2026 Volume: 02 Issue: 01 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-11

ENHANCING EXAMINATION INTEGRITY: AN OFFLINE-FIRST, QR CODE-BASED VERIFICATION SYSTEM FOR RESOURCE-CONSTRAINED ENVIRONMENTS

Ajaero Grace,[1*]Dimoji Tobias,[2] Anyata Dennis,[3] Chinwuba Chinyere C., [2]Ukwome Tochi P.,[2]

[1]Department of Computer Science, Imo State Polytechnic, Omuma, Imo State, Nigeria.

[2]Department of Computer Science, Federal College of Agriculture, Ishiagu, Ebonyi State Nigeria.

[3]Exams and Records Unit, Federal College of Agriculture, Ishiagu, Ebonyi State Nigeria.

Article Received: 11 December 2025
Article Revised: 31 December 2025
Published on: 19 January 2026

***Corresponding Author: Ajaero Grace**
Department of Computer Science, Imo State Polytechnic, Omuma, Imo State, Nigeria.

DOI: https://doi-doi.org/101555/ijrpa.3870

ABSTRACT:

Ensuring examination integrity in Nigerian higher institutions remains a persistent challenge, particularly in environments with unreliable internet connectivity. While our earlier work (Dimoji et al., 2025) introduced a cost-effective, QR code–based system to combat student impersonation, its reliance on real-time online database queries rendered it vulnerable to network outages, a common constraint in many examination settings. To address this critical limitation, we present an enhanced, offline-first verification system that operates independently of network availability at the point of use. The proposed architecture leverages securely encrypted, pre-downloaded examination rosters containing only essential data: student registration numbers mapped to official photographs. This minimalist approach enables rapid, secure, and reliable verification using standard low-cost mobile devices, without requiring biometric hardware or continuous connectivity. By shifting from dynamic online queries to static, pre-provisioned data packets, our solution retains the original system's speed and affordability while significantly improving robustness, privacy, and operational predictability. This offline-first model, designed specifically for resource-constrained contexts, offers a practical and scalable pathway to safeguard examination integrity where it is needed most.

KEYWORDS: Offline-first verification, QR code authentication, Examination integrity, Impersonation, Resource-constrained environments.

1. INTRODUCTION

The pursuit of examination integrity in Nigerian higher institutions is a continuous challenge. In Dimoji et al. (2025), we proposed a cost-effective, QR code-based system to combat student impersonation. That system relied on real-time database queries, presenting a significant limitation: a mandatory dependency on stable network connectivity, a resource often unreliable in many examination venues across the country. While the online model offered significant advantages over traditional paper-based methods, its network requirement posed a critical operational risk. Examination processes cannot afford delays or failures at the point of student verification. A system failure due to poor connectivity can lead to hall congestion, student anxiety, and a complete breakdown of the verification process, ultimately undermining the credibility of the examination itself.

This paper, therefore, presents a significant enhancement to the original model: an offline-first architecture. We redesigned the system to operate entirely independently of network at the point of use, while retaining all the benefits of cost-effectiveness, speed, and security. This is achieved through the use of secure, encrypted, and pre-downloaded examination rosters, ensuring verification can proceed seamlessly in any environment.

2. LIMITATIONS OF THE ONLINE MODEL AND RELATED WORK

2.1. Recapitulation of the Online QR Code System

In our preceding work (Dimoji et al, 2025) the system's core operation involved a real-time verification loop: a student presents an ID card with a unique, encoded QR code; an invigilator scans this code with a low-cost 2D scanner connected to an internet-enabled device; the system instantly queries a central student database and retrieves the student's official photograph; and finally, the invigilator performs a visual comparison between the live student and the displayed image. The primary strengths of this model were its **cost-effectiveness**, leveraging affordable scanners and existing devices; its **operational speed**, facilitating rapid student admission; and its **enhanced accuracy**, as it relied on the authoritative, up-to-date photo from the central registry rather than a potentially outdated or low-quality image on a physical card. This system was positioned as a viable middle-ground between inefficient paper-based methods and prohibitively expensive biometric solutions.

2.2. The Connectivity Challenge: The Primary Limitation

Despite its advantages, the online model possesses a critical point of failure: a fundamental dependency on stable, high-bandwidth internet connectivity at the examination venue. This requirement presents a significant operational risk within the context of many Nigerian higher institutions. Network connectivity can be unreliable with frequent power and network outages hampered by poor infrastructure, limited broadband penetration (especially in rural areas), high costs, and inconsistent bandwidth being common challenges (Akaeze & Akaeze, 2024; Chibuzor & Kolo, 2024; Whyte, 2025; Bunu et al., 2019; Olanrewaju et al., 2021; Dahunsi & Akinlabi, 2019). The situation can be exacerbated during high-stakes events like examinations, where concentrated, simultaneous access from multiple devices can lead to severe network congestion, slowing response times to a crawl or rendering the network entirely unavailable. A system failure at this critical juncture can lead to exam hall congestion, heightened student anxiety, and a complete breakdown of the verification process, ultimately compromising the integrity and smooth running of the examination it was designed to protect. Therefore, while the online system is theoretically sound, its practical applicability is severely constrained by this infrastructural vulnerability, creating a compelling need for a more resilient, offline-capable solution.

2.3. Survey of Offline-Capable Verification Systems and Inherent Challenges

The challenge of operating in low-connectivity environments has been addressed in other domains, primarily through localized biometrics and encrypted offline databases. However, a survey of these approaches reveals significant technical and security challenges, particularly concerning the trade-offs between security, privacy, and usability under resource constraints (Lien & Vhaduri, 2023). Biometric systems can operate offline by storing encrypted biometric templates (e.g., fingerprints, facial feature vectors) locally. While effective, they face core challenges: they require robust, costly sensors and significant computing power, which are often unavailable in resource-limited environments (Lien & Vhaduri, 2023; Yang et al., 2021). So-called "soft" biometrics offer a more feasible alternative but suffer from lower accuracy and stability. Furthermore, storing biometric templates locally, even in encrypted form, raises profound privacy risks and complex key management issues if the verification device is lost or compromised (Ali et al., 2018; Jeon & Lee, 2021; Bassit et al., 2021). Advanced cryptographic techniques like homomorphic encryption can enable matching on encrypted data but introduce high computational overhead, making them impractical for standard institutional hardware (Farid et al., 2021).

The alternative, using encrypted offline databases, is a well-established concept for

disconnected operation. Yet, deploying a full student database locally can be overly bulky and complex for the specific, narrow task of exam hall verification, complicating both security and key management without a central infrastructure (Jeon & Lee, 2021).

Our proposed system differentiates itself by strategically avoiding these well-documented pitfalls. Instead of relying on complex and costly biometric hardware or bulky databases, we employ a minimalist, data-lite approach. The system utilizes a secure, encrypted, and exam-specific data payload: a "roster" file containing only the essential mapping of student registration numbers to their official photographs. This design directly addresses the core challenges identified in the literature:

- **Resource Constraints**: It eliminates the need for specialized sensors, running efficiently on standard, low-cost smartphones or tablets.
- **Template Security and Privacy**: It avoids the privacy risks of biometric data altogether, storing only a photograph which, while sensitive, does not carry the same immutable, lifelong privacy implications as a fingerprint or iris template.
- **Computational Overhead**: By forgoing complex encrypted matching algorithms, the system performs a simple, fast lookup and decryption, ensuring rapid throughput without computational bottlenecks.
- **Usability versus Security**: It maintains a simple and intuitive verification process for invigilators while providing robust security through standard AES-256 encryption and HMAC integrity checks for the roster file.
- Our model leverages the established QR code infrastructure with a minimal data payload, creating a robust offline solution that is low-cost, practical, and perfectly suited for large institutions with few resources.

3. SYSTEM ARCHITECTURE: THE OFFLINE-FIRST MODEL

The core innovation of this work is the shift from a dynamic, online query to a static, pre-provisioned verification process.

3.1. Core Concept and Workflow

The system operates in two distinct phases:

1. Preparation Phase (Online): Prior to the examination, an authorized exam officer generates a digital roster for the specific course and session. This roster is a securely packaged file containing only the necessary data for verification.
2. Execution Phase (Offline): In the exam hall, invigilators use a dedicated mobile application. This app has pre-loaded the roster file. Scanning a student's QR code

performs an instant lookup against this local file, displaying the result without any network request.

3.2. Architectural Components and Data Flow

3.2.1. System Components:

1. Central Database (Online): The source of truth for student records.
2. Roster Generation Module (Online - Admin Portal): Creates secure, encrypted roster files for distribution.
3. Offline Verification App (Offline - Invigilator's Device): The core application for scanning and verification.
4. Physical ID Card (Offline): Unchanged from the first paper.

3.2.2. Data Flow Diagram:

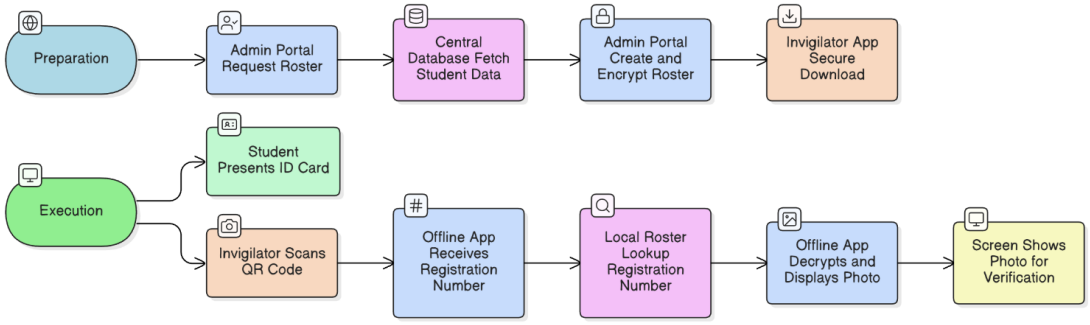

Fig. 1: System Architecture and Data Flow

4. IMPLEMENTATION AND SECURITY ANALYSIS

4.1. Secure Roster Generation

We implement here the roster generation with a focus on security and data minimization using a PHP code example.

PHP Code for Roster Generation:

```
1. <?php
2. // ... (Database connection)
3. $courseCode = "ENG101";
4. $query = "SELECT reg_number, photo_data FROM students WHERE course = '$courseCode'";
5. $result = mysqli_query($conn, $query);
6. $roster = [];
```

```
7. while($row = mysqli_fetch_assoc($result))
8. {
9.         $roster[$row['reg_number']]   =   base64_encode($row['photo_data']);   //Store   as
base64
10. }
11.
12. // Secure the roster: Encrypt and Sign
13. $jsonRoster = json_encode($roster);
14. $encryptionKey = openssl_random_pseudo_bytes(32); //Unique key per roster
15. $iv = openssl_random_pseudo_bytes(16);
16. $encryptedRoster = openssl_encrypt($jsonRoster, 'aes-256-cbc', $encryptionKey, 0, $iv);
17.
18. //Generate the HMAC signature using the same encryption key
19. $hmac = hash_hmac('sha256', $encryptedRoster, $encryptionKey, true);
20. //Package for distribution: [IV (16 bytes)] + [HMAC (32 bytes)] + [Encrypted Data]
21. file_put_contents("rosters/{$courseCode}.enc", $iv . $hmac . $encryptedRoster);
22. //The $encryptionKey is distributed to invigilators via a separate, secure channel.
23. ?>
24.
```

4.2. The Offline Verification Application

The mobile app (conceptualized here) is the cornerstone of the offline operation.

Key Features of the App:

1. Secure Key Import: Invigilators import the encryption key for the roster, separate from the roster file itself.
2. Roster Management: Allows loading of multiple roster files for different exams.
3. Instant Lookup: The core scanning and display functionality.

JavaScript Pseudocode for Verification Logic:

```
1. // On App Startup
2. async function loadRoster(encryptedFile, key) {
3.     let fileData = await readFile(encryptedFile);
4.
5.     // Extract the three parts based on fixed lengths
```

```
6.    // Lengths: IV (16 bytes), HMAC (32 bytes for SHA-256), Data (Remaining)
7.    let iv = fileData.slice(0, 16);
8.    let receivedHmac = fileData.slice(16, 48);
9.    let encryptedData = fileData.slice(48);
10.
11.    // Integrity Check: Recalculate HMAC and compare
12.    // Note: 'key' must be the same 32-byte key used in PHP
13.    let calculatedHmac = await generateHmac(encryptedData, key);
14.    //Using a crypto library like Web Crypto API
15.
16.    if (!isEqual(receivedHmac, calculatedHmac)) {
17.        throw new Error("Security Error: Roster file is corrupted or tampered with!");
18.    }
19.
20.    // Decrypt only after verification is successful
21.    let decryptedJson = await decrypt(encryptedData, key, iv); // AES-256-CBC
22.    this.rosterIsVerified = true;
23.    this.localRoster = JSON.parse(decryptedJson);
24. }
25.
26. // On QR Scan
27. function onScan(registrationNumber) {
28.    // Ensure the roster was successfully verified by HMAC during startup
29.    if (!this.rosterIsVerified) {
30.        displayError("System Error: Roster integrity not verified.");
31.        return;
32.    }
33.
34.    let studentPhotoBase64 = this.localRoster[registrationNumber];
35.
36.    if (studentPhotoBase64) {
37.        //Security: Ensure the string is a valid Data URL before displaying
38.        const safeDataUrl = `${studentPhotoBase64}`;
```

```
39.
40.         displayPhoto(safeDataUrl);
41.         logVerification(registrationNumber, "VERIFIED", timestamp());
42.     } else {
43.         displayError("Student not in roster.");
44.         logVerification(registrationNumber, "NOT_FOUND", timestamp());
45.     }
46. }
47.
```

4.3. Security Analysis

- **Data Minimization:** The roster contains only the data needed for the specific exam.
- **Confidentiality:** The roster file is encrypted with a strong algorithm (AES-256). Without the key, it is useless.
- **Integrity:** The roster file includes includes an integrity checksum (HMAC) generated with the secret key. The application verifies this signature during startup to ensure the file has not been altered; if the file and signature do not match, the system rejects the data before decryption.
- **Access Control:** The roster and key are distributed only to authorized invigilators.

5. COMPARATIVE ANALYSIS AND DISCUSSION

5.1. Advantages over the Online Model

- **Absolute Reliability:** Functions in zero-network environments.
- **Predictable Performance:** Lookup speed is constant and instantaneous, unaffected by network latency.
- **Enhanced Privacy:** Student data does not traverse the network during the exam, reducing exposure.
- **Reduced Network Load:** Eliminates bandwidth consumption from hundreds of devices querying a central server simultaneously.

5.2. Trade-offs and Mitigations

Trade-off: Administrative Overhead. Requires a pre-exam preparation step.

Mitigation: Automate the roster distribution process. The admin portal can push rosters to registered invigilator apps a day before the exam when devices are online.

Trade-off: Static Data. The roster is a snapshot in time.

Mitigation: Implement a cutoff time for roster generation (e.g., 2 hours before the exam). Legitimate late registrations can be handled via a separate, managed exception process.

Trade-off: Device Security. The invigilator's device now holds sensitive data.

Mitigation: The app can require a PIN. Rosters and keys can be set to auto-expire and delete 24 hours after the exam.

6. CONCLUSION AND FUTURE WORK

This paper has successfully addressed the primary limitation of our previously proposed online verification system by introducing a robust, offline-first architecture. The enhanced system maintains the core benefits of being quick and cost-effective while now offering unwavering reliability in the face of uncertain network conditions, making it profoundly suitable for the Nigerian context and similar resource-constrained environments. The model of using secure, pre-provisioned data packets for offline operation has broader applications beyond exam verification, such as class attendance, library book checkouts, and access control. Future work will involve the development of a production-ready mobile application, a formal usability study with invigilators, and the exploration of using digital signatures for end-to-end non-repudiation of the verification logs generated by the offline app.

REFERENCES

1. Adelakun, N., & Olanipekun, B. (2020). Outage analysis and system disturbances on 330 kV and 132 kV transmission system in Nigeria. *European Journal of Engineering Research and Science*, *5*(1). https://doi.org/10.24018/ejers.2020.5.1.1722
2. Akaeze, C., & Akaeze, N. (2024). Exploring the challenges of online learning in Nigerian higher education. *Frontiers of Contemporary Education*, *5*(2). https://doi.org/10.22158/fce.v5n2p1
3. Ali, Z., Hossain, M., Ghulam, M., Ullah, I., Abachi, H., & Alamri, A. (2018). Edge-centric multimodal authentication system using encrypted biometric templates. *Future Generation Computer Systems*, *85*, 76-87. https://doi.org/10.1016/j.future.2018.02.040
4. Bassit, A., Hahn, F., Peeters, J., Kevenaar, T., Veldhuis, R., & Peter, A. (2021). Fast and accurate likelihood ratio-based biometric verification secure

AGAINST MALICIOUS ADVERSARIES. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 16*, 5045-5060. HTTPS://DOI.ORG/10.1109/TIFS.2021.3122823

5. BUNU, S., MUHAMMAD, M., & ADAMU, H. (2019). REVIEW AND ANALYSIS ON TELECOMMUNICATION NETWORKS INFRASTRUCTURE IN THE NORTHWEST PROVINCE OF NIGERIA FOR OPTIMISATION: PROBLEMS AND SOLUTIONS. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & ENGINEERING SURVEY, 10*(1). HTTPS://DOI.ORG/10.5121/IJCSES.2019.10101
6. CHIBUZOR, O., & KOLO, S. (2024). STRENGTHENING NIGERIAN INSTITUTIONS OF HIGHER LEARNING THROUGH EFFECTIVE INTERNET SERVICE DELIVERY: A STUDY OF AHMADU BELLO UNIVERSITY ZARIA KADUNA. *FUGUS JOURNAL OF PUBLIC ADMINISTRATION AND MANAGEMENT, 3*(2). HTTPS://DOI.ORG/10.36349/FUJPAM.2024.V3I02.001
7. DAHUNSI, F., & AKINLABI, A. (2019). MEASURING MOBILE BROADBAND PERFORMANCE IN NIGERIA: 2G AND 3G. *NIGERIAN JOURNAL OF TECHNOLOGY, 38*(2). HTTPS://DOI.ORG/10.4314/NJT.V38I2.19
8. DIMOJI, T., AJAERO, G., ANYATA, D., CHINWUBA, C. C., & UKWOME, T. P. (2025). IMPLEMENTATION OF A QUICK AND COST-EFFECTIVE QR CODE-BASED SYSTEM FOR CURBING STUDENT IMPERSONATION IN NIGERIAN HIGHER INSTITUTION EXAMINATIONS. *INTERNATIONAL JOURNAL OF RESEARCH PUBLICATION AND REVIEWS, 6*(12), 8469-8475.
9. FARID, F., ELKHODR, M., SABRINA, F., AHAMED, F., & GIDE, E. (2021). A SMART BIOMETRIC IDENTITY MANAGEMENT FRAMEWORK FOR PERSONALISED IOT AND CLOUD COMPUTING-BASED HEALTHCARE SERVICES. *SENSORS (BASEL, SWITZERLAND), 21*(2). HTTPS://DOI.ORG/10.3390/S21020552
10. IMOIZE, A., UDEJI, F., ISABONA, J., & LEE, C. (2023). OPTIMIZING THE QUALITY OF SERVICE OF MOBILE BROADBAND NETWORKS FOR A DENSE URBAN ENVIRONMENT. *FUTURE INTERNET, 15*(5), 181. HTTPS://DOI.ORG/10.3390/FI15050181
11. JEON, S., & LEE, M. (2021). ACCELERATION OF INNER-PAIRING PRODUCT OPERATION FOR SECURE BIOMETRIC VERIFICATION †. *SENSORS (BASEL, SWITZERLAND), 21*(8). HTTPS://DOI.ORG/10.3390/S21082859
12. LIEN, C., & VHADURI, S. (2023). CHALLENGES AND OPPORTUNITIES OF BIOMETRIC USER AUTHENTICATION IN THE AGE OF IOT: A SURVEY. *ACM COMPUTING SURVEYS, 56*(3), 1-37. HTTPS://DOI.ORG/10.1145/3603705

13. Okeke, R., Ibokette, A., Ijiga, O., Anebi, E., Ebiega, G., & Olumubo, O. (2024). The reliability assessment of power transformers. *Engineering Science & Technology Journal, 5*(4). https://doi.org/10.51594/estj.v5i4.981
14. Olanrewaju, G., Adebayo, S., Omotosho, A., & Olajide, C. (2021). Left behind? The effects of digital gaps on e-learning in rural secondary schools and remote communities across Nigeria during the COVID19 pandemic. *International Journal of Educational Research Open*, *2*, 100092. https://doi.org/10.1016/j.ijedro.2021.100092
15. Olasunkanmi, O., Apena, W., Barron, A., White, A., & Todeschini, G. (2022). Impact of a HVDC link on the reliability of the bulk Nigerian transmission network. *Energies*, *15*(24). https://doi.org/10.3390/en15249631
16. Whyte, D. (2025). Telecommunication challenges and the path to integrating telemedicine in Nigeria's healthcare system. *International Journal of Research and Innovation in Social Science*, *9*(1). https://doi.org/10.47772/ijriss.2025.9010041
17. Yang, W., Wang, S., Sahri, N., Karie, N., Ahmed, M., & Valli, C. (2021). Biometrics for Internet-of-Things security: A review. *Sensors (Basel, Switzerland)*, *21*(18). https://doi.org/10.3390/s21186163