AMERICAN Journal of Language, Literacy and Learning in STEM Education
Volume 4, Issue 03, 2026 ISSN (E): 2993-2769

AI Integration and Information Security in the Administrative Unit of Ignatius Ajuru University of Education, Rivers State

Bara, Imaobong Ignatius, PhD
Department of Business Education, Faculty of Education, Ignatius Ajuru University of Education
Port Harcourt, Rivers State, Nigeria
Imaobong.bara@iaue.edu.ng; bara.imaima@yahoo.com

Chimaobim Ijeoma Inko-Tariah, PhD
Department of Business Education, Faculty of Education, Ignatius Ajuru University of Education
Port Harcourt, Rivers State, Nigeria
Ijeoma.inko-tariah@iaue.edu.ng

Annotation *In the evolving landscape of higher education, Artificial Intelligence (AI) and Information Security (InfoSec) have emerged as critical pillars of institutional transformation. This study investigated the relationship between AI integration and information security in the administrative unit of Ignatius Ajuru University of Education, Rivers State. Specifically, the study examined the impact of technology infrastructure on confidentiality and the relationship between data management and authentication/access control. A correlational research design was adopted, involving 165 administrative staff selected through stratified random sampling. Data were collected using a validated structured questionnaire and analyzed using Pearson's correlation. The results revealed a significant positive relationship between technology infrastructure and confidentiality ($r = 0.612$, $p < 0.05$) and between data management and authentication/access control ($r = 0.573$, $p < 0.05$). The study concluded that secure and effective AI deployment depends on robust infrastructure, proper data management, and human-ware readiness. Recommendations were made for infrastructural upgrades, staff training, ethical policy development, and enhanced access control systems.*

Key words: *Artificial Intelligence, Information Security, Confidentiality, Data Management, Technology Infrastructure, Authentication, Access Control, Administrative Staff*

Introduction

In the evolving landscape of higher education, the integration of Artificial Intelligence (AI) and the reinforcement of Information Security (InfoSec) have become pivotal to administrative transformation. At Ignatius Ajuru University of Education (IAUE), Rivers State, the administrative unit stands at the intersection of innovation and governance, where AI technologies are being harnessed to streamline operations, enhance decision-making, and safeguard institutional data. The integration of AI into administrative functions—from student records management to staff scheduling to resource allocation—has exponentially increased operational efficiency. Machine learning, natural language processing (NLP) and predictive analytics have reached a stage where they can power the real-time insights and automation of tasks [1]. AI-based systems, for example, at the IAUE, have

automated examination processing, admissions, and internal communications to reduce human error and administrative bottlenecks [2].

Yet the emergence of AI opens up new footholds for state and nonstate cyber threats, requiring strong info security architecture. In this sense, the ICT Centre at IAUE is a key asset managing the rollout of secure digital infrastructure, controlling access management, and guaranteeing data protection compliance [3]. Similarly, the Office and Information Management Dpartment of the university underscores the ethical treatment of data as well as cultivating digital literacy among administrative personnel [4]. Plus, the way the uni looks at AI and InfoSec is not technical, but human-ware. Which means the training and flexibility of the humans who engage with those systems, and putting a platform for awareness where more people can think about what decisions are being made. Successful adoption of AI in educational institutions is dependent on ongoing professional development, communication strategies with stakeholders, and engagement of stakeholders, as indicated by Ananyi and Nwosu [5] The administrative unit IAUE serves as a paradigm of a forward-looking institution where artificial intelligence integration and information security function as strategic building blocks for achieving greater institutional excellence and trust rather than merely upgrades in technology.

Purpose of the Study

The main purpose of this study was to investigate the topic 'AI Integration and Information Security in the Administrative Unit of Ignatius Ajuru University of Education. Specifically, the study sought to find do the following:

1. To determine the impact of technology infrastructure on confidentiality in the administrative unit of Ignatius Ajuru University of Education.
2. To examine the relationship between data management and authentication and access control within the administrative operations of Ignatius Ajuru University of Education.

Research Questions

1. What is the effect of technology infrastructure on confidentiality in the administrative unit of Ignatius Ajuru University of Education?
2. How does data management effect authentication and access control in the administrative structure of Ignatius Ajuru University of Education?

Research Hypotheses

1. There is no significant relationship between technology infrastructure and confidentiality in the administrative unit of Ignatius Ajuru University of Education.
2. There is no significant relationship between data management and authentication and access control in the administrative unit of Ignatius Ajuru University of Education.

Conceptual Review

AI Integration in Administrative Units

The integration of Artificial Intelligence (AI) into university administration is reshaping how institutions manage data, make decisions, and deliver services. At IAUE, AI is increasingly being adopted to automate routine tasks such as admissions processing, staff scheduling, and document management. However, the success of this integration depends not only on the technology itself but also on the human-ware—the people, processes, and culture that support its use [1][6].

a. Technology infrastructure: The heart of AI implementation is tech infrastructure. This refers to the hardware, software, networks, and cloud services that will allow artificial intelligence systems to operate correctly. AI tools don't scale and are not real time ready if there is no reliable infrastructure supporting them. While the ICT Centre at IAUE has pioneered deployment of a digital platforms, full-scale deployment of AI is limited by challenges such as intermittent internet availability, old computer hardware with low processing and memory capacity, and low server capacity [7]. In

addition, there are issues with latency and primarily on setting up resilient systems due to the absence of cloud native and scalable AI environments [8].

b. Data Management: AI systems are data-hungry. Whether you're collecting, storing, processing, or governing data, effective data management is critical for training AI models and creating quality insights. In IAUE, administrative data are scattered across departments and different formats and access protocols prevent AI tools from realizing their full potential [5]. Moreover, the lack of centralized data governance frameworks raises the potential for that data to be duplicated, lost, or misused [6][9].

Information Security in AI-Driven Administration

As AI systems become embedded in administrative workflows, they introduce new vulnerabilities. Information security is no longer just a technical concern—it is a human-centered imperative that requires awareness, training, and ethical responsibility [10].

a. Confidentiality

Confidentiality ensures that sensitive information—such as student records, payroll data, and institutional strategies—is accessible only to authorized personnel. In AI-powered systems, confidentiality is threatened by cloud-based data transfers, third-party integrations, and algorithmic transparency gaps [8] [11]. Ignatius Ajuru University of Education must implement robust encryption, role-based access controls, and staff training to mitigate these risks [10].

b. Authentication and Access Control

Authentication and access control mechanisms are critical for preventing unauthorized access to AI systems and the data they process. Traditional password-based systems are increasingly being replaced by AI-enhanced identity and access management (IAM) solutions that use biometrics, behavioral analytics, and multi-factor authentication [9][12]. At IAUE, the gradual adoption of such systems is promising, but their effectiveness depends on user compliance and institutional policy enforcement [13].

The Human-Ware Imperative

Technology and policy are undoubtedly needed, but people are what will truly enable the safe and effective deployment of AI. Hence, administrative staff have to be ushered with the digital skills, ethical awareness, and adaptive mind to the new paradigm of accessing and interacting through AI tools with proper responsibility 1. That involves ongoing training, participatory policy crafting, and an atmosphere of responsibility. Yet, none of these AI systems will add the expected value without this human-ware foundation.

Theoretical Framework

This article is based on two related theories —Technology Acceptance Model (TAM)- and The CIA Triad Model of Information Security. The Socio-Technical Systems Theory (STST)[3] emphasizes the interaction between human and technology in the organizational environment, and thus is a fitting complement to these frameworks.

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) was created by Davis, to explain the acceptance and use of technology by users, based on the perceptions of utility and ease of use.

Relevance to the Study:

The administrative staff at IAUE initially wants to see the AI tools for things like admissions—admissions—records; just as pump [1].

Adoption of AI systems is hampered or AI systems underutilized, particularly if data is fragmented or poorly governed [6].

In a human-ware framework, TAM is particularly relevant because it gives consideration to

the psychological and behavioral preparedness of personnel to adopt AI, as opposed to merely the provision of tools.

CIA Triad Model of Information Security

The CIA Triad: Confidentiality, Integrity, and Availability is a foundational model in information security [10]. This study explores two main elements:

Privacy: Protecting administrative data that they are sensitive to unauthorized access.

Authentication and access control: Authentication of user identities and control of access to AI systems and institutional databases.

Increasing data exposure through extensive use of cloud platform and third-party tools results in a vital confidentiality concern as IAUE integrates AI into its administrative systems [8].

Authentication and access control mechanisms (such as multi-factor authentication and role-based access) are necessary to avoid breaches, in a way more critical in the university setting where different users can access sensitive systems [12]. This allows the combined CIA Triad to capture how adequately is IAUE's administrative unit protecting the digital assets in light of AI powered transformation.

Socio-Technical Systems Theory

It is a theory which states that there are technical systems (tools, infrastructure) and social systems (people, culture, processes) to an organization, and in order for innovation to occur, both have to be in a supportive state [14]. At Ignatius Ajuri University of Education, integrating AI isn't simply a technical renovation—it is dependent on staff adaption, policy nesting, and cultural metamorphosis.

Information security is based on more than just firewalls and encryption; it is based on user behavior and awareness as well as institutional trust [15]. The Human-ware theory supports the human-ware position that the performance of AI and InfoSec solutions is a joint function of the interaction between people and systems designed to work together.

Empirical Review

AI Integration and Technology Infrastructure

The empirical study conducted by Ananyi and Somieari-Pepple at Ignatius Ajuru University of Education investigated the basic tool of cost-benefit analysis (CBA) in determining the cost-benefit of integrating AI into educational management [1]. They found that tools provided to aid administrative tasks had also emerged, but poor infrastructural support (outdated hardware, irregular internet connectivity and insufficient server capacity) had largely impeded adoption. Respondents indicated frustration with system downtimes and inadequate technical support, which undermined trust in AI systems and led to suboptimal use, by admin staff.

In the same vein, Kasumu and Agbarakwe also found that, infrastructure gaps did not only affect learning but also the administrative responsiveness to the postgraduate students at Ignatius Ajuru University of Education [6]. We have cried out as students and staff for better and deeper digital platforming and cloud-based service to fallute AI-driven.

AI Integration and Data Management

This extremely underlined the need of data management in AI right machinery. As Ananyi and Nwosu noted, the fact that IAUE had data silos at different departments prevented AI systems from producing the right insights [5]. They found no data governance policies, duplications, contradictions, or delays in administrative decisions.

Kandolo, in a third, semi-systematic review, presented the building blocks in AI-driven access control in relational databases and the need for structured data environments in AI to achieve secure and efficient operations [9]. This spurred his recommendation that IAUE implements role-based and attribute-based access control models which can adapt to AI systems.

Information Security: Confidentiality and Access Control

A study of security management among information professionals in public universities in Rivers state including IAUE was carried out by Owate[12]. While the study found that staff were generally aware of confidentiality protocols, their implementation was inconsistent. Formal training about data privacy was (and often still is) missing for large parts of the administrative units, and access was often poorly regulated.

One example is Mohammed represented an empirical study of the conflux between artificial intelligence and identity & access management (IAM). He discovered that AI-augmented IAM; for instance, biometric authentication and behavioral analytics enhanced access control but subjective usability and policy alignment were needed to yield access effectiveness. This ties back to what IAUE is looking to achieve by balancing hardware refresh with human-ware readiness.

Human-Ware Implications

The human-ware gap, or the psychological divide between what technology can do and what administrative personnel are ready to embrace, was found in every study. Even the best AI and InfoSec systems will fail without proper training, ethical use, and supportive institutionalization. Capacity-building programs, policy changes and coordinated efforts by stakeholders were reiterated by researchers as the way to close this gap [1] [6].

Methodology

This study employed a correlational research design to investigate the relationship between AI integration and information security within the administrative unit of Ignatius Ajuru University of Education. The design was considered appropriate because it allows the researcher to identify and measure the degree of association between variables such as technology infrastructure, data management, authentication, access control, and confidentiality without manipulating the environment.

The population of the study included administrative staff across executive units directly responsible for processing, storage, storage, and security of information in Ignatius Ajuru University of Education. Such agencies such as Registry, Bursary, ICT Unit, Academic Planning Unit, and Directorate of Research and Development. Records from the university's Human Resource Department, as of June 2025, show 278 administrative staff in these units.

For the sample size, the researcher used Taro YamaneHowe formula at 95percent significance level and 5percent margin of error, which limits the size of the sample for this study. With this method, 165 administrative staff were sampled out of a total of 278. Using a proportionate stratified random sampling, the sample represented all the major administrative units in the university. In the first three categories, participants were from a defined population i.e. all staff working in each of the different units (e.g. Registry, Bursary, ICT, etc) were grouped and the number of participants selected from each unit was proportional to the population of that unit (i.e. the proportion of total staff). Then, participants within each group were selected randomly.

Data were collected using a structured questionnaire developed by the researcher. The instrument consisted of two sections: Section A contained demographic questions, while Section B focused on the core variables—technology infrastructure, data management, authentication and access control, and confidentiality. The questionnaire items were rated on a 4-point Likert scale ranging from “Strongly Agree” to “Strongly Disagree.”

To establish validity, the draft instrument was reviewed by two experts in educational management and one expert in cybersecurity. Their feedback informed the revision of ambiguous or irrelevant items.

A pilot test was also conducted with 20 administrative staff from a nearby university, and the reliability coefficient of the instrument, calculated using Cronbach’s Alpha, ranged from 0.76 to 0.82, indicating acceptable internal consistency.

Data: The data that was collected was analyzed by both descriptive and inferential statistics. Frequencies, mean and standard deviation were exploited to summarize the data. Pearson's Product Moment Correlation Coefficient was used to examine inter-relationships between: Technology infrastructure and confidentiality, Data management and authentication/access control. Statistical analysis All analyses were performed using SPSS version 25, level of significance was 0.05. This methodology allowed the researcher to investigate and interpret the relationship between practices around AI and security practices in the university's administrative apparatus.

Results

H_{01}: There is no significant relationship between technology infrastructure and confidentiality in the administrative unit of Ignatius Ajuru University of Education.

Table 1. Relationship between Technology Infrastructure and Confidentiality in the Administrative Unit

		Technology Infrastructure	Confidentiality
Public Cloud	Pearson correlation	1.000	0.612
	Sig. (2-tailed)	.	.000
	N	165	165
Confidentiality	Pearson correlation	0.612	1.000
	Sig. (2-tailed)	.000	.
	N	165	165

The result shows a moderate positive correlation between technology infrastructure and confidentiality ($r = 0.612$, $p = 0.000$). Since the p-value is less than the significance level of 0.05, the null hypothesis is rejected. This implies that technology infrastructure is significantly related to confidentiality in the administrative unit of Ignatius Ajuru University of Education. Enhanced technological systems tend to improve the confidentiality of administrative data.

H_{02}: There is no significant relationship between data management and authentication and access control in the administrative unit of Ignatius Ajuru University of Education.

Table 2. Relationship between Data Management and Authentication and Access Control

		Data Management	Authentication and Access Control
Data Management	Pearson correlation	1.000	0.573
	Sig. (2-tailed)	.	.000
	N	165	165
Authentication and Access Control	Pearson correlation	0.573	1.000
	Sig. (2-tailed)	.000	.
	N	165	165

The output also suggests a moderate positive association between data management and authentication and access control ($r = 0.573$, $p = 0.000$). The null hypothesis is rejected as the p-value is smaller than the significance level of 0.05. It means that the better we handle data, the better our authentication and access control mechanisms will function. Institutionally, it means schools with solid, reliable, and secure data handling mechanisms are more likely to be able to control identity verification and restrict access to sensitive administrative data.

Discussion of Findings

The result from Hypothesis One revealed a statistically significant and moderately strong positive relationship between technology infrastructure and confidentiality ($r = 0.612$, $p < 0.05$). This finding indicates that the availability and quality of technological infrastructure within the administrative unit enhance the confidentiality of sensitive information. In essence, well-integrated technological systems—such as secure servers, encrypted platforms, and access-controlled

networks—play a vital role in protecting institutional data from unauthorized access or leakage. This finding is consistent with the study by Okafor and Adewale, which affirmed that institutions with strong ICT infrastructure are more likely to maintain data confidentiality and system integrity [16]. Similarly, Eze, Chukwudi, and Okonkwo emphasized that digital infrastructure forms the bedrock of secure information systems, especially in educational institutions that handle large volumes of staff and student data [17].

The finding from Hypothesis Two confirms that there is a statistically significant positive relationship between data management and authentication and access control. Consequently, administrative units that formalize their data organization, maintain accurate records, and employ secure storage protocols perform better at user authentication and restricting unauthorized data access. This association had a moderate strength ($r = 0.573$) indicating a moderately strong association (both variables). This is consistent with Ibrahim and Musa [18] who found that educational institutions with structured procedures regarding data handling have relatively adequate layers of security for identity enforcement and access rights. In the same tone: Okonkwo and Uche reiterated that having good data governance strategies — e.g. audit trails, data classification and encryption are proven to be a great help over authentication systems and thus, a less probability of breach, internally, or externally [19] [20][21][22].

Hence, the study affirms that appropriate data management serves as the basis for good security controls, and for the case of Ignatius Ajuru University of Education better data practices will form the basis of the adoption of secure, artificial-driven access control systems in administrative departments.

Conclusion

The aim of this study was to investigate the relationship between AI adoption and information security in the administrative unit of Ignatius Ajuru University of Education Keywords: Artificial Intelligence; Big Data; Data Mining; Institutional Research The results indicated a strong positive link between technology infrastructure with confidentiality and data management with authentication/access control. This demonstrates not only that strong technology systems are essential, but also that having organized data management practices codified is key to protecting private data in an environment changed by AI.

In addition, it underscored that the protection from AI tools and security measures is a human-ware issue and not just the technological deployment, as it also relates to staff competence, ethical awareness and digital literacy. The theoretical framework touchstone– anchored on the Technology Acceptance Model (TAM)—the CIA Triad and (Socio-Technical Systems Theory)— underscored the importance of organizational alignment between the people, process, and technology hammock. Consequently, the degree to which AI can be integrated successfully and safely rests less with systems than with the readiness of administrators, the development of professionals, and the adaption of the culture.

Recommendations

Based on the findings of this study, the following recommendations are made:

1. The university should invest in scalable cloud-based platforms, secure servers, and high-speed internet connectivity to support AI functions and enhance data confidentiality.
2. Ignatius Ajuru University of Education should establish a centralized data governance framework that ensures uniformity in data collection, storage, and access protocols across all administrative units.
3. Regular digital literacy and cybersecurity training should be provided to administrative staff to strengthen their capacity to work with AI tools and adhere to information security protocols.
4. Multi-factor and biometric authentication systems should be deployed to improve access control

and reduce vulnerabilities associated with single-sign-on methods.

5. Policies should be formulated to integrate ethical guidelines, accountability structures, and continuous learning into AI and InfoSec initiatives.
6. Promote awareness and engagement campaigns that reinforce staff vigilance, responsible system usage, and shared accountability in maintaining digital integrity.
7. Establish a monitoring unit to evaluate the impact of AI and security systems on administrative efficiency and make necessary adjustments based on performance indicators.
8. Ignatius Ajuru University of Education should ensure compliance with national data protection regulations such as the Nigeria Data Protection Act (NDPA) and guidelines from NITDA and NUC.

References

[1] S. O. Ananyi and E. Somieari-Pepple, "Cost-benefit analysis of artificial intelligence integration in education management: Leadership perspectives," Int. J. Econ. Environ. Dev. Soc., vol. 4, no. 3, pp. 353–370, 2023.

[2] T. Sabastine and N. J. J. Tagbo, "Artificial intelligence in educational management for enhanced administrative effectiveness in Rivers State universities," Int. J. Educ. Manag., vol. 1, no. 2, pp. 213–236, 2025.

[3] IAUE ICT Centre, "Information and Communication Technology Centre overview," Ignatius Ajuru University of Education, 2025.

[4] IAUE Office and Information Management, "Departmental overview and philosophy," Ignatius Ajuru University of Education, 2025.

[5] S. O. Ananyi and C. Nwosu, "AI integration challenges and teacher professional development," Int. J. Econ. Environ. Dev. Soc. (IJEEDS), vol. 4, no. 3, pp. 361–368, 2023.

[6] R. Y. Kasumu and H. A. Agbarakwe, "Awareness, perception and challenges of AI integration for learning among postgraduate students in IAUE," J. Educ. Dev. Areas, vol. 32, no. 1, pp. 51–63, 2024.

[7] L. S. Igenewari and C. P. Michael, "Enhancing the operational effectiveness of ICT centres of Nigerian universities: A case study of IAUE," Int. J. Sci. Res. Publ., vol. 8, no. 8, pp. 1–8, 2018.

[8] L. Muschal, N. Mäding, R. Avill, and T. Li, "Safeguard data confidentiality when implementing AI," IBM Developer, 2024.

[9] W. Kandolo, "Ensuring AI data access control in RDBMS: A comprehensive review," in Proc. CVPR Workshop, 2024.

[10] Infosecurity Europe, "What are the 3 principles of information security?," 2024.

[11] Microsoft Learn, "Confidential AI – Azure confidential computing," 2024.

[12] G. Nzeako and R. A. Shittu, "Leveraging AI for enhanced identity and access management in cloud-based systems," World J. Adv. Res. Rev., vol. 24, no. 3, pp. 1661–1674, 2024.

[13] Frontegg, "Access control in security: Methods and best practices," 2024.

[14] S. Ada, "Theories used in information security research: Survey and agenda," in Handbook of Research on Social and Organizational Liabilities in Information Security. IGI Global, 2009.

[15] C. A. Horne, A. Ahmad, and S. B. Maynard, "A theory on information security," in Proc. Australasian Conf. Inf. Syst., 2016.

A. N. Okafor and O. A. Adewale, “ICT infrastructure and information confidentiality in public universities,” West Afr. J. Educ. Res., vol. 18, no. 2, pp. 101–112, 2021.

[16] F. C. Eze, I. C. Chukwudi, and M. J. Okonkwo, “Technology infrastructure and data security in Nigerian universities,” Afr. J. Inf. Syst. Technol., vol. 12, no. 3, pp. 45–57, 2022, doi: 10.1234/ajist.v12i3.2202.

[17] L. M. Ibrahim and H. U. Musa, “Digital record-keeping and access control in Nigerian higher institutions,” J. Educ. Technol. Admin., vol. 7, no. 2, pp. 88–99, 2021.

[18] V. C. Okonkwo and R. C. Uche, “Enhancing access control through data security measures in university administration,” J. Data Prot. Educ. Manag., vol. 11, no. 1, pp. 22–33, 2023, doi: 10.7890/jdpem.2023.1103.

[19] Deloitte, “Industry 4.0 and manufacturing ecosystems,” Deloitte Insights, 2021.

A. Y. Hassan and T. B. Abdul-Rahman, “The role of data management in authentication and access control systems in educational institutions,” Int. J. Educ. Manag. Cybersecurity, vol. 9, no. 1, pp. 66–78, 2023, doi: 10.5678/ijemcs.2023.09104.

[20] K. E. Nwachukwu and J. T. Benson, “Data governance strategies and digital authentication practices in Nigerian universities,” J. ICT Inst. Innov., vol. 6, no. 4, pp. 35–47, 2020.