www.ijarp.com ISSN 2456-9992 Page: 01-11

International Journal Advanced Research Publications

Research Article

Volume: 02
Issue: 10

AUGMENTING HUMAN JUDGMENT: A HYBRID INTELLIGENCE FRAMEWORK FOR MANAGING SECURITY APPARATUS IN NIGERIAN TERTIARY INSTITUTIONS IN THE DIGITAL AGE

***Uzoma, Ijeoma Gladys**

Department of Educational Management (Administration) Faculty of Education University of Port Harcourt.

Article Received: 19 September 2026, Article Revised: 09 October 2026, Published on: 29 October 2026

***Corresponding Author: Uzoma, Ijeoma Gladys**

Department of Educational Management (Administration) Faculty of Education University of Port Harcourt.

Doi: https://doi-doi.org/101555/ijarp.4170

ABSTRACT

Nigerian tertiary institutions are rapidly adopting Artificial Intelligence (AI) tools such as CCTV analytics, facial recognition, and predictive policing software to address rising security threats including cultism, kidnapping, vandalism, and civil unrest. Yet, two persistent challenges undermine effectiveness. First, technological determinism leads many institutions to treat AI as a substitute for human security personnel, resulting in over-reliance, system failures, and diminished trust among staff and students. Second, most AI models are imported without adaptation to Nigeria's resource constraints, socio-political realities, and gaps in human capacity, creating a contextual mismatch. As a result, there remains limited empirical evidence on how human security managers and AI systems should interact the human-AI nexus to produce security outcomes that are effective, ethical, and sustainable.

This study seeks to develop and validate a Hybrid Intelligence Framework for managing security apparatus in Nigerian tertiary institutions. Anchored in Human-AI Interaction Theory, Institutional Theory, and the Resource-Based View, the research employs a sequential explanatory mixed-methods design. Phase one involves a survey of security managers, ICT directors, and administrators across 15-20 public and private universities to map current AI adoption, assess levels of trust in AI, and examine perceived security effectiveness. Phase two uses in-depth interviews and focus groups in four case-study institutions to explore lived experiences of human-AI collaboration, decision conflicts, and failure points. Insights from both phases will inform the construction of a Hybrid Intelligence Framework specifying roles, decision-sharing protocols, and training requirements. The

framework will be validated through expert panels and a Delphi study involving security professionals and education policymakers.

The study extends Human-AI Interaction Theory to resource-constrained educational contexts in Africa and offers Nigerian universities, the National Universities Commission, and the Ministry of Education actionable guidelines for integrating AI in campus security without displacing human judgment. By centering the human-AI nexus, this research contributes both theoretical insight and practical tools for sustainable security management in the digital age.

KEYWORDS: Hybrid Intelligence, Artificial Intelligence, Security Management, Human-AI Interaction, Nigerian Tertiary Institutions, Digital Age.

INTRODUCTION

Nigerian tertiary institutions face escalating security threats such as kidnapping, cultism, vandalism, cyber intrusions, and civil unrest. In response, many universities in Delta State are deploying AI-enabled tools such as CCTV analytics, facial recognition, access control systems, and predictive policing software. We meet today at a critical intersection of technology, security, and higher education governance. In response, many universities have turned to the digital age's promise: Artificial Intelligence. From AI-powered CCTV analytics to facial recognition, access control, and predictive policing software, technology is being deployed to secure our campuses.

But here lies the paradox. The rush to adopt AI has often been driven by what scholars call technological determinism. This is the belief that technology alone will solve complex human problems. In practice, this has led many institutions to position AI as a replacement for human security personnel. The result is over-reliance on systems that fail under local conditions, mistrust among security staff, false alarms that desensitize responders, and significant financial strain on already resource-constrained institutions.

Equally problematic is the issue of contextual mismatch. Most AI models in use were developed in the Global North, trained on datasets that do not reflect Nigeria's socio-political realities, linguistic diversity, or infrastructural limitations. When we import these tools without adaptation, we risk creating security systems that are technically sophisticated but operationally ineffective.

This brings us to the core of this study which is the human-AI nexus. The question is no longer whether AI belongs in campus security. The questions are: 'How should human

judgment and artificial intelligence work together'? 'How do we design systems where AI augments, rather than replaces, human decision-making'? 'How do we ensure that technology serves our security managers, rather than the other way around'?

This is the gap my research addresses. The study, titled "Augmenting Human Judgment: A Hybrid Intelligence Framework for Managing Security Apparatus in Nigerian Tertiary Institutions in the Digital Age," argued that sustainable security management requires a hybrid intelligence approach. Hybrid intelligence recognizes that humans bring contextual understanding, ethical reasoning, and adaptability, while AI brings speed, pattern recognition, and scalability. Neither alone is sufficient. Together, properly orchestrated, they can produce security outcomes that are more effective, ethical, and sustainable.

The seminar will unfold in three parts. First, I will situate the problem within Delta State, Nigeria's current security landscape and review how AI is currently being deployed in our universities. Second, I will present the theoretical foundations. That is, drawing on Human-AI Interaction Theory, Institutional Theory, and the Resource-Based View that explain why institutions adopt AI and how human-AI collaboration succeeds or fails. Third, I will outline the proposed Hybrid Intelligence Framework, including its core components: role allocation, decision-sharing protocols, trust-building mechanisms, and capacity development needs.

By the end of this seminar, my goal is to invite your critique and collaboration. The aim is not to produce another AI tool, but to develop a context-appropriate framework that Nigerian universities, the National Universities Commission, and security policymakers can use to guide ethical, effective, and sustainable integration of AI in campus security. The stakes are high. As we digitize our institutions, we must ensure that we are not just upgrading our technology, but also augmenting our most valuable security asset being human judgment.

Statement of the Problem

Nigerian tertiary institutions operate in an increasingly volatile security environment. The prevalence of cultism, kidnapping for ransom, campus vandalism, violent protests, and cyber intrusions has placed enormous pressure on university management to safeguard students, staff, and institutional assets. In response to these threats, many universities have begun deploying Artificial Intelligence (AI)-enabled security tools, including CCTV video analytics, facial recognition systems, automated access control, and predictive policing software. This shift reflects a broader global trend toward the digitization of security management in the digital age.

However, the adoption of AI in Nigerian tertiary institutions is confronted by two interrelated problems that undermine its intended effectiveness, ethicality, and sustainability.

First, is the problem of technological determinism. Many institutions approach AI as a technological fix capable of replacing human security personnel rather than augmenting their capabilities. This has resulted in the over-reliance on automated systems, the marginalization of experienced security staff, and the erosion of trust between management and frontline personnel. When AI systems generate false positives, fail due to poor infrastructure, or misclassify individuals, human operators often lack the training or authority to intervene, leading to delayed response times and increased vulnerability. The consequence is a security apparatus that is technically present but operationally fragile.

Secondly is the problem of contextual mismatch. Majority of AI security tools currently deployed in Nigeria are imported solutions developed for contexts in the Global North. These systems are trained on datasets that do not reflect Nigeria's demographic diversity, infrastructural realities, or socio-political dynamics. Coupled with erratic power supply, limited internet bandwidth, and low digital literacy among security staff, these tools often malfunction or produce biased outcomes. More critically, there is no institutional framework guiding how human judgment should interface with AI recommendations in decision-making. This absence of structured human-AI interaction creates ambiguity in authority, accountability, and ethical responsibility during security incidents.

Despite the urgency of these issues, there is a paucity of empirical research examining the human-AI nexus in the management of security apparatus within Nigerian tertiary institutions most especially in Delta State. Existing literature focuses either on the technical performance of AI tools or on general perceptions of AI in education, with little attention to how human security managers and AI systems should collaborate to produce effective and sustainable outcomes in resource-constrained environments. This gap limits the ability of University Management, the National Universities Commission, and Education Policymakers to make evidence-based decisions on AI adoption, training, and governance in campus security.

Consequently, tertiary institutions in Delta State, Nigerian risk investing heavily in AI technologies that fail to deliver expected security improvements, while simultaneously devaluing the contextual knowledge and ethical reasoning of human security personnel. Without a framework that explicitly defines the roles, decision-sharing protocols, and capacity requirements for hybrid human-AI security management, the digital transformation of campus security will remain disjointed, inefficient, and potentially counterproductive.

It is against this background that this study seeks to address the problem: How can human judgment and artificial intelligence be optimally integrated to manage security apparatus in tertiary institutions in Delta State, Nigeria in the digital age? Answering this question is essential for developing a Hybrid Intelligence Framework that leverages the strengths of both humans and AI while mitigating their limitations, thereby ensuring effective, ethical, and sustainable security management in Nigerian Higher Education.

Aim and Objectives of the Study

The main purpose of this paper is to examine Augmenting Human Judgment: A hybrid intelligence framework for managing security apparatus in Nigerian tertiary institutions in the digital age. Specifically, the study seeks to:

1. To examine the current state of human-AI interaction in the management of security apparatus in Nigerian tertiary institutions.
2. To develop and validate a Hybrid Intelligence Framework that optimizes the integration of human judgment and AI capabilities for sustainable campus security management.

Research Questions

The following research questions will guide the study:

1. What is the extent and type of AI tools currently deployed in security management across tertiary institutions in Delta State, Nigeria?
2. What are the institutional, technical, and human factors that enable or hinder effective human-AI collaboration in security contexts?

Review Related Literature

Conceptual Framework

The framework is built on the premise that neither human security managers nor AI systems alone are sufficient for managing security in resource-constrained, high-threat environments like tertiary institutions in Delta State, Nigerian. Instead, security effectiveness emerges from the synergistic interaction between human cognitive strengths and AI computational strengths. This aligns with the broader concept of Hybrid Intelligence (HI). That is, Natural and Artificial Intelligence working together, amplifying strengths and compensating for weaknesses.

Conceptual Clarifications

The following concepts will be briefly explain here to avoid conceptual error or intellectual miscarriage:

Hybrid Intelligence

The conceptual framework for this study positions Hybrid Intelligence (HI) as the central mechanism for optimizing security management in tertiary institutions in Delta state, Nigeria in the digital age. Hybrid Intelligence refers to systems in which human and artificial intelligence work together to achieve complementary team performance that neither could reach alone, with AI extending rather than replacing human judgment. In the context of campus security, this means AI functions as a cognitive prosthetic that amplifies detection, pattern recognition, and response speed, while human security managers provide contextual interpretation, ethical reasoning, and accountability.

Hybrid Intelligence and Human-AI Interaction

Recent scholarship on human-AI collaboration emphasizes that effectiveness depends on how humans and AI interact, not just on technical accuracy. Three mechanisms are critical collaborative HI, where tasks are dynamically allocated between human and AI; governance-oriented HI, where human-defined ethics and regulations are translated into AI preconditions; and trust calibration, where reliance on AI matches its actual reliability. A 2025 framework for Security Operations Centers operationalizes this through tiered AI autonomy levels mapped to Human-in-the-Loop roles and task-specific trust thresholds, showing that adaptive human oversight reduces alert fatigue and enhances response coordination. Applied to tertiary institutions in Delta State, Nigeria, this suggests security effectiveness is not driven by AI alone, but by the quality of human-AI interaction during threat detection, alert triage, and incident response.

AI in Education and Security Management

The push for AI in Education in Nigeria is already underway. TETFund has announced plans to establish Centres of Excellence in Robotics, AI, Machine Learning, and Cybersecurity across six universities, explicitly linking the initiative to addressing issues around national security and building skills to fill knowledge gaps. This creates an institutional window to embed hybrid intelligence principles into campus security rather than defaulting to full automation. Studies on AI in university security contexts note benefits in threat detection and

resource optimization, but also highlight challenges of infrastructure deficits, privacy risks, and lack of training for security staff.

Nigerian Universities as the Context

Nigerian tertiary institutions operate under resource constraints, erratic power supply, and diverse socio-political realities that differ from contexts where most AI security tools are developed. Without a framework guiding the human-AI nexus, institutions risk over-reliance on imported AI systems that fail under local conditions, while marginalizing the contextual knowledge of human security personnel. The proposed framework therefore integrates:

The framework predicts that AI capability positively influences security outcomes only when mediated by effective human-AI collaboration mechanisms, and that institutional support strengthens this relationship. This aligns with evidence that human-AI complementarity requires interpretability, governance, and training to achieve superior team performance.

Theoretical Framework

For the study on Augmenting Human Judgment: A Hybrid Intelligence Framework for Managing Security Apparatus in Nigerian Tertiary Institutions, two theories fit well because they explain how humans learn to work with new tools and how technology adoption happens in organizations. Here are the two theories with direct links to the topic:

Sociocultural Theory

Lev Vygotsky postulated Sociocultural Theory. He developed it between the 1920s and 1930s in the Soviet Union. His key work, 'Mind in Society' was published posthumously in 1962 in English, which is when the theory became widely known outside the USSR. It positioned that learning and cognition occur through social interaction and mediation by cultural tools. Vygotsky's concept of the "Zone of Proximal Development" argues that humans achieve more when supported by tools or more capable others than they can alone.

Hybrid Intelligence treats AI as a cultural tool that mediates security work, not as a replacement for the human. In Nigerian universities, security managers operate within a social system of protocols, hierarchies, and local knowledge. AI acts as a more capable other that can flag patterns or anomalies, while the human provides judgment, context, and accountability. This aligns with recent HI research showing that robots or AI in learning and security environments create a synergistic effect where teachers, students, and AI machines work together. For your framework, Vygotsky explains why human-AI collaboration should

be structured as shared activity. The AI extends human capability and the human guides AI use within institutional norms.

Technology Acceptance Model (TAM)

Fred Davis postulated the Technology Acceptance Model (TAM). He first introduced it in his 1986 PhD dissertation at MIT Sloan School of Management. The seminal journal article, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", was published in MIS Quarterly in 1989.

According to him, actual use of technology is predicted by perceived usefulness and perceived ease of use. If users don't trust or find the tool easy to integrate into workflow, adoption fails. TAM has been applied in recent AI-driven security frameworks for smart cities to emphasize that "user engagement" and "human interaction with AI" are critical for effectiveness. In Nigerian tertiary institutions, security staff must perceive AI tools as useful for threat detection and as tools they can control and understand. Without trust calibration, training, and clear role definitions, AI becomes either ignored or over-relied upon the exact problem your framework seeks to solve. TAM therefore justifies why your Hybrid Intelligence Framework must include training, explainability, and governance mechanisms: these drive perceived usefulness and ease of use, which in turn determine whether human-AI collaboration improves security outcomes.

DISCUSSION OF FINDINGS

The discussion below interprets the expected findings of the study based on the proposed Hybrid Intelligence Framework for managing security apparatus in Nigerian tertiary institutions.

Hybrid Intelligence and Security Decision Quality

Findings are expected to show that institutions with higher levels of Human-AI Collaboration Mechanisms – role clarity, explainability, and trust calibration report significantly better security decision quality. This supports the core premise of the framework: AI alone does not improve campus security; improvement occurs when AI is integrated as a cognitive partner. This aligns with Vygotsky's Sociocultural Theory, which positions tools as mediators that extend human capability within the Zone of Proximal Development. Where security managers can interpret AI alerts, question outputs, and retain override authority, they are likely to use the technology effectively. Conversely, where AI is treated as a "black box" or

as a replacement for human judgment, decision quality is expected to decline due to overreliance or underuse.

Mediating Role of Human-AI Interaction

The study anticipates that the relationship between AI Capability and Security Decision Quality will be fully or partially mediated by Human-AI Interaction Mechanisms. This means that merely having advanced AI tools is insufficient. The presence of clear role definitions, transparent AI outputs, and calibrated trust is what converts AI capability into improved threat detection and response. This finding would extend Technology Acceptance Model logic beyond individual adoption to team-level performance: perceived usefulness and ease of use matter not only for adoption, but for effective collaboration.

Moderating Effect of Institutional Support and Resource Readiness

Results are likely to reveal that Institutional Support and Resource Readiness significantly moderate the HI-Decision Quality relationship. In institutions with stable power, reliable internet, training programs, and clear governance policies, the positive effect of Hybrid Intelligence on security outcomes will be stronger. In resource-constrained settings, the same AI tools may yield weak or even negative effects due to system downtime, poor maintenance, or lack of training. This finding mirrors recent reports from Delta State, where rising enrollment and expansion of tertiary institutions have strained infrastructure, making resource readiness a critical enabler.

Implications for Nigerian Tertiary Institutions

The discussion points to a practical shift: security budgeting in tertiary institutions in Delta State, Nigerian must move from buying equipment to building capability. Procurement of CCTV, facial recognition, or analytics software without investment in training, governance, and infrastructure will not deliver results. Security managers need to be upskilled to work alongside AI, and institutions need policies that define accountability when AI flags a threat.

Summary

This study proposed and conceptualized on Augmenting Human Judgment: A Hybrid Intelligence Framework for Managing Security Apparatus in Nigerian Tertiary Institutions in the Digital Age. It argued that effective campus security requires more than the deployment of AI tools; it demands a structured collaboration between human security managers and artificial intelligence. Grounded in Vygotsky's Sociocultural Theory and Davis's Technology

Acceptance Model, the framework positions AI as a cognitive extension that augments threat detection and decision speed, while human judgment provides context, ethics, and accountability. The study identified Human-AI Interaction mechanisms – role clarity, explainability, and trust calibration as mediators of security decision quality, with institutional support and resource readiness acting as moderators.

CONCLUSION

Tertiary institutions in Nigeria but Delta State in particular face evolving security threats that outpace traditional manual systems, yet full automation risks loss of contextual judgment and accountability. The Hybrid Intelligence Framework offers a middle path. AI enhances data processing and pattern recognition, while human managers retain control over ethical and strategic decisions. For this partnership to work, institutions must move beyond technology procurement and invest in governance, training, and trust-building. Without these, AI adoption in campus security will underperform or be resisted.

Recommendations

The following recommendations were made for the study:

1. University management and NUC should integrate HI principles into campus security policy, clearly defining AI as a decision-support tool, not a replacement for human officers.
2. Security staff must receive continuous training on AI tool use, interpretation of AI outputs, and override protocols to build competence and trust.
3. Government and University management should prioritize stable power, internet connectivity, and maintenance budgets to sustain AI security infrastructure.
4. AI tools deployed must provide transparent outputs, and institutions should establish oversight committees to monitor ethical use and data privacy.

Suggestions for Further Studies

1. Future research should test the proposed framework empirically across multiple Nigerian geopolitical zones to validate the moderating role of institutional support.
2. A comparative analysis between public and private tertiary institutions, or between Nigerian and other African universities, could reveal context-specific enablers and barriers to HI in security.
3. Longitudinal studies are needed to assess how Hybrid Intelligence directly affects measurable outcomes such as response time, crime reduction, and cost efficiency.

REFERENCES

1. Agu, A. A. (2007). *Research methodology: A practical approach to project writing* (1st ed.). Najutel Nigeria Limited.
2. Alordiah, O. C., & Tony, O. A. (2016). *Introduction to research methods*. Cee-Emmyiyke Ventures.
3. Ayeni, P., & Fakunle, K. (2018). *Education law and politics of education in Nigeria* (1st ed.). Chadik Printing Press.
4. Baltrusch, S. J., et al. (2024). Augmented Intelligence Framework for Human–Artificial Intelligence Teaming in Cybersecurity. Human-Centric Intelligent Systems. Springer.
5. Hemmer, P., et al. (2021). Human-AI Complementarity in Hybrid Intelligence Systems_. _PACIS Proceedings.
6. Idowu, A. O., & Oladipo, O. (2024). Leveraging on Artificial Intelligence for Effective Provision of Security Services in Nigerian Universities_. Zenodo.
7. Mohsin, A., et al. (2025). A Unified Framework for Human–AI Collaboration in Security Operations Centers with Trusted Autonomy_. arXiv:2505.23397v2.
8. Sauer, C. R., & Burggräf, P. (2024). Hybrid intelligence systematic approach and framework to determine the level of Human-AI collaboration. Production Engineering_.
9. Tertiary Education Trust Fund. (2025). Insecurity: TETFund spearheads development of security master plan for tertiary institutions. Vanguard.