IKR Publishers

IKR Journal of Engineering and Technology (IKRJET)
Journal homepage: https://ikrpublishers.com/ikrjet/
Volume-2, Issue-6 (November-December) 2026
OPEN ACCESS
ISSN: 3107-7331 (Online)

A Systematic Review of RFID-Based Access Control Systems for Kwara State Polytechnic Campus: Technologies, Challenges, and Future Prospects

Ibisankale S. M.[1*], Akewushola M. O.[2], Sanni M. A.[3], Alonge P. O.[4], Mustapha H. K.[5], Ogundeji J. O.[6] & Sa'ad B. O.[7]

[1]Department of Mechatronic Engineering, Institute of Technology, Kwara State Polytechnic, Ilorin
[2,3,5,6]Department of Electrical and Electronics Engineering Institute of Technology, Kwara State Polytechnic, Ilorin
[4]Department of Mechanical Engineering, Institute of Technology, Kwara State Polytechnic, Ilorin
[7]Department of Metallurgical Engineering, Institute of Technology, Kwara State Polytechnic, Ilorin

DOI: *10.5281/zenodo.24442604*

ARTICLE INFO

Article history:
Received : 01-11-2026
Accepted : 08-11-2026
Available online : 22-11-2026

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial **4.0 International License (CC BY-NC 4.0),** which permits non-commercial use, sharing, and reproduction in any medium, provided the original author(s) and source are appropriately credited.

Citation: Ibisankale, S. M., Akewushola, M. O., Sanni, M. A., Alonge, P. O., Mustapha, H. K., Ogundeji, J. O., & Sa'ad, B. O. (2026). A Systematic Review of RFID-Based Access Control Systems for Kwara State Polytechnic Campus: Technologies, Challenges, and Future Prospects. *IKR Journal of Engineering and Technology (IKRJET), 2*(6), 46-51.

ABSTRACT **Review Article**

The increasing security challenges in tertiary institutions have highlighted the limitations of conventional manual access-control systems, particularly in managing unauthorized entry, identity verification, and movement monitoring. This review article examines the potential application of Radio Frequency Identification (RFID) technology for improving campus access control at Kwara State Polytechnic, Ilorin, Nigeria. The study adopts a systematic review framework to examine existing RFID technologies, authentication mechanisms, system architecture operational requirements, and implementation challenges relevant to institutional security. The review considers low-frequency (LF), high-frequency (HF), and ultra-high-frequency (UHF) RFID technologies, alongside their suitability for pedestrian and vehicular access management. The analysis identifies secure credential authentication, centralized database integration, real-time access logging, and automated entry verification as promising capabilities of RFID-based systems. However, challenges involving credential cloning, infrastructure reliability, power interruptions, data privacy, implementation costs, and maintenance requirements may constrain successful deployment. Consequently, a phased implementation framework encompassing institutional requirements assessment, system design, controlled pilot testing, and performance evaluation was proposed. The paper concludes that RFID technology offers a promising approach to strengthening campus security and access management, provided that appropriate cybersecurity safeguards, reliable infrastructure, and sustainable operational strategies are established. Further empirical evaluation is recommended to determine its effectiveness within the specific operational environment of Kwara State Polytechnic, Ilorin.

Keywords: Radio Frequency Identification (RFID), Access Control, Campus Security, Authentication, Smart Campus, Kwara State Polytechnic.

**Corresponding author: Ibisankale S. M.*
Department of Mechatronic Engineering, Institute of Technology, Kwara State Polytechnic, Ilorin

Introduction

Security on tertiary institution campuses is as fundamental as academic delivery, as a compromised security environment hinders the peaceful atmosphere required for effective teaching and learning (Jecha and Abdullahi, 2026). To ensure an optimal academic environment where knowledge transfer thrives, higher education institutions must invest significantly in modern security infrastructure. Kwara State Polytechnic, Ilorin, is no exception to this rule, as the institution has made substantial investments in its physical security framework over the years (Roberts et al., 2025). The institution relies not only on internal security personnel but also partners with

external security agencies, including public law enforcement and private security outfits, to safeguard staff, students, and institutional assets (Danyawo, 2025).

However, despite these concerted multi-agency efforts, the reliance on manual, human-centered security operations present critical structural and operational vulnerabilities (Flores-Salgado *et al.,* 2024). Given the vast geographical expanse, porous perimeter borders, and multiple entry points of the Kwara State Polytechnic main campus, manual access management lacks the required speed, accuracy, and real-time responsiveness. During peak morning hours, examination periods, and major campus events, human security guards must manually verify physical identification cards for thousands of converging students and staff (Ur Rehman *et al.*, 2019). This manual verification process creates severe traffic bottlenecks at entry gates, leading to operational fatigue among guards and frequently causing security personnel to loosen verification standards to alleviate crowd pressure.

Furthermore, human-operated security systems remain inherently susceptible to operational inefficiencies, unauthorized access, identity falsification, and potential security compromises. Physical identification cards are easily forged, shared among unauthorized individuals, or used for impersonation, while paper-based visitor logbooks generate fragmented records that cannot be queried quickly during security investigations (Pinggui and Xiuqing, 2017). Manual checkpoints are also vulnerable to human error, circumvention, and potential collusion at entry barriers, leaving the vast campus exposed to unmonitored intrusions (Ennibras *et al.*, 2024).

To address these structural and operational challenges, automated security systems offer a promising and scalable solution. Radio Frequency Identification (RFID) technology allows for contactless, high-speed authentication of student credentials by using radio waves to exchange data between encrypted smart cards and automated physical barriers like turnstiles and boom gates. When integrated with central institutional databases, automated systems eliminate gate congestion, maintain real-time entry and exit logs, and prevent unauthorized entry through spoofed credentials (Roslan-Umar *et al.*, 2015).

This paper presents a systematic review of the implementation of Radio Frequency Identification (RFID)-based access control systems tailored specifically to the operational, infrastructural, and geographical context of Kwara State Polytechnic, Ilorin. The article evaluates existing technical architectures, integration frameworks, deployment challenges, and prospects. This study provides a comprehensive roadmap for transitioning the institution from vulnerable manual entry protocols to a secure, technology-driven smart campus ecosystem.

Related Research Work

Security challenges in Nigerian tertiary institutions have continued to attract considerable research attention due to their implications for academic activities, institutional administration, and the safety of students and staff. These challenges manifest in various forms, including cultism, kidnapping, armed robbery, theft, sexual harassment, violent demonstrations, terrorism, and unauthorized access to institutional facilities. Although government agencies and institutional management have introduced different security measures to address these threats, maintaining a secure academic environment remains a significant concern. Consequently, researchers have investigated the nature, causes, and management of security threats in higher education institutions, with particular emphasis on preventive strategies and institutional security frameworks.

(Hina and Dominic, 2020) investigated the persistent security challenges confronting Nigerian universities and their implications for teaching, research, and institutional development. The study examined existing security management strategies with the aim of identifying sustainable approaches to addressing the multidimensional security challenges affecting higher education institutions. Its findings revealed systemic deficiencies in security funding, personnel training, intelligence gathering, inter-agency coordination, and stakeholder collaboration, which collectively undermine the effectiveness of existing security arrangements. The study recommended improved cooperation among university administrators, government agencies, security operatives, and campus communities to establish resilient and conducive learning environments. Although the research emphasized coordinated and sustainable security management, the supplied description did not indicate a detailed assessment of automated identification technologies, RFID system architectures, or their integration into institutional access-control infrastructure.

(Savolainen, 2023) emphasizing the role of digital technologies in strengthening campus security. The study acknowledged that institutional security policies and operational protocols are essential but argued that their effectiveness could be enhanced through the adoption of modern technological solutions. It further identified cybersecurity threats, privacy and data protection concerns, and inadequate funding as major challenges associated with technology-driven campus security. The study highlighted the need for institutions to integrate digital security solutions into their existing security frameworks while addressing the accompanying operational and financial constraints. However, the supplied account did not establish whether the study specifically evaluated RFID-based authentication, automated entry-point monitoring, or centralized access-control systems.

(Jannat, 2026) examined the increasing prevalence of crime in Nigerian tertiary institutions and its implications for the credibility, integrity, and effective administration of higher education. The study investigated the prevalence, causes, and management strategies associated with criminal activities in

universities, polytechnics, and colleges of education. Attention was given to cultism, sexual harassment, cybercrime, examination malpractice, theft, drug abuse, and financial fraud, alongside their social, economic, and institutional consequences. The study emphasized the importance of staff ethics training, student economic empowerment, community collaboration, and security awareness campaigns as sustainable crime-prevention strategies. It concluded that a holistic and human-centred approach to crime management, supported by accountability, inclusiveness, and proactive preventive measures, is essential for establishing safer academic environments. Nevertheless, the study concentrated on institutional crime management and preventive interventions, without specifically addressing the technical deployment of RFID-based access control for regulating and monitoring movement through campus entry points.

(Jecha and Abdullahi, 2026) examined the security threats affecting peaceful academic activities and effective administration in Nigerian universities. The study investigated various forms of campus insecurity and assessed the measures adopted by university management and security personnel to address these challenges. The findings identified inadequate intelligence gathering, incompetence among security personnel, corruption, negligence of duty, ageing security personnel, and insufficient strategic security training as major factors undermining campus security operations. The study concluded that these institutional and operational deficiencies significantly hinder effective security management in Nigerian universities. Although the research provided valuable insights into the challenges confronting conventional campus security arrangements, its emphasis was primarily on personnel effectiveness and administrative security practices rather than automated access-control technologies.

Despite the considerable attention given to campus insecurity in Nigerian tertiary institutions, existing studies have predominantly emphasized institutional security management, crime prevention, personnel effectiveness, and stakeholder collaboration, with limited consideration of the technological requirements for automated campus access control. In particular, the reviewed studies provide insufficient insight into the integration of RFID-based authentication, centralized identity management, real-time access monitoring, and electronic record management within the operational environment of Kwara State Polytechnic, Ilorin. Furthermore, the suitability of existing RFID access-control architectures in relation to the institution's geographical layout, multiple entry points, infrastructural limitations, implementation costs, and data security requirements remains inadequately addressed in the reviewed literature. Consequently, this study undertakes a systematic review of RFID-based access-control technologies, their implementation frameworks, associated challenges, and prospects, with the aim of identifying appropriate technological approaches and providing an evidence-informed basis for strengthening campus access management at Kwara State Polytechnic.

The present study therefore seeks to bridge this gap by synthesizing relevant technological approaches and identifying the considerations necessary for transitioning from predominantly manual security verification to a more automated and coordinated campus access-control environment.

Methodology

Research Design

This study presents the systematic review of Radio Frequency Identification (RFID)-based access-control technologies and their potential applicability to tertiary institutions, with particular attention to Kwara State Polytechnic, Ilorin. The review assessed technological architecture, authentication mechanisms, operational performance, implementation constraints, and prospects for institutional adoption. Reporting will be guided by PRISMA 2020, with the completed search and selection process documented transparently.

Search Strategy

Literatures were searched in IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar and other relevant scholarly repositories. The proposed publication window is 2015 October to October 2026, with older foundational references included where justified. A reproducible search log recorded the search date, database, exact query, filters, and number of records returned.

Illustrative search string: ("RFID" OR "radio frequency identification") AND ("access control" OR "campus security" OR "smart campus") AND (authentication OR identification OR "entry monitoring"). Search syntax was adapted to each database.

Eligibility Criteria

Include	Exclude
Research on RFID-based identification, authentication or access control	Unrelated RFID applications without an access-control component
Studies reporting system design, deployment, testing, or security analysis	Promotional or opinion-only material without substantiated evidence
Relevant educational or comparable controlled-entry settings	Duplicate records and inaccessible full texts
English-language full texts with extractable methods or findings	Studies with insufficient information for meaningful assessment

Screening and Study Selection

Retrieved records were deduplicated, screened by title and abstract, and assessed in full text against the eligibility criteria. Reasons for full-text exclusions was logged. The final article presents a PRISMA flow diagram populated only with actual record counts.

Data Extraction and Quality Assessment

A structured extraction sheet was used to capture author/year, study setting, RFID frequency and credential type, reader/controller architecture, authentication mechanism, database integration, barrier type, evaluation methods, reported performance, vulnerabilities, limitations, and relevance to campus deployment. Methodological quality was considered in terms of clarity of objectives, replicability, appropriateness of tests, completeness of reporting, and consistency between evidence and conclusions.

Synthesis

Findings were synthesized thematically across technology selection, system architecture, operating effectiveness, cybersecurity, deployment requirements and prospects. Comparable numerical results were tabulated descriptively, but no pooled effect or comparative ranking was asserted unless supported by sufficiently comparable studies. The present manuscript does not report field installation or experimental validation at Kwara State Polytechnic.

Results and Discussion

RFID Technology Options

RFID systems differ in operating frequency, reading distance, credential characteristics and application. A campus may require distinct configurations for pedestrian and vehicle access. Selection must balance throughput, physical access geometry, authentication security, interference and total cost. Presented in Table 1 is qualitative comparison of different RFID families application and the relevant design specification to be considered.

Table 1. Qualitative comparison of RFID technology families; application suitability is conditional, not a measured outcome of this review.

Technology	Typical application	Relevant design consideration
Low frequency (LF)	Short-range identification in selected applications	Reader/tag compatibility and limited data capability
High frequency (HF; 13.56 MHz)	Contactless smart cards at pedestrian checkpoints	Support for secure authentication depends on card and protocol
Ultra-high frequency (UHF)	Longer-range identification, potentially vehicles	Unintended reads and credential association require careful control

Proposed Access-Control Architecture

A prospective architecture comprises a registered credential, compatible reader, secure controller, authorization database, access barrier, and event logging. Access should depend on validated permissions rather than merely reading a card identifier. Centralized administration can simplify credential revocation and reporting, while resilience requires attention to network and power failures.

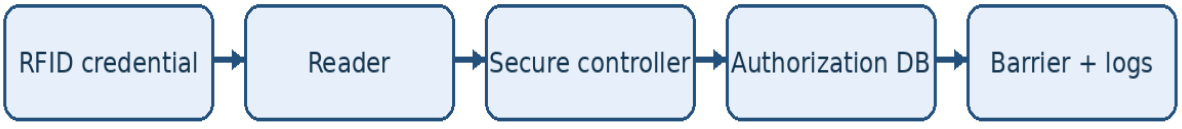


Figure 1. Conceptual RFID-enabled campus access-control sequence.

Operational Implications

Automated credential processing may reduce repetitive manual checks and produce searchable access records. Actual queue reduction, processing speed and reliability depend on reader performance, authentication latency, physical barrier operation, pedestrian flow, and infrastructure uptime. These benefits require empirical verification before being attributed to Kwara State Polytechnic.

Database Integration and Privacy

Integration with institutional identity records could support authorization updates, lost-card revocation, visitor administration and audit logs. Such functionality also creates obligations relating to access privileges, secure storage, retention periods, auditability and compliance with applicable Nigerian data protection requirements. A valid credential alone does not prove that the legitimate holder is presenting it.

Security and Deployment Challenges

Table 2. Risk–mitigation matrix for proposed institutional assessment; entries are design considerations rather than verified findings from a completed search.

Challenge	Possible consequence	Potential mitigation for evaluation
Card cloning / identifier copying	Unauthorized entry	Cryptographic mutual authentication; avoid UID-only access
Reader or network failure	Service disruption and queues	Offline policy, redundancy and tested recovery procedures
Power interruptions	Barrier and controller downtime	UPS/backup power and safe emergency operation
Credential sharing	Impersonation	Security staff oversight; additional checks at sensitive zones
Data misuse	Privacy and institutional risk	Role-based access, retention rules, encryption and audit logs
Budget and maintenance	Incomplete or unsustainable deployment	Pilot costing, staff training and maintenance planning

Contextual Suitability for Kwara State Polytechnic

The supplied Introduction describes manual identity checking, multiple entry points, peak-period congestion and fragmented visitor records as motivating concerns. These are institutional claims in the draft Introduction, not independently measured baseline data. A phased assessment should first establish gate-specific demand, existing connectivity, power resilience, student/staff credential governance and the ability to maintain equipment.

Proposed Phased Adoption Framework

Table 3. Proposed implementation and evaluation pathway; not an account of completed institutional activities.

Phase	Key activity	Evidence to collect
1. Requirements	Map entry points, access roles, traffic and security policy	Baseline queue times, user groups, risk register
2. Pilot design	Select credential, reader, controller, barrier and database	Architecture, threat model, procurement and maintenance costs
3. Controlled pilot	Test one representative entrance	Authentication time, false acceptance/rejection, uptime, queue length
4. Review and scale	Assess performance, usability, privacy and cost	Pilot evaluation and expansion decision

Conclusion

RFID-based access control is a potentially useful component of campus security modernization because it can support electronic credential verification, access-event recording and centralized administration. Its suitability for Kwara State Polytechnic cannot yet be established from the contextual studies supplied alone. Secure credential protocols, reliable infrastructure, privacy safeguards, financial sustainability and coordination with existing security personnel are essential considerations.

This completed systematic review established the strengths and weaknesses of documented RFID deployments and distinguish demonstrated outcomes from anticipated benefits. Subject to that evidence, a small, carefully evaluated pilot at a representative campus entry point is reasonable future research and implementation direction. The present document

supplies a review methodology and provisional discussion framework; it does not claim a completed systematic search, quantitative results, or a deployed system.

References

1. Danyawo, M. A. (2025). TERTIARY INSTITUTIONS IN NIGERIA AND CRIME MANAGEMENT STRATEGIES. *Multi-Disciplinary Research and Development Journals Int'l*, *2*(3), 34–41. https://doi.org/10.59795/m.v2i3.184
2. Ennibras, F., Aoula, E.-S., & Bouihi, B. (2024). AI in Preventing Dropout in Distance Higher Education: A Systematic Literature Review. *2024 4th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, 1–7. https://doi.org/10.1109/IRASET60544.2024.10548954
3. Flores-Salgado, B., Gonzalez-Ambriz, S.-J., Martínez-García-Moreno, C.-A., & Beltrán, J. (2024). IoT-based system for campus community security. *Internet of Things*, *26*, 101179. https://doi.org/10.1016/j.iot.2024.101179
4. Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: A perspective for higher education institutions. *Journal of Computer Information Systems*, *60*(3), 201–211. https://doi.org/10.1080/08874417.2018.1432996
5. Jannat, M. (2026). Cybersecurity in higher education: Strengthening secure learning environments. *Journal of Education, Society & Sustainable Practice*, *3*, 45–56. https://doi.org/10.63697/jessp.2026.10163
6. Jecha, A., & Abdullahi, M. Y. (2026). SECURITY MANAGEMENT STRATEGIES IN NIGERIAN UNIVERSITIES: A QUEST FOR LASTING SOLUTIONS. *African Journal of Educational Management, Teaching and Entrepreneurship Studies*, *17*(2). https://doi.org/10.65360/ajemates.v17i2.961
7. Pinggui, H., & Xiuqing, C. (2017). Design and Implementation of Campus Security System Based on Internet of Things. *2017 International Conference on Robots & Intelligent System (ICRIS)*, 86–89. https://doi.org/10.1109/ICRIS.2017.28
8. Roberts, N., Naisby, L., & Mulligan, A. (2025). Campus security and students' perceptions of safety: An evaluation of security practices. *Security Journal*, *38*(1), 52. https://doi.org/10.1057/s41284-025-00500-5
9. Roslan Umar, Shahirah Syafa, Atiq Wahidah Azlan, & Zainol Abidin Ibrahim. (2015). Radio Frequency Interference: The Study of Rain Effect on Radio Signal Attenuation. *Malaysian Journal of Analytical Science*, *9*(2), 1093–1098.
10. Savolainen, T. (2023). A safe learning environment from the perspective of Laurea University of applied sciences safety, security and risk management students and staff. *Heliyon*, *9*(3), e12836. https://doi.org/10.1016/j.heliyon.2023.e12836
11. Ur Rehman, S., Liu, R., Zhang, H., Liang, G., Fu, Y., & Qayoom, A. (2019). Localization of Moving Objects Based on RFID Tag Array and Laser Ranging Information. *Electronics*, *8*(8), 887. https://doi.org/10.3390/electronics8080887