*(1), 108–115. https://doi.org/10.11591/ijict.v13i1.pp108-115

Ojugo, A. A., & Ekurume, E. (2021). Deep Learning Network Anomaly-Based Intrusion Detection Ensemble For Predictive Intelligence To Curb Malicious Connections: An Empirical Evidence. *International Journal of Advanced*

Trends in Computer Science and Engineering, *10*(3), 2090–2102. doi: 10.30534/ijatcse/2021/851032021

Ojugo, A. A., & Nwankwo, O. (2021a). Forging a Spectral-Clustering Multi-Agent Hybrid Deep Learning Model To Predict Rainfall Runoff In Nigeria. *International Journal of Innovative Science, Engineering and Technology*, *8*(3), 140–147.

Ojugo, A. A., & Nwankwo, O. (2021b). Modeling Mobility Pattern for the Corona-Virus Epidemic Spread Propagation and Death Rate in Nigeria using the Movement-Interaction-Return Model. *International Journal of Emerging Trends in Engineering Research*, *9*(6), 821–826. https://doi.org/10.30534/ijeter/2021/30962021

Ojugo, A. A., & Nwankwo, O. (2021c). Multi-Agent Bayesian Framework For Parametric Selection In The Detection And Diagnosis of Tuberculosis Contagion In Nigeria. *JINAV: Journal of Information and Visualization*, *2*(2), 69–76. https://doi.org/10.35877/454ri.jinav375

Ojugo, A. A., & Nwankwo, O. (2021d). Spectral-Cluster Solution For Credit-Card Fraud Detection Using A Genetic Algorithm Trained Modular Deep Learning Neural Network. *JINAV: Journal of Information and Visualization*, *2*(1), 15–24. https://doi.org/10.35877/454ri.jinav274

Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ako, R. E., Adigwe, W., Anazia, K. E., & Geteloma, V. O. (2023). Evidence of Students' Academic Performance at the Federal College of Education Asaba Nigeria: Mining Education Data. *Knowledge Engineering and Data Science*, *6*(2), 145. doi: 10.17977/um018v6i22023p145-156

Ojugo, A. A., & Otakore, O. D. (2018a). Improved Early Detection of Gestational Diabetes via Intelligent Classification Models: A Case of the Niger Delta Region in Nigeria. *Journal of Computer Sciences and Applications*, *6*(2), 82–90. https://doi.org/10.12691/jcsa-6-2-5

Ojugo, A. A., & Otakore, O. D. (2018b). Redesigning Academic Website for Better Visibility and Footprint: A Case of the Federal University of Petroleum Resources Effurun Website. *Network and Communication Technologies*, *3*(1), 33. https://doi.org/10.5539/nct.v3n1p33

Ojugo, A. A., & Otakore, O. D. (2020). Intelligent Peer-To-Peer Banking Framework: Advancing The Frontiers of Agent Banking For Financial Inclusion In Nigeria Via Smartphones. *Quantitative Economics and Management Studies*, *1*(5), 300–311. https://doi.org/10.35877/454RI.qems140

Ojugo, A. A., & Otakore, O. D. (2021). Forging An Optimized Bayesian Network Model With Selected Parameters For Detection of The Coronavirus In Delta State of Nigeria. *Journal of Applied Science, Engineering, Technology, and Education*, *3*(1), 37–45. https://doi.org/10.35877/454ri.asci2163

Ojugo, A. A., & Yoro, R. E. (2013). Computational Intelligence in Stochastic Solution for Toroidal N-Queen. *Progress in Intelligent Computing and Applications*, *1*(2), 46–56. https://doi.org/10.4156/pica.vol2.issue1.4

Ojugo, A. A., & Yoro, R. E. (2020). Predicting Futures Price And Contract Portfolios Using The ARIMA Model : A Case of Nigeria ' s Bonny Light and Forcados. *Quantitative Economics and Management Studies*, *1*(4), 237–248. https://doi.org/10.35877/454RI.qems139

Ojugo, A. A., Yoro, R. E., Eboka, A. O., Yerokun, M. O., Anujeonye, C. N., & Efozia, F. N. (2015). Predicting Behavioural Evolution on a Graph-Based Model. *Advances in Networks*, *3*(2), 8. https://doi.org/10.11648/j.net.20150302.11

Okobah, I. P., & Ojugo, A. A. (2018). Evolutionary Memetic Models for Malware Intrusion Detection: A Comparative Quest for Computational Solution and Convergence. *International Journal of Computer Applications*, *179*(39), 34–43. doi: 10.5120/ijca2018916586

Okofu, S. N., Akazue, M. I., Oweimieotu, A. E., Ako, R. E., Ojugo, A. A., & Asuai, C. E. (2024). Improving Customer Trust through Fraud Prevention E-Commerce Model. *Journal of Computing, Science and Technoloogy*, *1*(1), 76.

Okofu, S. N., Anazia, K. E., Akazue, M. I., Okpor, M. D., Oweimieotu, A. E., Asuai, C. E., Nwokolo, G. A., Ojugo, A. A., & Ojei, E. O. (2024). Pilot Study on Consumer Preference, Intentions and Trust on Purchasing-Pattern for Online Virtual Shops. *International Journal of Advanced Computer Science and Applications*, *15*(7), 804–811. doi.org/10.14569/IJACSA.2024.0150780

Okonta, E. O., Ojugo, A. A., Wemembu, U. R., & Ajani, D. (2013). Embedding Quality Function Deployment In Software Development: A Novel Approach. *West African Journal of Industrial & Academic Research*, *6*(1), 50–64.

Okonta, E. O., Wemembu, U. R., Ojugo, A. A., & Ajani, D. (2014). Deploying Java Platform to Design A Framework of Protective Shield for Anti– Reversing Engineering. *West African Journal of Industrial & Academic Research*, *10*(1), 50–64.

Okpor, M. D., Aghware, F. O., Akazue, M. I., Eboka, A. O., Ako, R. E., Ojugo, A. A., Odiakaose, C.

C., Binitie, A. P., Geteloma, V. O., & Ejeh, P. O. (2024). Pilot Study on Enhanced Detection of Cues over Malicious Sites Using Data Balancing on the Random Forest Ensemble. *Journal of Future Artificial Intelligence and Technologies*, *1*(2), 109–123. doi.org/10.62411/faith.2024-14

Okpor, M. D., Aghware, F. O., Akazue, M. I., Ojugo, A. A., Emordi, F. U., Odiakaose, C. C., Ako, R. E., Geteloma, V. O., Binitie, A. P., & Ejeh, P. O. (2024). Comparative Data Resample to Predict Subscription Services Attrition Using Tree-based Ensembles. *Journal of Fuzzy Systems and Control*, *2*(2), 117–128. https://doi.org/10.59247/jfsc.v2i2.213

Okpor, M. D., Anazia, K. E., Adigwe, W., Okpako, A. E., Setiadi, D. R. I. M., Ojugo, A. A., Omoruwou, F., Ako, R. E., Geteloma, V. O., Ugbotu, E. V., Aghaunor, T. C., & Oweimieotu, A. E. (2025). Unmasking effects of feature selection and SMOTE-Tomek in tree-based random forest for scorch occurrence detection. *Bulletin of Electrical Engineering and Informatics*, *14*(3), 2393–2403. doi.org/10.11591/eei.v14i3.8901

Oladele, J. K., Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Abere, R. A., Nwozor, B., Ejeh, P. O., & Geteloma, V. O. (2024). BEHeDaS: A Blockchain Electronic Health Data System for Secure Medical Records Exchange. *Journal of Computing Theories and Applications*, *1*(3), 231–242. https://doi.org/10.62411/jcta.9509

Olaniyi, O. O., Okunleye, O. J., Olabanji, S. O., Asonze, C. U., & Ajayi, S. A. (2023). IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience. *Asian Journal of Research in Computer Science*, *16*(4), 354–371. doi: 10.9734/ajrcos/2023/v16i4397

Omede, E. U., Edje, A. E., Akazue, M. I., Utomwen, H., & Ojugo, A. A. (2024). IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defense System. *Journal of Computing Theories and Applications*, *1*(3), 273–283. https://doi.org/10.62411/jcta.9541

Omoruwou, F., Ojugo, A. A., & Ilodigwe, S. E. (2024). Strategic Feature Selection for Enhanced Scorch Prediction in Flexible Polyurethane Form Manufacturing. *Journal of Computing Theories and Applications*, *1*(3), 346–357. https://doi.org/10.62411/jcta.9539

Omosor, J. C., Onoma, P. A., Ojugo, A. A., Ako, R. E., Geteloma, V. O., Akhutie-Anthony, P., & Okperigho, S. U. (2025). Security Enhancement using Multifactor Authentication Strategy for the Solenoid Door Access Control and Management: A Pilot Study. *FUPRE Journal of Scientific and Industrial Research*, *6*(3), 80–94.

Onoma, P. A., Agboi, J., Geteloma, V. O., Max-Egba, A. T., Eboka, A. O., Ojugo, A. A., Odiakaose, C. C., Ugbotu, E. V., Aghaunor, T. C., & Binitie, A. P. (2025). Investigating an Anomaly-based Intrusion Detection via Tree-based Adaptive Boosting Ensemble. *Journal of Fuzzy Systems and Control*, *3*(1), 90–97. https://doi.org/10.59247/jfsc.v3i1.279

Onoma, P. A., Agboi, J., Ugbotu, E. V., Aghaunor, T. C., Odiakaose, C. C., Ojugo, A. A., Eboka, A. O., Binitie, A. P., Ezzeh, P. O., Ejeh, P. O., Onochie, C. C., Geteloma, V. O., Emordi, F. U., Orobor, A. I., & Obruche. (2025). Attrition Rate Prediction using a Frequency-Recency-Monetization-based SMOTEEN-Boosted Approach. *MSIS - International Journal of Advanced Computing and Intelligent System*, *3*(1), 1–11.

Onoma, P. A., Ako, R. E., Anazia, K. E., Oghorodi, D., Okpako, A. E., Onochie, C. C., Geteloma, V. O., Ezzeh, P. O., Ugboh, E., Ojugo, A. A., Eboka, A. O., & Idama, R. O. (2025). Quest for Ground-Truth or Stochastic Myth by Leveraging the AI-Powered Wearable Device for Dementia Disease Detection: A Pilot Study. *FUPRE Journal of Scientific and Industrial Research*, *9*(3), 343–358.

Onoma, P. A., Ako, R. E., Ojugo, A. A., Geteloma, V. O., Akhutie-Anthony, P., & Okperigho, S. U. (2025). Dementia Detection and Management using Wearable Device fused Deep Learning Scheme. *FUPRE Journal of Scientific and Industrial Research*, *6*(3), 80–94.

Onoma, P. A., Ugbotu, E. V., Aghaunor, T. C., Agboi, J., Ojugo, A. A., Odiakaose, C. C., Max-Egba, A. T., Niemogha, S. U., Binitie, A. P., & Abdullahi, M. B. (2025). Voice-based Dynamic Time Warping Recognition Scheme for Enhanced Database Access Security. *Journal of Fuzzy Systems and Control*, *3*(1), 81–89. https://doi.org/10.59247/jfsc.v3i1.293

Otorokpo, E. A., Okpor, M. D., Yoro, R. E., Brizimor, S. E., Ifioko, A. M., Obasuyi, D. A., Odiakaose, C. C., Ojugo, A. A., Atuduhor, R. R., Akiakeme, E., Ako, R. E., & Geteloma, V. O. (2024). DaBO-BoostE: Enhanced Data Balancing via Oversampling Technique for a Boosting Ensemble in Card-Fraud Detection. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *12*(2), 45–66. https://doi.org/10.22624/aims/maths/v12n2p4

Oyemade, D. A., Akpojaro, J., Ojugo, A. A., Ureigho, R. J., Imouokhome, F. A.-A., & Omoregbee, E. U. (2016). A Three Tier Learning Model for Universities in Nigeria. *Journal of Technologies in Society*, *12*(2), 9–20. doi.org/10.18848/2381-9251/cgp/v12i02/9-20

Oyemade, D. A., & Ojugo, A. A. (2020). A Property Oriented Pandemic Surviving Trading Model.

International Journal of Advanced Trends in Computer Science and Engineering, *9*(5), 7397–7404. doi.org/10.30534/ijatcse/2020/71952020

Oyemade, D. A., & Ojugo, A. A. (2021). An Optimized Input Genetic Algorithm Model for the Financial Market. *International Journal of Innovative Science, Engineering and Technology, 8*(2), 408–419.

Pratama, N. R., Setiadi, D. R. I. M., Harkespan, I., & Ojugo, A. A. (2025). Feature Fusion with Albumentation for Enhancing Monkeypox Detection Using Deep Learning Models. *Journal of Computing Theories and Applications*, *2*(3), 427–440. https://doi.org/10.62411/jcta.12255

Qasim, M. A. A. H., & Flayh, N. A. (2023). Phishing Website Detection Using Machine Learning. *Wasit Journal for Pure Sciences*, *2*(2), 270–281. doi.org/10.1109/ICNWC60771.2024.10537279

Rtayli, N., & Enneya, N. (2020). Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization. *Journal of Information Security and Applications*, *55*, 102596. https://doi.org/10.1016/j.jisa.2020.102596

Sasikala, G., Laavanya, M., Sathyasri, B., Supraja, C., Mahalakshmi, V., Mole, S. S. S., Mulerikkal, J., Chidambaranathan, S., Arvind, C., Srihari, K., & Dejene, M. (2022). An Innovative Sensing Machine Learning Technique to Detect Credit Card Frauds in Wireless Communications. *Wireless Communications and Mobile Computing*, *2022*, 1–12. https://doi.org/10.1155/2022/2439205

Setiadi, D. R. I. M., Muslikh, A. R., Iriananda, S. W., Warto, W., Gondohanindijo, J., & Ojugo, A. A. (2024). Outlier Detection Using Gaussian Mixture Model Clustering to Optimize XGBoost for Credit Approval Prediction. *Journal of Computing Theories and Applications*, *2*(2), 244–255. https://doi.org/10.62411/jcta.11638

Setiadi, D. R. I. M., Nugroho, K., Muslikh, A. R., Iriananda, S. W., & Ojugo, A. A. (2024). Integrating SMOTE-Tomek and Fusion Learning with XGBoost Meta-Learner for Robust Diabetes Recognition. *Journal of Future Artificial Intelligence and Technologies*, *1*(1), 23–38. https://doi.org/10.62411/faith.2024-11

Setiadi, D. R. I. M., Ojugo, A. A., Pribadi, O., Kartikadarma, E., Setyoko, B. H., Widiono, S., Robet, R., Aghaunor, T. C., & Ugbotu, E. V. (2025). Integrating Hybrid Statistical and Unsupervised LSTM-Guided Feature Extraction for Breast Cancer Detection. *Journal of Computing Theories and Applications*, *2*(4), 536–552. https://doi.org/10.62411/jcta.12698

Setiadi, D. R. I. M., Rustad, S., Sutojo, T., Akrom, M., Nguyen, M. T., Afendee, M., Sambas, A., & Ojugo, A. A. (2025). Hyperchaotic cross-coupled quantum 2D maps with interdependent rotational asymmetry for secure image encryption. *Optics Communications*, *600*(November 2025), 1–17. https://doi.org/10.1016/j.optcom.2025.132699

Setiadi, D. R. I. M., Susanto, A., Nugroho, K., Muslikh, A. R., Ojugo, A. A., & Gan, H. S. (2024). Rice Yield Forecasting Using Hybrid Quantum Deep Learning Model. *Computers*, *13*(8). https://doi.org/10.3390/computers13080191

Setiadi, D. R. I. M., Sutojo, T., Rustad, S., Akrom, M., Ghosal, S. K., Nguyen, M. T., & Ojugo, A. A. (2025). Single Qubit Quantum Logistic-Sine XYZ-Rotation Maps: An Ultra-Wide Range Dynamics for Image Encryption. *Computers, Materials and Continua*, *83*(2), 2161–2188. https://doi.org/10.32604/cmc.2025.063729

Setiadi, D. R. I. M., Widiono, S., Safriandono, A. N., & Budi, S. (2024). Phishing Website Detection Using Bidirectional Gated Recurrent Unit Model and Feature Selection. *Journal of Future Artificial Intelligence and Technologies*, *1*(2), 75–83. https://doi.org/10.62411/faith.2024-15

Setu, J. H., Halder, N., Islam, A., & Amin, M. A. (2025). RSTHFS: A Rough Set Theory-Based Hybrid Feature Selection Method for Phishing Website Classification. *IEEE Access*, *13*, 68820–68830. https://doi.org/10.1109/ACCESS.2025.3561237

Sinduja, S. (2021). Efficient Phishing Website Detection using Machine Learning Algorithm. *International Journal for Research in Applied Science and Engineering Technology*, *9*(4), 1442–1448. doi: 10.22214/ijraset.2021.33957

Sudheer, N., Divya, B., Deepa, P., Geethika, B., & Balaji, B. (2025). *Detection of phishing websites using a machine learning alogrithm*. 030059. https://doi.org/10.1063/5.0247187

Sun, D., Liu, M., Li, M., Shi, Z., Liu, P., & Wang, X. (2021). DeepMIT: A Novel Malicious Insider Threat Detection Framework based on Recurrent Neural Network. *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design*, 335–341. doi:10.1109/CSCWD49262.2021.9437887

Tahir, H. T., Aghaunor, T. C., Ugbotu, E. V., Onoma, P. A., Ojugo, A. A., Abere, R. A., Agboi, J., & Aherobo, V. O. (2025). Enhancing Security

with Blockchain-Enabled Privacy Preservation for Multi-and-Hybrid Cloud Environment: A Pilot Study. *Advances in Multidisciplinary & Scientific Research Journal Publication*, *16*(4), 25–44. doi: 10.22624/AIMS/CISDI/V16N4P3

Ugbotu, E. V., Aghaunor, T. C., Agboi, J., Max-Egba, A. T., Onoma, P. A., Geteloma, V. O., Eboka, A. O., Binitie, A. P., Ako, R. E., Nwozor, B., Onochie, C. C., Ojugo, A. A., Jumbo, E. F., Oweimieotu, A. E., & Odiakaose, C. C. (2025). Transfer Learning Using a CNN Fused Random Forest for SMS Spam Detection with Semantic Normalization of Text Corpus. *NIPES - Journal of Science and Technology Research*, *7*(2), 371–382. doi.org/10.37933/nipes/7.2.2025.29

Ugbotu, E. V., Ako, R. E., Odoh, A., Oghorodi, D., Okpako, A. E., Aghaunor, T. C., Emordi, F. U., Ugboh, E., Agboi, J., Odiakaose, C. C., Ojugo, A. A., Geteloma, V. O., Abere, R. A., Idama, R. O., Eboka, A. O., Ezzeh, P. O., Onochie, C. C., Oweimieotu, A. E., Ojo, B., & Onoma, P. A. (2025). Equipping the GREDDIoMT Device with Early Behavioural Risk Detection of Dementia via a Pre-Activated SENet fused BiGRU. *J. of Behavioral Informatics, Digital Humanities and Development Research*, *11*(3), 36–56. doi: 10.22624/AIMS/BHI/V11N3P4

Ugbotu, E. V., Emordi, F. U., Ugboh, E., Anazia, K. E., Odiakaose, C. C., Onoma, P. A., Idama, R. O., Ojugo, A. A., Geteloma, V. O., Oweimieotu, A. E., Aghaunor, T. C., Binitie, A. P., Odoh, A., Onochie, C. C., Ezzeh, P. O., Eboka, A. O., Agboi, J., & Ejeh, P. O. (2025). Investigating a SMOTE-Tomek Boosted Stacked Learning Scheme for Phishing Website Detection: A Pilot Study. *Journal of Computing Theories and Applications*, *3*(2), 145–159. https://doi.org/10.62411/jcta.14472

Umar, A. U. Z. (2025). Simple but Smart: Against the Pursuit of Endless Complexity in Deep Learning Models for Detecting Phishing URLs. *International Physical Sciences Conference*, *August*.

Varun Kumar, A., Prathiba, A., Ashritha, A., Harish Reddy, N., & Asha Shiny, D. X. S. (2025). Phishing Website Detection Based on URL Features. *International Journal Of Scientific Research In Engineering & Technology*, 73–78. https://doi.org/10.59256/ijsreat.20250502011

Wemembu, U. R., Okonta, E. O., Ojugo, A. A., & Okonta, I. L. (2014). A Framework for Effective Software Monitoring in Project Management. *West African Journal of Industrial and Academic Research*, *10*(1), 102–115.

Yoro, R. E., & Ojugo, A. A. (2019a). An Intelligent Model Using Relationship in Weather Conditions to Predict Livestock-Fish Farming Yield and Production in Nigeria. *American Journal of Modeling and Optimization*, *7*(2), 35–41. https://doi.org/10.12691/ajmo-7-2-1

Yoro, R. E., & Ojugo, A. A. (2019b). Quest for Prevalence Rate of Hepatitis-B Virus Infection in the Nigeria: Comparative Study of Supervised Versus Unsupervised Models. *American Journal of Modeling and Optimization*, *7*(2), 42–48. https://doi.org/10.12691/ajmo-7-2-2

Yoro, R. E., Okpor, M. D., Akazue, M. I., Okpako, A. E., Eboka, A. O., Ejeh, P. O., Ojugo, A. A., Odiakaose, C. C., Binitie, A. P., Ako, R. E., Geteloma, V. O., Onoma, P. A., Max-Egba, A. T., Ibor, A. E., Onyemenem, S. I., & Ukwandu, E. (2025). Adaptive DDoS detection mode in software-defined SIP-VoIP using transfer learning with boosted meta-learner. *Plos One*, *20*(6 June), 1–20. https://doi.org/10.1371/journal.pone.0326571

Zuama, L. R., Setiadi, D. R. I. M., Susanto, A., Santosa, S., Gan, H. S., & Ojugo, A. A. (2025). High-Performance Face Spoofing Detection using Feature Fusion of FaceNet and Tuned DenseNet201. *Journal of Future Artificial Intelligence and Technologies*, *1*(4), 385–400. https://doi.org/10.62411/faith.3048-3719-62