Research Article / Review Article FUPRE JOURNAL 8(4): 110-126(2024)

FUPRE Journal

of

Scientific and Industrial Research

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

http://fupre.edu.ng/journal

An Enhanced Learning Ensemble in Detection of Potential Threats via Anomalous Behaviour with Credit-Card Transactions

EJEH, P. O. [1,*], *ADJOGBE, F. O.* [2], *NWANZE, D.* [3]

[1,2,3] *Department of Computer Science, College of Computing and Telecommunications, Novena University, Ogume, Nigeria.*

ARTICLE INFO

Received: 02/06/2024

Accepted: 18/10/2024

Keywords

Credit-Card
Fraud Detection
Sentiment Analysis

ABSTRACT

The Internet as an effective model to advance resource sharing has consequently, led to the greater proliferation of adversaries, with unauthorized access to network resources. Adversaries achieve fraud activities via carefully crafted attacks of large magnitude targeted at personal gains and rewards. With a cost of over $1.3Trillion lost globally to financial crimes and the constant rise in fraudulent activities vis the use of credit-cards, financial institutions and stakeholders must explore and exploit improved measures to actively secure client data and funds. Financial services must harness the creative mode via machine learning schemes to help effectively manage such threats. Our study thus, proposes a cybersecurity machine learning XGBoost ensemble to detect fraud activities. This scheme aim to equip a system with altruistic knowledge to help detect credit card fraud transactions. Results show ensemble effectively differentiates fraudulent from genuine card transactions with a model accuracy of 99.1%.

1. INTRODUCTION

Financial crimes cost the global financial services over $42Trillion in 2022 – with these numbers always rapidly growing (Ejeh et al., 2024). Thus, anticipating growth in financial fraud, financial services firms must diversify via applying innovative measures to mitigate fraud (Akazue, Edje, et al., 2024; Akazue, Okofu, et al., 2024). If a system is abused, a method is needed to detect it. Detection aims to identify fraud cases via anomaly detection in user behaviour and data analysis (Aghware, Adigwe, et al., 2024; Albladi & Weir, 2018; Algarni et al., 2017). Its management must advance measures to curb such acts (Al-Qatf et al., 2018; Altman, 2019), combining the anomaly-correlation and analysis (Ifioko et al., 2024; Obasuyi et al., 2024) to yield early detection with enhanced user protection, and reduced risk (Aghware, Ojugo, et al., 2024; Amalraj & Lourdusamy, 2022; Ojugo & Ekurume, 2021a, 2021b).

The adoption today, of credit cards along with the added functionality of inclusiveness it proffers – has both, given more comfort to users, and attracted malicious adversary that are now interested in personal gains. Credit-cards have become easy targets of attack – as such crimes are discovered weeks afterwards (Ojugo & Yoro, 2013, 2020, 2021b, 2021a). It is achieved via: (a) card copy to steal user privacy data (on need), and (b) vendors extort money without a card-holder knowing (Yoro, Aghware, Malasowe, et al., 2023). With lose of money by banks, card holders are made to reimburse such loss via reduced benefits and higher interests. Thus, it is in the best interest of both users and banks to reduce card fraud by investing wisely into detection schemes (Akazue et al., 2023; De Kimpe et al., 2018).

*Corresponding author, e-mail:patrick.ejeh@dou.edu.ng
DIO

The dynamism in card fraud detection continues to puzzle administrators as these adversaries are continually poised with rising quest to tweak schemes to help them evade detection as businesses are poised to curb the threats. With such task as often inconclusive and continuous feat (Okonta et al., 2013, 2014) – many studies have been deployed to help with both its detection and prevention. Studies show that degraded performance in models can be attributed to either conflicts on heuristics, feature selection, imbalanced data, data encoding, (Goel et al., 2017; Halevi et al., 2013; Li et al., 2021). Even with intelligent classifiers, card-fraud persists as adversaries will continually evolve their exploit mode (Ako et al., 2024; Ojugo et al., 2021b; Okpor et al., 2024). Fraudsters will continually seek more efficient mode with improve dynamism to evade security measures and firewalls that profiles user behaviour at entry point, and minor hacks to steal client valuable data. Fraud monitor offers a combined risk monitor and detection analysis (Barlaud et al., 2019). Such schemes must gather data intelligently to enhance client protection, and reduce risks of fraud susceptibility (Gratian et al., 2018; Ojugo et al., 2014; Wemembu et al., 2014).

We seek to address these by adequately training our heuristic to devoid of structural conflicts and poor generalization using the XGBoost to detect credit card-fraud (Gao et al., 2021; Ojugo & Otakore, 2020b).

1.1. Credit-Cards and Fraud Detection

Fraud illegally disposes an unsuspecting user of valuable assets wilfully obtained by an adversary via intended misrepresentation. From a criminal view, fraud charges may theft, larceny, and embezzlement (Tingfei et al., 2020). It is a state where an unsuspecting, vulnerable user relies/depends on the false representative claims issued by an adversary for personal benefits (Huang et al., 2021). Fraud is often perpetuated by either an insider in an organization (as insider threat), or via an external user to compromise the workings of a system in an organization (Edirisooriya & Jayatunga, 2021; Vågsholm et al., 2020). Benchaji et al. (2022) Fraud either benefit an individual, or the organization itself – on a whole (Benchaji et al., 2021; Yoro, Aghware, Akazue, et al., 2023).

Credit-cards have today brought banks closer to her clients, and provisioned more financial inclusion for customers. It has also advanced and attracted malicious attackers for gains (Fatahi et al., 2016). A critical reason for adversaries, is that asides being an easy target – credit card crimes if committed, go unnoticed weeks after; And, in some cases they go unreported. Successful card-fraud methods include(s): (a) card cloning having acquired a compromised user confidential data, and (b) finance houses overcharge card holder even without their awareness (Ojugo, Akazue, Ejeh, Odiakaose, et al., 2023; Ojugo, Eboka, et al., 2015b). When banks lose money to fraud, cardholders are made to repay such loss wholly/partly, via either reduced benefits and/or higher interest rates. Thus, it is best for both cardholders and banks to take necessary actions to reduce card fraud (Akazue, Edje, et al., 2024; Laavanya & Vijayaraghavan, 2019; Malasowe, Aghware, et al., 2024; Malasowe, Ojie, et al., 2024; Malasowe, Okpako, et al., 2024; Okofu et al., 2024).

Eboka et al., (2020) proposed effective ensemble to extract signatures for detecting polymorphic worms to achieve their zero-day detections. This mode of analysis is called the position aware distribution signature (PADS). It utilizes worms by monitoring unexpected outgoing connections from an inbound to an outbound honeypot to easily identify worms. PADS was designed to increase the chances of detecting polymorphic worms by allowing possible variations in a signature, instead of all fixed symbols in the existing signatures. To control variations in each position in signatures, PADS uses frequency distribution to specify what variations are likely possible in each position in a signature string (Eboka & Ojugo, 2020). And is supported by (Mustofa et al., 2023; Oyemade et al., 2016).

Ileberi et al. (2022) trained RBF model with 7-parameters to recognize attack from a data packet, sent via filter alarm. Their design created profiles using stream sample mode. Their result shows we can: (a) accurately cluster and quantify packets as a profile, and (b) we can listen to low-error rates anomalies and correctly identify. Their study concludes that as routers listen and trace packet exchange, they harness key parameters and underlying features of interest for each packet; And thus, allows the model to create the corresponding profiles that in turn, improved their detection rate (Ileberi et al., 2022). Also, Aghware et al. (2023) used a deep learning reinforcement rule-based ensemble with 7-feats to detect packets traffic anomaly using profiling technique. Unsupervised ensemble seek to capture and profile packets explored to group (and classified into classes), with packet patterns in a traffic session (Aghware et al., 2023a, 2023b).

A remarkable innovation and landmark of digital transformation is the proliferation of credit-card(s) use and adoption in a variety of exchange platforms. This revolution also ushered forth the problem of credit card fraud, wherever clever, complicated methods are used to steal money (Abbasi et al., 2016; Ojugo et al., 2012). To implement schemes that ensure data security, confidentiality, non-repudiation, and privacy – even when faced with the continued attempts by adversaries to evade detection, has further advanced many studies which have also rippled across the following challenges as thus (Atuduhor et al., 2024; Chibuzo & Isiaka, 2020; Malasowe et al., 2023; Ojugo & Eboka, 2018a, 2021) as:

1. Constant revenue loss by banks alongside a variety of the hidden charges as accrued to clients (Brizimor et al., 2024).
2. The rise in adoption of e-commerce vis-à-vis the adoption of credit-card to foster financial inclusitivity has left more users complacent with the seamless transaction to buy and sell virtually. Adversaries are always steps ahead of security experts (Otorokpo et al., 2024).
3. Adversaries continue to leverage on user-trust, susceptibility behaviours cum traits (i.e. phishing) to commit fraud – since by nature, users yearn to improve their trust and dependence on techs that eases asnd improves their living. The need to protect client assets via the implementation of fraud detection schemes has become both critical and paramount.
4. The adoption of such techniques are often hampered due to the limited nature of fraud dataset and since, it is also very much unwise to describe in great details – the workings and structure of such fraud detection techniques and ensemble over public as these can arm adversaries with the needed knowledge to evade detection.
5. Issue of degraded performance is often triggered by the improper selection of feature, mismatched features, encoding of data, structural dependencies conflict, the use of non-optimized dataset vis-à-vis its lack thereof. Eliminating ambiguities, noise and partial truth further improve the classification properties of an ensemble.
6. The presentation of censored results and limited availability of datasets – has often hampered the performance of detection. Also, with the available dataset rippled with noise, partial truth, ambiguities, and imprecision the schemes must resolved in order to arrive at an optimal solution.
7. Card fraud can persist even with adoption of dynamic classifiers. So, new schemes must be able to address optimization tasks via learning approaches to yield ensemble via exploiting historic (numerical) dataset.

2. MATERIALS AND METHODS

2.1. Dataset Gathering

A major issue in the design and model of such system is appropriate retrieve properly formatted dataset for the task at hand. Dataset used for training (to fit the model) must have the requisite data features and parameters; Else such a dataset is said to be imbalanced (Al-Qudah et al., 2020; Maya Gopal P S & Bhargavi R, 2019; Taravat & Del Frate, 2013). We adopt Hochschule IDS datasets (CIDDS-2022) anomaly transaction dataset, split with training 70%, and testing 30% using 8-feats to adjust weights and coefficients as Table 1:

Table 1. Selected Features and Data Type

Features	Format	Data Types
Source IP	a.b.c.d	Object
Source Port	Numeric	Integer
Destination IP	a.b.c.d	Object
Destination Port	Numeric	Float
Protocol	String	Object
Duration	H:M:S	Float
Packets	Numeric	Integer
Attack Type	String	Object

2.2. Encoding Scheme

Unclassified and unformatted data are often ambiguous, incomplete, rippled with noise, imprecise and inconsistent. Encoding seeks to filter the dataset, mapping it unto the required format the model can easily understand. To encode the selected feats, we transform our dataset using the feats of interest as in table 1. This mode will seek to modulate the raw data unto the require dataset – so that data gathered from varying sources, is adequate for analysis. We employ data type in Pandas Library displayed by listing 1 algorithm (Ojugo et al., 2024; Ojugo & Otakore, 2021; Ojugo & Oyemade, 2021).

2.3. Deep Learning Approach

We adopt the extreme boosting algorithm with the following steps:

1. **Step 1**: Data Collection/Clean: With data recorded during production – we used the Google Play Scraper for Python to extract as in (Sunarjo et al., 2023). It is cleaned via pre-processing to yield a restructured dataset (G. Bhati, 2019; Ojugo, Akazue, Ejeh, Ashioba, et al., 2023; Ojugo, Ejeh, Odiakaose, Eboka, & Emordi, 2023; Ojugo, Odiakaose, Emordi, Ako, Adigwe, et al., 2023; Omede et al., 2024).
2. **Step 2**: Machine Learning Heuristic – We used eXtreme Gradient Boosting to help us effectively classify data-points. The Extreme Boosting (XGBoost) is a decision tree ensemble that leverages on a scalable Gradient Boost model (Paliwal et al., 2022). It becomes quite efficacious and stronger as it combines weak learners over a series of iteration to find an optimal fit solution. We achieved this via an additional expansion of its objective function by minimizing the loss function to create its variant used to control the trees' complexity. XGBoost yields better optimal fit by combining the predictive power of weak-learners (that contribute knowledge about task) to the ensemble (Bentéjac et al., 2019), and thus, yields a stronger learner. For each candidate to be trained x_i and its corresponding y_i – we use XGBoost to predict outcome using Equation 1 (Allenotor et al., 2015; Allenotor & Ojugo, 2017; Safriandono et al., 2024; Setiadi et al., 2024):

$$\hat{Y}_i^t = \sum_{k=1}^{t} f_k\,(x_i) = \hat{Y}_i^t + f_k(x_i) \qquad (1)$$

To yield a better outcome, we expand the objective function via a loss function $l(\,Y_i^t, \hat{Y}_i^t)$ and its regularization term $\Omega(f_t)$. These ensures that overtraining does not occur, ensures the training data are fitted well, and it re-calibrates the solution to ensure they are within the upper and lower bounds of solution. Regularization term ensures the tree complexity is fit appropriately. We tune a loss function to ensure ensemble yields higher accuracy. We tune the regularization terms to ensure our ensemble is simpler to avoid parameter overfitting as in Equation 2.

$$L^t = \sum_{i=1}^{n} l\left(Y_i^t, \hat{Y}_i^{t-1} + f_k(x_i)\right) + \Omega(f_t) \qquad (2)$$

3. **Step 3**: Hyper-Parameter Tuning controls how much of the tree complexity and its corresponding nodal weights need to be adjusted in place of gradient loss. The lower the value, the slower we travel on a downward slope. It also ensures how quickly a tree abandons old beliefs for new ones during the training. As the tree learns – it quickly differentiates between important feats and otherwise. A higher learning rate implies the tree can change, learn newer features as well as adapts

flexibly, and more easily. Ensemble uses the regularization term to ensure the model changes quickly, only to values that are within the lower and upper bounds. The ensemble does this to ensure that it adequately adjusts its learning rate to avoid over-fit and overtraining. Hyper-parameters tuned includes max_depth, learning_rate and n_estimator. For best performance, XGBoost is carefully tuned via these feats (Ojugo et al., 2015; Ojugo, Ugboh, Onochie, Eboka, et al., 2013; Ojugo & Eboka, 2014, 2018b; Ojugo & Otakore, 2018; Omoruwou et al., 2024).

4. Cross-Validation/Retrain in ML schemes estimates the learned skills of a heuristic on unseen data; while, evaluating model's performance about its accuracy on how well it has learned the underlying feats of interest via resampling technique. At re-train, we choose various data partitions to help a model devoid of overfit. Here, we use stratified k-partitions to rearrange the data to ensure that each, properly represents the whole dataset) as in Listing 1 (Camargo & Young, 2019; Ojugo et al., 2021a; Ojugo & Eboka, 2020; Oladele et al., 2024; Rukshan Pramoditha, 2020).

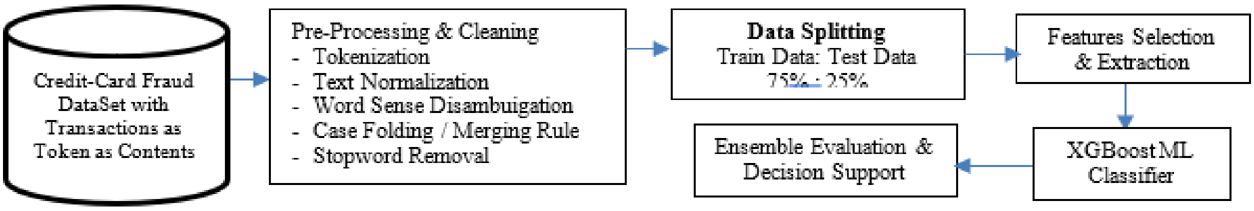

Figure 1. Extreme Gradient Boosting Ensemble with sources

3. RESULT FINDINGS & DISCUSSION

3.1. Data Cleaning and Pre-Processing

We apply pre-processing from (Ojugo & Nwankwo, 2021) and visualize the data. Thus, we mine the relations for credit card fraud via the use of cue (Rathi & Pareek, 2013; Yao et al., 2022), which seeks redirect the ensemble toward generated rules, classified into fraud or genuine classes (Akazue et al., 2022, 2023).

3.2. Training Phase

Here, we partition the retrieved dataset into 75 percent training data, and 25 percent test data. For the training dataset, we used 6,520 rows, and a test dataset of 2,173 rows. We then perform feature extraction using the TF-IDF vectorization method – which helps the ensemble to effectively convert our retrieved text contents into vectors. Also, we used Python's ScikitLearn ***TfidfVectorizer*** function to extract the desired features of interest – as defined in our ensemble. We then train the model using our train dataset.

Using hyper-parameters as in table 2, the ensemble effectively classified rules with a 0.97 (i,e, 97%), which agrees with (Oyemade & Ojugo, 2020, 2021). It effectively compute disparities in prediction accuracy for false-positives, true-negative, false-negative, and true-negatives (Maya Gopal & Bhargavi R, 2018; Muslikh et al., 2023; Yuan & Wu, 2021; Zareapoor & Shamsolmoali, 2015).

Table 2. Hyper-Parameter Tuning

Parameters	Trial-n-Error	Best
Learning Rate	[0.05, 0.1, 0.2, 0.3, 0.5, 0.75]	0.2
N_Estimators	[100, 200, 300, 500, 700, 800]	500
Max-Depths	[1, 2, 4, 5, 6, 8, 10]	6

We use trial-n-error to tune its weight for optimality, and prevent ensemble from poor generalization of over-train and overfit. Thus, for hyper-parameters using the trial-and-error mode, we observe that our best-fit values for training of learning_rate of 0.2, n_estimators as 500, and max_depth of 6 (Muslikh et al., 2023; Ojugo, Yoro, Oyemade, et al., 2013; Ojugo, Yoro, Yerokun, et al., 2013).

3.3. Ensemble Performance

Results from table 3 shows that of the 57,345-instances retrieved from dataset with 23-fields (pre-processed), 22-of-the-30 data were correctly classified (i.e. from test data) whereas 52,560 cases are genuine with over

5,411 benign cases as in first class labelled 0. Ensemble correctly identified 5,210-cases as benign true-positive instance;

The ensemble on retraining over a series of iterations (movement) yields an accuracy prediction of 0.991 (i.e. 99.1%) in detecting fraudulent transactions from genuine ones as in iteration 7 and 19 respectively. But, 8-out-of-30 cases were incorrectly classified as genuine transactions for the false-positives in class-1 (Ojugo & Otakore, 2020a). Also, 276-cases were incorrectly identified as fraud transactions as false-negative, and 233-cases correctly identified malicious instances of them were marked as true-negative.

Table 3. Hyper-Parameter Tuning

Iteration	F1	Transaction	Confusion Matrix	Attack
1	0.972	0.24069543	TP	Yes
2	0.981	0.92057455	TP	Yes
3	0.979	1.19477387	FN	Yes
4	0.978	0.54475628	FN	Yes
5	0.831	0.54754147	TP	No
6	0.901	1.49257306	FN	No
7	0.991	1.68077918	TP	Yes
8	0.809	1.46754675	TP	No
9	0.902	0.98409124	TP	Yes
10	0.917	1.58973958	TP	Yes
11	0.989	1.19001043	FN	Yes
12	0.971	0.73513175	TP	Yes
13	0.940	1.47307977	TP	No
14	0.902	1.91412663	TP	Yes
15	0.945	0.68066651	TP	Yes
16	0.967	0.78385333	FN	Yes
17	0.949	0.95404663	FN	Yes
18	0.982	0.76097431	TP	No
19	0.991	1.25818485	TP	No
20	0.812	1.34559804	FN	Yes
21	0.839	0.9708285	TP	Yes
22	0.912	1.42120613	TP	No
23	0.900	1.41576289	TP	Yes
24	0.891	1.25585408	FN	Yes
25	0.899	1.20401244	TP	Yes

To compute accuracy of the ensemble – we evaluate its performance to yield figure 2 as the confusion matrix. The Figure 2 shows that the ensemble yields performance of 99.1% classification accuracy with an improvement of 39% that agrees with (Ojugo et al., 2015, 2015; Ojugo & Okobah, 2017, 2018b, 2018a).

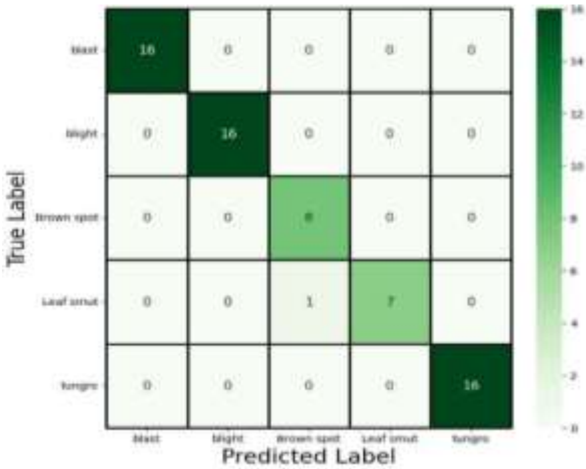

Figure 2. Model Accuracy prediction

4. CONCLUSİON

The proposed ensemble has a total of 56-rules were generated. Top rules were found to have fitness range of [0.809, 0.991] and are estimated effective for classification of such anomaly transaction with records retrieved via spatial process. It implies that achieving a set of good rules – is much better than single optimum rule, which in turn is better for such cluster, and profile dataset (Okobah & Ojugo, 2018; Yoro & Ojugo, 2019a, 2019b).

The war against intrusion is a concerted effort (Ojugo, Eboka, et al., 2015a) as many detection filters and schemes do profile user transaction requests with feats of interest to analyse each profile, and pro-actively decide, if a profile packet data is compromised vis-à-vis yield safety actions as further measures. Errors of misclassification spurs performance degradation (Ojugo, Abere, Orhionkpaiyo, Yoro, et al., 2013), and the needed ensemble must effectively group user request profiles (into various classes) with zero tolerance for error (Broadhurst et al., 2018; Ojugo & Eboka, 2019; Ojugo & Otakore, 2020c).

Our confusion matrix shows that model was found to have a sensitivity value of 0.81, specificity 0.08, and prediction accuracy of 0.991 with an improvement rate of 0.39 for data that were not originally used to train the model (Verma et al., 2018; Yan et al., 2018; F. Zhang & Lian, 2009; W. Zhang et al., 2015).

Conflict of Interest

The authors declare that there is no conflict of interest.

References

Abbasi, A., Zahedi, F. M., & Chen, Y. (2016). Phishing susceptibility: The good, the bad, and the ugly. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 169–174. https://doi.org/10.1109/ISI.2016.7745462

Aghware, F. O., Adigwe, W., Okpor, M. D., 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 (IJ-ICT)*, *13*(2), 178. https://doi.org/10.11591/ijict.v13i2.pp178-187

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., 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. https://doi.org/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. *Kongzhi Yu Juece/Control and Decision*, *38*(01), 653.

Akazue, M. I., Edje, A. E., Okpor, M. D., Adigwe, W., Ejeh, P. O., Odiakaose, C. C., Ojugo, A. A., Edim, B. E., 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. https://doi.org/10.11591/eei.v13i5.8084

Akazue, M. I., Ojugo, A. A., Yoro, R. E., Malasowe, B. O., & Nwankwo, O. (2022). Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *28*(3), 1756–1765. https://doi.org/10.11591/ijeecs.v28.i3.pp1756-1765

Akazue, M. I., Okofu, S. N., Ojugo, A. A., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., Ako, R. E., & Geteloma, V. O. (2024). Handling Transactional Data Features via Associative Rule Mining for Mobile Online Shopping Platforms. *International Journal of Advanced Computer Science and Applications*, *15*(3), 530–538. https://doi.org/10.14569/IJACSA.2024.0150354

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. https://doi.org/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

Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection. *IEEE Access*, *6*, 52843–52856. https://doi.org/10.1109/ACCESS.2018.2869577

Al-Qudah, D. A., Al-Zoubi, A. M., Castillo-Valdivieso, P. A., & Faris, H. (2020). Sentiment analysis for e-payment service providers using evolutionary extreme gradient boosting. *IEEE Access*, *8*, 189930–189944. https://doi.org/10.1109/ACCESS.2020.3032216

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, *8*(1), 5. https://doi.org/10.1186/s13673-018-0128-7

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems*, *26*(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y

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

Altman, E. R. (2019). Synthesizing Credit Card Transactions. *PeerJ Computer Science*, *14*.

Amalraj, J. R., & Lourdusamy, R. (2022). A Novel distributed token-based algorithm using secret sharing scheme for secure data access control. *International Journal of Computer Networks and Applications*, *9*(4), 374. https://doi.org/10.22247/ijcna/2022/214501

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

Barlaud, M., Chambolle, A., & Caillau, J.-B. (2019). *Robust supervised classification and feature selection using a primal-dual method*.

Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data*, *8*(1), 151. https://doi.org/10.1186/s40537-021-00541-8

Bentéjac, C., Csörgő, A., & Martínez-Muñoz, G. (2019). *A Comparative Analysis of XGBoost*. *February*. https://doi.org/10.1007/s10462-020-09896-5

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, *10*(1), 53–74. https://www.researchgate.net/publication/381032318_WiSeCart_Sensor-based_Smart-Cart_with_Self-Payment_Mode_to_Improve_Shopping_Experience_and_Inventory_Management

Broadhurst, R., Skinner, K., Sifniotis, N., & Matamoros-Macias, B. (2018). Cybercrime Risks in a University Student Community. *SSRN Electronic Journal*, *May*. https://doi.org/10.2139/ssrn.3176319

Camargo, J., & Young, A. (2019). Feature Selection and Non-Linear Classifiers: Effects on Simultaneous Motion Recognition in Upper Limb. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, *27*(4), 743–750. https://doi.org/10.1109/TNSRE.2019.2903986

Chibuzo, O. B., & Isiaka, D. O. (2020). Design and Implementation of Secure Browser for Computer-Based Tests. *International Journal of Innovative Science and Research Technology*, *5*(8), 1347–1356. https://doi.org/10.38124/ijisrt20aug526

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics*, *35*(5), 1277–1287. https://doi.org/10.1016/j.tele.2018.02.009

Eboka, A. O., & Ojugo, A. A. (2020). Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: A logical view. *International Journal of Modern Education and Computer Science*, *12*(6), 29–45. https://doi.org/10.5815/ijmecs.2020.06.03

Edirisooriya, T., & Jayatunga, E. (2021). Comparative Study of Face Detection Methods for Robust Face Recognition Systems. *5th SLAAI - International Conference on Artificial Intelligence and 17th Annual Sessions, SLAAI-ICAI 2021*, *December*. https://doi.org/10.1109/SLAAI-ICAI54477.2021.9664689

Ejeh, P. O., Okpor, M. D., Yoro, R. E., Ifioko, A. M., Onyemenem, I. S., 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. https://www.researchgate.net/publication/381785673_Effects_of_Data_Resampling_on_Predicting_Customer_Churn_via_a_Comparative_Tree-based_Random_Forest_and_XGBoost

Fatahi, M., Ahmadi, M., Ahmadi, A., Shahsavari, M., & Devienne, P. (2016). Towards an spiking deep belief network for face recognition application. *2016 6th International Conference on Computer and Knowledge Engineering (ICCKE)*, 153–158. https://doi.org/10.1109/ICCKE.2016.7802132

G. Bhati, R. (2019). A Survey on Sentiment Analysis Algorithms and Datasets. *Review of Computer Engineering Research*, *6*(2), 84–91. https://doi.org/10.18488/journal.76.2019.62.84.91

Gao, Y., Zhang, S., Lu, J., Gao, Y., Zhang, S., & Lu, J. (2021). Machine learning for credit card fraud detection. *Proceedings of the 2021 International Conference on Control and Intelligent Robotics*, 213–219. https://doi.org/10.1145/3473714.3473749

Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22–44.

https://doi.org/10.17705/1jais.00447

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web*, 737–744. https://doi.org/10.1145/2487788.2488034

Huang, D., Lin, Y., Weng, Z., & Xiong, J. (2021). Decision Analysis and Prediction Based on Credit Card Fraud Data. *The 2nd European Symposium on Computer and Communications*, 20–26. https://doi.org/10.1145/3478301.3478305

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 Behavioural Informatics, Digital Humanities and Development Research*, *10*(2), 53–74. https://www.researchgate.net/publication/381089158_CoDuBoTeSS_A_Pilot_Study_to_Eradicate_Counterfeit_Drugs_via_a_Blockchain_Tracer_Support_System_on_the_Nigerian_Frontier

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using GA algorithm for feature selection. *Journal of Big Data*, *9*(1), 24. https://doi.org/10.1186/s40537-022-00573-8

Laavanya, M., & Vijayaraghavan, V. (2019). Real Time Fake Currency Note Detection using Deep Learning. *International Journal of Engineering and Advanced Technology*, *9*(1S5), 95–98. https://doi.org/10.35940/ijeat.a1007.1291s52019

Li, C., Ding, N., Dong, H., & Zhai, Y. (2021). Application of Credit Card Fraud Detection Based on CS-SVM. *International Journal of Machine Learning and Computing*, *11*(1), 34–39. https://doi.org/10.18178/ijmlc.2021.11.1.1011

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

Malasowe, B. O., Akazue, M. I., Okpako, A. E., Aghware, F. O., Ojie, D. V., & Ojugo, A. A. (2023). Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities. *International Journal of Advanced Computer Science and Applications*, *14*(8), 135–142. https://doi.org/10.14569/IJACSA.2023.0140816

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://www.researchgate.net/publication/380752488_Co-Infection_Prevalence_of_Covid-19_Underlying_Tuberculosis_Disease_Using_a_Susceptible_Infect_Clustering_Bayes_Network

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*, *15*(2), 15–28. https://www.researchgate.net/publication/380514591_FePARM_The_Frequency-Patterned_Associative_Rule_Mining_Framework_on_Consumer_Purchasing-Pattern_for_Online_Shops

Maya Gopal, P. ., & Bhargavi R. (2018). Feature Selection for Yield Prediction Using BORUTA Algorithm. *International Journal of Pure and Applied Mathematics*, *118*(22), 139–144.

Maya Gopal P S, & Bhargavi R. (2019). Selection of Important Features for Optimizing Crop Yield Prediction. *International Journal of Agricultural and Environmental Information Systems*, *10*(3), 54–71. https://doi.org/10.4018/IJAEIS.2019070104

Muslikh, A. R., Setiadi, D. R. I. M., & Ojugo, A. A. (2023). Rice disease recognition using transfer xception convolution neural network. *Jurnal Teknik Informatika (JUTIF)*, *4*(6), 1541–1547. https://doi.org/10.52436/1.jutif.2023.4.6.1529

Mustofa, F., Safriandono, A. N., Muslikh, A. R., & Setiadi, D. R. I. M. (2023). Dataset and Feature Analysis for Diabetes Mellitus Classification using Random Forest. *Journal of Computing Theories and Applications*, *1*(1), 41–48. https://doi.org/10.33633/jcta.v1i1.9190

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. https://www.researchgate.net/publication/381032022_NiCuSBlockIoT_Sensor-based_Cargo_Assets_Management_and_Traceability_Blockchain_Support_for_Nigerian_Custom_Services

Ojugo, A. A., Abere, R. A., Orhionkpaiyo, B. C., Yoro, R. E., & Eboka, A. O. (2013). Technical Issues for IP-Based Telephony in Nigeria. *International Journal of Wireless Communications and Mobile Computing*, *1*(2), 58. https://doi.org/10.11648/j.wcmc.20130102.11

Ojugo, A. A., Aghware, F. O., Yoro, R. E., Yerokun, M. O., Eboka, A. O., Anujeonye, C. N., & Efozia, F. N. (2015). Dependable Community-Cloud Framework for Smartphones. *American Journal of Networks and Communications*, *4*(4), 95. https://doi.org/10.11648/j.ajnc.20150404.13

Ojugo, A. A., Aghware, F. O., Yoro, R. E., Yerokun, M. O., Eboka, A. O., Anujeonye, C. N., & Efozia, F. N. (2015). Evolutionary Model for Virus Propagation on Networks. *Automation, Control and Intelligent Systems*, *3*(4), 56. https://doi.org/10.11648/j.acis.20150304.12

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), 1–11. 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., Ben-Iwhiwhu, E., Kekeje, O. D., Yerokun, M. O., & Iyawa, I. J. (2014). Malware Propagation on Social Time Varying Networks: A Comparative

Study of Machine Learning Frameworks. *International Journal of Modern Education and Computer Science*, *6*(8), 25–33. https://doi.org/10.5815/ijmecs.2014.08.04

Ojugo, A. A., & Eboka, A. O. (2014). A Social Engineering Detection Model for the Mobile Smartphone Clients. *African Journal of Computing & ICT*, *7*(3), 91–100. 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. https://doi.org/10.5815/ijitcs.2018.10.07

Ojugo, A. A., & Eboka, A. O. (2018b). 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. (2020). 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. (2021). Empirical Bayesian network to improve service delivery and performance dependability on a campus network. *IAES International Journal of Artificial Intelligence (IJ-AI)*, *10*(3), 623. https://doi.org/10.11591/ijai.v10.i3.pp623-635

Ojugo, A. A., Eboka, A. O., Okonta, E. O., Yoro, R. E., & Aghware, F. O. (2012). Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS). *Journal of Emerging Trends In Computing Information Systems*, *3*(8), 1182–1194. http://www.cisjournal.org

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

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015b). Hybrid Model for Early Diabetes Diagnosis. *2015 Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, 55–65. https://doi.org/10.1109/MCSI.2015.35

Ojugo, A. A., Ejeh, P. O., Odiakaose, C. C., Eboka, A. O., & Emordi, F. U. (2023). Improved distribution and food safety for beef processing and management using a blockchain-tracer support framework. *International Journal of Informatics and Communication Technology*, *12*(3), 205. https://doi.org/10.11591/ijict.v12i3.pp205-213

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 (IJ-ICT)*, *13*(1), 108. https://doi.org/10.11591/ijict.v13i1.pp108-115

Ojugo, A. A., & Ekurume, E. O. (2021a). 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. https://doi.org/10.30534/ijatcse/2021/851032021

Ojugo, A. A., & Ekurume, E. O. (2021b). Predictive Intelligent Decision Support Model in Forecasting of the Diabetes Pandemic Using a Reinforcement Deep Learning Approach. *International Journal of Education and Management Engineering*, *11*(2), 40–48. https://doi.org/10.5815/ijeme.2021.02.05

Ojugo, A. A., & Nwankwo, O. (2021). 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., Obruche, C. O., & Eboka, A. O. (2021a). Empirical Evaluation for Intelligent Predictive Models in Prediction of Potential Cancer Problematic Cases In Nigeria. *ARRUS Journal of Mathematics and Applied Science*, *1*(2), 110–120. https://doi.org/10.35877/mathscience614

Ojugo, A. A., Obruche, C. O., & Eboka, A. O. (2021b). Quest For Convergence Solution Using Hybrid Genetic Algorithm Trained Neural Network Model For Metamorphic Malware Detection. *ARRUS Journal of Engineering and Technology*, *2*(1), 12–23. https://doi.org/10.35877/jetech613

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), 145–156. https://doi.org/10.17977/um018v6i22023p145-156

Ojugo, A. A., & Okobah, I. P. (2017). Hybrid Fuzzy-Genetic Algorithm Trained Neural Network Stochastic Model for Diabetes Diagnosis and Classification. *Journal of Digital Innovations & Contemp Res. In Sc., Eng & Tech*, *5*(4), 69–90. https://doi.org/10.22624

Ojugo, A. A., & Okobah, I. P. (2018a). Prevalence Rate of Hepatitis-B Virus Infection in the Niger Delta Region of Nigeria using a Graph-Diffusion Heuristic Model. *International Journal of Computer Applications*, *179*(39), 975–8887.

Ojugo, A. A., & Okobah, I. P. (2018b). Quest for an intelligent convergence solution for the well-known David, Fletcher and Powell quadratic function using supervised models. *Open Access Journal of Science*, *2*(1), 53–59. https://doi.org/10.15406/oajs.2018.02.00044

Ojugo, A. A., & Otakore, O. D. (2018). 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. (2020a). Computational solution of networks versus cluster grouping for social network contact recommender system. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *9*(3), 185. https://doi.org/10.11591/ijict.v9i3.pp185-194

Ojugo, A. A., & Otakore, O. D. (2020b). Intelligent cluster connectionist recommender system using implicit graph friendship algorithm for social networks. *IAES International Journal of Artificial Intelligence*, *9*(3), 497~506. https://doi.org/10.11591/ijai.v9.i3.pp497-506

Ojugo, A. A., & Otakore, O. D. (2020c). Investigating The Unexpected Price

Plummet And Volatility Rise In Energy Market: A Comparative Study of Machine Learning Approaches. *Quantitative Economics and Management Studies*, *1*(3), 219–229. https://doi.org/10.35877/454ri.qems12119

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., & Oyemade, D. A. (2021). Boyer moore string-match framework for a hybrid short message service spam filtering technique. *IAES International Journal of Artificial Intelligence*, *10*(3), 519–527. https://doi.org/10.11591/ijai.v10.i3.pp519-527

Ojugo, A. A., Oyemade, D. A., Allenotor, D., Longe, O. B., & Anujeonye, C. N. (2015). Comparative Stochastic Study for Credit-Card Fraud Detection Models. *African Journal of Computing & ICT*, *8*(1), 15–24. www.ajocict.net

Ojugo, A. A., Ugboh, E., Onochie, C. C., Eboka, A. O., Yerokun, M. O., & Iyawa, I. J. (2013). Effects of Formative Test and Attitudinal Types on Students' Achievement in Mathematics in Nigeria. *African Educational Research Journal*, *1*(2), 113–117. http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1216962&site=ehost-live

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). Forging A Smart Dependable Data Integrity And Protection System Through Hybrid-Integration Honeypot In Web and Database Server. *Technology Report of Kansai University*, *62*(08), 5933–5947.

Ojugo, A. A., & Yoro, R. E. (2021a). Extending the three-tier constructivist learning model for alternative delivery: ahead the COVID-19 pandemic in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(3), 1673. https://doi.org/10.11591/ijeecs.v21.i3.pp1673-1682

Ojugo, A. A., & Yoro, R. E. (2021b). Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack. *International Journal of Electrical and Computer Engineering*, *11*(2), 1498–1509. https://doi.org/10.11591/ijece.v11i2.pp1498-1509

Ojugo, A. A., Yoro, R. E., Oyemade, D. A., Eboka, A. O., Ugboh, E., & Aghware, F. O. (2013). Robust Cellular Network for Rural Telephony in Southern Nigeria. *American Journal of Networks and Communications*, *2*(5), 125. https://doi.org/10.11648/j.ajnc.20130205.12

Ojugo, A. A., Yoro, R. E., Yerokun, M. O., & Iyawa, I. J. (2013). Implementation Issues of VoIP to Enhance Rural Telephony in Nigeria. *Journal of Emerging Trends in Computing and Information Sciences ©2009-2013*, *4*(2), 172–179. http://www.cisjournal.org

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. https://doi.org/10.5120/ijca2018916586

Okofu, S. N., Anazia, K. E., Akazue, M. I., Okpor, M. D., Oweimieto, 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 Advances in Computer Science and Applications*, *15*(7), 804–811. https://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., 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

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*, *2*(1), 1–12. https://doi.org/10.33633/jcta.v2i19509

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

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*, *12*(2), 45–66. https://www.researchgate.net/publication/380875447_DaBO-BoostE_Enhanced_Data_Balancing_via_Oversampling_Technique_for_a_Boosting_Ensemble_in_Card-Fraud_Detection

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. https://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. https://ijiset.com/vol8/v8s2/IJISET_V8_I02_41.pdf

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

Paliwal, S., Mishra, A. K., Mishra, R. K., Nawaz, N., & Senthilkumar, M. (2022). XGBRS Framework Integrated with

Word2Vec Sentiment Analysis for Augmented Drug Recommendation. *Computers, Materials and Continua*, *72*(3), 5345–5362. https://doi.org/10.32604/cmc.2022.025858

Rathi, M., & Pareek, V. (2013). Spam Mail Detection through Data Mining – A Comparative Performance Analysis. *International Journal of Modern Education and Computer Science*, *5*(12), 31–39. https://doi.org/10.5815/ijmecs.2013.12.05

Rukshan Pramoditha. (2020). k-fold cross-validation explained in plain English. *Towards Data Science*, *December 2020*.

Safriandono, A. N., Setiadi, D. R. I. M., Dahlan, A., Zakiyah, F., Wibisono, I. S., & Ojugo, A. A. (2024). Analyzing Quantum Features Egineering and Balancing Strategy Effect for Liver Disease Classification. *Journal of Future Artificial Intelligence and Technologies*, *1*(1), 50–62.

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

Sunarjo, M. S., Gan, H.-S., & Setiadi, D. R. I. M. (2023). High-Performance Convolutional Neural Network Model to Identify COVID-19 in Medical Images. *Journal of Computing Theories and Applications*, *1*(1), 19–30. https://doi.org/10.33633/jcta.v1i1.8936

Taravat, A., & Del Frate, F. (2013). Weibull Multiplicative Model and Machine Learning Models for Full-Automatic Dark-Spot Detection From Sar Images. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *XL-1/W3*(September 2013), 421–424. https://doi.org/10.5194/isprsarchives-xl-1-w3-421-2013

Tingfei, H., Guangquan, C., & Kuihua, H. (2020). Using Variational Auto Encoding in Credit Card Fraud Detection. *IEEE Access*, *8*, 149841–149853. https://doi.org/10.1109/ACCESS.2020.3015600

Vågsholm, I., Arzoomand, N. S., & Boqvist, S. (2020). Food Security, Safety, and Sustainability—Getting the Trade-Offs Right. *Frontiers in Sustainable Food Systems*, *4*(February), 1–14. https://doi.org/10.3389/fsufs.2020.00016

Verma, S. S., Lucas, A., Zhang, X., Veturi, Y., Dudek, S., Li, B., Li, R., Urbanowicz, R., Moore, J. H., Kim, D., & Ritchie, M. (2018). Collective feature selection to identify crucial epistatic variants. *BioData Mining*, *11*(1), 5. https://doi.org/10.1186/s13040-018-0168-6

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.

Yan, C., Huanhuan, F., Ablikim, B., Zheng, G., Xiaoshuan, Z., & Jun, L. (2018). Traceability information modeling and system implementation in Chinese domestic sheep meat supply chains. *Journal of Food Process Engineering*, *41*(7), e12864. https://doi.org/10.1111/jfpe.12864

Yao, J., Wang, C., Hu, C., & Huang, X. (2022). Chinese Spam Detection Using a Hybrid BiGRU-CNN Network with Joint Textual and Phonetic Embedding. *Electronics*, *11*(15), 2418. https://doi.org/10.3390/electronics11152418

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *International Journal of Electrical and Computer Engineering*, *13*(2), 1943. https://doi.org/10.11591/ijece.v13i2.pp1943-1953

Yoro, R. E., Aghware, F. O., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(2), 1922. https://doi.org/10.11591/ijece.v13i2.pp1922-1931

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

Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. *Computers and Security*, *104*. https://doi.org/10.1016/j.cose.2021.102221

Zareapoor, M., & Shamsolmoali, P. (2015). Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier. *Procedia Computer Science*, *48*, 679–685. https://doi.org/10.1016/j.procs.2015.04.201

Zhang, F., & Lian, Y. (2009). QRS Detection Based on Multiscale Mathematical Morphology for Wearable ECG Devices in Body Area Networks. *IEEE Transactions on Biomedical Circuits and Systems*, *3*(4), 220–228. https://doi.org/10.1109/TBCAS.2009.2020093

Zhang, W., Yang, X., & Song, Q. (2015). Construction of Traceability System for Maintenance of Quality and Safety of Beef. *International Journal on Smart Sensing and Intelligent Systems*, *8*(1), 782–800. https://doi.org/10.21307/ijssis-2017-783