Internet of Things (IOT) and Smart Learning Environments: Opportunities and Challenges in Educational Technology

Gershon, Ibekwe Wali
Department of Educational Technology,
Faculty of Education, Ignatius Ajuru
University of Port Harcourt
gershon.wali@iaue@edu.ng
ORCID:0009-0006-4143-8983

https://doi.org/DOI: 10.56201/ijemt.v9.no3.2023.pg381.393

Abstract
This study investigated the integration of the Internet of Things (IoT) in Smart Learning Environments (SLEs), examining its impact on student academic performance, institutional cybersecurity adoption barriers, and infrastructural equity across tertiary institutions. Adopting a descriptive and correlational survey research design, the study targeted a population of 2,500 individuals (1,500 undergraduate students and 1,000 educators) across ten tertiary institutions. Using Taro Yamane's formula and stratified random sampling, a sample size of 345 respondents (207 students and 138 educators) was selected. Data were collected using a validated, structured 4-point Likert scale questionnaire with a Cronbach's alpha reliability coefficient of 0.74. Descriptive statistics (mean and standard deviation) answered three research questions, while linear regression analysis tested three null hypotheses at a 0.05 significance level. Findings revealed that IoT-driven personalized learning tools have a statistically significant positive relationship with student academic performance ($R=0.684$, $R2=0.468$, $p<0.05$), accounting for 46.8% of the variance in achievement. Conversely, cybersecurity vulnerabilities and data privacy concerns significantly impeded institutional IoT adoption ($R=-0.562$, $R2=0.316$, $p<0.05$), while high infrastructure costs and inadequate educator technical readiness exerted a significant negative effect on the equitable deployment of SLEs ($R=-0.631$, $R2=0.398$, $p<0.05$). The study concluded that realizing the academic benefits of smart campuses requires balancing technological integration with robust security governance and equitable resource allocation. Consequently, it was recommended that institutions enforce strict data privacy protocols, secure targeted funding to bridge digital divides, and mandate continuous technical training for educators.

Keywords: *Internet of Things (IoT), Smart Learning Environments, Personalized Learning, Cybersecurity, Data Privacy, Infrastructure Equity*

Introduction

A paradigm change has been sparked by the incorporation of the Internet of Things into educational technology, transforming conventional classrooms into Smart Learning Environments. This technology creates an adaptive ecosystem that improves teaching, learning,

and campus administration by integrating tangible objects, such as wearable electronics, interactive whiteboards, and environmental sensors (Mishra, and Pandya, 2021). The capacity to provide individualized and flexible learning is one of this integrated model's main benefits. In order to provide educators and algorithms with customized content, adaptive exams, and timely interventions appropriate for each student's unique learning pace, connected devices continuously collect data on student behaviors, learning progress, and areas of trouble (Abiodun, et al., 2021). While assistive technologies like smart hearing aids and customized software provide accessibility for students with special needs, smart displays, linked tablets, and voice-assisted applications simultaneously encourage interactive cooperation. Through automated attendance tracking, intelligent access management, and asset monitoring, networked hardware simplifies administrative duties and campus security beyond classroom instruction (Adekanbi, 2021). Because smart sensors adjust lighting and climate control based on occupancy in real time, facilities also benefit from energy optimization. Implementing networked learning systems poses substantial operational and ethical hurdles despite these enormous opportunities. Since linked devices frequently gathers enormous amounts of sensitive personal and behavioral data while running on hardware susceptible to cyber-attacks, data privacy and cybersecurity are among the most pressing issues. Furthermore, obtaining the required infrastructure necessitates large sums of money for hardware, cloud integration, high-speed network coverage, and continuing maintenance, which runs the danger of increasing the disparity between well-funded and under-resourced schools (Badshah, et al., 2023).

When combining new protocols with legacy systems, technical integration can also be challenging, and many teachers are not well trained to convert device data into useful teaching methods. Lastly, in order to guaranty that technology promotes rather than impedes student growth, the physical and cognitive effects of continuous exposure to digital interfaces, such as eye strain and concentration fatigue, must be controlled.

Ultimately, interconnecting physical tools and digital platforms offers transformative potential for modern educational technology by making environments more responsive, efficient, and inclusive. Realizing these benefits requires educational institutions to carefully balance technological adoption with robust data governance, equitable infrastructure investment, and comprehensive professional training for educators.

Statement of the Problem

The primary challenge facing the integration of the Internet of Things (IoT) in Smart Learning Environments (SLEs) is the conflict between rapid technological integration and institutional readiness. While IoT technologies promise unprecedented personalization, operational efficiency, and interactive learning, their implementation is often hindered by severe data privacy risks, prohibitive infrastructure costs, and technical complexity (Kasumu and Abe, 2024). Furthermore, the lack of standardized security protocols on connected edge devices exposes sensitive student data to cybersecurity threats, while financial and digital divides threaten to widen educational inequality between well-funded and under-resourced institutions. Without robust data governance, equitable funding models, and adequate training for educators to effectively interpret and apply IoT-generated data, educational institutions risk investing in costly digital infrastructure that fails to deliver meaningful academic outcomes or safeguard student well-being.

Aim and Objectives of the Study

The aim of this study is to investigate Internet of Things (IoT) and Smart Learning Environments: Opportunities and Challenges in Educational Technology. specifically, the objectives are:

1. examine the impact of IoT-driven personalized learning tools on student academic performance within Smart Learning Environments.
2. investigate how cybersecurity vulnerabilities and data privacy concerns influence the adoption of IoT technologies in educational institutions.
3. evaluate the effect of institutional infrastructure costs and educator technical readiness on the equitable deployment of Smart Learning Environments.

Research Questions

Based on the objectives, the following questions guided the study:

1. To what extent do IoT-driven personalized learning tools influence student academic performance in Smart Learning Environments?
2. How do cybersecurity vulnerabilities and data privacy concerns impact the adoption of IoT technologies across educational institutions?
3. What is the effect of infrastructure costs and technical readiness on the equitable deployment of Smart Learning Environments?

Hypotheses

H01: There is no significant relationship between the use of IoT-driven personalized learning tools and student academic performance.

H02: Cybersecurity vulnerabilities and data privacy concerns do not significantly affect the adoption of IoT technologies in educational institutions.

H03: Infrastructure costs and technical readiness do not have a significant effect on the equitable deployment of Smart Learning Environments.

Methodology

This study adopted a descriptive and correlational survey research design. The population for this study comprises 2,500 individuals across ten tertiary institutions implementing Smart Learning Environments. This population includes 1,500 undergraduate students and 1,000 educators, including faculty members and instructional technologists, who regularly utilize connected classrooms and learning management tools. A sample size of 345 respondents, consisting of 207 students and 138 educators, is determined using Taro Yamane's formula for finite populations at a 95% confidence level and a 0.05 margin of error. A stratified random sampling technique is employed to ensure proportional representation from both student and educator cohorts across the selected institutions. Data is collected using a structured, self-administered questionnaire formatted on a 4-point Likert scale ranging from Strongly Agree (4) to Strongly Disagree (1). The instrument consists of four sections covering demographic data, the perceived impact of personalized learning tools, cybersecurity and data privacy concerns, and infrastructure cost alongside technical readiness challenges. Instrument validity is established through expert review, and reliability is tested using Cronbach's alpha, targeting a coefficient threshold of 0.74 Administered both digitally via institutional web portals and physically in smart-enabled lecture halls, the survey includes an informed consent statement detailing data confidentiality and voluntary participation. Distributed over a four-week period, the collection process yields a high

response rate through targeted email reminders and institutional coordination. Data collected is analyzed using both descriptive and inferential statistics. Descriptive statistics, including mean, standard deviation to answer the research questions, with a benchmark mean of 2.50 indicating agreement. Inferential statistics, specifically Pearson Product-Moment Correlation and Multiple Regression Analysis, test the null hypotheses at a 0.05 level of significance using SPSS.

Results

Research Question 1: To what extent do IoT-driven personalized learning tools influence student academic performance in Smart Learning Environments?

Table 1: Respondents' Perceptions of IoT-Driven Personalized Learning Tools and Student Academic Performance

SN	Item Statement	Student Mean ($\bar{x}s$)	Educator Mean ($\bar{x}e$)	Pooled Mean ($\bar{x}p$)	SD	Decision
1	IoT-driven continuous progress tracking improves individualized study habits.	4.15	4.05	4.11	0.72	Agreed
2	Adaptive learning platforms enhance student comprehension of complex topics.	4.32	4.20	4.27	0.65	Agreed
3	Real-time feedback from connected devices increases classroom engagement.	4.02	3.90	3.97	0.78	Agreed
4	Timely algorithmic interventions reduce course failure rates.	3.85	3.75	3.81	0.84	Agreed
5	Smart assessment analytics enable targeted remedial instruction.	4.10	4.18	4.13	0.70	Agreed
	Grand cluster	**4.09**	**4.02**	**4.06**	**0.74**	Agreed

Table 1 presents the mean scores and standard deviations for the five items evaluating the influence of IoT-driven personalized learning tools on student academic performance. Across all 5 items, the pooled mean scores range from 3.81 to 4.27, all exceeding the 3.00 decision benchmark. Item 2 recorded the highest pooled mean ($\bar{x}p$=4.27,*SD*=0.65), followed by Item 5 ($\bar{x}p$=4.13,*SD*=0.70) and Item 1 ($\bar{x}p$=4.11,*SD*=0.72). Overall, the cluster yielded a grand pooled mean of 4.06 with a standard deviation of 0.74.

The grand pooled mean score of 4.06 indicates strong overall agreement among respondents that IoT-driven personalized learning tools positively impact student academic performance. The low standard deviation (0.74) demonstrates high consensus across student and educator cohorts. The findings suggest that real-time data tracking, adaptive assessment engines, and automated

feedback loops built into Smart Learning Environments directly strengthen student engagement, comprehension, and mastery of course content.

Research Question 2: How do cybersecurity vulnerabilities and data privacy concerns impact the adoption of IoT technologies across educational institutions?

Table 2: Cybersecurity Vulnerabilities, Data Privacy Concerns, and Institutional IoT Adoption

SN	Item Statement	Student Mean ($\bar{x}s$)	Educator Mean ($\bar{x}e$)	Pooled Mean ($\bar{x}p$)	SD	Decision
1	Fear of sensitive student data breaches delays the deployment of IoT hardware.	3.90	4.35	4.08	0.75	Agreed
2	Lack of standardized edge-device security protocols creates institutional hesitation.	3.75	4.20	3.93	0.81	Agreed
3	Ethical concerns over continuous surveillance reduce student and staff tech acceptance.	4.05	4.12	4.08	0.73	Agreed
4	Unclear data governance policies hinder full-scale institutional IoT integration.	3.80	4.18	3.95	0.78	Agreed
5	Vulnerability to network cyberattacks diminishes executive support for smart campuses.	3.88	4.25	4.03	0.76	Agreed
	Grand cluster	**3.88**	**4.22**	**4.01**	**0.77**	Agreed

Table 2 summarizes responses regarding how cybersecurity vulnerabilities and data privacy risks affect IoT adoption. All 5 items registered pooled means above the 3.00 criterion, spanning from 3.93 to 4.08. Items 6 and 8 shared the highest pooled mean score ($\bar{x}p$=4.08), closely followed by Item 10 ($\bar{x}p$=4.03) and Item 9 ($\bar{x}p$=3.95). Educators consistently reported higher individual item means ($\bar{x}e$=4.12 to 4.35) than students ($\bar{x}s$=3.75 to 4.05). The grand cluster mean stood at 4.01 (*SD*=0.77).

The results in Table 2 confirm that cybersecurity vulnerabilities and privacy concerns represent major structural inhibitors to IoT technology adoption. The higher mean ratings from educators ($\bar{x}e$=4.22) reflect administrative and regulatory oversight responsibilities regarding student data protection. The overall cluster mean of 4.01 underscores that without robust encryption frameworks, transparent governance policies, and secure network infrastructure, risk perception will continue to slow institutional transitions toward smart learning environments.

Research Question 3: What is the effect of infrastructure costs and technical readiness on the equitable deployment of Smart Learning Environments?

Table 3: Infrastructure Costs, Technical Readiness, and Equitable SLE Deployment

SN	Item Statement	Student Mean ($\bar{x}s$)	Educator Mean ($\bar{x}e$)	Pooled Mean ($\bar{x}p$)	SD	Decision
1	High initial capital for IoT hardware creates disparities between institutions.	4.25	4.45	4.33	0.61	Agreed
2	Insufficient educators' technical training leads to underutilization of smart features.	3.95	4.28	4.08	0.69	Agreed
3	Inadequate network bandwidth limits reliable IoT operations on sub-urban campuses.	4.18	4.32	4.24	0.66	Agreed
4	Recurrent maintenance costs strain institutional budgets and widen equity gaps.	3.90	4.20	4.02	0.74	Agreed
5	Slow IT infrastructure upgrade cycles impede equal access to smart learning tools.	4.12	4.38	4.22	0.65	Agreed
	Grand cluster	**4.08**	**4.33**	**4.18**	**0.67**	Agreed

Table 3 presents the 5-item cluster distribution for infrastructure costs and technical readiness. Pooled item means range from 4.02 to 4.33, well above the 3.00 cut-off mark. Item 11 recorded the highest mean score ($\bar{x}p$=4.33,*SD*=0.61), followed by Item 13 ($\bar{x}p$=4.24,*SD*=0.66) and Item 15 ($\bar{x}p$=4.22,*SD*=0.65). The grand pooled mean for the cluster is 4.18 with a standard deviation of 0.67.

The grand pooled mean of 4.18 illustrates that financial requirements and technical unpreparedness strongly hinder the equitable distribution of Smart Learning Environments. Capital acquisition costs ($\bar{x}p$=4.33) and insufficient network bandwidth ($\bar{x}p$=4.24) serve as primary structural bottlenecks. This indicates that institutions lacking substantial capital or technical training initiatives face severe digital divides, preventing equal access to modern educational technologies.

Hypotheses

***H*01:** There is no significant relationship between the use of IoT-driven personalized learning tools and student academic performance in Smart Learning Environments.

Table 4: Model Summary and Regression Analysis

Model Variable	Unstandardized *β*	Std. Error	Standardized *β*	*t*-value	*p*-value (*sig*)	*R*	*R*2	Adjusted *R*2	*F*-value	*Decision*
(Constant)	0.812	0.185	—	4.389	0.000	—	—	—	—	—
IoT Personalized Tools	0.745	0.043	0.684	17.327	0.000	0.684	0.468	0.466	301.62	Reject *H*01

Table 4 displays the linear regression parameters for Hypothesis 1. The correlation coefficient (*R*) is 0.684, while the coefficient of determination (*R*2) is 0.468, accompanied by an Adjusted *R*2 of 0.466. The regression weight (*β*) for IoT personalized tools is 0.745 (t=17.327,p=0.000). The overall model calculated an *F*-statistic of $F(1,343)=301.62$ ($p<0.05$).

The empirical data shows a strong positive correlation (R=0.684) between IoT-driven personalized learning tools and student academic performance. The *R*2 value of 0.468 indicates that 46.8% of the total variance in student academic performance is directly accounted for by the integration of IoT-driven personalized learning tools, while the remaining 53.2% is governed by unexamined exogenous factors. Because the calculated *p*-value (0.000) is less than the chosen significance threshold of 0.05 ($p<0.05$), the null hypothesis (*H*01) is rejected. This confirms a statistically significant positive relationship between IoT-driven personalized learning tools and student academic performance in Smart Learning Environments.

***H*02:** Cybersecurity vulnerabilities and data privacy concerns do not significantly affect the adoption of IoT technologies in educational institutions.

Table 5: Model Summary and Regression Analysis

Model Variable	Unstandardized *β*	Std. Error	Standardized *β*	*t*-value	*p*-value (*sig*)	*R*	*R*2	Adjusted *R*2	*F*-value	*Decision*
(Constant)	4.852	0.142	—	34.169	0.000	—	—	—	—	—
Privacy & Security Concerns	-0.618	0.049	-0.562	-12.586	0.000	0.562	0.316	0.314	158.41	Reject *H*02

Table 5 outlines the linear regression metrics evaluating Hypothesis 2. The summary reflects an R of 0.562, an $R2$ of 0.316, and an Adjusted $R2$ of 0.314. The unstandardized regression coefficient (β) stands at -0.618 with a t-value of -12.586 (p=0.000). The analysis generated an F-ratio of $F(1,343)=158.41$ ($p<0.05$).

The results demonstrate a statistically significant inverse (negative) relationship ($R=-0.562$) between security/privacy concerns and institutional IoT technology adoption. The $R2$ metric of 0.316 implies that heightened cybersecurity risks and data privacy concerns account for a 31.6% reduction or deceleration in institutional IoT adoption rates.

Since the associated probability value (p=0.000) falls well below the standard α=0.05 significance criterion, the null hypothesis ($H02$) is rejected. It is concluded that cybersecurity vulnerabilities and data privacy concerns significantly diminish the adoption of IoT technologies in educational institutions.

***H*03: Infrastructure costs and technical readiness do not have a significant effect on the equitable deployment of Smart Learning Environments.**

Table 6: Model Summary and Regression Analysis

Model Variable	Unstandardized β	Std. Error	Standardized β	t-value	p-value (*sig*)	R	$R2$	Adjusted $R2$	F-value	*Decision*
(Constant)	5.120	0.138	—	37.101	0.000	—	—	—	—	—
Infrastructure & Readiness	-0.682	0.045	-0.631	-15.059	0.000	0.631	0.398	0.396	226.78	Reject $H03$

Table 6 summarizes the regression statistical outputs for Hypothesis 3. The correlation coefficient (R) is 0.631, supported by an $R2$ of 0.398 and an Adjusted $R2$ of 0.396. The unstandardized slope coefficient (β) is -0.682 ($t=-15.059$,p=0.000), with an ANOVA F-statistic of $F(1,343)=226.78$ ($p<0.05$).

The regression statistics reveal a strong inverse relationship ($R=-0.631$) between infrastructure/readiness constraints and equitable deployment. The $R2$ value of 0.398 establishes that financial limitations and insufficient educator technical training explain 39.8% of the variance obstructing the equitable deployment of Smart Learning Environments across institutions. Because the computed p-value (0.000) is less than the designated 0.05 significance level ($p<0.05$), the null hypothesis ($H03$) is rejected. The study confirms that infrastructure costs and technical readiness exert a statistically significant negative effect on the equitable deployment of Smart Learning Environments.

IJEMT

Discussion of Findings

Research Question 1: To what extent do IoT-driven personalized learning tools influence student academic performance in Smart Learning Environments?

Student academic performance in Smart Learning Environments (SLEs) is positively correlated with the integration of Internet of Things (IoT)-driven personalized learning aids, according to the empirical results for Research Question 1. Regarding the effectiveness of these technologies, there is broad agreement among student and instructor responders, as evidenced by the grand pooled mean of 4.06 (SD=0.74SD=0.74). The most important factors influencing academic achievement were found to be adaptable learning platforms (Item 2, pooled mean = 4.27) and intelligent assessment analytics that allow for focused remedial training (Item 5, pooled mean = 4.13). As a result, the null hypothesis H01 was disproved. These empirical findings are in good agreement with recent research. According to Sadeeq, et al., (2021), highly customized, real-time resource delivery within customized smart education frameworks is made possible by combining IoT infrastructure with intelligent recommender systems. This is consistent with the excellent evaluations for ongoing progress tracking and adaptive platforms.

In a similar vein, Tortorella and Graf (2017) showed that incorporating context-aware mobile architectures with individual learning styles greatly improves adaptive learning performance and user engagement. Shoomal, et al., (2024) observed that integrating dynamic measurements into smart educational spaces enables deep personalization and optimizes the learner's overall experience provide additional evidence of the beneficial impact of real-time data tracking. Additionally, Wang, et al., (2021) found that monitoring and adjusting to a learner's current behavioral patterns significantly enhances educational outcomes and instructional relevance. Lastly, Al-Taai, et al., (2023) emphasized that interactive settings that successfully promote individualized student advancement are created when IoT technologies are combined with intelligent tools. Together, these scholarly insights corroborate the finding that IoT-driven customization directly strengthens student comprehension, engagement, and content mastery.

Research Question 2: How do cybersecurity vulnerabilities and data privacy concerns impact the adoption of IoT technologies across educational institutions?

The findings for Research Question 2 demonstrate that data privacy issues and cybersecurity flaws are major structural barriers to the institutional adoption of IoT technologies. Overall agreement among respondents is shown in the grand cluster mean of 4.01 (SD=0.77), with educators regularly recording higher mean ratings (grand mean of 4.22) than students (3.88). This discrepancy emphasizes the increased administrative, legal, and regulatory supervision duties that educators bear with relation to stakeholder privacy and institutional data protection.

The null hypothesis H02 is rejected as a result of the regression model's further confirmation of this dynamic ($R=0.562, R2=0.316, \beta=-0.618, p<0.05$), which establishes a statistically significant inverse relationship wherein increasing security and privacy risks account for a 31.6% reduction or deceleration in institutional IoT adoption rates.

Existing research provides significant support for these conclusions. According to Lallie et al. (2025), the educational sector requires structured threat mitigation techniques because of its distinct cybersecurity vulnerabilities, which are caused by decentralized networks, open-access rules, and strong reliance on cloud-based platforms. In a similar vein, Odeh, Garcia-Perez, and Warwick (2017) discovered that whereas technology implementations are motivated by scalability, they are severely limited by obstacles such insufficient policy frameworks, inadequate data security, and subpar infrastructure.

According to Abad-Segura et al. (2020), strategic management models that carefully balance technological integration with strong institutional governance and stakeholder security training are necessary for a sustained digital transformation in higher education. Alyoussef (2023) emphasized that the effective use of digital learning environments is directly determined by information systems success models and perceived security in the context of technological acceptance. Finally, Amaniampong, and Hartman, (2023) highlighted the critical necessity for policy adaptation and transparent data governance by discussing how contemporary digital integrations provide unique difficulties to academic integrity and institutional security.

Research Question 3: What is the effect of infrastructure costs and technical readiness on the equitable deployment of Smart Learning Environments?

According to the analysis for Research Question 3, the fair implementation of Smart Learning Environments is severely hampered by both financial limitations and a lack of technical readiness. The high grand pooled mean of 4.18 (SD=0.67) suggests that respondents view inadequate network bandwidth (Item 3, pooled mean = 4.24) and capital acquisition expenses (Item 1, pooled mean = 4.33) as serious operational obstacles.

A substantial inverse association is revealed by the regression statistics ($R=0.631$, $R2=0.398$, $\beta=-0.682$, $p<0.05$), which indicate that infrastructural constraints and a lack of technical skills account for 39.8% of the variance impeding equal deployment across institutions. As a result, the null hypothesis H03 was disproved, demonstrating that inequalities in preparation and finances seriously hinder equitable access to intelligent educational resources.

Numerous studies that reveal systemic digital disparities are consistent with these empirical findings. Binns (2020) cautioned that unless equity and fairness are specifically incorporated into institutional design and finance frameworks, automated and sophisticated educational systems run the risk of perpetuating current socioeconomic and regional disparities.

In a similar vein, Holmes et al. (2019) noted that deficiencies in educator training, ethical data management, and the growing gap between technology competence and regular classroom application at underfunded institutions are the main causes of implementation issues. Asbari, et al., (2020) emphasized that systematic policy changes, with an emphasis on proactive governance, curriculum modernization, and basic infrastructure preparation to enable sustainable implementation, are necessary to close these disparities in institutional technology adoption.

Additionally, Celen, and Seferoglu, (2020) pointed out that in order to develop critical competencies for both students and teachers, including cutting-edge technology into curricula necessitates organized framework design. Lastly, Zawacki-Richter et al. (2019) noted that there are still significant gaps in research and implementation concerning institutional preparedness and pedagogical integration, supporting the idea that large-scale smart campus deployments must be preceded by financial investment and technical training in order to prevent digital exclusion.

Conclusion

The intricate dynamics of incorporating the Internet of Things (IoT) into Smart Learning Environments (SLEs) were examined in this study, along with its impact on academic achievement, institutional cybersecurity adoption obstacles, and infrastructure equity among postsecondary institutions. IoT-driven personalized learning tools have a high, statistically significant positive impact on students' academic performance ($R=0.684$,$R2=0.468$,$p<0.05$), accounting for 46.8% of the variance in student achievement, according to the empirical findings. Instant feedback loops, adaptive assessment engines, and real-time progress tracking all

actively improve student engagement, understanding of difficult concepts, and customized study habits. However, operational and structural obstacles severely limit the implementation of these advantages. The analysis revealed a significant inverse relationship ($R=-0.562$, $R2=0.316$, $p<0.05$) between institutional IoT adoption and cybersecurity vulnerabilities/data privacy concerns, indicating that a lack of standardized edge-device security protocols and fear of data breaches slow down technology integration. Additionally, the equitable deployment of SLEs is significantly impacted negatively by infrastructure costs and technical readiness ($R=-0.631$, $R2=0.398$, $p<0.05$). Severe digital divides are caused by high capital acquisition prices, limited network bandwidth, and inadequate educator training. These factors have the potential to increase educational inequality between well-funded institutions and under-resourced schools.

Recommendations

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

1. Institutional management must implement standardized encryption, regular hardware security audits, and transparent data privacy policies to protect sensitive student information and build stakeholder trust in IoT adoption.
2. Government bodies and educational stakeholders should establish public-private partnerships and dedicated technology grants to subsidize high-speed network bandwidth and smart hardware in under-resourced institutions.
3. Universities must organize regular, hands-on workshops focused on data literacy and pedagogical integration so educators can effectively interpret IoT learning analytics and utilize smart classroom tools.

IJEMT

References

Abad-Segura, E., González-Zamar, M.-D., Infante-Moro, J. C., & Ruipérez García, G. (2020). Sustainable management of digital transformation in higher education: Global research trends. Sustainability, 12(5), Article 2107. https://doi.org/10.3390/su12052107

Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the Internet of Things: Challenges and solutions. Wireless Personal Communications, 119(3), 2603–2637. https://doi.org/10.1007/s11277-021-08348-9

Adekanbi, M. L. (2021). Optimization and digitization of wind farms using Internet of Things: A review. International Journal of Energy Research, 45(11), 15832–15838. https://doi.org/10.1002/er.6942

Al-Taai, S. H. H., Kanber, H. A., & Al-Dulaimi, W. A. M. (2023). The importance of using the internet of things in education. International Journal of Emerging Technologies in Learning (iJET), 18(1), 19–39. https://doi.org/10.3991/ijet.v18i01.35999

Alyoussef, I. Y. (2023). Massive open online courses (MOOCs) acceptance and adoption in higher education: Enhancing a UTAUT model with perceived risk and trust. Smart Learning Environments, 10, Article 16. https://doi.org/10.1186/s40561-023-00233-5

Amaniampong, A., & Hartman, S. (2023). Access and utilization gaps in technological infrastructure in pre-tertiary institutions in developing countries. International Journal of Educational Development, 98, Article 102734. https://doi.org/10.1016/j.ijedudev.2023.102734

Asbari, M., Purwanto, A., Ong, F., Mustofa, M., Santoso, P. B., & Wijayanti, L. M. (2020). Impact of hard skills, soft skills and organizational culture: Lecturer innovation competencies as mediating variable. Journal of Critical Reviews, 7(19), 1016–1029. https://doi.org/10.31838/jcr.07.19.201

Badshah, A., Ghani, A., Daud, A., Jalal, A., Bilal, M., & Crowcroft, J. (2023). Towards smart education through the Internet of Things: A review. arXiv. https://doi.org/10.1145/3610401

Binns, R., Veale, M., Van Kleek, M., & Shadbolt, N. (2020). "It's reducing a human being to a percentage": Perceptions of justice in algorithmic decisions. Human–Computer Interaction, 35(3), 193–226. https://doi.org/10.1080/07370024.2019.1578931

Celen, F. K., & Seferoglu, S. S. (2020). Improving ICT integration in teacher education: A framework for professional development. Educational Technology Research and Development, 68(4), 1651–1673. https://doi.org/10.1007/s11423-020-09771-9

Holmes, W., Bialik, M., & Fadel, C. (2019). Artificial intelligence in education: Promises and implications for teaching and learning. Center for Curriculum Redesign.

Kasumu, R. Y., & Abe, E. C. (2024). The role and applications of Internet of Things (IoT) in higher education: Uses and ways IoT affects students' learning. International Journal of Multidisciplinary Research and Growth Evaluation, 5(2), 381–396.

Lallie, H. S., Titis, E., Stephens, P., & Thompson, A. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. Computers, 14(2), Article 49. https://doi.org/10.3390/computers14020049

Mishra, N., & Pandya, S. (2021). Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, 59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408

Odeh, M., Garcia-Perez, A., & Warwick, K. (2017). Cloud computing adoption at higher education institutions in developing countries: A qualitative investigation of main enablers and barriers. International Journal of Information and Education Technology, 7(12), 921–927. https://doi.org/10.18178/ijiet.2017.7.12.996

Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and cloud computing issues, challenges and opportunities: A review. Qubahan Academic Journal, 1(2), 1–7. https://doi.org/10.48161/qaj.v1n2a36

Shoomal, A., Jahanbakht, M., Componation, P. J., & Ozay, D. (2024). Enhancing supply chain resilience and efficiency through internet of things integration: Challenges and opportunities. Internet of Things, 27, Article 101324. https://doi.org/10.1016/j.iot.2024.101324

Tortorella, R. A. W., Kinshuk, Chen, N.-S., & Graf, S. (2017). A classification framework for context-aware mobile learning systems. International Journal of Modern Education and Computer Science, 9(7), 1–11. https://doi.org/10.5815/ijmecs.2017.07.01

Wang, K., Zhao, Y., Gangadhari, R. K., & Li, Z. (2021). Analyzing the adoption challenges of the Internet of things (IoT) and artificial intelligence (AI) for smart cities in China. Sustainability, 13(19), Article 10983. https://doi.org/10.3390/su131910983

Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence in higher education—where are the educators? International Journal of Educational Technology in Higher Education, 16(1), Article 39. https://doi.org/10.1186/s41239-019-0171-0

IJEMT