VOL. 09 NO. 9,
AUGUST, 2025
E-ISSN 3026-958X
P-ISSN 3027-1169

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Science Innovation & Technology Research (JSITR)

Enhancing Security and Privacy in EdTech Tools: Safeguarding Student Data in the Digital Learning Era

Binitie Amaka Patience; Onyemenem Sunday Innocent; & Okoh Felix Jigiedous

Computer Science Department, Federal College of Education (T) Asaba
Corresponding Author: philpat4sure@gmail.com
DOI: https://doi.org/10.70382/ajsitr.v9i9.041

Abstract

The rapid shift to digital learning during and after the COVID-19 pandemic has led to widespread adoption of educational technologies (EdTech) in higher education, including in Nigeria. This trend, while improving access and flexibility, raises serious concerns about the security and privacy of sensitive student data. In Nigeria's context, these concerns are compounded by nascent legal frameworks and varying awareness among stakeholders. This study investigates the security and privacy issues faced by undergraduate students using EdTech tools in Delta State, Nigeria, aiming to identify key threats and propose measures to protect student data. A cross-sectional survey was administered to a sample of Delta State undergraduates, gathering perceptions of security risks, privacy awareness, and recommended safeguards. Descriptive statistics (mean and standard deviation) were computed for questionnaire items related to three research questions. The results indicate high levels of student concern about data breaches and unauthorized access limited trust in privacy practices and awareness of data protection laws, and strong support for institutional measures like encryption and training to improve security. These findings are consistent with global literature on EdTech vulnerabilities. The study concludes that stakeholders in Nigerian higher education must urgently implement robust data protection policies, technical safeguards, and awareness programs to uphold student privacy. Recommendations include enforcing Nigeria's new Data Protection Act, training faculty and students on privacy rights, and adopting privacy-by-design approaches in EdTech deployment.

Keywords: EdTech, Data breach, privacy, security, vulnerabilities, higher education.

Introduction

Educational technology has transformed higher education, offering flexible and personalized learning opportunities. During the COVID-19 pandemic, students and instructors "abruptly shifted from the classroom to an online mode of learning," leading to an explosion of cloud-based tools, apps, and platforms that are now embedded in the learning experience. However, this rapid digitization has also introduced significant cybersecurity and privacy challenges. Globally, cyber threats in education (ransomware, phishing, unauthorized data harvesting, etc.) have escalated, exposing student information to risks. UNESCO reported that by 2022 about 5% of global ransomware attacks targeted the education sector, increasing the risk of identity theft and data breaches. Similarly, Adeyemo *et al.* (2025) noted that the "unprecedented shift to digital learning platforms" left institutions storing vast amounts of sensitive student data "while frequently lacking robust security measures," making students "particularly susceptible" to breaches and cyberattacks (Binitie et al., 2013).

In Nigeria, these issues are especially pressing. The expansion of online and hybrid learning (often driven by necessity) has outpaced the development of data protection policies. A recent review emphasizes that the "rapid growth of online education in Nigeria raises ethical concerns about data privacy and security (Prinsloo & Kaliisa, 2022)," highlighting gaps in consent, transparency, and accountability. Until mid-2023, Nigeria lacked a comprehensive data protection law specific to education; only recently was the Nigeria Data Protection Act (NDPA) 2023 signed into law (June 12, 2023) to establish a regulatory framework. Nonetheless, awareness and implementation of such regulations remain low. Within Nigerian universities, faculty often choose EdTech tools independently, potentially compelling students to accept vendors' privacy policies without institutional oversight. The cumulative effect is that Nigerian higher education institutions face rising cybersecurity threats (malware, phishing, AI-driven attacks, etc.) in their "digitally connected classrooms", while many stakeholders (faculty, administrators, students) lack training on data privacy.

Given this backdrop, it is crucial to examine how undergraduate students perceive security and privacy in EdTech tools, and to identify strategies for safeguarding their data. This study focuses on Delta State, Nigeria, surveying undergraduates to understand their concerns, awareness, and recommendations. The findings will inform educators, policymakers, and EdTech developers on improving privacy protection in Nigerian higher education.

Problem Statement

The integration of EdTech tools in higher education exposes vast volumes of personal and academic data to potential misuse. Students routinely enter sensitive information into learning management systems, assessment platforms, and interactive apps. However, many educational institutions in Nigeria have not yet fully implemented rigorous data protection measures. There is a widespread gap between

EdTech adoption and data governance. Students often accept terms of service from vendors without scrutiny, and faculty lack guidance on privacy compliance. This situation creates a problem. Student data, including demographic details, academic records, and behavioral analytics, may be vulnerable to breaches, unauthorized sharing, or unethical usage. Recent research warns that without informed consent and oversight, student data can be misused, undermining trust in online learning systems (Kelso et al., 2024). In Nigeria's higher education context, the challenge is compounded by low cybersecurity awareness and previous regulatory gaps, though was only recently addressed by the NDPA 2023. Thus, this study addresses the problem of insufficient security and privacy safeguards in EdTech tools, which jeopardize the confidentiality and integrity of student information in the digital learning era.

Aim and Objectives

Aim: To investigate and enhance security and privacy in EdTech tools used by undergraduates in Delta State, Nigeria, in order to safeguard student data.

Objectives

1. Assess undergraduate students' perceptions of security threats such as, breaches and hacking in the EdTech platforms they use.
2. Evaluate students' privacy concerns and awareness regarding collection, use, and protection of their personal data within EdTech systems.
3. Identify the level of awareness among students of relevant data protection policies (example, Nigeria's Data Protection Act) and institutional guidelines.
4. Determine student attitudes toward possible security and privacy measures that could improve data protection in their digital learning environment.

Review of Related Literature

Educational technology has been widely studied for its pedagogical benefits, but concerns about data privacy have grown with its proliferation. Sheridan (2022) notes that while K-12 education often has strong protocols (e.g. FERPA in the U.S.), higher education typically allows faculty autonomy, leading to inconsistent adoption of privacy measures. Sheridan warns that unchecked use of free or ad-hoc EdTech can "compel students to accept the vendor's policies concerning their personal information," potentially eroding data privacy rights. This reflects a broader theme. Many studies find that the rush to implement technology (especially during COVID-19) outpaced governance (Janssen & Van der Voort, 2020). Adeyemo *et al.* (2025) argue that institutions now hold "vast amounts of sensitive student data while frequently lacking robust security measures," exposing students to threats like phishing, ransomware, and unauthorized monitoring. They cite cases like the 2021 Blackbaud breach affecting universities, to show that even well-known universities have experienced serious data incidents (Ulven & Wangen, 2021; Chapman & Maguire, 2022; Marseille, 2020)..

In the African and Nigerian context, privacy in education is gaining attention but still under-

researched. Prinsloo and Kaliisa (2022) conducted a scoping review of privacy laws across 32 African countries and emphasized that student data privacy must become part of institutional fiduciary duty. They found that while many countries are enacting data protection legislation, higher education institutions need to "consider student data privacy when entering into service level agreements with educational technology and platform providers" (Komljenovic, 2022; Jones, 2019). In other words, contractual vigilance is crucial. Similarly, Akinloye (2023) highlighted that Nigerian educational institutions (especially private schools) are often non-compliant with basic data protection norms, despite recent laws. Akinloye's analysis points out that the 1999 Constitution and the 2023 Nigeria Data Protection Act (NDP Act) form the legal foundation for personal data rights in Nigeria, but many schools continue to "collect superfluous personal information" in breach of privacy principles.

Nigerian studies also underscore practical challenges. Bisong *et al.* (2023) systematically reviewed online education in Nigeria and noted multiple ethical concerns, such as informed consent, data retention policies, and transparency are often lacking. They conclude that there are "gaps and challenges" in current practices and stress the need for awareness, policy, and technological solutions. Adedayo *et al.* (2025) focus on cyber threats in Nigerian higher education, identifying risks such as ransomware, spoofing, and AI-enabled plagiarism ("Open AI-giarism") in digitally rich classrooms. They call for ongoing cybersecurity education and stakeholder engagement to combat these threats. These African-context studies illustrate that the issues of student data security and privacy are recognized but not yet fully addressed (Iyawa & Binitie, 2025).

On the technical side, Imohimi (2025) discussed advanced privacy-preserving methods (differential privacy, federated learning, and encryption) in EdTech, noting regulatory lags, especially in the Global South. Imohimi shows that current AI-driven learning platforms often process personal data without strong protection; for example, the ProctorU breach of 2020 highlighted how remote exam proctoring can expose student information. Imohimi's review underscores that without privacy-by-design, AI and analytics in education can lead to data leaks and bias. This work suggests that robust technical frameworks (and training) are needed to safeguard data in modern EdTech systems (Rehan, 2023; Perisic, 2023).

EdTech tools carry significant privacy and security risks, students are often unaware or concerned about these risks, and measures (both policy and technical) are needed. Globally and in Africa, research emphasizes the importance of encryption, audits, data governance policies, and education about privacy rights. However, there is limited research specifically on undergraduates' perceptions in Nigerian universities. This study fills that gap by surveying students in Delta State, linking empirical data to the broader findings from the literature (Binitie & Okoh, 2025).

Research Questions and Hypothesis

Based on the aim and literature gaps, the study poses the following research questions:

1. What security threats and vulnerabilities do undergraduate students in Delta State perceive in the EdTech tools they use?

2. What concerns do these students have about the privacy of their personal and academic data in EdTech platforms, and how aware are they of data protection policies (like the NDPA)?
3. What measures (technical or managerial) do students believe should be implemented to enhance security and privacy in their digital learning environment?

From these questions, we derive the following hypothesis:

Hypothesis: Undergraduate students will exhibit significant concern about their data privacy and security in current EdTech tools, indicating a mean agreement above neutral on related survey items.
This implies, for example, that responses to concern-based items will be statistically above the neutral midpoint (assuming a 1–5 Likert scale), reflecting overall agreement that data protection is insufficient.

Area of Study
The study was conducted in Delta State, located in southern Nigeria. Delta State hosts several higher education institutions, including Delta State University, Abraka (DELSU); Delta State University of Science and Technology, Ozoro (formerly DELSU, Abraka campus); University of Delta Agbor (UNIDEL), and Dennis Osadebay University (DOU), Asaba. These institutions have implemented varying degrees of online learning and EdTech usage. By focusing on Delta State, the research captures a representative mix of urban and semi-urban Nigerian undergraduates who engage with digital learning.

Population, Sample and Sampling Technique
The population for this study comprises all undergraduate students currently enrolled in Delta State's public universities. Based on university enrollment figures, this population is estimated at several thousand. Due to logistical constraints, a sample of 200 students was selected for the survey. The sample included students from different faculties (Education, Sciences, Social Sciences, and Computing) to ensure diverse perspectives. A stratified random sampling approach was employed. First, two major universities (UNIDEL, Agbor and DOU, Asaba) were chosen, then departments were stratified to ensure faculty representation, finally, students were randomly approached and invited to participate. This technique helps generalize findings across the undergraduate population in the state. Demographically, the sample balanced gender and year of study.

Data Collection Method
Data were collected using a structured questionnaire developed for this research. The questionnaire contained items grouped by the three research questions. Most items were statements rated on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree).

The sections are divided into 3. Section A deals on Security Threats (such as perceptions of hacking, breaches), Section B considers Privacy Concerns and Awareness (example; data collection concerns, policy awareness) and Section C deals with Suggested Safeguards (example, encryption, training, policy enforcement). The instrument was pre-tested with a small group of students for clarity and reliability. Cronbach's alpha was > 0.7 for each section. The survey was administered in person in lecture halls and common areas, with assistance from research assistants. Participation was voluntary and anonymous. Completed questionnaires were coded and entered into SPSS for analysis. Descriptive statistics (means and standard deviations) were computed for each item. These statistics are presented in Tables 1–3, organized by research question. Higher mean values above 3.5 indicate stronger agreement with the statement. This descriptive approach aligns with the exploratory nature of the study and allows identification of patterns in student perceptions.

Result Presentation

Table 1: Perceived security threats in EdTech tools

Items	Mean	SD
I am concerned that EdTech platforms used in my courses may be hacked or compromised.	4.10	0.79
I worry about unauthorized access to my personal information in EdTech tools.	4.25	0.73
There have been reports of data breaches involving educational platforms.	3.50	1.05
EdTech providers take adequate steps to protect student data.	2.68	0.95
I sometimes avoid using certain EdTech tools due to security concerns.	3.52	1.11

Table 2: Privacy concerns and awareness

Items	Mean	SD
I am concerned about how my personal data is collected and used by EdTech platforms.	4.00	0.86
I trust that EdTech companies respect my privacy.	2.70	0.98
My university clearly communicates its data privacy policies to students.	2.82	0.91
I am aware of data protection laws (e.g. Nigeria's Data Protection Act) regarding my educational data.	2.10	0.87
I know how to adjust privacy settings on the EdTech tools I use.	3.00	1.00

Table 3: Preferred security/privacy measures

Items	Mean	SD
Educational institutions should provide cybersecurity training for students using EdTech tools.	4.10	0.82
EdTech platforms should implement strong encryption and secure networks for student data.	3.95	0.89

Items	Mean	SD
Students should have control over sharing their personal data in EdTech tools (e.g. opt-in mechanisms).	3.85	0.94
Universities should conduct regular security audits of their digital learning platforms and EdTech systems.	3.78	0.99
Only EdTech tools that guarantee data privacy should be adopted by universities.	4.05	0.76

Discussion of Results

Table 1 reveals that students expressed high concern about EdTech security issues. The items "concern about hacking" (M=4.10, SD=0.79) and "worry about unauthorized access" (M=4.25, SD=0.73) show strong agreement, indicating most respondents recognize vulnerabilities in their online learning tools. Over 80% likely agreed or strongly agreed. The item on reported data breaches (M=3.50) suggests moderate awareness that such incidents occur. In contrast, the item "providers take adequate steps to protect data" has a low mean (2.68), implying distrust: students generally disagree that EdTech firms are doing enough to safeguard information. Finally, about half the students (M=3.52) admit avoiding some tools due to security worries, confirming that fear of threats affects their behavior.

These findings are consistent with global observations. Adeyemo *et al.* (2025) identified common threats (data breaches, phishing, malware) in online learning and noted that student data often lack robust protection. Similarly, UNESCO's report highlights rising cyberattacks in education, remarking that such attacks increase exposure to identity theft and personal data loss. Our students' high concern levels reflect this reality. They are aware that the "rapid expansion of online education" has come with cybersecurity gaps. The lack of confidence in providers' protections also echoes Sheridan's warning that in higher education, "ad hoc decisions" can erode privacy protections. Therefore, research question 1 results confirm that Delta State undergraduates perceive significant security risks in current EdTech tools, in line with literature on global and Nigerian contexts (Kelso et al., 2024).

As Table 2 shows, students are very concerned about personal data collection (M=4.00). This aligns with the security findings, that students worry not just about technical breaches but also about how their information is used. Notably, the trust item "EdTech companies respect my privacy" scored very low (M=2.70), indicating general skepticism. Similarly, students disagree that their universities clearly communicate privacy policies (M=2.82), and display very low awareness of legal protections (M=2.10 on NDPA awareness). Only about one-third feel they know how to manage privacy settings (M=3.00). Taken together, these suggest an awareness gap, that students lack both trust in current privacy practices and knowledge of their rights under laws like the Nigeria Data Protection Act.

These survey results echo findings by Bisong *et al.* (2023), who reported that issues like informed consent and user rights are often inadequately addressed in Nigeria's online education sector. The low NDPA awareness (M=2.10) is telling, since only very recently

(2023) has Nigeria established a formal data protection framework. This suggests students have not yet been educated about the NDPA or institutional policies. UNESCO's global data supports that, only 16% of countries explicitly guarantee data privacy in education by law, highlighting that legal awareness is limited worldwide. Moreover, Prinsloo and Kaliisa (2022) stress that African institutions must treat data privacy seriously, such as in contracts. The students' responses (low trust and policy communication) indicate that such measures are still lacking locally. Thus, research question 2 analysis shows that while students care deeply about privacy, they currently have little assurance of it and little knowledge of safeguards.

Table 3 indicates strong student support for proactive measures. All items yielded relatively high means (3.78–4.10). Students "agree" or "strongly agree" on average that institutions should provide cybersecurity training (M=4.10) and mandate encryption on platforms (M=3.95). They also endorsed giving students control over their data sharing (M=3.85), conducting regular security audits (M=3.78), and adopting only privacy-guaranteeing tools (M=4.05). In essence, respondents favor a combination of technical safeguards (encryption, audits) and awareness/policy actions (training, user control, vetted providers).

This aligns with recommendations in the literature. Adeyemo *et al.* (2025) proposed comprehensive measures like encryption, training, and audits to secure student data. Imohimi (2025) similarly highlighted advanced solutions (homomorphic encryption, differential privacy) for protecting educational data. On the policy side, Prinsloo & Kaliisa (2022) suggested institutions include privacy clauses in their service agreements, reflecting students' call to only use "certified" platforms. The elevated mean associated with "cybersecurity training" underscores students' recognition of education as a pivotal factor, corroborating Adedayo et al. (2025), who contend that sustained awareness initiatives for all stakeholders are imperative in mitigating cyber threats..

The students' responses to research question 3 indicated they are well-informed about potential solutions and strongly encouraged implementation of best practices. This confirms that if institutions and providers take students' preferences seriously (by enacting these measures), trust and data protection can be significantly improved.

Conclusion

This study examined how Delta State undergraduates perceive and experience security and privacy in EdTech tools. The findings reveal a clear pattern that, students are highly aware of the risks to their data but feel unprotected by current systems. They expressed strong concern about hacking, unauthorized access, and data breaches, and simultaneously reported distrust in EdTech vendors and low awareness of policies. These results mirror global trends that, as learning becomes digital, student data faces new threats. Importantly, students also articulated concrete solutions, indicating readiness to engage in mitigating actions. This reinforces the problem statement that, within the digital learning era, student data in higher education continues to be exposed to vulnerabilities in the absence of sufficient safeguards. This research confirms that Nigerian undergraduates recognize these vulnerabilities and demand stronger

privacy protections. The analysis underscores the critical need for educational institutions in Delta State (and broadly) to bridge the gap between EdTech use and data governance.

Recommendations

Based on the findings and related literature, the following actions are recommended to enhance security and privacy in EdTech:

i. Institutions should develop and enforce clear data privacy policies specifically for EdTech. This includes updating terms of service agreements, ensuring compliance with the Nigeria Data Protection Act (NDPA 2023), and requiring that all EdTech tools used on campus meet privacy standards.
ii. Institutions might establish dedicated offices or officers to oversee digital privacy, as recommended by NDPA authorities.
iii. Faculty and administrators should be trained to vet and approve any new educational technology, preventing "ad hoc" adoption that Sheridan warns can erode privacy.
iv. EdTech platforms should incorporate strong encryption for data at rest and in transit, as students and researchers alike advocate.
v. When selecting EdTech tools, institutions must demand privacy-by-design features. Contracts (SLAs) with providers should include clauses on data ownership, limits on data sharing, and breach notification protocols.

References

Adeyemo, D., Muhammad, I., Alagbe, J., Ifelola, A., & Muritala, N. (2025). *Global Cybersecurity Challenges for Students Using Online Learning in Higher Education*. SSRN.

Adedayo, A. O. T. (2025). Discerning cybers' threats in an era of digitally connected classrooms: Lessons for the Nigerian higher education system and society. *Discover Computing, 28*, Article 68.

Akinloye, M. (2023). *An Analysis of Data Protection and Compliance in Nigeria's Educational Institutions: A Study of Private Schools*. (Preprint).

Binitie, A. P. & Okoh, C. K. (2025). Issues and Challenges to the Successful Integration of ICT in Engineering/Technical Education in Secondary Schools: Teachers Perspective. *Educational Perspectives*, *13*(2).

Binitie, A. P., Blamah, N. V., & Ogah, U. S. (2013). Synthetic software method: panacea for combating internet fraud in Nigeria. *The International Journal of Engineering and Science*, *2*(10), 43-50.

Bisong, A. E., Eteng, I. J., & Mary, I. J. (2023). A systematic review of data privacy and security in Nigeria's online education: Ethical consideration and challenges. *Inter-Disciplinary Journal of Science Education, 5*(1), 98–112.

Chapman, J., & Maguire, D. (2022). The Impact of Cyber Security Attacks on Colleges and Universities: Who, How and Why. *Campus Crime: Legal, Social, and Policy Perspectives; Charles C Thomas Pub Ltd.: Springfield, MA, USA*, 333

Imohimi, E. O. (2025). Building privacy and preserving AI models for secure student data management in educational technology platforms. *Journal of Intelligent Learning Systems and Applications, 17*, 149–171.

Iyawa, I. J. B., & Patience, B. A. (2025). Assessing the Impact of ICT Integration on Learning Outcomes in Nigerian Tertiary Institutions. *Journal of Science Innovation and Technology Research*.

Janssen, M., & Van der Voort, H. (2020). Agile and adaptive governance in crisis response: Lessons from the COVID-19 pandemic. *International journal of information management*, *55*, 102180.

Jones, K. M. (2019). Learning analytics and higher education: a proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. *International Journal of Educational Technology in Higher Education*, *16*(1), 1-22

Komljenovic, J. (2022). The future of value in digitalised higher education: why data privacy should not be our biggest concern. *Higher Education*, *83*(1), 119-135.

Marseille, E. (2020). *The Rapid Growth of Data Breaches in Today's Society* (Master's thesis, Utica College

Nigeria Data Protection Commission (NDPC). (2023). *About Us*. Nigeria Data Protection Commission.

Perisic, A., Perisic, I., Lazic, M., & Perisic, B. (2023). The foundation for future education, teaching, training, learning, and performing infrastructure-The open interoperability conceptual framework approach. *Heliyon*, *9*(6)

Prinsloo, P., & Kaliisa, R. (2022). Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. *British Journal of Educational Technology, 53*(4), 894–913.

Rehan, H. (2023). Shaping the future of education with cloud and AI technologies: enhancing personalized learning and securing data integrity in the evolving edtech landscape. *Australian Journal of Machine Learning Research & Applications*, *3*(1), 359-395

Sheridan, P. M. (2022). Edtech in higher education: Protecting student data privacy in the classroom. *North Carolina Journal of Law & Technology, 24*(1), 49–82.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 39

UNESCO. (2023). *Global Education Monitoring Report 2023: Technology in education*.

UNESCO Publishing.