FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 16, June, 2026, pp 409 – 419
DOI: https://doi.org/10.33003/fjs-2026-1016-5858

Hybrid RFID-Geolocation Smart Attendance Unit for Enhanced Inclusivity and Efficiency

***[1]Reuben Akpos Abere, [2]Taibat Onome Asunogie, [3]Margaret Dumebi Okpor, [4]Emeke Ugboh, [5]Nelson Asheshemi, [6]Kingsley Theo Igulu, [7]Eferhire Valentin Ugbotu, [8]Tabitha Chukwudi Aghaunor, [1]Samuel Okperigho, [1]Ovie Victor Aherobo, [1]Paul Avwerosuo Onoma, [1]Arnold Adim Ojugo, [4]Adesuwa Inaya and [1]Star Umiyeromesu Niemogha**

[1]Federal University of Petroleum Resources, Effurun, Delta State, Nigeria.
[2]Edo University, Iyamho, Edo State, Nigeria.
[3]Faculty of Computing, Southern Delta University, Ozoro, Delta State, Nigeria.
[4]Federal College of Education (Technical), Asaba, Delta State, Nigeria.
[5]Department of Computer Science, Federal Polytechnic, Orogun, Delta State, Nigeria.
[6]Ignatius Ajuru University of Education, Port-Harcourt, Rivers State, Nigeria.
[7]University of Salford, Manchester, United Kingdom
[8]Robert Morris University, Pittsburgh, Pennsylvania, United States of America.

*Corresponding authors' email: abere.reuben@fupre.edu.ng

Received: 15 Jul. 2026
Accepted: 22 Jul. 2026
Published: 01 Sep. 2026

ABSTRACT
Adoption of Internet of Things (IoTs) in attendance management rebirths pedagogical practices to advance operational differentiation as modern procedural standards in learning citadels. Its utilization yields a transformative platform with smart access points towards inclusivity for teachers and learners while providing the needed reachability cum availability for ubiquitous learning with substantial cost reduction as an expansive tool. With its converged technology, wireless sensor networks and educational pedagogy – it equips administration with intelligent units that ease data exchange. Result shows the proposed artifact yielded a throughput with an average successful authenticated login time of 3.2secs with a zero false acceptance/rejection rate(s) (FAR/FRR) in properly configured sessions. Also, the peak Auth_Server response of 1.6secs for successful login helped to affirms the system's high authentication accuracy, and an exceptional reliability for a 30-days testing period with an uptime of 0.997, and no latency for remote management. System also showed a recovery rate of 1.000 with an average recovery time of 4.2secs. The study has successfully demonstrated a working prototype that integrates knowledge-factor (PIN+OTP), possession-factor (RFID), and inherence-factor (biometrics) – utilized as authentication modes secured via the hashed MFA-records tokenization approach.

Keywords: IoTs, Attendance Management, Smart Campus, Access control, RFiDs, Wireless sensor networks

INTRODUCTION

Rapid deployment and evolution of IoTs, from a conceptual framework to observable reality (Rangga et al., 2026) that propagates cutting-edge effects across various domains, continues to foster its rise in adaptation as the new nexus (Eboka et al., 2025). It advances a set of Internet-enabled units, interconnected within a coverage range to capture various resources and facilitate its exchange using unified protocols. As a convergence nexus, its aims to simplify living across various domains (Kumar et al., 2019), provisioning an ecosystem framework (Fan et al., 2020) with its persuasive expansive nature to facilitate its range of benefits in application frontiers such as smart access control (Aworonye et al., 2024), fire detection (Akazue et al., 2024), medicine (Kakhi et al., 2022), etc. Its rise is adoption has been attributed to its portability, ease of mobility, accessibility, and low-power consumption, etc that continues to render it popular. Algorithmically encoded to facilitate continuous data acquisition, this IoT ecosystem proffers pre-analysis with fault-tolerant abilities that allow it continuous functioning even in harsh conditions (Allam et al., 2024), and so render results to exceed its traditional-counterpart solutions. Its operational efficiency and substantial cost-saving feats have led to its utilization in eco-friendly design to demonstrate tailored solutions with its strict compliance to safety regulations (Omede et al., 2024). Seamlessly fused with traditional solutions, it extends the converged architecture with capabilities that enhance its original objectives – proffering a platform with resources to execute notable applications (Lin et al., 2023; Mishra et al., 2023; Okofu, Akazue, et al., 2024; Okofu, Anazia, et al., 2024).

While attendance management is a basic metric capture in organizations, its management as record-keeping serves a crucial role in productivity enhancement, performance evaluation, administrative decision-making, and access control (Asheshemi et al., 2026; Şentürk & Terazi, 2023a). Traditional attendance monitoring often utilizes signatures and biometrics for roll calls, and this has proven inefficient due to human error, as they are susceptible to mishandling and tampering. Then came RFID-based attendance, which curbed earlier demerits by a coalescence for seamless integration and interoperability of IoT for broader infrastructure coverage. This fusion, as adopted in institutions, employs RFID readers that interact over the cloud infrastructure with software as service (Og & Ying, 2021). Equipped with greater scalability, it yields improved resilience to mitigate network latency (Arachchige et al., 2024) and enhanced modularity to equip the infrastructure with interactive interfaces to monitor notifications, enhanced performance with support for higher

concurrency, and reduced transaction latency (Al-Turjman et al., 2019; Hao & Wang, 2025; Huang et al., 2019).

Attendance monitoring in institutions of learning has since become a fundamental metric and foundational faculty for accountability, improved productivity, resource allocation cum optimization, and enhanced task efficiency (Malasowe et al., 2023, 2024). Effective attendance monitoring provides requisite data that underpin processes and structures that support student enrolment in classes, formative tests for development of learner attitudinal types, compliance monitoring of learner performance evaluation, and strategic planning with pedagogical approaches that leverage both forms of educational technology and technology education (Eboka & Ojugo, 2020). Some demerits are administrative discrepancies, unequal resource utilization, loss of funding, lowered trust, and vulnerable security (Islam et al., 2021). Smart attendance management in an academic environment ensures strict regulatory practices, robust and flexibly reinforced adherence to educational policies, and is highly correlated with learner engagement, learner outcome assimilation, and learner educational achievements. On a teacher's part, attendance monitoring helps to maintain workforce discipline, track productivity, and uphold/upscale regulatory protocols (Ojugo & Oyemade, 2021; Ojugo & Yoro, 2021; Oyemade et al., 2016).

The emergence of radio-frequency identification (RFID) is a transformative shift for users (i.e. teachers and learners) towards a highly scalable, contactless attendance scheme (Ou et al., 2024). RFID automatically identifies, verifies, and tracks coded tags on a device, enabling a seamless capture of attendance and its consequent monitor using a near-feature capability without physical interaction of user devices (Kafetzopoulos et al., 2020). This contactless approach eliminates the risk of disease transmission and accelerates throughput by processing numerous devices (users) in a shorter time. RFIDs as integrated onto cards, wearables, and badges, provide a frictionless, non-contact user experience with potential to greatly reduce fraud, device compromise, and human errors (Sheikhtaheri & Sabermahani, 2022). Unlike biometrics, RFIDs do not use a direct line-of-sight or physical engagement. They are suited for high-traffic scenarios with a disparate user population. Its earliest deployments in attendance aimed to replace manual roll calls and signature sheets (Zhao & Otteson, 2024). It tracks attendance via embedded passive tags on a card, and read-off over an interfaced reader to demonstrate its real-time data capture. The ease of access control in RFID attendance is evident via its effective rapid generation cum reliable management of crucial records. Its utilization in education yields expanded capabilities for automated decision support, predictive maintenance, and smart systems interoperability (Chans & Portuguez Castro, 2021). Whilst integrated with cloud infrastructure, the RFID attendance management offers data-driven access control (Olaniyi et al., 2023) – its major constraints were the limited read range and WSN-latency from its generic database integration (Salunkhe et al., 2025); Making them prone to attacks (Abdul Hannan, 2023; Dwivedi et al., 2019), single-point entry failure (Jin & Omote, 2024), data mishandling (Kizilkaya et al., 2022), etc.

The NextGen employed these deployments as proof-of-concept to resolve its bottlenecks of data centralization and processing speed. Salunkhe et al. (Salunkhe et al., 2025) surveyed its growing landscape and hybridization in attendance systems; And posited that the multi-user concurrency and scalability have become a major concern in its usage. To curb this, Hayati et al. (2023) transitioned from a standalone to a networked platform, utilizing WiFi to transmit attendance records to a nexus central server. They witnessed improved throughput with over 60-learners processed in 60-seconds (Hayati & Nugraha, 2023). However, the extra units birthed integration complexities that degraded system reliability across institutional networks. Also, Hussein et al (2024) resolved this via a middleware approach that aimed to bridge RFIDs with legacy management data systems to enable real-time database synchronization (Hussien et al., 2024). While this was successful, it increased system complexity and birthed new points of failure with fluctuating network quality (Ojugo & Eboka, 2018, 2019; Ojugo & Otakore, 2020). Furthermore, its utilization in high-density scenarios facilitated numerous contactless processing attendees, and eliminated single-point failures – providing a framework with event-driven programs that enabled real-time updates with cloud support for enhanced analytics and crowd-flow tracking. These emergent solutions utilized UHF that degraded overtime due to the rising cross-read rates in the simultaneous detection of multiple tags (Rahman et al., 2025). But, this resulted in data ambiguity, reduced reliability of the system due to signal attenuation in crowded scenarios, and the demand for complex error correction and filtering algorithms to preserve data integrity (Anwar & Uma, 2021).

An in-depth literature review identified several knowledge gaps as persistent across the RFID-IoT ecosystem – which include: (a) privacy concerns about the tracking and monitoring of an individual, (b) threats to security due to unauthorized device access to infrastructure resources, and (c) lack of standardized security protocols for cross-platform data exchanges. To address these challenges, this study advances a hybrid RFID Geolocation Smart Attendance for enhanced organizational efficiency. Its main contributions are summarized as follows:

i. An IoT ecosystem with predictive analysis to generate actionable insights/knowledge to proactively identify low-performing at-risk students
ii. The RFID system was explored to operate on attendance monitoring
iii. A multifactor authentication (MFA) strategy to verify/validate each user across the infrastructure (Brijwani et al., 2024). In addition, this can become the nexus to uncover new approaches to resolve emerging gaps.
iv. A zero-trust model to ensure tamper-proof records management, improved data privacy and safety, standardization, user acceptance, perceived usefulness and interoperability (Dhinakaran, 2023),
v. A geolocation approach that will ensure that users are within a certain defined coverage (Bamashmos et al., 2024),
vi. A mobile application with an interactive dashboard for improved user experience

The remainder of Section 2 presents explored materials and methods with proposed RFID-fused Geolocation-based attendance for smart campus. Section 3 shows experimental testbed configurations and discusses the performance results as obtained. Section 5 discusses key findings, implications, threat validity, limitations, and concludes the research.

MATERIALS AND METHODS

The Proposed Methodology

We explore the CRISP-DM method for the development and deployment of the hybrid attendance system, which leans towards a highly scalable, contactless scheme that effectively

verifies and monitors its coded tags via a contactless strategy to provide seamless capture of attendance as in Figure 1.

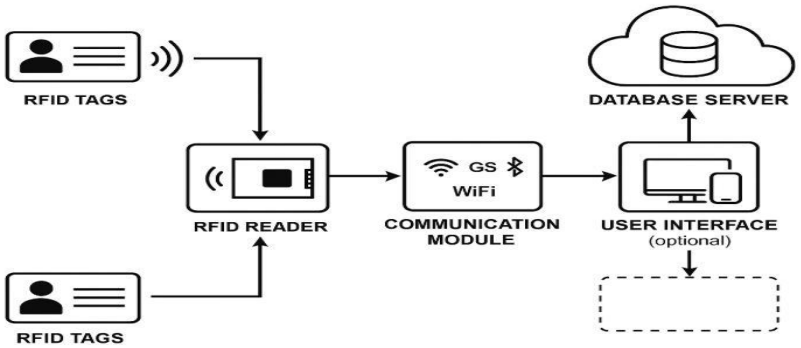

Figure 1: Schematic of the RFID-based attendance framework

The details are as follows:

Phase 1 – User Enrolment

Here, we modeled and built the foundational logic for user (device) registration within the mobile app, and the corresponding backend server. This included the creation of the database schemas, and deployment of the processes to bind a user's (device) account to their specific RFID-based fob card, the consequent creation of user PIN, and device UIDs (Akazue et al., 2024; Ukadike et al., 2023).

Phase 2 – Artifact/Firmware Prototyping

Here, the physical IoT-based attendance device was assembled using the ESP32 microcontroller, RFID-fobs and RFID-reader, biometric sensor, and other components. The firmware will be written and flashed to the device to handle the core authentication logic (card scans, PIN entry, biometric capture) and establish secure communication with the backend (Aworonye et al., 2024; Binitie et al., 2025; Şentürk & Terazi, 2023b).

Phase 3 – Backend Logic for Processing

Here, we explore the cloud backend using Supabase and Postgres software to create the enabling API endpoints and services as required for deployment to process incoming attendance data resources in real-time. Next, we performed the logic for computing/analyzing cumulative attendance percentages, managing of session workflows, and validating device geolocation data (Finlow-bates, 2020; Geteloma et al., 2024; Ojugo, Okpor, et al., 2026).

Phase 4 – Mobile App and Analytics Integration

Here, the focus is on the user-facing mobile application. The UI/UX will be developed for both students and lecturers, including the interactive dashboards and color-coded progress bars. The app will be connected to the backend APIs to fetch and display live attendance data. This phase aims to improve user experience (UX) via the interactive user interface (UI) (Anthony-Akhutie et al., 2025; Omosor et al., 2025).

Phase 5 – Integration, Testing and Deploy

Here, we integrated all the various interacting components, hardware, firmware, backend, and mobile app, into a cohesive ecosystem. Next, rigorous end-to-end testing (adopting the alpha and beta testing modes) to ensure reachability and availability of the system was explored and conducted. Furthermore, this approach ensured that system functionality, security, data privacy and reliability was strictly adhered to. Following successful testing, a pilot deployment will be carried out in a controlled environment to gather user feedback for final refinements (Aghaunor et al., 2025; Brizimor et al., 2024; Obasuyi et al., 2024).

This methodology allows for focused development and testing at each stage, while reducing risk as well as ensuring that the final integrated system meets all the specified requirements. Furthermore, data for the various multifactor authentication approaches for the enhanced attendance management to be captured automatically (and during signup via the mobile app) included: (a) user-provided data includes user name, matriculation number (for students), staff ID (for staff), email address, department, college, level, sex, age, etc., (b) enrolment cum authentication data such as RFID UID, QR-PIN, and biometric (fingerprint), (c) transactional attendance data which are check-in records generated and logged for every successful/failed log-in such as student/staff ID, course or session ID, timestamp with date and time, (d) environmental verification data such as geolocation coordinates captured from the device's GPS/IP-based lookup at check-in, ensuring the user is in the authorized location. Lastly, a secure transmission of records (data) is encrypted in transit using the MQTT over TLS. The token is then stored in a central cloud database in real time, guaranteeing up-to-date and tamper-resistant records.

Technical Requirements and Configuration

The system is designed to interact with users and its environment through a variety of input and output channels across both its hardware and software components.

Table 1: The Hardware Requirements

Components	Specification	Function	Quantity
Microcontroller	ESP32-WROOM-32	Core processing unit	1
RFID Reader/Scanner	MFRC522	RFID card authentication	1
Matrix Keypad	4×4 Membrane	PIN code input	1
LCD Display	SH1106 1.3-inch OLED	User feedback interface	1
Power Supply	5V/2A DC Adapter	Primary power source	1
Backup Battery	3.7V 2000mAh LiPo	Power redundancy	1

Components	Specification	Function	Quantity
Charge Controller	TP4056	Battery management	1
Voltage Regulator	LM2596	Power stabilization	1
PCB	Custom Designed	Component integration	1
Enclosure	IP65 Weatherproof	Environmental protection	1
Jumper Wires	Various	Component connections	1 set
RFID Cards	ISO/IEC 14443A	User credentials	2

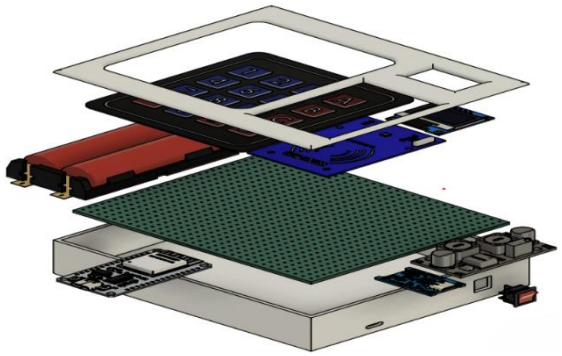

Figure 2. Exploded 3D view of proposed unit

Figure 3. Final rendering of the Proposed Unit

Hardware Design and Configuration

For the hardware design, we have as in Table 1. Figure 2 shows the exploded assembly and 3D model of the resultant artifact with its final rendering as in Figure 3 respectively.

Software Design and Configuration

For the software tools explored, we have as in Table 2 (Govea et al., 2024). Also, the mobile application was developed using React Native, a cross–platform framework that enables deployment to both Android and iOS devices from a single codebase. To simplify development and avoid the complexity of native build configuration, the Expo Managed Workflow was adopted. Expo provides preconfigured native modules, seamless device testing, and over-the-air update support, which accelerated the development process. The following core dependencies (from *package.json*) were used in building the mobile application:

Table 2: The Software Requirements

Components	Function
@supabase orsupabase-js	JavaScript client for Supabase – handles user authentication (login and sign-up), retrieve course lists, register attendance logs, and sync user profile data with the cloud database.
paho-mqtt	Supports MQTT protocol for real-time communication between the mobile app and RFID-IoT unit via HiveMQ MQTT broker. Allows app to subscribe to topics (e.g., *session_status*) and receive alerts such as *"session is active"*
expo-location	Obtains device GPS-coordinates for attendance verification, ensuring the attendance is only recorded when within authorized classroom radius.
react-native-calendar	provides visual displays of course schedules and attendance logs with improved accessible clarity
xlsx	Generates downloadable Excel (.xlsx) reports on lecturers' mobile device with attendance summaries without requiring a laptop or backend report-generation service.

The Experimental Hybrid RFID-IoT

Our hybrid RFID Geolocation smart attendance leans on 3-core components: (a) a custom portable hybrid RFID-IoT to capture attendance, (b) an app to ease user interaction and experience, and (c) robust cloud backend for data processing and storage (Hayati & Nugraha, 2023). From the Figure 3 – the mobile app details to support the core processes for the RFID-IoT attendance management system is as follows (Ibor et al., 2026; Nur et al., 2025):

Step 1 – User Enrolment

New users (i.e. students or lecturers) initiate enrolment by entering their personal details via the mobile application. They then register their RFID card, create a unique 4-digit PIN using device keypad, and complete biometric registration through fingerprint scanning. Additionally, their device ID is captured and bound to their account. All this data is securely stored in the system's database, completing enrolment process (Binitie et al., 2025). Figure 4 shows the sequence diagram for the user enrollment action (Okpor et al., 2025; Okpor et al., 2024; Okpor et al., 2024).

Step 2 – Session Initiation

Lecturers begin a class session by authenticating themselves through multifactor authentication (RFID+PIN+Biometric). Upon successful verification, a list of their assigned courses is displayed. They select the appropriate course to activate the attendance session, allowing student check-in to begin.

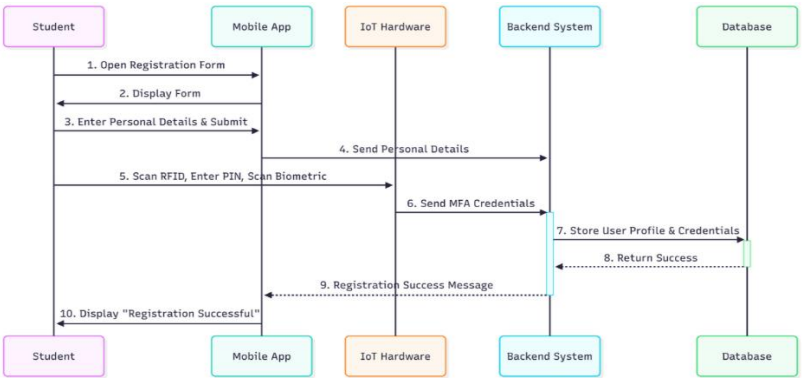

Figure 4: Sequence diagram for student account attendance

Step 3 – Check-In with Geolocation Verification

Students check in for attendance during an active session using the same multifactor authentication approach: RFID card scan, PIN entry, and biometric verification. This ensures that only legitimate students enrolled in the course can mark attendance (Aghaunor et al., 2025). During each check-in, the device captures GPS coordinates through an integrated geolocation module. These coordinates are cross-checked against the predefined location of the lecture hall. If the location is valid (within an approved radius), the check-in proceeds; otherwise, it is denied and flagged for review. The steps are as follows

i. Factor Collection: User initializes the system for authentication by swiping an ID card over the artifact's RFID card reader, connected to ESP32 on an Arduino board. Extracted unique identifier (UID) is sent via the challenge-response mode to verify legitimacy on the authentication server (Auth_Server) as in Figure 2. If UID is valid, artifact accepts, and then encrypts record as a token in its registry – to proceed with next stage; Else, access is immediately denied, and a failed attempt alert is logged for audit trail by the Auth_Server (Ojugo, Okpor, et al., 2026; Oziegbe et al., 2026).

ii. PIN Verify: With RFID successful, the artifact presents a second challenge-response mode that prompts for a user's genuine PIN, which is inputted via the artifact's keypad module, and displayed on the OLED screen as in Figure 3. This PIN is hashed and passed securely as a token to the Auth_Server for template match. If the hashed PIN matches, this confirms the user's identity. And where it fails, access is denied, and the attempt alert is logged on the audit server (Jose et al., 2023; Ojugo et al., 2014; Ojugo, Agboi, et al., 2026).

iii. In-App Token Validation: With a successful PIN, the artifact generates a one-time password (OTP) as reference identifier (RID) and logged internally with the Auth_Server to associate a two-factor (2FA) verified user. This OTP initiate the mobile app for biometric authentication of a user. Once validated, the user can perform remote access management. The token ensures that only verified (RFID-PIN passed) users can proceed to the app-level for biometric verification (Ohwomado et al., 2026; Singh et al., 2022).

iv. Biometric Verification: The artifact exercises biometric verification via the mobile app. This extra layer of security protects against spoofing and shoulder-surf attacks. Consequently, a user device's international mobile equipment identity (IMEI) number is used as a Geo-locator to anchor a user to the coverage server location. And thus, dissuade adversarial exploits, device compromise cum theft vulnerabilities. If the biometric matches, the hashed token, as validated, is then associated with each/all tethered user's session. The correct token as matched verifies ownership or authenticity of the user interacting with the artifact in real-time (Almadani et al., 2023).

v. Logs with Audit Trail: Where the token for biometric is unsuccessful, a time-stamped trail is logged onto the Auth_Server. If access attempt is successful/fails (RFID, PIN, or biometric), all events are transparently recorded to ensure an audit trail for administrative reviews at any time without the risk of records tamper, corruption, mishandle, or deletion. For each successful check-in, the system records the student's ID, course ID, timestamp, and device ID into the PostgreSQL database. These contribute to the cumulative attendance statistics for both students and lecturers.

The Figure 5 shows the sequence diagram for the secure middleware structure that interoperates the artifact and the mobile application for the attendance system.

Step 4– Real-Time Feedback and Progress Tracking

The mobile app provides real-time updates to users. Students can view their attendance percentages with visual indicators, green if ≥ 70%, red if < 70%. Lecturers can access a dashboard of session logs and attendance trends.

Step 5 – Session Termination

At the end of the lecture, the lecturer terminates the session through either the IoT device or mobile app. This sets the session status to inactive and disallows further check-ins, effectively closing the attendance record for that class.

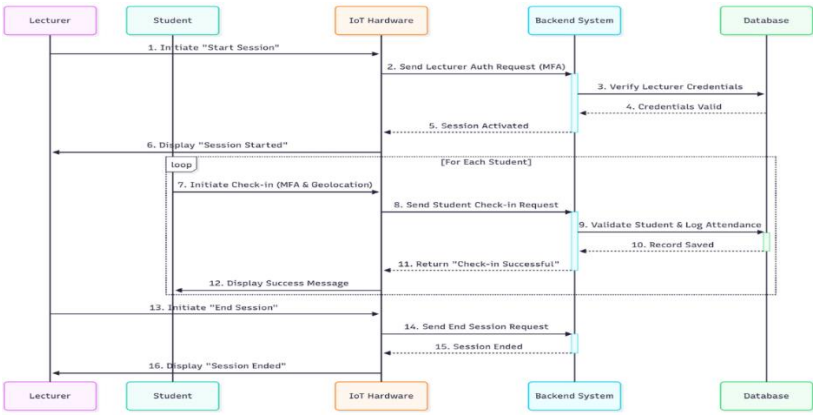

Figure 5: Sequence diagram for student check-ins

RESULTS AND DISCUSSION

Throughput Performance

We evaluate the overall system performance on its authentication accuracy, speed, and consistency in validating legitimate users; while rejecting unauthorized attempts. A total of ten (10) trials were conducted to observe how each authentication layer (i.e. RFID, PIN, token-OTP, and biometric) contributes to performance and how quickly each cycle is completed using the success rate, false rejection rate (FRR), false acceptance rate (FAR), and average response time (Omosor et al., 2025). Figure 6a shows the OTP verification; the and Figure 6b show the sign-up with Auth_Server page; Figure 6c and 6d respectively shows the session for both scheduled and unscheduled class(es).

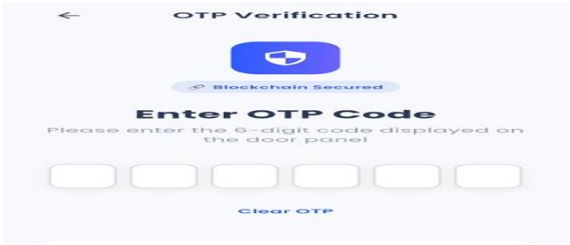

Figure 6a. The OTP verification page

Figure 6b. Sign-Up with Auth_Server authentication

Figure 6c. Session for the scheduled class

Figure 6d. Session for unscheduled class

System successfully validated all legitimate users with correct credentials while blocking unauthorized attempts at every stage. 3-out-of-8 trials were recorded as successful; while, 5-trials were denied due to spoofing, shoulder surf attacks, incorrect inputs, and expired tokens. The average time for successful authenticated login was 3.2secs – to showcase its realtime capability, and confirms the false acceptance rate (FAR) and false rejection rate (FRR) of 0% as properly configured sessions. This affirms the system's high authentication accuracy (Ako et al., 2026), its resistance to user misuse, and its operational efficiency, making it suitable for secure access deployment.

Throughput Performance

We evaluate the overall system performance on its authentication accuracy, speed, and consistency in validating legitimate users; while rejecting unauthorized attempts. A total of ten (10) trials were conducted to observe how each authentication layer (i.e. RFID, PIN, token-OTP, and biometric) contributes to performance and how quickly each cycle is completed using the success rate, false rejection rate (FRR), false acceptance rate (FAR), and average response time. Table 2 shows proposed system successfully validated genuine users with correct credentials while blocking unauthorized attempts at every stage with 3-out-of-8 trials successful; while, 5-trials were denied due to spoofing, shoulder surf attacks, incorrect inputs, and expired tokens. The average time for successful authenticated login was 3.2secs – to yield realtime capability, and confirms the false acceptance rate (FAR) and false rejection rate (FRR) of 0% as properly configured sessions. This affirms the system's high authentication accuracy (Ugbotu et al., 2025), its resistance to user misuse, and its operational efficiency, making it suitable for secure access deployment (Tahir et al., 2025; Yoro et al., 2025).

Table 2: Performance Evaluation

Trial No.	User Type	Input Factors	Auth Result	Time in Secs	Remarks
1	Legitimate User	Valid RFID, PIN, Token, Biometric	Success	3.2	All factors correct
2	Legitimate User	Valid RFID, wrong PIN	Failure	2.1	Blocked at PIN stage
3	Intruder	Cloned RFID	Failure	1.5	RFID not registered
4	Legitimate User	Valid RFID, PIN, expired token	Failure	2.9	Token expired
5	Legitimate User	All correct factors	Success	3.0	Smooth flow
6	Legitimate User	Biometric mismatch	Failure	3.1	Blocked at final stage
7	Legitimate User	All correct	Success	3.4	Slight biometric delay
8	Intruder	Token replay attempt	Failure	2.5	Rejected by OAuth contract

System Reliability

We assess the flexibility, robustness, adaptability cum consistency via a series of reliability tests that measured the system's behavior under repeated, valid access attempts, varying time intervals, and from disparate cum varying user inputs. It determines how reliably the system authenticates without failure, lag, or inconsistency across multi-sessions. Table 4 displays repeated successful authentication attempts over several trials for registered users across multiple sessions without failure (Aghaunor et al., 2026; Binitie et al., 2026).

Table 1: System Integration and Unit Testing Results

Trials	User Type	Authentication Attempted	Time (s)	Result	Remarks
1	Registered User	RFID → PIN → Token → Biometric	3.1	Success	Smooth and consistent
2	Registered User	RFID → PIN → Token → Biometric	3.3	Success	No delay observed
3	Registered User	RFID → PIN → Token (delayed) → Biometric	3.5	Success	Token expiration handled
4	Registered User	RFID → PIN → Token → Biometric	3.0	Success	Fast response
5	Registered User	RFID → PIN → Token → Biometric	3.2	Success	Consistent performance
6	Registered User	RFID → PIN → Token → Biometric (low light)	3.7	Success	Slight biometric delay

Result shows consistent average feedback or response from the server at 3.7seconds. This resultant value indicates a minimal latency and delay as witnessed under varying conditions (Fereidooni et al., 2023), etc. Each trial successfully completed its authentication cycle even with faults to affirm the system's high reliability, stability, and realtime responsiveness as practically deployed in a secure access environment where its dependability and uptime are both quite critical and crucial (Roy et al., 2025). It yielded exceptional reliability for a 30-days test uptime of 0.997 and no errors and latency for remote management capabilities. Furthermore, its extended operation time enhances its suitability for critical security applications and demonstrates its ability to recover from various faults. With a 1.000 recovery rate on an average recovery time of 4.2seconds yields the effectiveness of the proposed system's offline fallback mechanism implemented in ESP32 firmware. This resilience ensures its authentication remained functional even in scenarios with unstable networks (Aherobo et al., 2026).

CONCLUSION

System fuses PIN+RFID+OTP+biometric authentication as managed via an Auth's contracts. This hybrid RFID-IoT attendance supported by the mobile app, has demonstrated its functionality in a realtime setting. With key components that include: (a) the ESP32 interfaced with the RFID readers, biometric sensors, and OLED, (b) Auth_Server with contracts for credential(s) validation, to ensure events/records logs, and decentralized access management, and (c) mobile app for biometric verification and access management. The system was evaluated for authentication accuracy, latency, resistance to spoofing and tampering attacks, and overall operational efficiency. The results demonstrated significant improvements in security, transparency, and auditability compared to traditional centralized access control mechanisms. The study portends a breakthrough in attendance management with distributed access points, particularly in environments where data privacy and unauthorized access pose critical risks. The decentralized structure addresses key limitations such as single-point failure and credential vulnerabilities. The system not only improves access control but also ensures forensic traceability of every authentication attempt, making it a viable solution for institutions with high-security needs.

REFERENCES

Abdul Hannan, S. (2023). a Blockchain Technology and Internet of Things To Secure in Healthcare System. Journal of Advance Research in Computer Science & Engineering (ISSN: 2456-3552), 9(4), 12–19. https://doi.org/10.53555/nncse.v9i4.1641

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

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

Aherobo, O. V., Okpor, M. D., Agboi, J., Ugboh, E., Asheshemi, N., Onoma, P. A., Ojugo, A. A., Ako, R. E., Geteloma, V. O., Max-Egba, A. T., Ugbotu, E. V., Aghaunor, T. C., Okperigho, S., Igulu, K. T., Asunogie, T. O., & Abere, R. A. (2026). GeoSMATS: geolocation smart attendance management unit for secured learner verification and educational inclusivity. Dutse Journal of Pure and Applied Sciences, 12(2d), 410–425. https://doi.org/10.4314/dujopas.v12i2d.33

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

Ako, R. E., Okpako, A. E., Okoro, D. A., Ojie, D. V., Ojugo, A. A., Geteloma, V. O., Niemogha, S. U., Nwankwo, P. C., & Nwankwo, W. (2026). Proactive Fall Risk Prediction in Construction Sites: An Explainable AI Approach. 2026 IEEE ICCOMTECH, 1–6.

Al-Turjman, F., Zahmatkesh, H., & Mostarda, L. (2019). Quantifying uncertainty in internet of medical things and big-data services using intelligence and deep learning. IEEE Access, 7, 115749–115759. https://doi.org/10.1109/ACCESS.2019.2931637

Allam, A. H., Gomaa, I., Zayed, H. H., & Taha, M. (2024). IoT-based eHealth using blockchain technology: a survey. Cluster Computing, 0123456789. https://doi.org/10.1007/s10586-024-04357-y

Almadani, M. S., Alotaibi, S., Alsobhi, H., Hussain, O. K., & 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

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

Anwar, T., & Uma, V. (2021). Comparative study of recommender system approaches and movie recommendation using collaborative filtering. International Journal of System Assurance Engineering and Management, 12(3), 426–436. https://doi.org/10.1007/s13198-021-01087-x

Arachchige, K. G., Branch, P., & But, J. (2024). An Analysis of Blockchain-Based IoT Sensor Network Distributed Denial of Service Attacks. Sensors, 24(10), 3083. https://doi.org/10.3390/s24103083

Asheshemi, N. O., Okpor, M. D., Agboi, J., Ugboh, E., Ugbotu, E. V., Abere, R. A., Odim-Kalu, T. V., Onoma, P. A., Ojugo, A. A., Max-Egba, A. T., Aghaunor, T. C., Igulu, K. T., Asunogie, T. O., Okoh, K. C., Inaya, A., & Niemogha, S. U. (2026). Adaptive Content-Aware Model for Learner-Centric Blended-Learning: A Pilot Study. FUDMA Journal of Sciences, 10(14), 27–37. https://doi.org/10.33003/fjs-2026-1014-5735

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

Binitie, A. P., Onyemenem, S. I., Anujeonye, N. C., Ojugo, A. A., Egbokhare, F. A., & Aghaunor, T. C. (2026). A Graph-Augmented Isolation Forest Using Node2Vec and GraphSAGE for Mobile User Behavior Anomaly Detection. Journal of Computing Theories and Applications, 3(3), 369–383. https://doi.org/10.62411/jcta.15494

Brijwani, G. N., Ajmire, P. E., Jewani, V., Thawani, P. V., Mohammad, D., Junaid, M. A., Khan, T., & Pawar, D. S. (2024). HealthShield: A Blockchain-Based Electronic Health Recording System with Enhanced Security Algorithm for Immutable and Confidential Health Data Management. International Journal of Scientific Research in Science and Technology, 11(3), 794–814. https://doi.org/10.32628/ijsrst24113234

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

Chans, G. M., & Portuguez Castro, M. (2021). Gamification as a Strategy to Increase Motivation and Engagement in Higher Education Chemistry Students. Computers, 10(10), 132. https://doi.org/10.3390/computers10100132

Dhinakaran, E. al. (2023). IoT-Based Environmental Control System for Fish Farms with Sensor Integration and Machine Learning Decision Support. International Journal on Recent and Innovation Trends in Computing and Communication, 11(10), 203–217. https://doi.org/10.17762/ijritcc.v11i10.8482

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors, 19(2), 326. https://doi.org/10.3390/s19020326

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

Eboka, A. O., & 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

Fan, K., Bao, Z., Liu, M., Vasilakos, A. V., & Shi, W. (2020). Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. Future Generation Computer Systems, 110, 665–674. https://doi.org/10.1016/j.future.2019.10.014

Fereidooni, H., König, J., Rieger, P., Chilese, M., Gökbakan, B., Finke, M., Dmitrienko, A., & Sadeghi, A.-R. (2023). AuthentiSense: A Scalable Behavioral Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms.
Finlow-bates, K. (2020). Towards a Decentralized Certificate Authority (Issue April 2019).

Geteloma, V. O., Aghware, F. O., Adigwe, W., Odiakaose, C. C., Ashioba, N. C., Okpor, M. D., Ojugo, A. A., Ejeh, P. O., Ako, R. E., & Ojei, E. O. (2024). 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

Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience. Computers, 13(5), 122. https://doi.org/10.3390/computers13050122

Hao, L., & Wang, X. (2025). Application of EM-transformer hybrid model in real-time detection of directed DDoS attacks on botnet devices. Discover Internet of Things, 5(1). https://doi.org/10.1007/s43926-025-00247-w

Hayati, N., & Nugraha, A. E. (2023). Design and Implementation Proximity Based IoT for Smart Attendance System. Bulletin Pos Dan Telekomunikasi, 21(2), 16–31. https://doi.org/10.17933/bpostel.v21i2.380

Huang, M., Liu, W., Wang, T., Song, H., Li, X., & Liu, A. (2019). A queuing delay utilization scheme for on-path service aggregation in services-oriented computing networks. IEEE Access, 7, 23816–23833. https://doi.org/10.1109/ACCESS.2019.2899402

Hussien, S. H. T., Vinukumar, L., Alexander, C. H. C., & Sivakumar, S. (2024). Smart Campus Attendance and Security Systems : AIP Conference Proceedings, 020153. https://doi.org/10.1063/5.0229386

Ibor, A. E., Ashishie, D. U., Odey, J. A., Ele, B. I., & Ojugo, A. A. (2026). Can We Unchain the Blockchain? A Review of Attacks on Elliptic Curve Cryptography and Countermeasures. Security and Privacy, 9(4). https://doi.org/10.1002/spy2.70234

Islam, N., Farhin, F., Sultana, I., Kaiser, S., Rahman, S., Mahmud, M., Hosen, S., & Cho, G. H. (2021). Towards Machine Learning Based Intrusion Detection in IoT Networks. Computers, Materials and Continua, 69(2), 1801–1821. https://doi.org/10.32604/cmc.2021.018466

Jin, X., & Omote, K. (2024). An efficient blockchain-based authentication scheme with transferability. PLoS ONE, 19(9 September), 1–16. https://doi.org/10.1371/journal.pone.0310094

Jose, J., Rivera, D., Akbar, W., Khan, T. A., & Muhammad, A. (2023). Secure Enrollment Token Delivery Mechanism for Zero Trust Networks Using Secure enrollment token delivery mechanism for Zero Trust networks using blockchain ‡. July. https://doi.org/10.1587/trans.E0.

Kafetzopoulos, D., Stylios, C., & Skalkos, D. (2020). Managing traceability in the meat processing industry: Principles, guidelines and technologies. CEUR Workshop Proceedings, 2761(2010), 302–308.

Kakhi, K., Alizadehsani, R., Kabir, H. M. D., Khosravi, A., Nahavandi, S., & Acharya, U. R. (2022). The internet of medical things and artificial intelligence: trends, challenges, and opportunities. Biocybernetics and Biomedical Engineering, 42(3), 749–771. https://doi.org/10.1016/j.bbe.2022.05.008

Kizilkaya, B., Ever, E., Yatbaz, H. Y., & Yazici, A. (2022). An Effective Forest Fire Detection Framework Using Heterogeneous Wireless Multimedia Sensor Networks. ACM Transactions on Multimedia Computing, Communications, and Applications, 18(2), 1–21. https://doi.org/10.1145/3473037

Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6(1), 111. https://doi.org/10.1186/s40537-019-0268-2

Lin, H. C., Chen, M. J., Lee, C. H., Kung, L. C., & Huang, J. T. (2023). Fall Recognition Based on an IMU Wearable Device and Fall Verification through a Smart Speaker and the IoT. Sensors, 23(12). https://doi.org/10.3390/s23125472

Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., Ako, R. E., & Ojugo, A. A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment. NIPES - 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., Ojugo, A. A., & Ojie, D. V. (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

Mishra, S., Ngangbam, B., Raj, S., & Pradhan, N. R. (2023). CURA: Real Time Artificial Intelligence and IoT based Fall Detection Systems for patients suffering from Dementia. EAI

Endorsed Transactions on Pervasive Health and Technology, 9(1), 1–6. https://doi.org/10.4108/eetpht.9.3967

Nur, M. J., Setiadi, D. R. I. M., Ojugo, A. A., & Nguyen, M. T. (2025). Improving Customer Churn Prediction Using Domain-Driven Feature Engineering, Resampling, and CatBoost with Explainability Extensions. 2025 International Seminar on Application for Technology of Information and Communication (ISemantic), 493–499. https://doi.org/10.1109/ISemantic67418.2025.11291801

Obasuyi, D. A., Yoro, R. E., Okpor, M. D., Ifioko, A. M., Brizimor, S. E., Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ako, R. E., Geteloma, V. O., Abere, R. A., Atuduhor, R.

R., & Akiakeme, E. (2024). NiCuSBlockIoT: Sensor-based Cargo Assets Management and Traceability Blockchain Support for Nigerian Custom Services. Advances in Multidisciplinary & Scientific Research Journal Publications, 15(2), 45–64. https://doi.org/10.22624/aims/cisdi/v15n2p4

Og, S., & Ying, L. (2021). The Internet of Medical Things. ICMLCA 2021 - 2nd International Conference on Machine Learning and Computer Application, 273–276.

Ohwomado, K., Akazue, M. I., & Ojugo, A. A. (2026). A Systematic Ablation-Based Optimisation Protocol for Convolutional Neural Networks in Electronic Banking Fraud Detection. FUDMA Journal of Sciences, 10(12), 79–84. https://doi.org/10.33003/fjs-2026-1012-5285

Ojugo, A. A., Agboi, J., Ugboh, E., Asunogie, T. O., Igulu, K. T., Onoma, P. A., Abere, R. A., Aherobo, O. V., & Okperigho, S. U. (2026). Unmasking High Performance Phishing Detection with Feature Fusion of a Tree-based Transfer Learning Boosted Approach using SMOTE-Tomek Balancing: A Pilot Study. FUPRE Journal of Scientific and Industrial Research, 10(1), 43–58. https://doi.org/10.60787/FJSIR.v10i1.43-58

Ojugo, A. A., Ben Iwhiwhu, E., Kekeje, O. D., Yerokun, M. O., & Iyawa, I. J. (2014). Malware Propagation on Social Time Varying Networks: A Comparative Study of Machine Learning Frameworks. International Journal of Modern Education and Computer Science, 6(8), 25–33. https://doi.org/10.5815/ijmecs.2014.08.04

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

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

Ojugo, A. A., Okpor, M. D., Igulu, K. T., Ugboh, E., Asunogie, T. O., Usiobaifo, R., Onoma, P. A., Aghaunor, T. C., Binitie, A. P., Ezzeh, P. O., Ugbotu, E. V., & Okperigho, S. U. (2026). Pilot Investigation on Security Enhancement for a Door Access Management for a Commercial Manufacturing Environment. Dutse Journal of Pure and Applied Sciences, 12(2a), 145–159. https://doi.org/10.4314/dujopas.v12i2a.14

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

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

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

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

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

Okpor, M. D., Aghware, F. O., Akazue, M. I., Eboka, A. O., Ako, R. E., Ojugo, A. A., Odiakaose, C. C., Binitie, A. P., Geteloma, V. O., & Ejeh, P. O. (2024). Pilot Study on Enhanced Detection of Cues over Malicious Sites Using Data Balancing on the Random Forest Ensemble. Journal of Future Artificial Intelligence and Technologies, 1(2), 109–123. https://doi.org/10.62411/faith.2024-14

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

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

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

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

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

Ou, H.-H., Pan, C.-H., Tseng, Y.-M., & Lin, I.-C. (2024). Decentralized Identity Authentication Mechanism: Integrating FIDO and Blockchain for Enhanced Security. Applied Sciences, 14(9), 3551. https://doi.org/10.3390/app14093551

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

Oziegbe, T. E., Ojugo, A. A., Edje, A. E., & Osezele, A. N. (2026). Convolutional neural network deep learning and digital twin technology for intrusion detection, realtime analytics and digital transformation of the Oil and Gas Industry: a review of literature. FUDMA Journal of Sciences, 10(7), 287–295. https://doi.org/10.33003/fjs-2026-1007-5024

Rahman, K., Hussain, T., Ayaan, S., & Yasmeen, H. (2025). Automated Attendance System Using Opencv With Face And Iris Detection. International Journal of Information Technology and Computer Engineering, 13(2), 285–291. https://doi.org/10.62647/IJITCE2025V13I2sPP285-291

Rangga, D., Zuhdiyanto, O., & Asriningtias, Y. (2026). Real-Time Location Monitoring and Routine Reminders Based on Internet. 5(158), 9–10.

Roy, D. G., Bhattacharjee, A., Das, R., & Das, P. (2025). Trigger Based Smart Attendance Framework with Machine Learning for Predictive Student Performance Analysis. International Journal of Research and Review, 12(May), 321–330.

Salunkhe, A., Pawar, V., Pise, P., Mule, S., Survase, A., Godase, V., & Zambre, S. (2025). A Review on Real-Time RFID-Based Smart Attendance Systems for Efficient Record Management. Advance Research in Analog and Digital Communications, 2(2).

Şentürk, A., & Terazi, S. (2023a). IoT security with blockchain: A review. The European Journal of Research and Development, 3(4), 117–132. https://doi.org/10.56038/ejrnd.v3i4.370

Şentürk, A., & Terazi, S. (2023b). IoT security with blockchain: A review. The European Journal of Research and Development, 3(4), 117–132. https://doi.org/10.56038/ejrnd.v3i4.370

Sheikhtaheri, A., & Sabermahani, F. (2022). Applications and Outcomes of Internet of Things for Patients with Alzheimer's Disease/Dementia: A Scoping Review. BioMed Research International, 2022(1). https://doi.org/10.1155/2022/6274185

Singh, J., Patel, C., & Chaudhary, N. K. (2022). Resilient Risk based Adaptive Authentication and Authorization (RAD-AA) Framework. https://doi.org/10.48550/arXiv.

Tahir, H. T., Aghaunor, T. C., Ugbotu, E. V., Onoma, P. A., Ojugo, A. A., Abere, R. A., Agboi, J., & Aherobo, O. V. (2025). Enhancing Security with Blockchain-Enabled Privacy Preservation for Multi-and-Hybrid Cloud Environment: A Pilot Study. Advances in Multidisciplinary & Scientific Research Journal Publication, 16(4), 25–44. https://doi.org/10.22624/AIMS/CISDI/V16N4P3

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

Ukadike, I. D., Akazue, M. I., Omede, E. U., & Akpoyibo, T. . (2023). Development of an IoT based Air Quality Monitoring System. International Journal of Innovative Technology and Exploring Engineering, 7(4), 53–62. https://doi.org/10.35940/ijitee.J1004.08810S19

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

Zhao, Y., & Otteson, A. (2024). AI-Driven Strategies for Reducing Student Withdrawal -- A Study of EMU Student Stopout.