Voice-based Dynamic Time Warping Recognition Scheme for Enhanced Database Access Security

Paul Avweresuo Onoma [1,*], Eferhire Valentin Ugbotu [2], Tabitha Chukwudi Aghaunor [3], Joy Agboi [4], Arnold Adimabua Ojugo [5], Christopher Chukwufunaya Odiakaose [6], Asuobite ThankGod Max-Egba [7], Star Umiyemeromesu Niemogha [8], Amaka Patience Binitie [9], and Mustapha Barau Abdullahi [10]
[1,5,7,8,10] Department of Computer Science, Federal University of Petroleum Resources Effurun, Nigeria
[2] Department of Data Science, University of Salford, United Kingdom
[3] Department of Data Intelligence and Technology, Robert Morris University, Pittsburg, Pennsylvania, USA
[4] Department of Computer Science, Delta State University Abraka, Nigeria
[6] Department of Computer, Dennis Osadebay University Asaba, Nigeria
[9] Department of Computer Science, Federal College of Education (Technical) Asaba, Nigeria
Email: [1] kenbridge14@gmail.com, [2] eferhire.ugbotu@gmail.com, [3] tabitha.aghaunot@gmail.com, [4] agboijoy0@gmail.com, [5] ojugo.arnold@fupre.edu.ng, [6] osegalaxy@gmail.com, [7] max-egbaasuobite@fupre.edu.ng, [8] niemogha.star@fupre.edu.ng, [9] amaka.binitie@fcetasaba.edu.ng, [10] abdullahi.mustapha@fupre.edu.ng
*Corresponding Author

***Abstract*—Rapid transformation with database security has remained imperative as unauthorized access exposes sensitive data to adversaries. To curb this, we suggest using a secured dynamic time-warp scheme to improve access to the database schemas. The study integrates voice biometrics with two-factor authentication to yield a robust, user-friendly platform, which utilizes time-warping to authenticate voice patterns against the variability in utterance speed. Results showcase high accuracy and resiliency in its usage against spoofing attacks as compared to state-of-the-art voice recognition systems. The model ensures the minimal possibility of credential theft by binding the access of databases to the voice features of authorized users. The study shows the system's architecture, implementation, and performance evaluation, highlighting its potential to revolutionize database security in various applications. The findings underscore the importance of leveraging advanced biometric techniques to safeguard critical information systems.**

Keywords*—*Time-warping; Voice-based Biometrics; Convolution Neural Network

I. INTRODUCTION

The database houses data in a tabular structure that yields efficient storage with eased retrieval and management of data [1]. The tabular mode for the relational model has been widely used to organize and access data in various industries [2]. Distributed databases allow us to replicate and share data across networks – enhancing access and its availability [3][4]. Conventional username and password-based database login is susceptible as the passwords can be corrupted or stolen, posing heavy security and integrity threats to the confidential information stored [5][6]. This requires a better login process, having a more robust and reliable authentication method [7]. With key benefits such as improved security, model accuracy, improved usability, enhanced user experience, and scalability [8][9] – we propose a secure database fused with voice recognition via dynamic time warping as an authentication process [10][11]. Previous studies on database security weaknesses, but did not propose a complete data integrity and security model [12][13]. Rather, they proposed an authentication scheme for the relational database via a one-time password (OTP) [14]; Nevertheless, it still left scope for exploitable and compromisable vulnerability in front of malicious users [15][16].

Knowledge-based authentication is an essential element of identity verification methods and solutions [17]. KBA is used in various ways – making them an efficient authentication mode [18][19]. KBA factoids are established on the knowledge that the user is alone required to possess (i.e. personal identification number, username, etc). Two commonly used authentications are [20][21]: (a) static KBA which has pre-defined questions with shared data amongst users [22]. A typical static factoid question is "What is the mother's maiden name?" or "What is the date of birth?" This technique is used by banks, and enterprises for user authentication [23]–[26].

Instant KBA dynamically generates a set of personalized questions and answers to enable user authentication. It does not require users to provide questions and answers in advance for users [27][28]. These challenge questions are dynamic and contain the correct and incorrect answers placed randomly by using data made available to the KBA system. Both of these need an advance registration against a previously existing database for credentialing [29][30]. However, KBA needs online or remote server access for checking the factoids or credentials during login. Aghware *et al*. [31] used a fusion-based multimodal system with face and voice biometrics. Their technique is feature-level, match score-level, rank-level, and decision-level fusion. They explored Log Gabor and LBP for face feature extraction and MFCC and LPC for voice feature extraction. It also touches on the number of fusion layers and investigates the constraints affected by various methods at the extraction and recognition level [32]–[34]. Otorokpo *et al*. [35] proposed face and voice biometric fusion for verification of users. Its combined score level is applied to both face/voice gait feats to bypass the limitations of the unimodal system. Setiadi *et al*. [36] used a multimodal biometric identification system based on voice and face recognition. The study assessed the scheme's feasibility via statistical coefficients for voice-and-

face extraction techniques such as Eigenface and Principal Component Analysis [37][38].

Previously used classifiers include Gaussian mixture [39], Neural Net [40], etc – all of which yield great results. Pande and Khampe [41] studied an android-based multimodal biometric authentication that explored both face and voice to yield a stronger face gait extraction local binary pattern with voice activity detection. It demonstrated a high accuracy of 98% for face and 89% for voice on Android-based smart terminals. Other studies have showcased significant progress in biometric modalities such as face recognition [42], voice recognition [43], vein patterns [44], and ultrasound images [45]. A holistic multimodal system can seamlessly integrate multi-biometric modalities, and enhance the expected cum requisite authentication accuracy and robustness [46].

A. Machine Learning Approaches

Many machine learning (ML) approaches/schemes are successfully implemented as Logistic Regression [47], Deep Learning [48], Adaboost [49], Naive Bayes [50], SVM [51], Random Forest [52], and others [53] as it has been effectively used to detect credit card fraud. Many of these MLs as mentioned, have their drawbacks, especially with their flexibility in feature selection/extraction approach (as either filter or wrapper) in the quest for ground truth, selected feature importance in its capability to yield faster model construction and training, and model's fitness in place of its performance accuracy. As in Table 1, a variety of ML approach contributions are as thus [54]:

Table 1. Related Literatures Contributions

Features	Efficient Selected Algorithms	Accuracy
Btoush et al. [55]	Deep Learning approach	95.76%
Sinayob et al. [56]	KNN, LR, SVM, DT and RF	98.45%
Ojugo et al. [57]	Deep learning modular ensemble	99.6%
Roselin et al [58]	Long Term Short Memory	99.58%

B. Study Motivation and Rationale

Gaps in previous studies include [59]–[62]:

1. **Imbalanced Dataset:** A major challenge with available datasets for training is that most models use the major class [63], and often ignore the minor class since they have been found to lag. We must harness the prowess of models that are explicitly tailored to mitigate the issues with imbalanced datasets [64][65].
2. **Cross-Platform:** With an increase in the number of OS available [66]–[68] – today's systems must integrate cross-platform data to enhance the requisite accuracy and performance accuracy.

To address these, we propose a voice recognition system that utilizes Dynamic Time Warp (DTW) as a component of a multimodal authentication system. The study contributes to the use of a comprehensive, secure biometric authentication via the utilization of DTW, a specialized technique for aligning and comparing time series data, which holds promise in enhancing the accuracy and reliability of voice-based authentication within a multimodal context [69][70].

II. Materials and Methods

A. Overview of the Existing System

Resource security often relied on traditional password-based authentication. Users authenticate their devices by inputting a password they had either chosen or been assigned [71]. A major vulnerability is in complex passwords that are susceptible to brute-force or dictionary attacks. Users reuse passwords on multiple accounts – and it poses a significant risk [72][73]. With one account compromised, other accounts become vulnerable [74]. Thus, passwords lean towards user-friendliness, potentially compromising security. Users may forget passwords, leading to recovery and reset challenges that can affect user experience. To address these issues, [75] used an enhanced security system that builds upon traditional authentication schemes using OTPs. This has several merits: (a) OTPs are dynamically generated [76], (b) reduce risk of unauthorized access from stolen passwords [77], (c) can be used with OS login as added security prior OTP generation, (d) are time-sensitive and valid only for a short burst [78] to mitigate their risk of reuse [79], and (e) often yields complexity that makes them more challenging for the adversary to crack the digital credentials [80][81]. Thus, Fig. 1 shows security architecture with privileges.

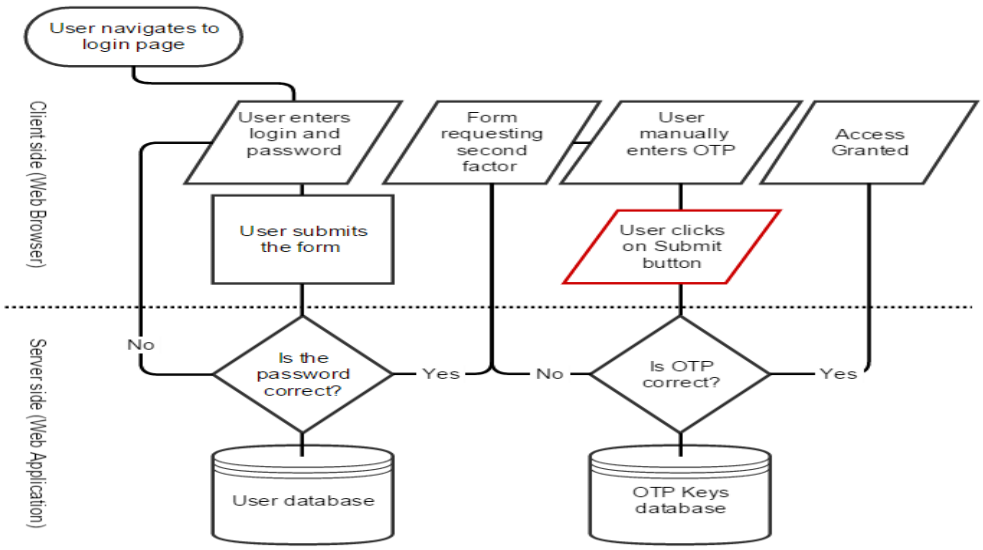

Fig. 1. The architecture of database security

The existing system is made of four modules:

a. The authentication server generates OTP – and checks for username and password, and OS user authentication. Having inputted the correct OTP, a user is then connected to the database,
b. Availability: data is uploaded on a database server with access provided to the user after the system validates user input OTP. The database makes available user privileges provided by the database admin to read, run, or update the data,
c. Access: The Admin registers users and provides them with the requisite login username and password. Registration of user(s) is performed by Admin [82][83],
d. Integrity: The data that is created or modified by the user is governed by a set of pre-defined rules. These rules are defined by the application administrator or database developer [84]–[86].

B. The Proposed System Architecture

The proposed system explores a voice recognition scheme as an authentication layer for users. Fig. 2 shows parts of secure authentication by its functionality integrating the Dynamic Time Warp (DTW) algorithm.

1. Acoustic Front-End serves thus: (a) transforms the speech signal as recorded via the microphone, into suitable features. The features are needed for voice recognition [87][88]. In this process of feature extraction, the DTW algorithm can be utilized, and (b) helps match the input audio waveform (recorded voice at the time of login) and an enrolled voice template, and both sequences lining up considering differences in timing and speed, which is of excellent utility in voice recognition [89].
2. The Acoustic Model does the following: (a) it estimates the word or phone model parameters from the acoustic vectors obtained from the training data. In the process, DTW can also be applied in training to map reference voice patterns against the recognized command or text, and (b) DTW alignment during training is used to produce accurate acoustic models that can be used for identifying words or phrases in the login process [90].
3. Lexicon does the following: (a) maintains a lexicon of words or phrases which can be identified by the system. It acts as a reference for acoustic patterns to be converted into linguistic units, and (b) assists in mapping acoustic patterns to the entries of the lexicon to allow spoken words or phrases to be recognized.
4. Language Model accomplishes: (a) it defines the word sequence probability in a specific language [91][92], which allows the system to compute the probability of each word sequence, and (b) DTW is oriented towards acoustic alignment, it enhances the language model by ensuring that the accepted words or phrases spoken are highly correlated with the expected acoustic patterns.
5. Decoder performs the following functions: (a) examines all the word-sequence sets to determine the most likely word-sequence that is likely to have generated the input speech signal, and (b) DTW can be applied in this decoding procedure to compute the similarity between the captured voice and registered voice templates and assess the likelihood of a match.

Fig. 3 describes a working structure of the complete model for database access security as proposed.

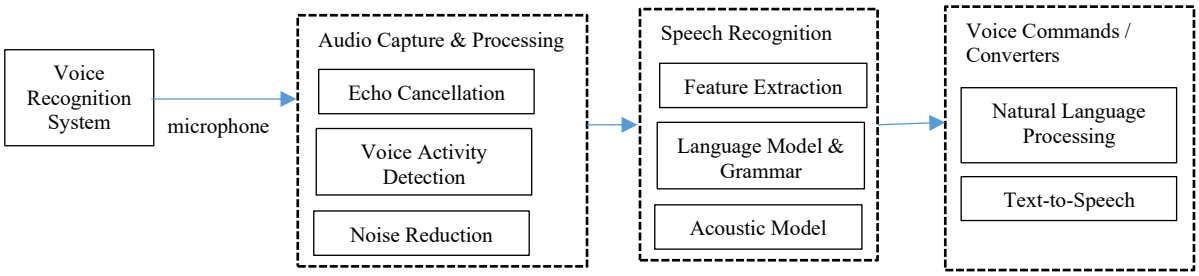

Fig. 2. System architecture and design of the DTW model

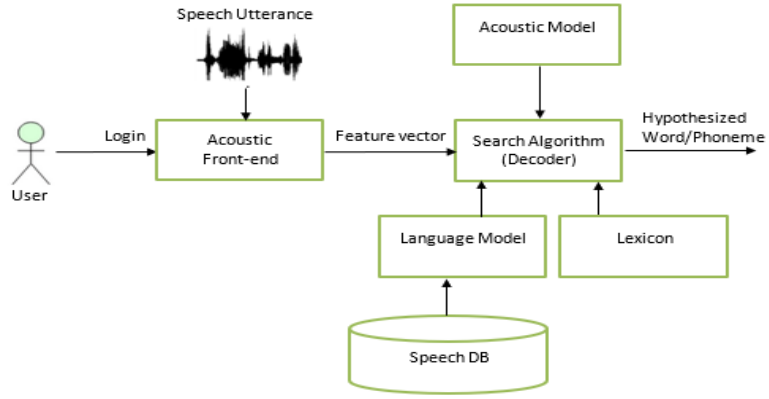

Fig. 3. High-level schematics for the proposed DWT voice-based recognition framework

Performance evaluation is pivotal/crucial to validate its effectiveness as hinged on 3 key metrics of accuracy, precision, and sensitivity [93] – to proffer insights into the system's capabilities. Computations make use of historical data that was not encountered during system training, ensuring the system's reliability and accuracy in securing database access. The app domains highlight the versatility and broad relevance of the proposed database security solution that includes dynamic time-warping voice recognition [94]. Implementing the system will enhance security, protect sensitive data, and ensure robust user authentication while also adapting to the specific requirements of each industry.

III. Result Findings and Discussion

A. System Design Interface

The system explores two (2) distinct sessions, namely: (a) user session – which starts with a user access of a default application installed. The activation of the program app is initialized by clicking the displayed icon on the desktop – from which the launched program presents the user with a voice-login page. It acts as a gateway to authenticate the user via their voice (signal) pattern using the API that consists of a variety of active buttons such as start voice authentication, exit, signup, and alternative login button(s) as illustrated in Fig. 4.

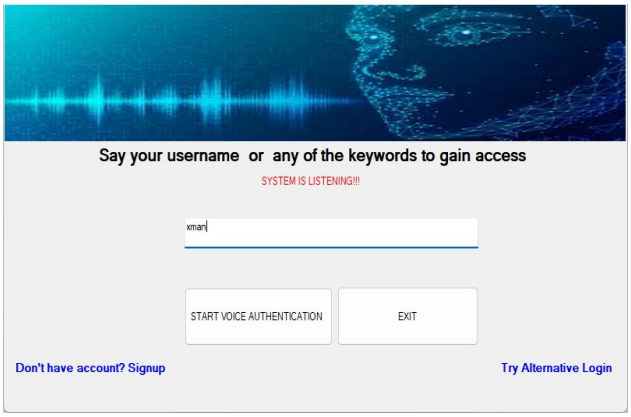

Fig. 4. Voice login interface

Sequel to the successful registration of user details, a user can then proceed with voice enrollment to register their voice (unique) signal for which the system provides the needed flexibility via command keywords such as "Login," "Open," "Close," etc – for access to the system [95][96]. Upon completion of the registration process, user accounts undergo verification by the administrator. This crucial step ensures the integrity and security of the system before granting users access to their respective dashboards [97]–[99] – as in Fig. 5, which displays the voice enrollment to enable users' interaction with the application.

A successful voice enrolment process will then redirect a user to the login page as in Fig. 6 – whereas, Fig. 7 functions as the pivotal page that requests input of a user's details (i.e. username and password) to access the system. In addition, the pivotal page acts also as a secure gateway to help validate user credentials for registered accounts in the new system. A correctly inputted user credential will authenticate a valid user's identity, granting access to the array of resources available. Conversely, a denied user can utilize the voice authentication page to log in to the platform cum app. Utilization of this mode often prompts the users also to compile a series of whitelisted (acceptable) keywords that were engaged during the user voice enrollment process. Upon the successful voice-verified mode for user credentials, the user is granted secure access to their personalized account, to ensure an intuitive, seamless user experience.

Fig. 5. Voice enrolment interface

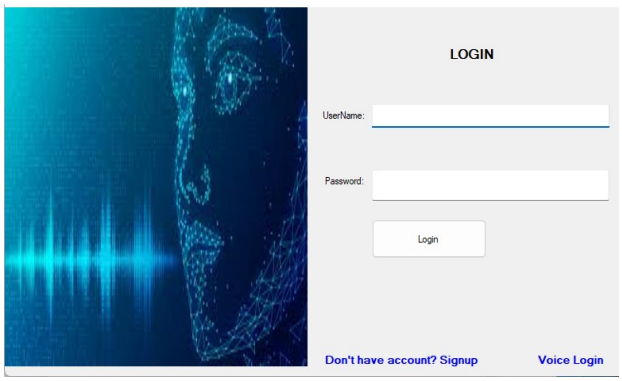

Fig. 6. Alternate login interface

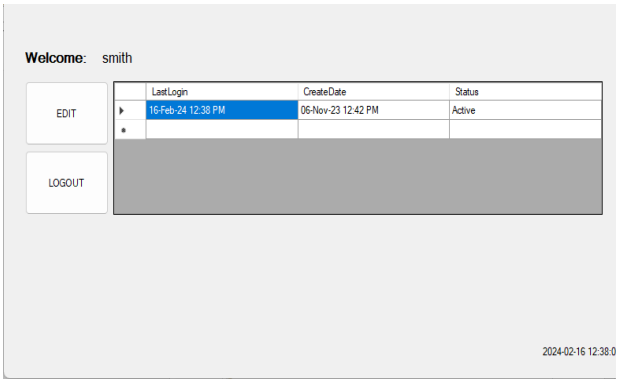

Fig. 7. User dashboard

Fig. 7 shows a user dashboard to establish interaction between the user and a plethora of the system's diverse functionalities [100][101]. Its user-centric and friendly design provisions an intuitive interface that emboldens a user's seamless navigation across the various regions of the system vis-à-vis render access to crucial data [102][103], helps the user to enact administrative roles, reprise user account settings – amongst others. It thus acts as a dynamic control pane that empowers its validated users to effectively

harness its capabilities, and ensure an efficient coordination of diverse tasks. Where the user wishes to access critical data, customize settings/preferences for the user, and initialize other system actions [104], this dashboard acts as the navigation pane to optimize user productivity and experience [105][106].

The admin session helps an Admin to navigate the login page to exert control policies and preferences within the app or system as in Fig. 8. The Admin login page presents a familiar interface, prompting an Admin to provide their designated username and password. Functioning as the gateway to administrative functionalities, the admin login page serves as a crucial checkpoint for verifying the administrator's identity and authorization. By accurately entering their login credentials, the administrator validates their entitlement to wield administrative control, thus gaining access to a comprehensive suite of system management tools. This rigorous login process underscores the system's commitment to security, ensuring that only duly authorized individuals with administrative privileges can oversee and govern the system's operations with precision and authority [107].

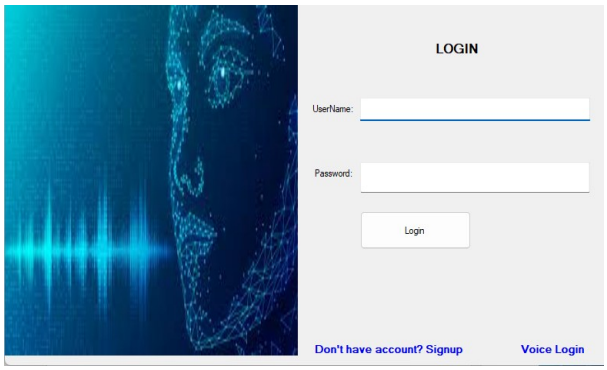

Fig. 8. Admin login

Successfully authenticated admin redirects such a user to the admin dashboard as in Fig. 9, which furnishes an admin with a table view of all users' logs captured in the system [108]–[110]. It renders a host of buttons that serve specific administrative needs and tasks. The ***suspend*** button deactivates user accounts (where necessary), temporarily; while the ***verification*** button activates user accounts for integration into the system [111]. The ***delete-account*** button permanently removes a user account, while, the ***logout*** button allows the admin to terminate a (group of) user's session.

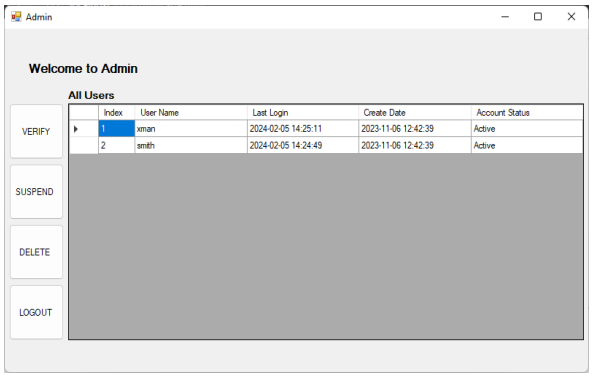

Fig. 9. Admin dashboard

This pane acts also as a nexus for admin tasks as well as provision tools for swift actions as well as insight cum monitoring of user activities. Thus, it equips the admin with robust functionalities via its intuitive API that enables the admin to efficiently oversee all system operations, monitor user activities/interactions, and execute administrative tasks with precision and efficiency [112].

IV. Conclusion

The proposed platform uses a conventional username and password authentication method, which is vulnerable to risk, and demands an innovative approach. We then integrated the dynamic time-warp voice recognition to enhance security and user experience for sensitive data access. The literature revealed numerous pitfalls with conventional authentication mode. Thus, the proposed system draws from earlier work carried out on one-time passwords, incorporating best practices to enhance both security and dependability. The system yields a framework with enhanced usability and robust security. Its performance validated its efficiency with well-documented training to ensure that administrators and end-users can effectively manage the system. Our changeover procedure offers a clear transition path from an existing-to-new, secure database model aimed at minimizing disruptions, while preserving data integrity [104].

This study presents an innovative, comprehensive solution to the pressing issue of database security. It not only addresses the limitations of traditional authentication methods but also provides a systematic approach to system development, implementation, and ongoing maintenance. By emphasizing the importance of user training, documentation, and changeover procedures, it ensures that the proposed system can be effectively integrated into existing infrastructure, delivering an elevated level of security and user authentication. The project represents a significant step forward in the ongoing effort to safeguard sensitive data [104] and ensure the integrity of databases.

References

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

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

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

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

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

[6] S. Saeed, "A customer-centric view of E-commerce security and privacy," *Applied Sciences*, vol. 13, no. 2, 1020, 2023, https://doi.org/10.3390/app13021020.

[7] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "NovidChain: Blockchain-based privacy-preserving platform for COVID-19

test/vaccine certificates," *Software: Practice and Experience*, vol. 52, no. 4, pp. 841-867, 2022, https://doi.org/10.1002/spe.2983.

[8] A. A. Ojugo and A. O. Eboka, "Modeling the Computational Solution of Market Basket Associative Rule Mining Approaches Using Deep Neural Network," *Digit. Technol.*, vol. 3, no. 1, pp. 1–8, 2018, https://doi.org/10.11591/ijict.v8i3.pp128-138.

[9] A. Ali *et al*., "Financial fraud detection based on machine learning: a systematic literature review," *Applied Sciences*, vol. 12, no. 19, p. 9637, 2022, https://doi.org/10.3390/app12199637.

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

[11] E. U. Omede, A. E. Edje, M. I. Akazue, H. Utomwen, and A. A. Ojugo, "IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defense System," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 273–283, 2024, https://doi.org/10.62411/jcta.9541.

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

[13] A. P. Binitie, "Design of a Resilient System against Shoulder Surfing Attack : Adaptable to USSD Channel," *Res. Sq.*, pp. 1–19, 2023, https://doi.org/10.21203/rs.3.rs-2793844/v1.

[14] A. A. Ojugo *et al.*, "CoSoGMIR: A Social Graph Contagion Diffusion Framework using the Movement-Interaction-Return Technique," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 37–47, 2023, https://doi.org/10.33633/jcta.v1i2.9355.

[15] S. Anderson *et al*., "A decision analytic model for prevention of hepatitis B virus infection in Sub-Saharan Africa using birth-dose vaccination," *International Journal of Gynecology & Obstetrics*, vol. 141, no. 1, pp. 126-132, 2018, https://doi.org/10.1002/ijgo.12434.

[16] S. Hemalatha, T. Kavitha, T. M. Saravanan, K. Chitra and N. Dinesh, "Forecasting Crop Using Machine Learning Model," *2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pp. 783-788, 2022, https://doi.org/10.1109/ICESC54411.2022.9885377.

[17] O. O. Olaniyi, O. J. Okunleye, S. O. Olabanji, C. U. Asonze, and S. A. Ajayi, "IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience," *Asian J. Res. Comput. Sci.*, vol. 16, no. 4, pp. 354–371, 2023, https://doi.org/10.9734/ajrcos/2023/v16i4397.

[18] K. M. Vinoth, K. Venkatachalam, P. Prabu, A. Almutairi, and M. Abouhawwash, "Secure biometric authentication with de-duplication on distributed cloud storage," *PeerJ Comput. Sci.*, vol. 7, pp. 1–20, 2021, https://doi.org/10.7717/peerj-cs.569.

[19] M. I. Akazue, I. A. Debekeme, A. E. Edje, C. Asuai, and U. J. Osame, "UNMASKING FRAUDSTERS : Ensemble Features Selection to Enhance Random Forest Fraud Detection," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 201–212, 2023, https://doi.org/10.33633/jcta.v1i2.9462.

[20] A. Borucka, "Logistic regression in modeling and assessment of transport services," *Open Eng.*, vol. 10, no. 1, pp. 26–34, 2020, https://doi.org/10.1515/eng-2020-0029.

[21] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, https://doi.org/10.1109/ACCESS.2019.2895334.

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

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

[24] F. Salahdine, Z. El Mrabet and N. Kaabouch, "Phishing Attacks Detection A Machine Learning-Based Approach," *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 0250-0255, 2021, https://doi.org/10.1109/UEMCON53757.2021.9666627.

[25] A. A. Ojugo and A. O. Eboka, "Inventory prediction and management in Nigeria using market basket analysis associative rule mining: memetic algorithm based approach," *Int. J. Informatics Commun. Technol.*, vol. 8, no. 3, p. 128, 2019, https://doi.org/10.11591/ijict.v8i3.pp128-138.

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

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

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

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

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

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

[32] B. O. Malasowe, F. O. Aghware, M. D. Okpor, B. E. Edim, R. E. Ako, and A. A. Ojugo, "Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech)," *J. Sci. Technol. Res.*, vol. 6, no. 2, pp. 293–311, 2024, https://doi.org/10.5281/zenodo.12617068.

[33] R. De', N. Pandey, and A. Pal, "Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice," *Int. J. Inf. Manage.*, vol. 55, no. June, p. 102171, 2020, https://doi.org/10.1016/j.ijinfomgt.2020.102171.

[34] O. Ahmad *et al.*, "Mechanism for Securing Smart Cities," *Sensors*, vol. 23, 2023, https://doi.org/10.3390/s23052757.

[35] E. A. Otorokpo *et al.*, "DaBO-BoostE: Enhanced Data Balancing via Oversampling Technique for a Boosting Ensemble in Card-Fraud Detection," *Adv. Multidiscip. Sci. Res. J. Publ.*, vol. 12, no. 2, pp. 45–66, 2024, https://doi.org/10.22624/AIMS/MATHS/V12N2P4.

[36] D. R. I. M. Setiadi, D. Marutho, and N. A. Setiyanto, "Comprehensive Exploration of Machine and Deep Learning Classification Methods for Aspect-Based Sentiment Analysis with Latent Dirichlet Allocation Topic Modeling," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 1, pp. 12–22, 2024, https://doi.org/10.62411/faith.2024-3.

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

[38] A. A. Ojugo, D. A. Oyemade, R. E. Yoro, A. O. Eboka, M. O. Yerokun, and E. Ugboh, "A Comparative Evolutionary Models for Solving Sudoku," *Autom. Control Intell. Syst.*, vol. 1, no. 5, p. 113, 2013, https://doi.org/10.11648/j.acis.20130105.13.

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

[40] A. Raza, K. Munir, M. S. Almutairi, and R. Sehar, "Novel Transfer Learning Based Deep Features for Diagnosis of Down Syndrome in Children Using Facial Images," *IEEE Access*, vol. 12, no. January, pp. 16386–16396, 2024, https://doi.org/10.1109/ACCESS.2024.3359235.

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

[42] S. Sandhya, A. Balasundaram, and A. Shaik, "Deep Learning Based Face Detection and Identification of Criminal Suspects," *Comput.*

Mater. Contin., vol. 74, no. 2, pp. 2331–2343, 2023, https://doi.org/10.32604/cmc.2023.032715.

[43] W. J. Sheng, I. F. Kasmin, S. Amin, and N. K. Zainal, "Addressing user perception and implementing Hedera Hashgraph and voice recognition into Multi-Factor Authentication (MFA) system," *Int. J. Data Sci. Adv. Anal.*, vol. 4, pp. 194–201, 2023, https://doi.org/10.69511/ijdsaa.v4i0.165.

[44] S. Bamashmos, N. Chilamkurti, and A. S. Shahraki, "Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment," *Sensors*, vol. 24, no. 11, 2024, https://doi.org/10.3390/s24113575.

[45] F. Jerbi, N. Aboudi, and N. Khlifa, "Automatic classification of ultrasound thyroids images using vision transformers and generative adversarial networks," *Sci. African*, vol. 20, p. e01679, 2023, https://doi.org/10.1016/j.sciaf.2023.e01679.

[46] F. U. Emordi *et al.*, "TiSPHiMME: Time Series Profile Hidden Markov Ensemble in Resolving Item Location on Shelf Placement in Basket Analysis," *Digit. Innov. Contemp. Res. Sci.*, vol. 12, no. 1, pp. 33–48, 2024, https://doi.org/10.22624/AIMS/DIGITAL/V11N4P3.

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

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

[49] L. K. Y. Loh *et al*., "An ensembling architecture incorporating machine learning models and genetic algorithm optimization for forex trading," *FinTech*, vol. 1, no. 2, pp. 100-124, 2022, https://doi.org/10.3390/fintech1020008.

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

[51] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Credit Card Fraud Detection - Machine Learning methods," in *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1–5, 2019, https://doi.org/10.1109/INFOTEH.2019.8717766.

[52] M. S. Bhadriraju and K. Dasari, "SSDP DDoS Attacks Detection using Naïve Bayes Classifiers with Wrapper Feature Selection Methods," *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)*, pp. 1-5, 2024, https://doi.org/10.1109/DELCON64804.2024.10866135.

[53] M. Zareapoor and P. Shamsolmoali, "Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier," *Procedia Comput. Sci.*, vol. 48, pp. 679–685, 2015, https://doi.org/10.1016/j.procs.2015.04.201.

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

[55] E. A. L. Marazqah Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, "A systematic review of literature on credit card cyber fraud detection using machine and deep learning," *PeerJ Comput. Sci.*, vol. 9, p. e1278, 2023, https://doi.org/10.7717/peerj-cs.1278.

[56] O. Sinayobye, R. Musabe, A. Uwitonze, and A. Ngenzi, "A Credit Card Fraud Detection Model Using Machine Learning Methods with a Hybrid of Undersampling and Oversampling for Handling Imbalanced Datasets for High Scores," In *International Conference on Applied Machine Learning and Data Analytics*, pp. 142–155, 2022, https://doi.org/10.1007/978-3-031-34222-6_12.

[57] A. A. Ojugo *et al.*, "Forging a User-Trust Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 1–11, 2023, https://doi.org/10.33633/jcta.v1i2.9259.

[58] J. Femila Roseline, G. Naidu, V. Samuthira Pandi, S. Alamelu alias Rajasree, and D. N. Mageswari, "Autonomous credit card fraud detection using machine learning approach☆," *Comput. Electr. Eng.*, vol. 102, p. 108132, 2022, https://doi.org/10.1016/j.compeleceng.2022.108132.

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

[60] B. N. Supriya and C. B. Akki, "Sentiment prediction using enhanced xgboost and tailored random forest," *Int. J. Comput. Digit. Syst.*, vol. 10, no. 1, pp. 191–199, 2021, https://doi.org/10.12785/ijcds/100119.

[61] S. Meghana, B. . Charitha, S. Shashank, V. S. Sulakhe, and V. B. Gowda, "Developing An Application for Identification of Missing Children and Criminal Using Face Recognition.," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 12, no. 6, pp. 272–279, 2023, https://doi.org/10.17148/IJARCCE.2023.12648.

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

[63] M. K. G. Roshan, "Multiclass Medical X-ray Image Classification using Deep Learning with Explainable AI," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 6, pp. 4518–4526, 2022, https://doi.org/10.22214/ijraset.2022.44541.

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

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

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

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

[68] A. A. Ojugo, P. O. Ejeh, C. C. Odiakaose, A. O. Eboka, and F. U. Emordi, "Improved distribution and food safety for beef processing and management using a blockchain-tracer support framework," *Int. J. Informatics Commun. Technol.*, vol. 12, no. 3, p. 205, 2023, https://doi.org/10.11591/ijict.v12i3.pp205-213.

[69] C. Wright and A. Serguieva, "Sustainable blockchain-enabled services: Smart contracts," in *2017 IEEE International Conference on Big Data (Big Data)*, pp. 4255–4264, 2017, https://doi.org/10.1109/BigData.2017.8258452.

[70] A. A. Ojugo, E. Ugboh, C. C. Onochie, A. O. Eboka, M. O. Yerokun, and I. J. Iyawa, "Effects of Formative Test and Attitudinal Types on Students' Achievement in Mathematics in Nigeria," *African Educ. Res. J.*, vol. 1, no. 2, pp. 113–117, 2013, https://eric.ed.gov/?id=EJ1216962.

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

[72] F. O. Aghware *et al.*, "Effects of Data Balancing in Diabetes Mellitus Detection : A Comparative XGBoost and Random Forest Learning Approach," *NIPES - J. Sci. Technol. Res.*, vol. 7, no. 1, pp. 1–11, 2025, https://doi.org/10.37933/nipes/7.1.2025.1.

[73] R. E. Ako *et al.*, "Pilot Study on Fibromyalgia Disorder Detection via XGBoosted Stacked-Learning with SMOTE-Tomek Data Balancing Approach," *NIPES - J. Sci. Technol. Res.*, vol. 7, no. 1, pp. 12–22, 2025, https://doi.org/10.37933/nipes/7.1.2025.2.

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

[75] V. Kumar, "A Study on Perceived Risk in Online Consumer Behaviour of Youth: An Indian Perspective.," *SSRN Electron. J.*, no. April, 2013, https://doi.org/10.2139/ssrn.2351725.

[76] J. Jose Diaz Rivera, A. Muhammad, and W.-C. Song, "Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication," *IEEE Open J.*

Commun. Soc., vol. 5, pp. 2792–2814, 2024, https://doi.org/10.1109/OJCOMS.2024.3391728.

[77] M. A. Hassan and Z. Shukur, "A Secure Multi Factor User Authentication Framework for Electronic Payment System," *2021 3rd International Cyber Resilience Conference (CRC)*, pp. 1-6, 2021, https://doi.org/10.1109/CRC50527.2021.9392564.

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

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

[80] A. Bouras, I. Khalil, and B. Aouni, "Blockchain driven supply chains and enterprise information systems," *Blockchain Driven Supply Chain. Enterp. Inf. Syst.*, no. September, pp. 1–222, 2022, https://doi.org/10.1007/978-3-030-96154-1.

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

[82] A. A. Ojugo and E. O. Ekurume, "Deep Learning Network Anomaly-Based Intrusion Detection Ensemble For Predictive Intelligence To Curb Malicious Connections: An Empirical Evidence," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 10, no. 3, pp. 2090–2102, 2021, https://doi.org/10.30534/ijatcse/2021/851032021.

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

[84] E. O. Okonta, A. A. Ojugo, U. R. Wemembu, and D. Ajani, "Embedding Quality Function Deployment In Software Development: A Novel Approach," *West African J. Ind. Acad. Res.*, vol. 6, no. 1, pp. 50–64, 2013, https://www.ajol.info/index.php/wajiar/article/view/87437.

[85] U. R. Wemembu, E. O. Okonta, A. A. Ojugo, and I. L. Okonta, "A Framework for Effective Software Monitoring in Project Management," *West African J. Ind. Acad. Res.*, vol. 10, no. 1, pp. 102–115, 2014, https://www.ajol.info/index.php/wajiar/article/view/105798.

[86] E. O. Okonta, U. R. Wemembu, A. A. Ojugo, and D. Ajani, "Deploying Java Platform to Design A Framework of Protective Shield for Anti–Reversing Engineering," *West African J. Ind. Acad. Res.*, vol. 10, no. 1, pp. 50–64, 2014, https://www.ajol.info/index.php/wajiar/article/view/105790.

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

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

[89] A. M. Ifioko *et al.*, "CoDuBoTeSS: A Pilot Study to Eradicate Counterfeit Drugs via a Blockchain Tracer Support System on the Nigerian Frontier," *J. Behav. Informatics, Digit. Humanit. Dev. Res.*, vol. 10, no. 2, pp. 53–74, 2024, https://doi.org/10.22624/AIMS/BIJ/V10N1P6.

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

[91] G. Nguyen *et al.*, "Machine Learning and Deep Learning frameworks and libraries for large-scale data mining: a survey," *Artif. Intell. Rev.*, vol. 52, no. 1, pp. 77–124, 2019, https://doi.org/10.1007/s10462-018-09679-z.

[92] M. Aljabri and S. Mirza, "Phishing Attacks Detection using Machine Learning and Deep Learning Models," *2022 7th International Conference on Data Science and Machine Learning Applications (CDMA)*, 2022, https://doi.org/10.1109/CDMA54072.2022.00034.

[93] Y. Srivastava, P. Khanna and S. Kumar, "Estimation of Gestational Diabetes Mellitus using Azure AI Services," *2019 Amity International Conference on Artificial Intelligence (AICAI)*, pp. 321-326, 2019, https://doi.org/10.1109/AICAI.2019.8701307.

[94] M. S. Sunarjo, H.-S. Gan, and D. R. I. M. Setiadi, "High-Performance Convolutional Neural Network Model to Identify COVID-19 in Medical Images," *J. Comput. Theor. Appl.*, vol. 1, no. 1, pp. 19–30, 2023, https://doi.org/10.33633/jcta.v1i1.8936.

[95] A. A. Ojugo *et al.*, "Evidence of Students' Academic Performance at the Federal College of Education Asaba Nigeria: Mining Education Data," *Knowl. Eng. Data Sci.*, vol. 6, no. 2, pp. 145–156, 2023, https://doi.org/10.17977/um018v6i22023p145-156.

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

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

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

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

[100] A. A. Ojugo, C. O. Obruche, and A. O. Eboka, "Quest For Convergence Solution Using Hybrid Genetic Algorithm Trained Neural Network Model For Metamorphic Malware Detection," *ARRUS J. Eng. Technol.*, vol. 2, no. 1, pp. 12–23, 2021, https://doi.org/10.35877/jetech613.

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

[102] S. Rajendran and P. Jayagopal, "Accessing Covid19 epidemic outbreak in Tamilnadu and the impact of lockdown through epidemiological models and dynamic systems," *Measurement*, vol. 169, p. 108432, 2021, https://doi.org/10.1016/j.measurement.2020.108432.

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

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

[105] L. R. Zuama, D. R. I. M. Setiadi, A. Susanto, S. Santosa, and A. A. Ojugo, "High-Performance Face Spoofing Detection using Feature Fusion of FaceNet and Tuned DenseNet201," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 4, pp. 385–400, 2025, https://doi.org/10.62411/faith.3048-3719-62.

[106] A. O. Eboka *et al.*, "Pilot study on deploying a wireless sensor-based virtual-key access and lock system for home and industrial frontiers," *Int. J. Informatics Commun. Technol.*, vol. 14, no. 1, p. 287, 2025, https://doi.org/10.11591/ijict.v14i1.pp287-297.

[107] N. R. Pratama, D. R. I. M. Setiadi, I. Harkespan, and A. A. Ojugo, "Feature Fusion with Albumentation for Enhancing Monkeypox Detection Using Deep Learning Models," *J. Comput. Theor. Appl.*, vol. 2, no. 3, pp. 427–440, 2025, https://doi.org/10.62411/jcta.12255.

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

[109] A. A. Ojugo and R. E. Yoro, "Predicting Futures Price And Contract Portfolios Using The ARIMA Model: A Case of Nigeria's Bonny Light

and Forcados," *Quant. Econ. Manag. Stud.*, vol. 1, no. 4, pp. 237–248, 2020, https://doi.org/10.35877/454RI.qems139.

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

[111] F. Omoruwou, A. A. Ojugo, and S. E. Ilodigwe, "Strategic Feature Selection for Enhanced Scorch Prediction in Flexible Polyurethane Form Manufacturing," *J. Comput. Theor. Appl.*, vol. 1, no. 3, pp. 346–357, 2024, https://doi.org/10.62411/jcta.9539.

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