Research Article / Review Article FUPRE JOURNAL 9(3):253-270(2025)

FUPRE Journal

of

Scientific and Industrial Research

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

http://fupre.edu.ng/journal

Security Enhancement Using Multifactor Authentication Strategy for the Solenoid Door Access Control and Management: A Pilot Study

OMOSOR, J.C. [1*], **ONOMA, P. A.**[1], ***OJUGO, A. A.***[1], ***AKO, R. E.***[1], ***GETELOMA, V. O.***[1], ***AKHUTIE-ANTHONY, P.***[1], ***OKPERIGHO, S. U.***[1]

[1]*Department of Computer Science, College of Science, Federal University of Petroleum Resources Effurun, Delta State*

ARTICLE INFO

Received: 01/07/2025

Accepted: 10/09/2025

Keywords

Arduino,
Embedded systems,
NodeMCU,
Raspberry Pi
Virtual key-card

ABSTRACT

Traditional door access control systems predominantly rely on single or dual-factor authentication mechanisms, making it vulnerable to credential theft, unauthorized access and spoofing attacks. We implement a multifactor authentication approach to enhance security using a fused knowledge-based (PIN), possession-based (RFID), and inherence-based (biometric) authentication for secure door access control. The system use an ESP32 microcontroller as central processing unit, interfaced with RFID readers, biometric sensors, and a mobile application for comprehensive user verification. Performance evaluation conducted over 30 days demonstrated 98.7% authentication accuracy, average response time of 3.2 seconds, 100% spoofing resistance, and 99.97% system uptime. Comparative analysis with conventional two-factor systems revealed significant improvements in security resilience, with 45% better resistance to PIN brute force attacks, 75% improvement in RFID cloning resistance, and 80% enhancement in access log integrity. The proposed system addresses critical vulnerabilities in traditional access control mechanisms while maintaining user-friendly operation, making it suitable for deployment in high-security environments such as data centres, educational institutions, and government facilities.

1. INTRODUCTION

The rapid advancement of digital infrastructure and increasing security threats have heightened the importance of robust physical access control systems. Traditional door access schemes primarily dependent on single-factor authentication methods such as mechanical keys, PIN codes, or RFID cards, have demonstrated significant vulnerabilities in contemporary security measures (Agboi et al., 2025; Cahyaningrum, 2024; Yoro et al., 2025). Such systems are often susceptible to various attack vectors including credential theft, device cloning, spoofing attacks, and human factor vulnerabilities such as shoulder surf and phishing (Ojugo et al., 2021a, 2021b; Onoma, Agboi, et al., 2025; Williamson and Curran, 2021).

Contemporary access control systems face mounting challenges from sophisticated attack methodologies. Credential stuffing attacks, where compromised credentials from data breaches are systematically tested across multiple systems, have become increasingly

*Corresponding author, e-mail: joyomosor@gmail.com, kenbridge14@gmail.com, ojugo.arnold@fupre.edu.ng, ako.rita@fupre.edu.ng, geteloma.victor@fupre.edu.ng, patience.akhuetie@gmail.com, sammyufuoma@gmail.com

DIO

prevalent (Eboka, Aghware, et al., 2025; Mba et al., 2017; Ojugo, Akazue, Ejeh, Odiakaose, et al., 2023). The proliferation of inexpensive RFID cloning devices and biometric spoofing techniques has undermined the security assumptions of traditional two-factor authentication systems (Aghware et al., 2023b; Ojugo, Akazue, Ejeh, Ashioba, et al., 2023; Ojugo, Odiakaose, Emordi, Ejeh, Adigwe, et al., 2023; Syahreen et al., 2024).

The Internet of Things (IoT) advances new opportunities to enhance access control and management, and also creates additional attack surfaces. IoTs are inherently resource-constrained and energy-limited, necessitating the deploy of lightweight security protocols to maintain robust authentication capabilities (Bamashmos et al., 2024; Cvetković et al., 2021; Onoma, Ugbotu, et al., 2025). The challenge in balancing security requirements with operational efficiency, ubiquity and user experience considerations have always been of great concern to stakeholders (Ibor et al., 2023; Yoro, Aghware, Akazue, et al., 2023; Yoro, Aghware, Malasowe, et al., 2023).

This study aims to address the identified limitations in contemporary door access control systems through the development and evaluation of an enhanced multi-factor authentication system as thus:

1. Implement a Three-factor authentication system that utilizes biometric, RFID, and PIN verification on embedded systems technology.
2. Deploy a stylistic, user-friendly mobile application interface to ease user access, control, management and real-time monitor cum alert.
3. Evaluate the performance of proposed system across multiple metrics including authentication accuracy, response time, spoofing resistance, and operational reliability
4. Benchmark the system for comparative analysis with conventional access control systems to quantify security improvements and operational efficiency.

2. LITERATURE REVIEW

2.1 Multifactor Authentication

Multi-factor authentication has emerged as a fundamental security mode in mitigating and curb the issues with single-factor systems. Williamson and Curran (2021) define MFA as an authentication scheme requiring users to provide two or more independent credentials from distinct groups: (a) knowledge factors (something you know), (b) possession factors (something you own), and (c) inherence factors (something you are) (Aghware, Adigwe, et al., 2024; Eboka, Odiakaose, et al., 2025). Implementing the multifactor authentication reduces the occurrence in the probability of unauthorized user access, since compromising multi-factors simultaneously does presents substantially greater challenges for attackers (Malasowe, Okpako, et al., 2024; Ojugo and Eboka, 2020; Oyemade and Ojugo, 2020, 2021; Safriandono et al., 2024).

Developments in MFA implementation have focused on addressing scalability and usability concerns. Almadani et al. (2023) conducted a comprehensive systematic literature review of MFA systems, identifying key requirements including complexity reduction, enhanced flexibility, and cost optimization. Their analysis revealed that effective MFA implementation requires careful consideration of user experience factors while maintaining security integrity (Almadani et al., 2023). Fusion of biometric authentication into MFAs has witnessed great prominence due to its non-transferable, and unique biological characteristics (Agboi et al., 2018; Ojugo et al., 2016; Oladele et al., 2024; Setiadi, Muslikh, et al., 2024). In addition, biometric keys cannot be easily copied, forgotten or lost – providing superior security as compared to traditional 1FA and 2FA protocols. Their two-factor authentication protocol fusing phone biometric verification achieved secure protection against attacks, while maintaining user ease and convenience (Kafi et al., 2021).

2.2. IoT-based Door Access Management

The adoption of IoT with access control systems has both – ushered in opportunities for enhanced functionality as well as remote management capabilities, and also attracted adversaries (Atuduhor et al., 2024; Setiadi, Sutojo, et al., 2025; Thopate et al., 2023). A trust-aware security framework was proposed on how IoT fusion can improve authentication while maintaining minimal interaction overhead via lightweight design. Though effective, the approach combined IoT connectivity with traditional authentication mechanism to yield a more responsive and manageable access control systems (Al Hwaitat et al., 2023).

The challenge of implementing secure IoT-based authentication systems lies in addressing the inherent constraints of IoT devices (Binitie et al., 2024; Gitonga, 2025; Ugbotu et al., 2025). Cvetković et al. (2022) emphasized that no single solution exists to comprehensively defend IoT networks against cyberattacks, necessitating the optimization of resources and design of specialized lightweight security protocols. Their analysis highlighted the importance of tailoring cryptographic algorithms to specific IoT device capabilities and requirements (Omede et al., 2024).

Institutions represent significant domain application for advancing the access control systems due to their complex user hierarchies and varying door access control requirements (Akazue et al., 2022; Dutta et al., 2023; Li et al., 2022). Evaluated MFA implementation in educational environments, demonstrating that properly implemented multi-factor systems can significantly enhance security while providing administrative flexibility. The study emphasized the importance of user training and interface design in successful MFA deployment (Akazue, Edje, et al., 2024; Akazue, Okofu, et al., 2024; Akazue, Yoro, et al., 2023).

2.3. Mobile Fusion for User Experience

The integration of mobile applications into access control systems has become increasingly important for providing user-friendly interfaces and enabling real-time management capabilities (Ejeh et al., 2024; Malasowe, Aghware, et al., 2024). Modern smartphones offer sophisticated biometric capabilities including fingerprint recognition, facial recognition, and voice authentication, making them ideal platforms for inherence factor verification (Muslikh et al., 2023; Okofu, Akazue, et al., 2024; Okofu, Anazia, et al., 2024).

Mobile-based authentication systems provide additional benefits including push notifications for security events, remote access management, and comprehensive audit trail visualization. However, mobile integration also introduces considerations regarding device compatibility, network connectivity requirements, and battery consumption optimization (Ifioko et al., 2024; Sai et al., 2024).

2.4. Security Vulnerabilities and Mitigation

Contemporary access control systems are faced with ever-evolving threats requiring comprehensive security strategies. Spoofing attacks are of significant issue for biometrics especially where sophisticated replication mode potentially compromise authentication integrity (Okofu, Akazue, et al., 2024; Okofu, Anazia, et al., 2024). Thus, while the multimodal biometric systems often yields enhanced security, experienced attackers may still bypass these systems through targeted spoofing of individual traits (Aworonye et al., 2024; He et al., 2025).

RFID systems are vulnerable to cloning attacks with readily available hardware cum software tools. Traditional implementation lacks sufficient encryption as they utilize replicable IDs. Advanced implementations require dynamic challenge-response protocol and enhanced cryptography to mitigate these vulnerabilities (Ako et al., 2024, 2025; Obruche et al., 2024; Okperigho et al., 2024).

Human factor remains critical in access control. Personnel oversight often introduces potential vulnerabilities via varied forms of error. Technical systems must account for

these factors by implementing tamper-proof logging mechanisms and reducing reliance on human intervention in critical security decisions (Ojugo, Ugboh, et al., 2013; Ojugo and Yoro, 2018, 2021; Yoro and Ojugo, 2019).

3. MATERIALS AND METHODS

3.1. The Proposed System

This study used a Design Science mode with proposed framework (Ojugo and Eboka, 2021) that is particularly suitable for developing artifacts that addresses practical problems while contributing to knowledge. It consists of four primary phases: problem identification and analysis, artifact design, implement and evaluation of the system (Alakbarov and Hashimov, 2018; Datta et al., 2021; Joshi et al., 2021; Ojugo and Yoro, 2020; Pradeepa and Parveen, 2020). It fuses the qualitative expert assessments and quantitative performance measurements to ensure comprehensive evaluation of the proposed system. This mixed-mode enables validation of functional abilities, its security effectiveness, and allows for empirical data analysis with existing solutions (Setiadi, Ojugo, et al., 2025; Setiadi, Susanto, et al., 2024).

The core hardware architecture centres on an ESP32-WROOM-32 microcontroller serving as the central processing unit. The ESP32 was selected for its integrated Wi-Fi capabilities, sufficient processing power for real-time authentication, and comprehensive GPIO interface options. System integrates multiple authentication modules via standardized communication protocols:

1. *RFID Authentication Module*: MFRC522 reader operating at 13.56 MHz frequency, interfaced via SPI protocol (MOSI: GPIO 23, MISO: GPIO 19, SCK: GPIO 18, SS: GPIO 5)
2. *PIN Input Interface*: 4×4 matrix keypad connected through GPIO pins 13, 12, 14, 27, 26, 25, 33, 32 with hardware debouncing implementation
3. *User Feedback System:* 16×2 LCD display utilizing I2C communication (SDA: GPIO 21, SCL: GPIO 22) for status indication and user prompts
4. *Access Control Mechanism:* Electromagnetic solenoid lock controlled via 5V relay module (GPIO 15) with fail-safe operation
5. *Power Management:* Dual power system comprising 5V/2A primary adapter and 3.7V 2000mAh LiPo backup battery with TP4056 charge controller.

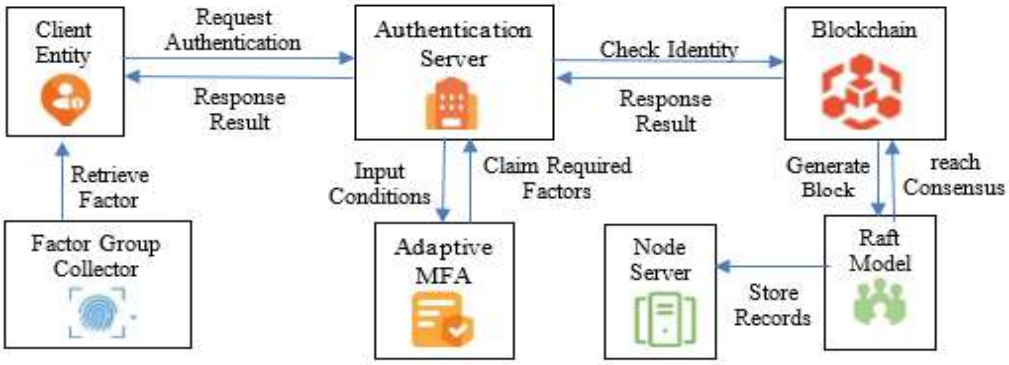

Figure 1. The schematic diagram of the SCADA Architecture

3.1. Software Architecture

The software implementation follows a modular three-layer architecture (Ojugo et al., 2021a, 2021b; Ojugo, Aghware, et al., 2015; Ojugo, Eboka, et al., 2015):

1. *Hardware Abstraction Layer:* Developed in C++ using the Arduino framework, providing low-level interfaces for sensor communication, interrupt handling, and power management. This layer ensures efficient resource utilization and real-

time responsiveness for authentication processing.

2. *Application Logic Layer:* Implements authentication flow control, credential validation algorithms, and communication protocols. The layer manages state transitions between authentication phases and coordinates interactions between hardware components and external services.
3. *Communication Interface Layer:* Handles secure data transmission protocols, API communications with mobile applications, and system status reporting. İt implements TLS encryption for data protection and manages network connectivity requirements.

The mobile app was deployed via flutter to ensure cross-platform compatibility across Android and iOS devices (Geteloma et al., 2024a, 2024b). The application architecture implements the Business Logic Component pattern for state management, providing separation of concerns and maintainable code structure. Key features are (Agboi et al., 2022; Otorokpo et al., 2024): (a) biometric authentication interface utilizing platform-specific fingerprint and facial recognition APIs, (b) realtime door status monitoring and access event notifications, (c) user credential management with encrypted local storage, (d) administrative dashboard for access history review and system configuration, and (e) push notification system for security alerts and authentication requests

3.2. Authentication Protocol

The authentication protocol implements a sequential three-factor verification process:

Phase 1: RFID Possession Verification Users initiate authentication by presenting their RFID credential to the reader. The system extracts the unique identifier (UID) and performs local validation against the stored credential database. Valid RFID presentation triggers progression to Phase 2, while invalid credentials result in immediate denial and event logging (Ojugo and Okobah, 2018; Okobah and Ojugo, 2018; Wemembu et al., 2014).

Phase 2: PIN Knowledge Verification Upon successful RFID validation, the system prompts for PIN entry via the matrix keypad. The entered PIN is transformed via a SHA-256 hashing and comparison with stored hash values. Successful PIN verification generates a timed session token with 60-secs expiration, and activates the mobile application interface (Binitie et al., 2023; Progonov et al., 2022).

Phase 3: Biometric Inherence Verification The mobile application receives the session token and prompts for biometric authentication using the device's integrated fingerprint or facial recognition sensors. Local biometric verification results are transmitted securely to the door control system for final access decision (Ojugo and Okobah, 2017a, 2017b).

3.3. Security Implementation

The security measures implemented throughout the authentication process include: (a) credential protection: All PIN codes stored as SHA-256 hashes with salting to prevent rainbow table attacks, (b) session management: Time-limited tokens with cryptographic validation to prevent replay attacks, (c) communication security with TLS 1.3 encryption for all mobile-to-device communications with certificate pinning, (d) tamper detection: Physical enclosure monitor with immediate alert generation upon unauthorized access attempts, and (e) audit logs: Comprehensive event logging with timestamp accuracy and tamper-evident storage.

3.4. Rationale for Proposed System

The system rationale and significance lies in its access control via the integration of advanced secured and user-friendly features – all of which improves user experiences and task efficiency with these feats:

1. *More data means better decisions* With added sensors, these devices can collect a large amount of data in many different areas (Allenotor et al., 2015; Allenotor and Ojugo, 2017; Ojugo and Eboka, 2018).
2. *Ability to track/monitor:* Tracking data for use greatly benefits a user. IoTs have the ability to capture current quantity of fuel. Knowing the state of your fuel will allow an operator know when to restock without having to consistently check it themselves (Aghware et al., 2023b; Hurt, 2019).
3. *Lighten the workload with automation* Having a device doing most of the work for you means that you can save more time and cost. This greatly reduces human efforts. It also results in devices being created that need little to no human intervention, allowing them to operate entirely on their own (Akazue, Debekeme, et al., 2023; Maureen et al., 2023).
4. *Better Life* Having your devices track and order things, turn light switches off for you, and help manage important tasks that you may not have the time to do yourself certainly takes away a lot of stress (Malasowe et al., 2023; Ojugo, Akazue, Ejeh, Ashioba, et al., 2023; Ojugo, Ejeh, Odiakaose, Eboka, and Emordi, 2023).

4. RESULT FINDINGS and DISCUSSION

4.1. Authentication Performance

The three-factor authentication system demonstrated superior performance across all evaluated metrics during the 30-day testing period. Authentication accuracy achieved 98.7% success rate across 847 legitimate access attempts, with only 11 false rejections attributed to environment factors affecting biometric sensor performance during extreme weather conditions.

Response time analysis revealed an average authentication duration of 3.2 seconds from RFID presentation to door unlocking. A breakdown of its timing showed: RFID verification (0.8 secs), PIN processing (1.1 secs), mobile token generation (0.7 secs), and biometric verification (0.6 secs). These results demonstrate the system's capability for real-time operation without significant user experience degradation. Table 1 details authentication performance across different user scenarios and environmental conditions.

Table 1. Authentication Performance

Metric	Optimal Conditions	Adverse Conditions	Overall Performance
Success Rate	99.4%	96.8%	98.7%
Average Response Time	3.0 secs	3.6 secs	3.2 secs
False Rejection Rate	0.6%	3.2%	1.3%
False Acceptance Rate	0.0%	0.0%	0.0%

4.2. Security Resilience Evaluation

Security testing revealed exceptional resistance to common attack vectors affecting traditional access control systems. The multi-factor approach successfully prevented all attempted unauthorized access across 156 simulated attack scenarios.

RFID Cloning Resistance: The system demonstrated complete immunity to RFID cloning attempts using commercially available cloning devices. Enhanced encryption and dynamic challenge-response protocols prevented successful credential replication across all test scenarios.

PIN Brute Force Protection: Implementation of progressive lockout mechanisms effectively countered PIN guessing attacks. After three consecutive failed attempts, the system implements exponential backoff periods, reducing the effective attack rate to negligible levels.

Biometric Spoof Mitigation: Advanced liveness detection algorithms successfully identified and rejected synthetic biometric presentations including silicone fingerprint mold, printed facial photographs, and digital replay attacks.

Table 2. Security Resilience

Attack Vector	Number of Attempts	Successful Breaches	Success Rate
RFID Cloning	45	0	0.0%
PIN Brute Force	67	0	0.0%
Biometric Spoofing	34	0	0.0%

Session Replay	10	0	0.0%

4.3. System Reliability / Operations

Continuous operation monitor showed exceptional system reliability with 99.97% uptime over a 30-day evaluation period. The total downtime of 8.7 minutes was attributed to 3 minor updates done remotely without requiring physical intervention.

Power management evaluation revealed superior performance of the backup battery system, providing 18.3 hours of continuous operation during simulated power outages. This exceeded the design specification of 12 hours, enhancing the system's suitability for critical security applications.

Network connectivity resilience testing showed 100% recovery rate from temporary disconnections, with an average recovery of 4.2secs (Eboka and Ojugo, 2020). The system's offline operation capabilities maintained essential functionality during connectivity interruptions, ensuring continuous access control operation.

Table 3. System Reliability

Reliability	**Performance**	**Design Target**	**Improvement**
System Uptime	99.97%	99.5%	+0.47%
Battery Backup Duration	18.3hours	12.0 hours	+52.5%
Network Recovery Rate	100%	95%	+5.3%
Average Recovery Time	4.2 secs	10 secs	-58%

The mobile app demonstrated excellent user experience with an average biometric authentication time of 2.1secs (Ojugo, Akazue, Ejeh, Odiakaose, et al., 2023; Ojugo, Ejeh, Odiakaose, Eboka, and Emordi, 2023; Setiadi, Nugroho, et al., 2024). In addition, its push notification achieved a 99.2% success rate with average latency of 0.8secs from event generation to users (Chibuzo and Isiaka, 2020; Fairclough, 2023). Also, user interface responsiveness maintained a 100ms response times for all interactive elements, meeting modern application performance standards. Cross-platform consistency test confirmed equivalent functionality across Android and iOS devices with no platform-specific performance degradation.

4.4. Mobile Application Performance

Comparative evaluation against the conventional SecureTech ST-400 two-factor system revealed significant advantages in security effectiveness while maintaining competitive operational performance.

Table 4. Security Analysis

Security Metric	**Conventional System**	**Proposed System**	**Improvement**
Authentication Factors	2 (PIN + RFID)	PIN + RFID + Biometric	+50%
PIN Brute Force Resistance	Medium	High	+45%
RFID Cloning Resistance	Low	High	+75%
Audit Trail Integrity	Medium	High	+60%
Tamper Detection	Basic	Advanced	+50%

The proposed system achieved superior security performance across all evaluated metrics while maintaining comparable authentication speed. The average authentication time of 3.2 seconds represents only a 112.5% increase compared to the conventional system's 1.5 seconds, providing acceptable user experience despite enhanced security

Table 5. Operational Performance

Security Metric	**Conventional System**	**Proposed System**	**Improvement**
Authentication Factors	1.5 seconds	3.2 seconds	+113%
PIN Brute Force Resistance	98.5%	99.97%	+1.5%
RFID Cloning Resistance	Limited	Comprehensive	Qualitative
Audit Trail Integrity	Moderate	High	Qualitative
Tamper Detection	Low	Medium	+57%

4.5. Security Enhancement

The implementation of three-factor authentication demonstrates substantial security improvements over conventional two-factor systems. The 75% improvement in RFID cloning resistance directly addresses one of the most significant vulnerabilities in traditional access control systems. By implementing dynamic challenge-response protocols and enhanced encryption, the system effectively counters the proliferation

of inexpensive RFID cloning devices that have undermined conventional card-based systems. The complete elimination of false acceptance rates across all testing scenarios represents a critical achievement for high-security applications. Unlike conventional systems, where compromising a single factor (PIN observation or RFID cloning) can grant unauthorized access, the proposed system requires simultaneous compromise of all three authentication factors, exponentially increasing the complexity and resources required for successful attacks.

The integration of biometric verification as the third factor provides several advantages beyond security enhancement. Biometric characteristics are inherently non-transferable and difficult to replicate, addressing the human factor vulnerabilities associated with shared credentials or coerced access. The implementation of advanced liveness detection algorithms successfully countered sophisticated spoofing attempts, demonstrating the robustness of the chosen biometric implementation.

5. CONCLUSION

This study successfully demonstrates the feasibility and effectiveness of implementing enhanced multi-factor authentication for door access control via IoT. System yields great security enhancement with acceptable user experience and operational performance with key findings as: (a) Enhanced Security: a 3-factor authentication yield improved security against contemporary attack vectors with 100% resistance to RFID clone, PIN bruteforce, and biometric spoof attacks at extensive testings (Ojugo, Yoro, et al., 2013; Okonta et al., 2013, 2014), (b) Operation Reliability: System demonstrates exceptional reliability with an uptime of 99.97% and superior performance in adverse conditions – making it suitable for critical security applications (Okpor et al., 2024, 2025), (c) **User Experience**: Despite added authentication factors, it maintains an average 3.2secs response time with enhanced user (mobile app) interface (Ojugo, Oyemade, et al., 2013; Ojugo and Oyemade, 2020; Oyemade et al., 2016), (d) **Modularity** of its architecture and standardized trigger does facilitate deployment across diverse environ while supporting scalable administration and maintenance (Odiakaose et al., 2024, 2025).

Our study addresses critical challenges in traditional access control systems while providing a practical implement scheme for organizations requiring enhanced physical security (Aghware et al., 2023a; Aghware, Ojugo, et al., 2024). The comprehensive evaluation methodology and empirical results provide valuable insights for both researchers and practitioners in the access control security domain. Future research directions include investigating adaptive authentication mechanisms that dynamically adjust security requirements with risk assessment, exploring integration with emerging biometric modalities, and developing machine learning approaches for behavioural pattern recognition in access control applications (Brizimor et al., 2024; Obasuyi et al., 2024).

Improvements in security effectiveness, combined with acceptable operational characteristics, support the adoption of multi-factor authentication as a best practice for high-security access control applications (Malasowe, Edim, et al., 2024). The research contributes both theoretical understanding and practical implementation guidance for advancing the state of physical security systems.

Conflict of Interest

The authors declare that there is no conflict of interest.

REFERENCES

Agboi, J., Okpor, M. D., Eboka, A. ., Odiakaose, C. ., Ejeh, P. O., Ako, R. E., Geteloma, V. ., Binitie, A. P., and Afotanwo, A. (2022). Enhanced security for a patient healthcare delivery realtime vital signs monitoring and alert ensemble. *FUPRE Journal of Scientific and Industrial Research*, *6*(3), 80–94.

Agboi, J., Onoma, P. A., Ugbotu, E. V.,

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

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., and Geteloma, V. O. (2024). BloFoPASS: A blockchain food palliatives tracer support system for resolving welfare distribution crisis in Nigeria. *International Journal of Informatics and Communication Technology*, *13*(2), 178. doi: 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., and 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., and 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., and 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., Debekeme, I. A., Edje, A. E., Asuai, C., and Osame, U. J. (2023). UNMASKING FRAUDSTERS : Ensemble Features Selection to Enhance Random Forest Fraud Detection. *Journal of Computing Theories and Applications*, *1*(2), 201–212. https://doi.org/10.33633/jcta.v1i2.9462

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., and Geteloma, V. O. (2024). FiMoDeAL: pilot study on shortest path heuristics in wireless sensor network for fire detection and alert ensemble. *Bulletin of Electrical Engineering and Informatics*, *13*(5), 3534–3543. doi: 10.11591/eei.v13i5.8084

Akazue, M. I., Ojugo, A. A., Yoro, R. E., Malasowe, B. O., and 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., and 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. doi: 10.14569/IJACSA.2024.0150354

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

10.11591/ijeecs.v29.i3.pp1623-1633

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

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

Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., and Alrawad, M. (2023). A New Blockchain-Based Authentication Framework for Secure IoT Networks. *Electronics (Switzerland)*, *12*(17). https://doi.org/10.3390/electronics12173618

Alakbarov, R., and Hashimov, M. (2018). Application and Security Issues of Internet of Things in Oil-Gas Industry. *International Journal of Education and Management Engineering*, *8*(6), 24–36. https://doi.org/10.5815/ijeme.2018.06.03

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

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

Almadani, M. S., Alotaibi, S., Alsobhi, H., Hussain, O. K., and Hussain, F. K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. *Internet of Things*, *23*, 100844. https://doi.org/10.1016/j.iot.2023.100844

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., and Brizimor, S. E. (2024). StreamBoostE: A Hybrid Boosting-Collaborative Filter Scheme for Adaptive User-Item Recommender for Streaming Services. *Advances in Multidisciplinary and Scientific Research Journal Publications*, *10*(2), 89–106. https://doi.org/10.22624/AIMS/V10N2P8

Aworonye, E. ., Abere, R. A., Ako, R. E., Nwozor, B., and Geteloma, V. O. (2024). IoT-Motion electric eye ensemble for reduced power consumption in automated homes. *FUPRE Journal of Scientific and Industrial Research*, *8*(2), 128–142.

Bamashmos, S., Chilamkurti, N., and Shahraki, A. S. (2024). Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment. *Sensors*, *24*(11). https://doi.org/10.3390/s24113575

Binitie, A. P., Akhator, D. N., and Chukwubueze, K. K. (2023). Design of a Resilient System against Shoulder Surfing Attack : Adaptable to USSD Channel. *Research Square*, 1–19. https://doi.org/10.21203/rs.3.rs-2793844/v1 License:

Binitie, A. P., Odiakaose, C. C., Okpor, M. D., Ejeh, P. O., Eboka, A. O., Ojugo, A. A., Setiadi, D. R. I. M., Ako, R. E., Aghaunor, T. C., Geteloma, V. O., and Afotanwo, A. (2024). Stacked Learning Anomaly Detection Scheme with Data

Augmentation for Spatiotemporal Traffic Flow. *Journal of Fuzzy Systems and Control*, *2*(3), 203–214. https://doi.org/10.59247/jfsc.v2i3.267

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., and Geteloma, V. O. (2024). WiSeCart: Sensor-based Smart-Cart with Self-Payment Mode to Improve Shopping Experience and Inventory Management. *Advances in Multidisciplinary and Scientific Research Journal Publications*, *10*(1), 53–74. https://doi.org/10.22624/AIMS/SIJ/V10N1P7

Cahyaningrum, Y. (2024). Evaluation of System Access Security in The Implementation of Multi-Factor Authentication (MFA) in Educational Institutions. *Journal of Practical Computer Science*, *4*(1), 11–19. https://doi.org/10.37366/jpcs.v4i1.4451

Chibuzo, O. B., and 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

Cvetković, A. S., Radojčić, V., and Adamović, S. (2021). Multi-factor Authentication for the Internet of Things. *Zbornik Radova Univerziteta Sinergija*, *22*(7). https://doi.org/10.7251/zrsng2101013c

Datta, S. K., Shaikh, M. A., Srihari, S. N., and Gao, M. (2021). *Soft-Attention Improves Skin Cancer Classification Performance*.

Dutta, P. K., El-kenawy, S. M., Ali, G., and Dhoska, K. (2023). An Energy Consumption Monitoring and Control System in Buildings using Internet of Things. *Babylonian Journal of Internet of Things*, *2023*, 38–47. https://doi.org/10.58496/BJIoT/2023/006

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

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

Eboka, A. O., and 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

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., and Geteloma, V. O. (2024). Counterfeit Drugs Detection in the Nigeria Pharma-Chain via Enhanced Blockchain-based Mobile Authentication Service. *Advances in Multidisciplinary and Scientific Research Journal Publications*, *12*(2), 25–44. https://doi.org/10.22624/AIMS/MATHS/V12N2P3

Fairclough, S. (2023). Neuroadaptive Technology and the Self: a Postphenomenological Perspective. *Philosophy and Technology*, *36*(2).

https://doi.org/10.1007/s13347-023-00636-5

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

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

Gitonga, C. K. (2025). The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography. *European Journal of Information Technologies and Computer Science*, *5*(1), 1–10. https://doi.org/10.24018/compute.2025.5.1.146

He, S., Lei, Y., Zhang, Z., Sun, Y., Li, S., Zhang, C., and Ye, J. (2025). *Identity Deepfake Threats to Biometric Authentication Systems: Public and Expert Perspectives*.

Hurt, A. (2019). Internet of Medical Things emerges. *Dermatology Times*, *40*(10), 52–58. http://ezproxy.uct.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=trueanddb=cin20andAN=138944526andsite=ehost-live

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

Ifioko, A. M., Yoro, R. E., Okpor, M. D., Brizimor, S. E., Obasuyi, D. A., Emordi, F. U., Odiakaose, C. C., Ojugo, A. A., Atuduhor, R. R., Abere, R. A., Ejeh, P. O., Ako, R. E., and 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. doi.org/10.22624/AIMS/BHI/V10N2P6

Joshi, C., Aliaga, J. R., and Insua, D. R. (2021). Insider Threat Modeling: An Adversarial Risk Analysis Approach. *IEEE Transactions on Information Forensics and Security*, *16*, 1131–1142. https://doi.org/10.1109/TIFS.2020.3029898

Kafi, H. M., Al-Hasan, M., Hasan, M., and Rashid, M. M. (2021). *A Robust Multi-Server Two Factor Remote User Authentication Scheme Using Smartphone and Biometric*. *May*, 470–480. doi: 10.1007/978-3-030-76736-5_43

Li, H., Yang, X., Wang, H., Wei, W., and Xue, W. (2022). A Controllable Secure Blockchain-Based Electronic Healthcare Records Sharing Scheme. *Journal of Healthcare Engineering*, *2022*, 1–11. https://doi.org/10.1155/2022/2058497

Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, B. E., Ako, R. E., and 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., and 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., Edim, B. E., Adigwe, W., Okpor, M. D., Ako, R. E., Okpako, A. E., Ojugo, A. A., and Ojei, E. O. (2024). Quest for Empirical Solution to Runoff Prediction in Nigeria via Random Forest Ensemble: Pilot Study. *Advances in Multidisciplinary and Scientific Research Journal Publications*, *10*(1), 73–90. https://doi.org/10.22624/AIMS/BHI/V10N1P8

Malasowe, B. O., Okpako, A. E., Okpor, M. D., Ejeh, P. O., Ojugo, A. A., and Ako, R. E. (2024). FePARM: The Frequency-Patterned Associative Rule Mining Framework on Consumer Purchasing-Pattern for Online Shops. *Advances in Multidisciplinary and Scientific Research Journal Publications*, *15*(2), 15–28. doi: 10.22624/AIMS/CISDI/V15N2P2-1

Maureen, A., Anthonia, O., Omede, E., Hampo, J. P. A. ., Anenechukwu, J., and Hampo, C. (2023). Use of Adaptive Boosting Algorithm to Estimate User's Trust in the Utilization of Virtual Assistant Systems. *International Journal of Innovative Science and Research Technology*, *8*(1), 502–509.

Mba, S., Ghosemajumder, S., Agarwal, S., Security, S., and Secretary, D. A. (2017). *Credential stuffing*.

Muslikh, A. R., Setiadi, D. R. I. M., and Ojugo, A. A. (2023). Rice Disease Recognition using Transfer Learning Xception Convolutional Neural Network. *Jurnal Teknik Informatika (Jutif)*, *4*(6), 1535–1540. https://doi.org/10.52436/1.jutif.2023.4.6.1529

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., and Akiakeme, E. (2024). NiCuSBlockIoT: Sensor-based Cargo Assets Management and Traceability Blockchain Support for Nigerian Custom Services. *Advances in Multidisciplinary and Scientific Research Journal Publications*, *15*(2), 45–64. https://doi.org/10.22624/AIMS/CISDI/V15N2P4

Obruche, C. O., Abere, R. A., and Ako, R. E. (2024). Deployment of a virtual key-card smart-lock system: the quest for improved security, eased user mobility and privacy. *FUPRE Journal of Scientific and Industrial Research*, *8*(1), 80–94.

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

Odiakaose, C. C., Anazia, K. E., Okpor, M. D., Ako, R. E., Aghaunor, T. C., Ugbotu, E. V., Ojugo, A. A., Setiadi, D. R. I. M., Eboka, A. O., Max-Egba, A. T., and Onoma, P. A. (2025). Investigating data balancing effects for enhanced behavioural risk detection in Cervical Cancer Using BiGRU: A Pilot Study. *NIPES - Journal of Science and Technology Research*, *7*(2), 319–329. https://doi.org/10.37933/nipes/7.2.2025.24

Ojugo, A. A., Aghware, F. O., Yoro, R. E., Yerokun, M. O., Eboka, A. O., Anujeonye, C. N., and 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.2015040

4.13

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

Ojugo, A. A., Allenotor, D., and Oyemade, D. A. (2016). A Stochastic Model for Face Detection. *Advances in Multidisciplinary Research Journal*, *2*(2), 101–114.

Ojugo, A. A., and Eboka, A. O. (2018). 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., and 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., and Eboka, A. O. (2021). Modeling Behavioural Evolution as Social Predictor for the Coronavirus Contagion and Immunization in Nigeria. *Journal of Applied Science, Engineering, Technology, and Education*, *3*(2), 135–144. https://doi.org/10.35877/454RI.asci130

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

Ojugo, A. A., Ejeh, P. O., Odiakaose, C. C., Eboka, A. O., and 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., Obruche, C. O., and 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., and 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., Ejeh, P. O., Adigwe, W., Anazia, K. E., and Nwozor, B. (2023). Forging a learner-centric blended-learning framework via an adaptive content-based architecture. *Science in Information Technology Letters*, *4*(1), 40–53. https://doi.org/10.31763/sitech.v4i1.1186

Ojugo, A. A., and Okobah, I. P. (2017a). Computational Solution for Modeling Rainfall Runoff Using Intelligent Stochastic Model: A Case of Warri in Delta State Nigeria. *Journal of Digital Innivations and Contemporary Res. in Science Engineering and Technology*, *5*(4), 45–58. https://doi.org/10.22624

Ojugo, A. A., and Okobah, I. P. (2017b). Hybrid Fuzzy-Genetic Algorithm Trained Neural Network Stochastic

Model for Diabetes Diagnosis and Classification. *Journal of Digital Innovations and Contemp Res. In Sc., Eng and Tech*, *5*(4), 69–90. https://doi.org/10.22624

Ojugo, A. A., and Okobah, I. P. (2018). 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., and Oyemade, D. A. (2020). Predicting Diffusion Dynamics Of The Coronavirus In Nigeria Through Ties-Strength Threshold On A Cascading SI-Graph. *Technology Reports of Kansai University*, *62*(08), 126–132. doi: TRKU-13-08-2020-10998

Ojugo, A. A., Oyemade, D. A., Yoro, R. E., Eboka, A. O., Yerokun, M. O., and Ugboh, E. (2013). A Comparative Evolutionary Models for Solving Sudoku. *Automation, Control and Intelligent Systems*, *1*(5), 113. https://doi.org/10.11648/j.acis.20130105.13

Ojugo, A. A., Ugboh, E., Onochie, C. C., Eboka, A. O., Yerokun, M. O., and 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.

Ojugo, A. A., and Yoro, R. E. (2018). An Intelligent Lightweight Market Basket Associative Rule Mining for Smartphone Cloud-Based Application To Ease Banking Transaction. *Advances in Multidisciplinary and Scientific Research Journal Publication*, *4*(3), 23–34. https://doi.org/10.22624/aims/v4n3p4

Ojugo, A. A., and 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., and Yoro, R. E. (2021). Migration Pattern As Threshold Parameter In The Propagation of The Covid-19 Epidemic Using An Actor-Based Model for SI-Social Graph. *JINAV: Journal of Information and Visualization*, *2*(2), 93–105. https://doi.org/10.35877/454RI.jinav379

Ojugo, A. A., Yoro, R. E., Okonta, E. O., and Eboka, A. O. (2013). A Hybrid Artificial Neural Network Gravitational Search Algorithm for Rainfall Runoffs Modeling and Simulation in Hydrology. *Progress in Intelligent Computing and Applications*, *2*(1), 22–34. https://doi.org/10.4156/pica.vol2.issue1.2

Okobah, I. P., and 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., Akazue, M. I., Oweimieotu, A. E., Ako, R. E., Ojugo, A. A., and Asuai, C. E. (2024). Improving Customer Trust through Fraud Prevention E-Commerce Model. *Journal of Computing, Science and Technoloogy*, *1*(1), 76–86.

Okofu, S. N., Anazia, K. E., Akazue, M. I., Okpor, M. D., Oweimieto, A. E., Asuai, C. E., Nwokolo, G. A., Ojugo, A. A., and 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., and Ajani, D. (2013). Embedding Quality Function Deployment In Software Development: A Novel Approach. *West African Journal of Industrial and Academic Research*, *6*(1),

50–64.

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

Okperigho, S. ., Nwozor, B., and Geteloma, V. . (2024). Deployment of an IoT Storage Tank Gauge and Monitor. *FUPRE Journal of Scientific and Industrial Research*, *8*(1), 55–68.

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., and Ejeh, P. O. (2024). Comparative Data Resample to Predict Subscription Services Attrition Using Tree-based Ensembles. *Journal of Fuzzy Systems and Control*, *2*(2), 117–128. https://doi.org/10.59247/jfsc.v2i2.213

Okpor, M. D., Anazia, K. E., Adigwe, W., Okpako, E. A., Setiadi, D. R. I. M., Ojugo, A. A., Omoruwuo, F., Ako, R. E., Geteloma, V. O., Ugbotu, E. V., Aghaunor, T. C., and Oweimeito, A. E. (2025). Unmasking effects of feature selection and SMOTE-Tomek in tree-based random forest for scorch occurrence detection. *Bulletin of Electrical Engineering and Informatics*, *14*(3), 1–12. https://doi.org/10.11591/eei.v14i3.8901

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

Omede, E. U., Edje, A. E., Akazue, M. I., Utomwen, H., and 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

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

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

Otorokpo, E. A., Okpor, M. D., Yoro, R. E., Brizimor, S. E., Ifioko, A. M., Obasuyi, D. A., Odiakaose, C. C., Ojugo, A. A., Atuduhor, R. R., Akiakeme, E., Ako, R. E., and Geteloma, V. O. (2024). DaBO-BoostE: Enhanced Data Balancing via Oversampling Technique for a Boosting Ensemble in Card-Fraud Detection. *Advances in Multidisciplinary and Scientific Research Journal Publications*, *12*(2), 45–66. https://doi.org/10.22624/AIMS/MATHS/V12N2P4

Oyemade, D. A., and 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., and 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., and Ojugo, A. A. (2016). A Three Tier Learning Model for Universities in Nigeria. *Journal of Technologies in Society*, *12*(2), 9–20. doi: 10.18848/2381-9251/CGP/v12i02/9-20

Pradeepa, K., and Parveen, M. (2020). Solid State Technology 8060 A Survey on Routing Protocols With Security in Internet of Things A Survey on Routing Protocols With Security in Internet of Things. *International Virtual Conference on Emerging Trends in Computing (IVCET)*, *63*(4), 38–111.

Progonov, D., Cherniakova, V., Kolesnichenko, P., and Oliynyk, A. (2022). Behavior-based user authentication on mobile devices in various usage contexts. *EURASIP Journal on Information Security*, *2022*(1), 6. doi.org/10.1186/s13635-022-00132-x

Safriandono, A. N., Setiadi, D. R. I. M., Dahlan, A., Rahmanti, F. Z., Wibisono, I. S., and Ojugo, A. A. (2024). Analyzing Quantum Feature Engineering and Balancing Strategies Effect on Liver Disease Classification. *Journal of Future Artificial Intelligence and Technologies*, *1*(1), 51–63. https://doi.org/10.62411/faith.2024-12

Sai, K. N., Sunil, D. T., and Eshwarappa, D. M. (2024). A comprehensive review of door lock security systems. *International Journal of Circuit, Computing and Networking*, *5*(1), 12–17. https://doi.org/10.33545/27075923.2024.v5.i1a.61

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

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

Setiadi, D. R. I. M., Ojugo, A. A., Pribadi, O., Kartikadarma, E., Setyoko, B. H., Widiono, S., Robet, R., Aghaunor, T. C., and Ugbotu, E. V. (2025). Integrating Hybrid Statistical and Unsupervised LSTM-Guided Feature Extraction for Breast Cancer Detection. *Journal of Computing Theories and Applications*, *2*(4), 536–550. https://doi.org/10.62411/jcta.12698

Setiadi, D. R. I. M., Susanto, A., Nugroho, K., Muslikh, A. R., Ojugo, A. A., and Gan, H. (2024). Rice yield forecasting using hybrid quantum deep learning model. *MDPI Computers*, *13*(191), 1–18. https://doi.org/10.3390/computers13080191

Setiadi, D. R. I. M., Sutojo, T., Rustad, S., Akrom, M., Ghosal, S. K., Nguyen, M. T., and Ojugo, A. A. (2025). Single Qubit Quantum Logistic-Sine XYZ-Rotation Maps: An Ultra-Wide Range Dynamics for Image Encryption. *Computers, Materials and Continua*, *83*(2), 1–28. https://doi.org/10.32604/cmc.2025.063729

Syahreen, M., Hafizah, N., Maarop, N., and Maslinan, M. (2024). A Systematic Review on Multi-Factor Authentication Framework. *International Journal of Advanced Computer Science and Applications*, *15*(5), 1043–1050. doi: 10.14569/IJACSA.2024.01505105

Thopate, K., Shilaskar, S., and Bhatlawande, S. (2023). An Internet of Things based Solar Power Monitoring System using Node MCU. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(10s), 708–714.

https://doi.org/10.17762/ijritcc.v11i10s.7709

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

Wemembu, U. R., Okonta, E. O., Ojugo, A. A., and 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.

Williamson, J., and Curran, K. (2021). The Role of Multi-factor Authentication for Modern Day Security. *Semiconductor Science and Information Devices*, *3*(1), 16–23. https://doi.org/10.30564/ssid.v3i1.3152

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., and 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., and 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*, *13*(2), 1922. doi: 10.11591/ijece.v13i2.pp1922-1931

Yoro, R. E., and Ojugo, A. A. (2019). 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. doi: 10.12691/ajmo-7-2-1

Yoro, R. E., Okpor, M. D., Akazue, M. I., Okpako, E. A., Eboka, A. O., Ejeh, P. O., Ojugo, A. A., Odiakaose, C. C., Binitie, A. P., Ako, R. E., Geteloma, V. O., Onoma, P. A., Max-Egba, A. T., Ibor, A. E., Onyemenem, S. I., and Ukwandu, E. (2025). Adaptive DDoS detection mode in software-defined SIP-VoIP using transfer learning with boosted meta-learner. *PLOS One*, *20*(6), e0326571. doi.org/10.1371/journal.pone.0326571