Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 8 – No. 1, November 2025 – www.caeaccess.org

Design of a Pedagogy-Driven Secure Adaptive Mobile Learning System for Blended Higher Education in Nigeria

Arome Junior Gabriel
Department of Cybersecurity,
School of Computing,
Federal University of Technology,
Akure, Nigeria

Ibrahim Akindeji Makinde
Dept. of Information Systems
School of Computing,
Federal University of Technology,
Akure, Nigeria

Peter Adebayo Aborisade
Institure of Tech-Enhanced
Learning & Dig. Humanities,
Federal Univ. of Technology,
Akure, Nigeria

ABSTRACT
The transition to technology-enhanced learning in Nigerian higher education has been hampered by existing e-learning platforms (such as Moodle) which are often web-centric, lack pedagogical depth, and fail to meet critical data security standards. Empirical data confirms that a vast majority of university students rely exclusively on mobile devices, necessitating the development of an intrinsically mobile-first solution. This paper presents the architectural blueprint and detailed design specification of the Pedagogy-Driven Secure Adaptive Mobile Learning (PD-SAML) system for blended learning environments. The PD-SAML design is realized as a four-layer modular architecture that integrates three core principles: Sociocultural Pedagogy (to mandate peer-interaction and scaffolding), Dynamic Adaptivity (managed by an Adaptive Learning Engine that employs behavioral analytics and user profiling), and a Defense-in-Depth Security Strategy (enforcing Nigerian Data Protection Regulation (NDPR) compliance via secure authentication and AES-based data encryption). By providing a clear technical specification of the system's modules, including its mobile-optimized interface, offline access capabilities, and security protocols, this work contributes a robust, context-aware engineering artifact to address the specific mobile, pedagogical, and security challenges faced by developing world higher institutions.

General Terms
Education, Cybersecurity, Information Systems, Pedagogy, Learning.

Keywords
Global data protection, Blended higher education, Sociocultural pedagogy, Mobile learning.

1. INTRODUCTION
The fast digitization of higher education, enhanced by the impact of events (such as natural disasters and even pandemics) in the world has revealed profound gaps in technology integration, especially in the developing economies. In Nigeria, mobile phone usage as a means of accessing internet, which most students require to undertake their various studies, makes the use of traditional, web-based Learning Management Systems (LMS) ineffective. This deficiency is threefold: insufficient mobile optimization, inability to comply with pedagogical theories that encourage deep learning, and critical failure to implement security-by-design principles, including the adherence to the Nigerian Data Protection Regulation (NDPR).

The current literature and the practical failure of modern LMS imply that a successful mobile learning system must seamlessly incorporate three different pillars, namely a pedagogical model to control the delivery process, an adaptive learning mechanism to customize the delivery experience, and a strong security architecture to protect user information. While prior research in this stream established the conceptual framework and functional requirements derived from stakeholder analysis in the Nigerian context, it did not detail the system's engineering blueprint.

Therefore, this paper transitions from the conceptual to the concrete, presenting the detailed architectural blueprint and technical design specification of the Pedagogy-Driven Secure Adaptive Mobile Learning (PD-SAML) system. The central contribution is the articulation of a four-layer modular architecture that operationalizes the requirements of sociocultural pedagogy, dynamic adaptivity, and defense-in-depth security. Specifically, this work details the components, data flow, and technical specifications of the Adaptive Learning Engine and the NDPR-compliant Security Layer, offering a deployable engineering artifact for blended higher education.

The remainder of the paper is structured as follows: Section 2 summarizes the theoretical foundations that anchor the design. Section 3 presents the PD-SAML System Architecture and its four modular layers. Section 4 details the specification of the Adaptive Learning Engine and the security protocols. Finally, Section 5 concludes the paper and discusses future work.

2. FOUNDATIONAL THEORIES GUIDING THE PD-SAML SYSTEM DESIGN
The architectural design and functional specifications of the Pedagogy-Driven Secure Adaptive Mobile Learning (PD-SAML) system are not arbitrary but are anchored in three distinct theoretical pillars. These theories established the non-negotiable design requirements that the subsequent system architecture must satisfy to be successful, contextually relevant, and academically sound [1].

2.1 The Pedagogical Foundation: Sociocultural Theory
The system's pedagogical model is grounded in Vygotsky's Sociocultural Theory and the concept of the Zone of Proximal Development (ZPD) [2]. This framework shifts the focus from passive content consumption to learning through social interaction, collaboration, and timely scaffolding [3].

The design requirement is that the PD-SAML system must be designed to promote peer-to-peer communication particularly

reflecting the Moore's Learner-Learner Interaction and facilitate scaffolding by enabling lecturers to deliver adaptive support based on real-time feedback [4-5]. The ongoing relevance of Vygotsky's principles is found in modern applications that emphasize collaborative, technology-mediated activities [6-7]. This requirement directly mandates the functionality of the Pedagogical Model Layer to host and manage collaborative activity types.

2.2 The Adaptivity Foundation: Adaptive Learning Theory

Adaptive learning systems are designed to personalize the educational experience by adjusting content, pace, and sequencing based on the learner's characteristics and performance [8]. This is crucial in mobile environments where context can change rapidly and individualized support is paramount.

The design requirement in this case is that the system must incorporate a dedicated, decoupled component capable of dynamic personalization. This requires the creation of an Adaptive Learning Engine (ALE) that will need to create a complex User Model a representation of the individual user, which is critical in adaptation [9]. The ALE has to monitor and profile three main dimensions the cognitive state of the learner (knowledge), the affective state of this learner (engagement/style), and the contextual state of this learner (mobile device and network capabilities). Adaptive e-learning architectures are still being defined and refined by the contemporary literature, utilizing extensively learning analytics and AI-based personalization to inform the user models [1, 7]. This requirement drives the need for the specific Adaptation Logic detailed in Section 4.

2.3 The Security and Trust Foundation: Data Protection Regulation

Any digital platform developed in Nigeria has to be developed in accordance with the Nigerian Data Protection Regulation (NDPR), determining the principles of legal data processing, consent, and user rights [10]. Noncompliance is very dangerous to user trust and institutional integrity. Security, privacy cannot be an add on but should be designed in (Privacy-by-Design). This is a requirement of a Defense-in-Depth security architecture that penetrates through the system layers [11]. The current existing related studies highlight the importance of introducing privacy-protective systems in e-learning platforms because student information is highly sensitive [12]. Some of the main specifications are the application of secure authentication measures, implementation of Role-Based Access Control (RBAC) to make sure that the data is minimized, and the use of strong encryption standards (such as AES) [13] to all sensitive data storage and transmission.

2.4 Gaps in Current Systems

Available systems in Nigeria do not normally combine the principles of security-by-design with pedagogical adaptivity. Global e-learning platforms are use-centric, but they have not considered the sociocultural and infrastructural reality of developing areas. As a result, the learners experience technical, cognitive and security barriers that reduce participation and trust. The proposed PD-SAML will address these gaps with a single model that integrates pedagogical validity, adaptability and data protection.

Figure 1 shows where Adaptive Learning Theory, Security (Data Protection), and Sociocultural pedagogy intersect. These three have become the foundational guidelines to the design of the system that this current study is proposing.

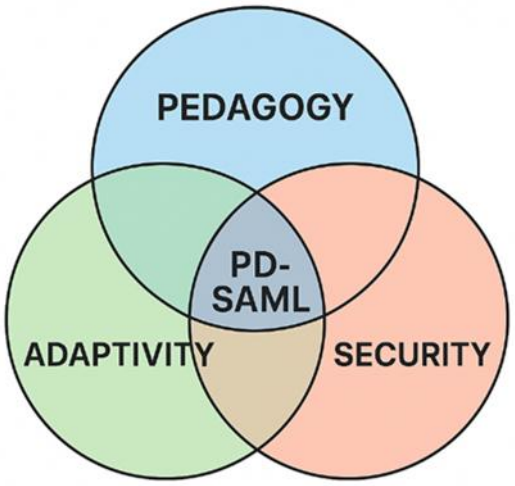

Fig. 1: The Conceptual Framework of the proposed system

3. PD-SAML SYSTEM ARCHITECTURE AND MODULAR LAYERS

Pedagogy-Driven Secure Adaptive Mobile Learning (PD-SAML) system is achieved by using a multilayered architectural pattern. The design provides a separation of concerns, that is, the interface is not bound to the core intelligence, to increase the scalability of the system, maintainability, and modular integration of the three design requirements: pedagogy, adaptivity, and security. The system is based on a normal Client-Server architecture with the mobile application acting as the client that communicates with a server-side environment that contains the core logic and data.

3.1 Overview of the Layered Architecture

The PD-SAML system is based on a powerful, multilayered, architectural pattern which is designed to provide separation of concerns and easy integration. The innovation of the system is the presence of three functional engines (Pedagogical Model, Adaptive Engine, and Security Layer) as depicted in Figure 1a that are interdependent. These functional engines are implemented in the four fundamental architecture layers essential to a scalable clientserver system the Presentation Layer, the Data Exchange/API Layer, the Business/Logic Layer, and the Database Layer. The complete architectural blueprint is formally presented in Figure 2b.

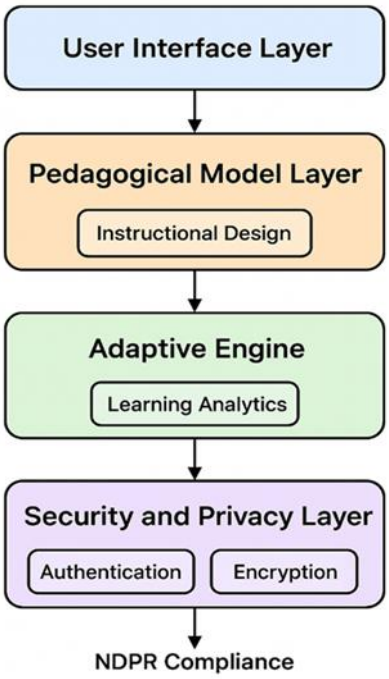

Fig. 2 (a): Functional Decomposition and Core Mandates of the PD-SAML System.

Figure 2(a) highlights the three specialized engines; Pedagogical Model, Adaptive Engine, the Security & Privacy Layer, and their core technical focuses (Instructional Design, Learning Analytics, and NDPR Compliance). On the other hand, Figure 2(b) is the technical blueprint. It shows the four standard architectural layers (Presentation, Data Exchange/API, Business/Logic, Database) and where the functional engines (from Figure 1a) are physically housed. The design adheres to a standard layered pattern, with the Business/Logic Layer serving as the core intelligence hub that explicitly integrates the three functional engines (Pedagogical Model, Adaptive Engine, and Security Engine) to ensure modularity and scalability.

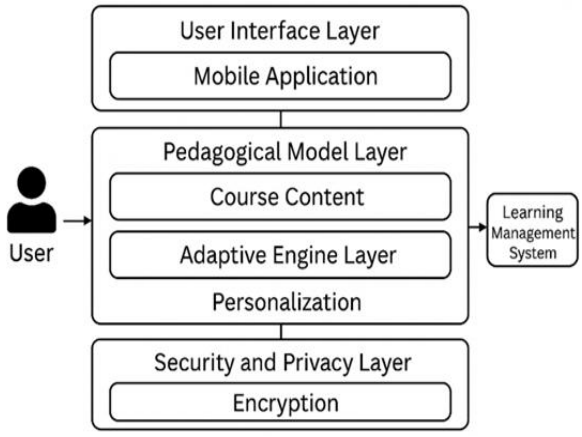

Fig. 2b: Detailed Four-Layer System Architecture of the PD-SAML Platform.

These architectures separate the client interface from the Core Logic to ensure scalability and facilitate the modular integration of the three central design mandates: Sociocultural Pedagogy, Dynamic Adaptivity (via the ALE), and Defence-in-Depth Security.

3.2 Data Persistence Layer

This layer is the foundational repository, responsible for securely managing the heterogeneous data required for course content delivery, user authentication, and adaptive profiling. Its separation from the Core Logic ensures data integrity and supports robust access control policies.

The components of this layer include;

- Course Content Repository (CCR): Stores all learning assets (videos, documents, quizzes) and their descriptive metadata (e.g., topic, difficulty, prerequisite).
- Learner Profile Database: The central component for adaptivity. It stores the dynamic User Model, which includes the cognitive, affective, and contextual states of the learner.
- Security Logs & Policy Database: Stores hashed user credentials, Role-Based Access Control (RBAC) policies, and all system audit and activity logs required for NDPR compliance and security monitoring.

Using a dedicated, structured database for the Learner Profile can provide the real-time data input needed by the Adaptive Learning Engine (ALE) [9].

3.3 Core Logic / System Services Layer

This layer represents the intelligence hub of the PD-SAML design, containing the primary application logic. It implements the system's functional requirements by deploying the three specialised, modular engines shown in Figure 1.

3.3.1. Pedagogical Model Engine

This module is responsible for operationalising the Sociocultural Theory by structuring content into scaffolded learning activities [2-3]. It maps raw content to activity types (Acquisition, Practice, Discussion, etc.) [5], manages activity sequencing, and provides structured environments for both individual practice and peer-to-peer discussion boards to satisfy the interaction requirements [4].

3.3.2. Adaptive Learning Engine (ALE)

The ALE is the decoupled intelligence unit responsible for processing the Learner Model data and generating personalised adaptation instructions in real-time [9]

- **Design Rationale:** This dedicated engine ensures adaptive decisions are based on dynamic, multi-dimensional data, enabling the system to provide context-appropriate and timely scaffolding [7].
- **Interaction Flow:** It receives processed student data from the Data Persistence Layer and sends a Recommendation String (e.g., suggesting a remedial quiz or a collaborative activity) back to the API Layer for delivery to the client.

3.3.3. Security and Privacy Engine

This engine implements the Defence-in-Depth security strategy [11] and enforces compliance with the Nigerian Data Protection Regulation (NDPR) [10].

- Key Services: It manages RBAC enforcement across the API, handles secure multi-factor authentication, and controls the encryption/decryption of sensitive data, preventing unauthorised access and ensuring

data integrity [12].

3.4 API Layer and Communication

The API Layer serves as the robust, standardised interface, managing all secure communication between the mobile client and the Core Logic. The API is designed using RESTful architecture principles, utilising lightweight JSON payloads for data exchange. All communication must be secured end-to-end using TLS 1.2+ encryption for data in transit. The design includes secure endpoints for content retrieval, authentication, and a dedicated Learner Data Submission endpoint for the mobile client to securely push activity logs and profile updates to the server.

3.5 User Interface (UI) Layer / Mobile Client

The client application is the user-facing component, engineered specifically for the constraints of the mobile-first environment in Nigeria.

- Offline Capability: The UI is designed to utilise local, platform-specific secure storage (e.g., Android Keystore) for offline caching of critical content and queueing of activity data.
- Synchronisation Module: A core client component that manages the secure and verifiable pushing of offline activity logs to the server's API when a stable internet connection is re-established, thereby ensuring the continuous accuracy of the Learner Profile.

Section 4 will detail the technical operation of the two core components.

4. SPECIFICATION OF THE ADAPTIVE LEARNING AND SECURITY ENGINES

This section provides the functional and technical specifications for the two key architectural modules, the Adaptive Learning Engine (ALE) and the Security and Privacy Engine, which are essential for realizing the PD-SAML system's core design requirements (as established in Figure 1).

4.1 Specification of the Adaptive Learning Engine (ALE)

The Adaptive Learning Engine (ALE) is the system's decoupled intelligence unit, responsible for processing learner data against defined rules to generate personalized instructional paths and scaffolding support. Its function is based on three interconnected sub-components: the Learner Model (LM), the Adaptation Logic, and the Recommendation Generator. The complete operational flow of the ALE is illustrated in Figure 3.

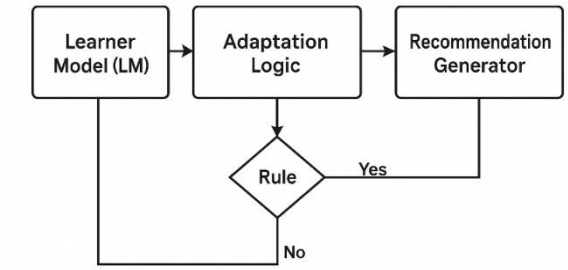

Fig 3: Internal Operational Flow and Components of the Adaptive Learning Engine (ALE).

4.1.1. The Learner Model (LM) Structure

The Learner Model is the central data structure that the ALE relies upon. It is dynamic and updated continuously via the API Layer based on user interactions. It is explicitly structured to track multi-dimensional data points to support context-aware adaptation:

Table 1: The LM Structure

LM Dimension	Key Data Points Tracked	Relevance to Adaptivity
Cognitive State	Knowledge Mastery Score (per topic), Quiz Performance, Time-on-Task, Pre-requisite Completion Status.	Determines content difficulty and sequencing (i.e., when to move to the next topic or suggest remediation).
Affective/Style State	Preferred Activity Type (e.g., collaborative or individual), Self-Reported Confidence, Engagement Score (based on activity rate).	Determines activity type recommendation (e.g., suggesting a collaborative task for low confidence) [7].
Contextual State	Device Type, Network Stability Index, Offline Activity Queue Status, Last Synchronization Timestamp.	Determines the delivery format and ensures the provision of offline-friendly content and tasks [1].

4.1.2. Adaptation Logic and Rule Set

The ALE operates on a **rule-based logic system** that dynamically maps the learner's current state (from the LM) to a recommended action. This rule set operationalizes the concept of scaffolding within the Zone of Proximal Development (ZPD) [2].

- **Logic Implementation:** The Adaptation Logic is implemented as a set of nested *IF-THEN-ELSE* rules designed to prioritize pedagogical scaffolding and mobile context:
  - **Rule A (Remediation):** IF Knowledge Mastery Score (Topic X) < 65% AND Quiz Performance (Topic X) < 50% THEN Recommend remedial content (e.g., video lecture) and trigger a Practice Activity with higher frequency.
  - **Rule B (Peer-to-Peer Scaffolding):** IF Self-Reported Confidence is Low AND Preferred Activity Type = Collaborative THEN Recommend a Discussion/Collaboration Activity on the current topic with a peer who has a Knowledge Mastery Score > 85%.
  - **Rule C (Mobile Context Handling):** IF Network Stability Index is Poor THEN Serve content from

the offline cache (UI Layer) and prioritize low-bandwidth content (e.g., text, light quizzes) over video streaming.

4.2 Specification of the Security and Privacy Engine

The Security and Privacy Engine implement a Defense-in-Depth strategy [11] across the PD-SAML architecture to ensure data confidentiality, integrity, and compliance with the Nigerian Data Protection Regulation (NDPR) [10]. The functional components and data flow for this engine are detailed in Figure 4a and Figure 4b.

4.2.1. Access Control and Authentication Protocols

Access control mechanisms ensure that users only interact with data and functions appropriate for their role, enforcing data minimization.

Table 2: Access Control and Authentication Protocols

Feature	Technical Specification	Rationale and Compliance
Authorization Model	**Role-Based Access Control (RBAC)**	Segregates data access based on user roles (Student, Lecturer, Administrator) to enforce NDPR data minimization principles.
Authentication Protocol	**OAuth 2.0 / OpenID Connect**	Enables secure token-based access and facilitates potential institutional Single Sign-On (SSO) integration.
Credential Storage	**Hashing with Salt (e.g., bcrypt)**	Ensures that all user passwords are non-reversible and never stored in plaintext within the Data Persistence Layer.

4.2.2. Data Confidentiality and Encryption

This engine dictates the mandatory protocols for protecting sensitive data, particularly the Personally Identifiable Information (PII) within the Learner Profile.

- **Data in Transit (NDPR Requirement):** All communication between the mobile client and the API Layer must be encrypted using Transport Layer Security (TLS) version 1.2 or higher. This protocol is enforced at the API Layer [12] to prevent Man-in-the-Middle (MITM) attacks.
- **Data at Rest (NDPR Requirement):** All sensitive data (including academic performance, affective state profiles, and PII) in the Learner Profile Database must be encrypted using Advanced Encryption Standard (AES) 256-bit encryption. This is applied within the Data Persistence Layer, ensuring that if the database is breached, the data remains unintelligible.

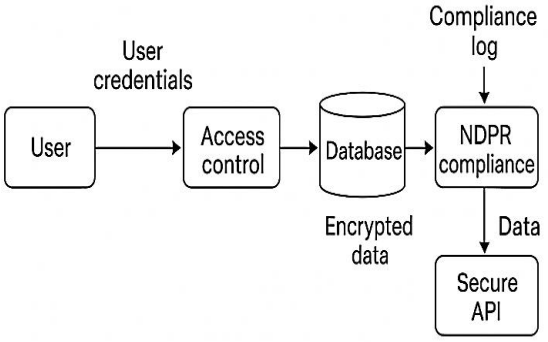

Fig 4a: Components and Functional Roles of the Security and Privacy Engine, illustrating the application of authentication, authorization (RBAC), and encryption techniques

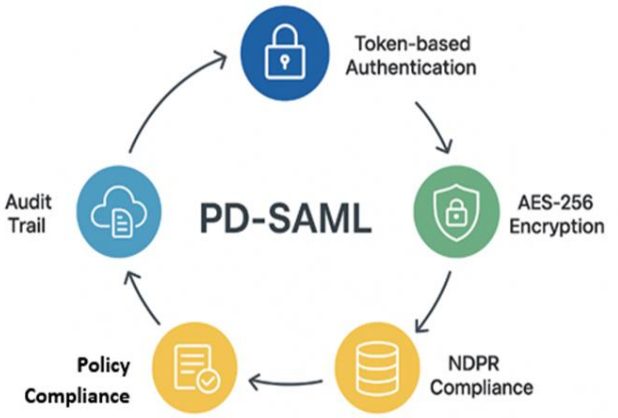

Fig. 4b: Defense-in-Depth Data Flow Diagram, illustrating the mandatory TLS encryption in transit and AES-256 encryption at rest, ensuring NDPR compliance

Figures 4 (a) and 4 (b) has to do with the security and privacy workflow of the PD-SAML System. (a) Linear workflow illustrating the sequential process from authentication to NDPR compliance. (b) Enhanced circular model showing the continuous cycle of secure data flow, encryption, access control, and audit trail.

5. CONCLUSION AND FUTURE WORK

The work presented in this paper successfully concludes the design phase of the Pedagogy-Driven Secure Adaptive Mobile Learning (PD-SAML) system, providing a robust and detailed architectural specification intended for deployment in blended higher education environments in Nigeria. The design process was rigorously driven by three foundational mandates: Sociocultural Pedagogy, Adaptive Learning Theory, and the strict requirements of the Nigerian Data Protection Regulation (NDPR). The primary contribution of this paper is the detailed technical specification of the system artefact, which validates that the proposed architecture

effectively translates theory into a working blueprint. This was achieved through the design of a modular, layered architecture (Figure 2a/2b) that separates concerns, and the in-depth specification of the two core intelligence modules: the Adaptive Learning Engine (ALE) (Figure 3), which details the dynamic Learner Model and Rule Set Logic for personalization, and the Security and Privacy Engine (Figure 4a/4b), which enforces a comprehensive Defense-in-Depth strategy involving Role-Based Access Control (RBAC), mandatory TLS 1.2+ encryption for data in transit, and AES-256 encryption for all sensitive data at rest. By formalising these specifications, the PD-SAML system is positioned to offer a secure, context-aware, and pedagogically sound solution that directly addresses the documented limitations of existing, non-mobile-optimised e-learning platforms.

The completion of this design specification marks the successful conclusion of the first phase of this design science research project. The immediate future work must now transition the project into the realization and validation phases. This includes the Implementation and Development of a working prototype, which will involve translating the architectural blueprint and the algorithmic logic (such as the Adaptation Logic Rule Set) into functional code for the server and the cross-platform mobile application. Following development, the prototype requires Experimental Validation through two critical assessments. First, a Security Assessment must be performed, utilizing penetration testing and audit compliance checks to rigorously verify that the Security and Privacy Engine meets the mandated NDPR confidentiality and integrity protocols. Second, a Usability and Efficacy Study is necessary, utilizing an appropriate experimental design (e.g., A/B testing) with students and lecturers to measure the system's usability, acceptance, and pedagogical efficacy by comparing learning gains and engagement using the PD-SAML system versus traditional mobile access methods. These steps are essential to validate the core hypotheses and confirm the positive impact of this novel design on blended learning outcomes.

6. ACKNOWLEDGMENT

This research was supported by the Tertiary Education Trust Fund (TETFund), Nigeria, under the 2024 Institution-Based Research (IBR) Grant, Federal University of Technology Akure.

7. REFERENCES

[1] Alshammari, M. A. (2020). Adaptivity in mobile learning: A systematic review. *Education and Information Technologies*, *25*(2), 937–963.

[2] Anderson, T., & Garrison, D. R. (1998). Learning in a networked world. In *Distance Learners in Higher Education*. Atwood.

[3] Brusilovsky, P. (2007). The Adaptive Web: Methods and Solutions. In P. Brusilovsky, A. Kobsa, & W. Nejdl (Eds.), *The adaptive web: Methods and solutions* (pp. 3–35). Springer.

[4] Brusilovsky, P., & Millán, A. (2007). User models for adaptive educational systems. In P. Brusilovsky, A. Kobsa, & W. Nejdl (Eds.), *The adaptive web* (pp. 3-35). Springer.

[5] Dillenbourg, P. (1999). What do you mean by collaborative learning? In P. Dillenbourg (Ed.), *Collaborative-learning: Cognitive and computational approaches* (pp. 1-19). Elsevier.

[6] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105.

[7] Laurillard, D. (2007). Pedagogical forms of mobile learning: Framing research questions. In *Learning with Mobile Devices: Research and Development*.

[8] Levy, M., & Stockwell, G. (2008). *CALL dimensions: Options and issues in computer-assisted language learning*. Routledge.

[9] Liu, H., Zeng, Y., Li, Q., Tang, S., Cao, J., & Li, M. (2020). Privacy-preserving e-learning systems: A survey. *IEEE Access*, *8*, 675–693.

[10] Moore, M. (1989). Editorial: Three types of interaction. *American Journal of Distance Education*, *3*(2), 1–6.

[11] National Information Technology Development Agency (NITDA). (2019). *Nigerian Data Protection Regulation (NDPR)*.

[12] Stallings, W. (2020). *Computer security: Principles and practice* (4th ed.). Pearson.

[13] Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Harvard University Press.

[14] Zhang, X., & Cui, Y. (2023). Designing an adaptive learning environment based on learning analytics: A pedagogical framework for personalized education. *Educational Technology & Society*, *26*(2), 78–91.

[15] Zou, Y., Kuek, F., Feng, W., & Cheng, X. (2025). Digital learning in the 21st century: Trends, challenges, and innovations in technology integration. *Frontiers in Education*, *10*, Article 1562391.10.5120/ijca2018916579.