# Biometric Control in Nigeria: Applications, Challenges and Implications for Management Information Systems

**Oluwadare Victor O; Bisong, Nancy Owan; Anaele Chidera Precious; Prof. Bassey E. Bassey**
Department of Accounting
University of Calabar

https://doi.org/10.56201/jafm.vol.12.no11.2026.pg286.296

***Abstract***
*This study critically examines biometric control in Nigeria as a component of management information systems (MIS), identity governance and organisational internal control. Drawing on established biometric systems literature and official Nigerian institutional documentation, it distinguishes identification from verification and reviews fingerprint, facial, iris, retinal and behavioural methods. Particular attention is paid to the Bank Verification Number (BVN), voter accreditation, national identity management, and the use of facial and fingerprint verification to reduce payroll irregularities and monitor attendance. The analysis shows that biometrics can strengthen identity assurance, but cannot independently establish employment legitimacy, actual hours worked or the absence of fraud. Successful implementation requires reliable enrolment, exception procedures, human oversight, independent payroll reconciliation, secure system integration and compliance with the Nigeria Data Protection Act 2023. The paper recommends risk-based deployment, accessible alternatives, privacy-by-design, regular audit and performance evaluation. It is a desk-based conceptual review; it does not claim primary fieldwork or quantified Nigerian impact estimates.*

***Keywords:*** *biometric control; management information systems; Nigeria; payroll; ghost workers; identity verification; data protection.*

## Introduction

Passwords, identity cards and personal identification numbers may be lost, shared or compromised. Biometric systems provide an additional method of verifying an identity claim, but their effectiveness depends on enrolment quality, matching performance and controls over the surrounding information system (Jain et al., 2008; Wayman et al., 2005). In Nigeria, documented institutional applications include the Bank Verification Number (BVN) framework in banking and the Bimodal Voter Accreditation System (BVAS) in elections. Other uses in workplaces, schools, healthcare and access management are discussed as potential or organisation-specific applications; this paper does not claim that their national adoption rates have been established (Central Bank of Nigeria, 2021; Independent National Electoral Commission, 2024). Biometric control is a means of testing identity claims through measurable physiological or behavioural characteristics. A biometric match is not absolute proof of identity: it is a probabilistic comparison of a newly captured sample against enrolled reference data (Jain

et al., 2008; Wayman et al., 2005). In a management information system (MIS), the identity decision must connect to authorised user roles, transaction records, exception reports and management oversight. The principal question is not simply whether a scanner recognises a person but whether the whole process improves accountability without excluding legitimate users. Identity impersonation, weak personnel records and unauthorised access create risks for organisational accountability. Conventional credentials may be shared or compromised, while biometric controls introduce additional risks of false rejection, spoofing, inappropriate enrolment and sensitive-data exposure (Jain et al., 2008; Wayman et al., 2005). The Nigerian BVN and BVAS initiatives demonstrate policy interest in stronger identity assurance, but programme documentation alone cannot establish the extent to which fraud or impersonation has been reduced (Central Bank of Nigeria, 2021; Independent National Electoral Commission, 2024). Where organisations maintain disconnected identity and personnel records, reconciliation may be difficult. This is an organisational control risk rather than evidence that all Nigerian identity databases are inaccurate. Implementation may be constrained by electricity, connectivity, costs, privacy and operational capability. These are plausible risks to be assessed at each deployment site; their nationwide prevalence is not quantified in this narrative review.

**Concept and Operating Principles**

Biometric control refers to the use of unique biological or behavioral characteristics of individuals to monitor, identify, verify, or control access to systems, devices, locations, or information. Biometric verification compares a sample with one claimed identity (one-to-one); identification searches for a matching identity among multiple records (one-to-many). These are different tasks with different error and privacy implications (Jain et al., 2008). A typical process involves identity proofing, enrolment, sample quality assessment, feature extraction, template creation, storage, subsequent sample capture, matching and a decision threshold. False matches, false non-matches, failure to acquire and failure to enrol are distinct measures of system performance. A biometric template is derived from biological or behavioural data. Although it is not necessarily the original image, it remains sensitive because compromise can have long-lasting consequences. Systems therefore require encryption, restricted access, monitoring, retention policies and breach-response plans.

**Physiological Biometrics**

Physical biometric control, also known as physiological biometric control, is a method of identifying and verifying individuals using their unique physical or biological characteristics. These characteristics are naturally occurring features of the human body and are generally permanent and difficult to duplicate. Physical biometric control is widely used because physical traits are unique to each person, making identification more accurate and secure than traditional methods such as passwords or identity cards.

**Fingerprint recognition**

This involves the identification of individuals based on the unique patterns of ridges and valleys found on their fingertips. It is one of the most common biometric technologies used in Nigeria. Fingerprints are practical for access control and attendance, but damaged fingers, dirt, scanner quality and presentation attacks can cause failures. Fingerprint capture is used in national identity enrolment, although exact enrolment procedures should be verified against current NIMC guidance (Wayman et al., 2005).

**Facial recognition**

Facial recognition identifies individuals by analyzing facial features such as the distance between the eyes, nose shape, and jaw structure. It is commonly used in security and surveillance systems. Face recognition is contactless, but its performance depends on lighting, angle, image quality and liveness checks. INEC describes facial authentication as an alternative when fingerprint authentication is unsuccessful (Independent National Electoral Commission, n.d.; Wayman et al., 2005).

**Iris recognition**

The iris is the colored part of the eye surrounding the pupil. Each person's iris has a unique pattern of rings, furrows, and freckles that remains stable throughout life. Even identical twins have different iris patterns. Iris scanning is the process of capturing a high-quality image of a person's iris using a specialized camera or scanner. The scanner uses visible or infrared light to take a detailed picture of the iris without physically touching the eye. Iris recognition measures texture in the coloured part of the eye. Its accuracy depends on sensor quality and correct capture. Iris recognition must not be confused with retinal recognition (Wayman et al., 2005).

**Retinal recognition**

Retinal recognition is a biometric identification technology that uses the unique pattern of blood vessels found in the retina, which is the light-sensitive layer located at the back of the eye. Since every person has a unique retinal blood vessel pattern, it can be used for accurate identification and authentication. Retinal recognition is considered one of the most secure biometric technologies because the retina is located inside the eye and is difficult to copy or alter.

The retinal recognition process involves the following steps:

The scanner captures the pattern of blood vessels in the retina.

During verification, a new scan is compared with the stored template.

Retinal recognition has one of the lowest error rates among biometric systems because retinal blood vessel patterns are highly distinctive.

Since the retina is inside the eye, it is very difficult for criminals to copy or manipulate.

The retinal pattern remains relatively unchanged throughout a person's lifetime.

The uniqueness of retinal patterns makes it difficult, though not impossible for another person to gain unauthorized access. It is suitable for military installations, research laboratories, and other highly restricted environments. The equipment required for retinal scanning is costly to purchase and maintain. Many users find the scanning process uncomfortable because they must place their eye very close to the scanner. Retinal scanning may take longer than fingerprint or facial recognition systems. Some users may be hesitant to use retinal scanners due to concerns about eye safety, even though the infrared light used is generally safe.

People may be reluctant to use retinal recognition because it feels intrusive.

Retinal scanning analyses blood-vessel patterns at the back of the eye. The original account of its advantages, disadvantages and operating steps is retained above, but absolute claims of impossibility of impersonation should be rejected. Claims of routine Nigerian deployment in banking or healthcare would require specific evidence (Wayman et al., 2005).

**Hand geometry and DNA**

This system measures the shape, size, and structure of a person's hand for identification purposes. Hand geometry measures the dimensions of a hand; palm prints analyse ridge and texture patterns. DNA is useful for specialised forensic identification but is generally unsuitable for routine real-time employee attendance (Wayman et al., 2005).

**Iris and retina compared**

Less comfortable because the eye must be close to the scanner.

Retina recognition examines the blood vessel patterns at the back of the eye. It provides a high level of security but is less commonly used due to its complexity.

**Behavioral Biometrics**

Behavioral biometric control is the use of an individual's distinctive behavioral characteristics to authenticate identity, monitor access, and prevent unauthorized use of systems, devices, or facilities. Voice recognition uses the unique characteristics of a person's voice to verify identity. It is often used in telephone banking and customer service systems. This analyzes the way an individual signs their signature, including speed, pressure, and movement patterns. It is commonly used for document verification. Walking style, also known as gait recognition, is a behavioral biometric technique that identifies or verifies a person based on the unique way they walk. Every individual has a distinctive walking pattern influenced by factors such as body structure, muscle movement, posture, stride length, and limb coordination.

**Data Capture:** Cameras or motion sensors record a person's movement while walking.

**Feature Extraction:** The system measures characteristics such as:

**Pattern Analysis:** Artificial intelligence or machine learning algorithms analyze these features.

**Identity Verification:** The walking pattern is compared with stored biometric records to confirm the person's identity.

Can continuously verify a user's identity while they are using a system.

May change gradually because of age, injury, illness, stress, or emotional state.

Voice biometrics attempts to verify who is speaking, while speech recognition determines what is said. Signature dynamics measures movement, pressure and timing; gait recognition analyses walking patterns. Behavioural features may vary with injury, fatigue, emotion and context. Such systems should allow appeal and should not be treated as infallible (Wayman et al., 2005).

**Multimodal Systems and Performance**

Many modern high-security systems are multimodal, meaning they combine two or more biometric traits (e.g., requiring both a fingerprint scan and facial recognition simultaneously) to reduce some matching errors and increase overall security. Performance claims should be based on independent evaluation rather than vendor marketing. Recognition errors vary with capture quality, population, thresholds and deployment conditions; performance testing should therefore be documented before implementation (Jain et al., 2008; National Institute of Standards and Technology, n.d.). Multimodal systems can combine two or more traits or offer a fallback modality. Requiring both traits to match differs from accepting either: the former may strengthen some security properties while increasing false rejections; the latter may improve accessibility. Neither arrangement eliminates false positives (Jain et al., 2008). Procurement should compare false-match and false-non-match rates, acquisition failure, throughput, operating costs,

demographic variation and the ability to function offline. Field tests should reproduce actual Nigerian lighting, power and connectivity conditions.

**Nigerian Applications**

Banks use biometric systems for customer verification, ATM transactions, account opening, and fraud prevention. Biometric voter registration and verification help prevent multiple registrations and electoral fraud during elections. Biometric control is used for passport issuance, visa processing, and border security management. Schools and universities use biometric systems for staff attendance, student registration, examination verification, and access control. Hospitals use biometric identification to manage patient records and prevent medical identity fraud. Telecommunication companies use biometrics for SIM card registration and subscriber identification. Government organizations use biometric systems for national identity management, civil service verification, and social welfare programs. Biometric systems are used to verify travelers' identities and strengthen transportation security.

Banking: The Central Bank of Nigeria (2021) framework describes BVN operations and watch-list governance. BVN is an identity-management tool, not a guarantee against every form of fraud.

**National identity:** Nigeria's national identity programme uses demographic and biometric enrolment to support identity management and deduplication. Specific capture requirements and operational performance should be confirmed from current NIMC guidance rather than presumed uniform across all enrolment centres.

**Elections:** Independent National Electoral Commission (n.d.) documents fingerprint and facial verification in its Bimodal Voter Accreditation System. This illustrates an operational Nigerian multimodal fallback rather than a promise of perfect election integrity.

Education, healthcare, border administration and security agencies may benefit from biometric verification, but each use requires proportionate data collection, oversight, lawful access and safeguards against mistaken matches.

**Biometric Attendance and Ghost Workers**

Law enforcement: fingerprint and other biometric records may support investigations, but their use requires a lawful basis, reliable provenance, independent oversight and safeguards against mistaken matches.

**Face and fingerprint verification as a tool for eliminating ghost workers and verifying daily staff attendance**

Ghost workers are fictitious or nonexistent employees whose names appear on an organization's payroll, allowing salaries to be fraudulently collected. Universities and other public institutions can reduce this problem by implementing a biometric attendance system that uses facial recognition and fingerprint verification. Since every person's fingerprint and facial features are unique, biometric verification helps ensure that only genuine staff members receive salaries and that employees physically report to work

Every staff member registers their fingerprint and facial image.

Personal information and staff number are linked to the biometric database.

On arrival at work, each staff member scans their fingerprint or face. The system verifies the biometric data against the stored records. If the identity matches, attendance is recorded automatically with the date and time. A timestamp is an automatically generated system record that pairs a date with an exact time. Unlike plain time (which only shows the hour and minute), a timestamp captures a precise, unique moment in time.

**How It Works:** Devices like fingerprint scanners, facial recognition units, card readers, and mobile apps log a timestamp whenever an employee clock in or out.

Attendance & Lateness: Verifies physical presence and flags lateness by comparing clock-in times against official schedules.

**Payroll & Work Hours:** Calculates recorded time between attendance events (not necessarily actual hours worked), tracks overtime, identifies absences, and supports authorised payroll review, subject to labour rules and human approval.

**Management & Records:** Helps institutions resolve attendance disputes, verify duty shifts, and generate monthly reports.

Management can monitor punctuality, absenteeism, and staff presence.

Before salaries are processed, attendance records are reviewed.

Staff who consistently fail biometric verification can be investigated.

Unverified records should be investigated against employment authorisations and personnel files before any lawful payroll decision is made. Organizations use biometric attendance systems and access control mechanisms to monitor employee activities and enhance security. A ghost worker may be fictitious, duplicated, retired, terminated or otherwise improperly retained on a payroll. Biometric presence can support investigation but cannot alone confirm appointment validity, salary grade, bank account ownership or entitlement. A sound process starts with independent HR verification, authorised enrolment and a unique staff identifier. Biometric attendance should then feed exception reports rather than directly authorise salary deductions or deletions. Employees on leave, external duty or medical absence must have a documented alternative route. The payroll control cycle should compare the authorised establishment, personnel master file, attendance logs, payroll register, payment instructions and general ledger. Changes to staff records and salary rates require dual approval and audit logs. For example, if 40 staff records show no biometric events in a month, the records are exceptions for review, not automatically 40 ghost workers. Investigators must examine approved leave, field duty, equipment failures and employment documents before deciding whether fraud occurred.

Measures of success include verified duplicate records removed, confirmed improper payments prevented, false exclusion rates, dispute-resolution time, operational cost and audit exceptions closed.

**Management Information Systems Integration**

An MIS transforms operational events into information for planning and control. Biometric terminals are only capture devices. The wider system includes enrolment records, employee master data, approval workflows, secure synchronisation, attendance rules, exception dashboards, payroll calculation and accounting reports.

Recommended flow: verified identity enrolment → unique staff record → biometric event → validation and secure transfer → attendance interpretation → exception review → approved payroll input → independent reconciliation → authorised payment.

Role-based access and segregation of duties are essential. A supervisor who can both create an employee and authorise payment creates a serious fraud opportunity even when a fingerprint

scanner is present. MIS dashboards should show unmatched identities, repeat failed captures, offline devices, duplicate enrolments, overrides, unapproved attendance amendments and payroll changes after cut-off. Reports should distinguish risk indicators from proven misconduct.
Data quality, backups, time synchronisation, device maintenance and business continuity are core internal controls. Audit logs should be tamper-evident and access to biometric templates strictly limited.

**Challenges in Nigeria**

The implementation of biometric control in Nigeria has improved security, identity management, banking operations, and electoral processes. However, several challenges affect its effectiveness Poor integration among these databases can create inconsistencies, duplication of records, and verification challenges. Many rural communities lack the infrastructure needed for effective biometric enrollment and verification. Limited access to electricity, internet services, and enrollment centers can exclude some citizens from biometric-based programs
One of the major challenges facing biometric systems in Nigeria is the unstable electricity supply. Biometric devices such as fingerprint scanners, facial recognition cameras, and databases require constant power to function effectively. Frequent power outages can disrupt operations and reduce system reliability. Some Nigerians are reluctant to provide biometric information because of fears regarding surveillance, misuse of personal data, or government monitoring. This lack of trust can reduce public acceptance of biometric programs. Many biometric systems depend on internet access for real-time verification and data synchronization. In rural and remote areas of Nigeria, poor network coverage can delay authentication processes and affect service delivery.
The acquisition, installation, maintenance, and upgrading of biometric equipment require significant financial investment. Many organizations, especially small businesses and public institutions, may find it difficult to afford these costs. Biometric databases contain sensitive personal information. Weak cybersecurity measures may expose such data to hackers, identity thieves, or unauthorized users. Concerns about data protection have become more important with the increasing digitization of records in Nigeria. There is a shortage of highly skilled personnel capable of managing, maintaining, and troubleshooting advanced biometric systems. This can lead to operational failures and increased dependence on foreign technical support.
Fingerprint recognition may fail when users have worn-out fingerprints due to manual labor, injuries, or aging. Facial recognition systems may also be affected by poor lighting conditions, facial coverings, or significant physical changes. Biometric systems are attractive targets for cybercriminals. Although biometric traits are difficult to replicate, criminals may attempt to use artificial intelligence, deepfake technology, or stolen biometric templates to bypass security systems. Although Nigeria has data protection regulations, enforcement remains a challenge. Stronger legal frameworks and compliance mechanisms are needed to ensure that biometric data is collected, stored, and used responsibly.

**The challenges interact:** a power outage may produce missing attendance data, while a punitive no-scan-no-pay rule may then harm legitimate employees. A design that appears secure on paper can therefore become unreliable or inequitable in practice. Cybersecurity risks include stolen templates, compromised devices, replay attacks, insider misuse, spoofing, poor access management and insecure interfaces. Countermeasures include encryption, patching, multifactor administrative access, device attestation, liveness testing and periodic independent security reviews. A practical rural deployment should support secure offline capture and later

reconciliation without allowing unlimited local modification. Organisations should measure failure rates by location and user group to detect systematic exclusion.

**Legal and Ethical Considerations**

Nigeria's Data Protection Act 2023 provides the principal contemporary statutory framework for personal-data protection (Federal Republic of Nigeria, 2023). Biometric information used to identify an individual demands particularly careful handling. Organisations must identify an appropriate lawful basis, communicate clear purposes, minimise data collection and limit retention. Consent is not always freely given in an employment relationship, so organisations should not assume that a signed consent form resolves every legal question. They should document the applicable lawful basis and consider whether a data protection impact assessment is required. Data-sharing between NIN, BVN, voter and employment databases should not be proposed as unrestricted consolidation. Interoperability should be purpose-specific, authorised, secure, auditable and accompanied by correction and complaint procedures. Ethical controls include accessibility for people with disabilities, human review of consequential decisions, safeguards against function creep and transparent rules on surveillance. Security and privacy are complementary governance obligations, not competing afterthoughts.

**Implementation and Control Evaluation**

Implementation should begin with a documented business case and risk assessment. Identify the precise control failure to be addressed, assess alternative solutions and specify measurable performance standards. During procurement, require evidence of accuracy testing, offline resilience, liveness detection, secure template storage, vendor support, export capability, audit trails and independent testing. Avoid proprietary lock-in where feasible. Pilot deployment should include representative staff groups, varied lighting and working conditions, clear enrolment procedures and accessible fallback mechanisms. Document error rates and investigate unexpected demographic or occupational differences. Operational governance should allocate responsibilities to HR, Finance, ICT, Internal Audit, Legal/Data Protection and line management. A steering group should review monthly exception reports and material incidents. Evaluate outcomes against a baseline: duplicate records, unauthorised payments, attendance disputes, failed matches, resolution times, downtime, security incidents and total cost. A biometric programme should be expanded only when demonstrated benefits justify the cost and risks.

Evidence and limitations. Official documents establish the existence and intended functions of the BVN and BVAS programmes, but their existence alone does not demonstrate the size of fraud reductions. INEC's report of the 2023 general election describes mock accreditation and training lessons; those findings should not be generalised to all polling units or elections (Independent National Electoral Commission, 2024). Similarly, NIST evaluations show that facial recognition accuracy depends on the algorithm, image conditions and demographic characteristics, so performance must be tested in the intended Nigerian setting (Grother et al., 2019). Claims about ghost-worker savings require audited before-and-after payroll data and controls for other reforms. The National Institute of Standards and Technology (n.d.) also maintains an ongoing face-recognition evaluation programme. Evidence appraisal. Official policy documents establish what BVN and BVAS are designed to do; they are not independent impact evaluations. The Nigerian IPPIS studies cited here use different observational and survey approaches and should not be pooled into a single national effectiveness estimate. NIST findings about algorithmic

demographic differences are laboratory evaluations, not Nigerian field-performance measurements (Grother et al., 2019).

**Synthesis of Findings**

Biometric systems can strengthen identity assurance, but successful adoption depends on appropriate infrastructure, cybersecurity, legal compliance and public confidence. These are governance requirements rather than demonstrated national outcome estimates. The documented Nigerian cases reviewed here concern banking identity controls and electoral accreditation. Potential applications in education, healthcare, telecommunications and government administration require institution-specific verification before conclusions can be drawn about effectiveness or scale (Central Bank of Nigeria, 2021; Independent National Electoral Commission, 2024). The central conclusion is that biometrics can improve identity assurance, but effective organisational control requires reliable master records, authorisation, reconciliation, accountability and legal safeguards. For Nigerian institutions, investment in governance and infrastructure is as important as investment in scanners.

**Critical appraisal of Nigerian adoption**

The existence of a biometric programme does not itself prove improved outcomes. In banking, the Central Bank of Nigeria describes the BVN as a centralised biometric identity initiative intended to support customer identification and Know Your Customer controls (Central Bank of Nigeria [CBN], n.d.). This supports a claim about the programme's design, not a quantified claim that it has eliminated fraud. Likewise, INEC documents that its Bimodal Voter Accreditation System (BVAS) can authenticate eligible voters through fingerprints or facial recognition (Independent National Electoral Commission, n.d.). The electoral effect depends additionally on enrolment accuracy, device availability, trained personnel, procedural compliance and independent oversight. For organisations considering biometric attendance, the relevant question is not whether fingerprints are unique, but whether the complete process prevents unauthorised enrolment, proxy attendance, retrospective alteration of records and unjustified payroll payments. As Wayman et al. (2005) explain, biometric performance must be evaluated as a system rather than as an isolated sensor. The same principle applies to public payroll systems and university administration.

**System controls, evidence and limitations**

An audit trail should preserve the employee identifier, device identifier, transaction timestamp, authentication outcome, operator interventions and approved corrections. Access to raw biometric images should be restricted; templates and transaction logs should be protected according to their sensitivity. Exception workflows must accommodate worn fingerprints, disability, illness, device malfunction and network outages. A failed match is a signal for review, not proof of misconduct (Jain et al., 2008; Wayman et al., 2005). A control evaluation should distinguish (a) biometric matching accuracy, (b) process integrity, (c) payroll accuracy, (d) operational continuity and (e) lawful processing. Measures include false-match and false-non-match rates, enrolment failures, average verification time, device uptime, unresolved exceptions, unmatched payroll records and timely deactivation of departed employees. Metrics should be disaggregated where practicable to detect exclusion and unfair outcomes.

**Legal and ethical implications for Nigeria**

The Nigeria Data Protection Act 2023 classifies genetic and biometric data used to uniquely identify a natural person as sensitive personal data (Federal Republic of Nigeria, 2023). Accordingly, organisations should identify a lawful basis, communicate a specific purpose, minimise collection, restrict access, establish retention and deletion rules, document third-party arrangements and assess heightened processing risks. Consent alone should not automatically be assumed to be freely given in an employment relationship. Cross-database sharing should be governed by necessity, authorisation and proportionality rather than a blanket objective of centralisation.

**Recommendations**

**1.** Governance and accountability. Assign executive sponsorship, appoint responsible data and system owners, and approve written identity, attendance, exception and retention policies.
2. Verified enrolment. Reconcile every enrolled person to authorised HR records, verify source documents, prevent duplicate identities and independently approve changes.
3. Payroll segregation of duties. Separate enrolment, attendance corrections, payroll preparation, payroll approval and payment release; investigate discrepancies before adjusting pay.
4. Privacy and security. Conduct a documented privacy and security risk assessment, encrypt sensitive data, limit administrator privileges, log access, test backups and plan incident response.
5. Continuity and inclusion. Provide offline procedures, backup power, alternative verification and appeal routes for failed captures or disability-related barriers.
6. Interoperability with safeguards. Use purpose-limited, authorised interfaces between systems rather than unrestricted merging of biometric databases.
7. Performance monitoring. Publish periodic internal measures of device uptime, failed enrolment, false matches, outstanding exceptions and payroll reconciliation findings.
8. Capacity development. Train HR, ICT, finance, internal audit and users on enrolment quality, cybersecurity, data protection and grievance procedures.
9. Independent evaluation. Review cost-effectiveness and outcomes against a documented pre-deployment baseline; do not infer success from the mere purchase of devices.
10. Local research. Encourage Nigerian empirical studies of exclusion, adoption costs, usability and control effectiveness across public and private institutions.

**Conclusion**

Biometric control can improve identity assurance and the integrity of selected organisational processes in Nigeria. Its contribution is most credible when it forms part of a broader MIS control environment involving reliable identity enrolment, secure records, exception management, reconciliations and independent review. Fingerprint and facial verification can discourage proxy attendance and support investigation of suspicious payroll entries, but neither can establish employment legitimacy or actual work performance in isolation. Nigerian deployment must address electricity and connectivity constraints, user inclusion, cybersecurity and the legal obligations associated with sensitive personal data. Sustainable benefits therefore depend on sound governance and measurable results, not technological adoption alone.

**References**

Agboola, T. O. (2018). Effectiveness of integrated personnel and payroll information system in addressing ghost worker syndrome in Nigerian public sector. Global Journal of Human-Social Science. https://socialscienceresearch.org/index.php/GJHSS/article/view/2494

Central Bank of Nigeria. (2021). Regulatory framework for Bank Verification Number (BVN) operations and watch-list for the Nigerian banking industry. https://www.cbn.gov.ng/Out/2021/CCD/REVISED%20REGULATORY%20FRAMEWORK%20FOR%20BANK%20VERIFICATION%20NUMBER%20%28BVN%29%20OPERATIONS%20AND%20WATCH-LIST%20FOR%20THE%20NIGERIAN%20BANKING%20INDUSTRY%20121021%20FINAL.pdf

Central Bank of Nigeria. (n.d.). Bank Verification Number (BVN). https://www.cbn.gov.ng/PaymentsSystem/BVN.html

Danbala, I. N., Suleiman, E., & Bala, B. (2024). An appraisal of effectiveness of integrated payroll and personnel information system (IPPIS) in eliminating ghost workers in Nigerian public service. *African Multidisciplinary Journal of Sciences and Artificial Intelligence, 1*(1), 509–531. https://doi.org/10.58578/amjsai.v1i1.3682

Federal Republic of Nigeria. (2023). Nigeria Data Protection Act, 2023. https://ndpc.gov.ng/wp-content/uploads/2024/03/Nigeria_Data_Protection_Act_2023.pdf

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test (FRVT) part 3: Demographic effects (NISTIR 8280). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.IR.8280

Independent National Electoral Commission. (2024). Report of the 2023 general election. https://www.inecnigeria.org/wp-content/uploads/2024/02/2023-GENERAL-ELECTION-REPORT-1.pdf

Independent National Electoral Commission. (n.d.). Voter education and guidelines. https://inecnigeria.org/voters/education

Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2008). Handbook of biometrics. Springer. https://doi.org/10.1007/978-0-387-71041-9

National Institute of Standards and Technology. (n.d.). Face recognition vendor test (FRVT). https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (Eds.). (2005). Biometric systems: Technology, design and performance evaluation. *Springer*. https://doi.org/10.1007/b138151

Zukbee, J. D., & Benjamin, U. U. (2026). Integrated payroll and personnel information system (IPPIS) and the incidence of ghost workers and payroll fraud in Nigeria's public sector. *International Journal of Research and Innovation in Social Science, 10*(7), 17576–17595. https://doi.org/10.47772/IJRISS.2026.100701207