Eastern Africa Journal of Contemporary Research (EAJCR)

Technological Determinants of Adoption of In-House Student Management Software in Public Universities in Kenya

Benjamin Opicho Kemboi, Robert Mutua Murungi, and Salesio Mbogo Kiura

Article information:

To cite this article:

Kemboi B.O., Murungi R. M., & Kiura M.S. (2025). *Technological Determinants of Adoption of In-House Student Management Software in Public Universities in Kenya. Eastern Africa Journal of Contemporary Research, 5*(2), 94-.109

For Authors

If you would like to publish your conceptual/theoretical and empirical research articles, case studies and book reviews with EAJCR, please use for authors information about how to write your work and submission guidelines. Please, visit https:// www.eajcr.org/

About Eastern Africa Journal of Contemporary Research (EAJCR)

The Eastern Africa Journal of Contemporary Research (EAJCR) is both an online (ISSN: 2663-7367) and print (ISSN: 2663-7359) double-blind peer-reviewed quarterly journal published by the Directorate of Research and Publications of Gretsa University, Kenya.

EAJCR aims at advancing the frontiers of knowledge by publishing contemporary multidisciplinary conceptual/ theoretical and empirical research articles as well as case studies and book reviews.

Vol. 5, Issue 2, 2025, ISSN: 2663-7367 (Online) & ISSN: 2663-7359

Technological Determinants of Adoption of In-House Student Management Software in Public Universities in Kenya

Benjamin Opicho Kemboi
Assistant Librarian
Technical University of Kenya
Email:benjamin.kemboi@tukenya.ac.ke

Robert Mutua Murungi
Department of Computer Science.
Kenya Methodist University
Email: robert.murungi@kemu.ac.ke

Salesio Mbogo Kiura
Department of computer science
Technical University of Kenya
Email: kiura-salesio.kiura@gmail.com

Abstract

This study investigated the effect of technological factors specifically security features and software compatibility on the adoption of in-house student management software (SMS) in Kenyan public universities. The problem addressed was the inconsistent implementation of such systems due to concerns over data security and lack of compatibility with existing institutional infrastructure. The objectives were to examine how security influences user trust and how compatibility impacts adoption. The study was limited to eight public universities within Nairobi's Central Business District (CBD) and focused on administrators and IT staff, excluding private institutions and other influencing variables. Guided by the Technology Acceptance Model (TAM) and the Technology-Organization-Environment (TOE) framework, the study employed a quantitative research design. The target population was 250, with a sample of 152 selected through stratified random sampling. Structured questionnaires were used for data collection. Validity and reliability were ensured through expert review and Cronbach's Alpha testing. Data analysis involved descriptive and inferential statistics, including correlation and regression. Findings showed that both security and compatibility significantly influence system adoption, with a regression model indicating strong predictive power ($\beta = 0.25$, $p = .003$, $R^2 = 0.68$). The study concluded that enhancing security frameworks and ensuring system compatibility are critical. It recommends universities implement robust access controls, conduct infrastructure audits, involve end-users, and offer targeted training to ensure successful software adoption and sustainability.

Key Words: *Public Universities, Security Features, Software Compatibility, Student Management Software, System Adoption and Technological Factors*

1. Introduction

The rapid digital transformation in higher education has accelerated the need for robust student management software (SMS) to streamline academic, administrative, and service delivery functions. Globally, universities are increasingly adopting in-house SMS solutions to

enhance customization, strengthen data privacy, and optimize system integration (Huang & Teo, 2020). These platforms manage critical functions such as student registration, grading, communication, and record-keeping, and their effectiveness depends on technological factors such as security, compatibility, and in some contexts system integration.

In Sub-Saharan Africa, universities face unique barriers to SMS adoption, including limited ICT infrastructure, low digital literacy, and persistent concerns about data security (Ngugi & Kimani, 2021). However, there is growing momentum toward locally developed digital solutions that are cost-effective, adaptable to regional contexts, and aligned with institutional needs (Wambugu & Chang, 2022).

In Kenya, public universities are under increasing pressure to modernize their systems to accommodate rising student enrolments, enhance service delivery, and comply with regulatory frameworks such as the Data Protection Act (2019) and national university ICT policies. Despite these drivers, adoption of in-house SMS remains uneven, often hindered by doubts about software compatibility with existing IT infrastructure, gaps in security assurances, and uncertainty about integration with current workflows (Wachira, 2021).

For this study, security refers to measures that protect sensitive student and institutional data from unauthorized access, breaches, or loss. Compatibility is defined as the software's ability to operate seamlessly with existing databases, networks, and systems clarifying that "integration" is considered a subcomponent of compatibility rather than a separate construct unless explicitly identified in the research problem. Understanding how these technological factors influence adoption measured through user willingness, system usage, and institutional uptake will guide universities in developing secure, compatible, and sustainable digital platforms

1.1 Statement of the Problem

Despite the national and institutional drive toward digital transformation in higher education, the adoption of in-house student management software (SMS) in Kenyan public universities remains inconsistent and often problematic. While such systems have the potential to enhance data accuracy, streamline workflows, and improve institutional efficiency, their uptake has been hindered by persistent technical setbacks, low user acceptance, and underutilization (Kariuki & Waema, 2023). Recent reports indicate that fewer than 40% of public universities in Kenya have fully implemented in-house SMS solutions that meet both operational and regulatory standards (Commission for University Education [CUE], 2024).

Two critical technological factors software compatibility and security features consistently emerge as central to successful adoption. Compatibility issues, such as the inability of new systems to integrate seamlessly with legacy databases and existing ICT infrastructure, frequently lead to workflow disruptions, increased maintenance costs, and reduced staff confidence (Anwar, Shaikh, & Shaikh, 2022). Security concerns, including inadequate data encryption, weak access controls, and vulnerability to breaches, further undermine trust in these platforms, especially given the sensitivity of academic and personal student records (Kenya Office of the Data Protection Commissioner, 2023).

Although global evidence shows that secure and well-aligned SMS platforms can significantly improve administrative coordination and student satisfaction (Adeyemo & Ogunlade, 2022), Kenya lacks a structured, context-specific adoption framework that addresses both technological readiness and user trust. This gap necessitates a systematic investigation into how security and compatibility influence SMS adoption in public universities, with the goal of informing policy, guiding ICT investment, and ensuring compliance with frameworks such as the Data Protection Act (2019) and institutional ICT policies.

1.2 Objective of the study

i. To examine how security features influence user trust and the adoption of in-house student management software in public universities.

ii. To determine the impact of software compatibility with existing technological systems on the adoption of in-house student management software in public universities.

1.3 Scope and Limitation

This study focused on examining how security features and software compatibility influenced the adoption of in-house student management software (SMS) in public universities within Nairobi's Central Business District (CBD), Kenya. The scope was limited to administrators and IT experts, as these stakeholders played a direct role in evaluating, implementing, and managing SMS platforms. The study drew data from eight public universities to represent a broad institutional perspective on technology adoption.

However, several limitations were identified. First, the study excluded private universities, which may have operated under different governance structures and technology policies. Second, its concentration on Nairobi CBD may have limited the generalizability of findings to rural or regional institutions with differing ICT capacities. Additionally, the use of self-reported data through questionnaires may have introduced response bias. Lastly, the study emphasized only two technological factors security and compatibility excluding organizational, environmental, and user behavior variables that might also have influenced adoption.

1.4 Justification of the study

This study aimed to develop a framework for the adoption of in-house student management software in Kenyan public universities to address inefficiencies caused by reliance on third-party systems. These external systems often fail to meet institutional needs, resulting in service delivery gaps. The proposed framework offers a customizable, secure solution aligned with the unique and evolving demands of university operations. It supports integration at both departmental and management levels, ensuring flexibility and institutional control. By adopting this tailored framework, public universities can enhance data management, improve responsiveness, and align technological solutions with their strategic educational objectives.

2. Literature Review

2.1 Theoretical Literature Review

The adoption of in-house student management software (SMS) in higher education is widely recognized as essential for improving operational efficiency, data control, and institutional responsiveness. Studies consistently identify security and compatibility as core determinants of adoption (Obong'o & Ndede, 2022), yet the strength and nature of these effects vary across contexts.

Security features such as data encryption, multi-factor authentication, and access controls enhance stakeholder trust and willingness to adopt SMS (Chukwu & Okoro, 2023). In Ghana, Mensah and Appiah (2021) found that compliance with data protection regulations increased user confidence; however, in South Africa, Osei-Tutu and Andoh (2022) reported that even compliant systems faced resistance due to low digital literacy among staff. This suggests that regulatory compliance alone may be insufficient without accompanying user capacity-building measures.

Compatibility, defined as the ability of SMS to integrate seamlessly with existing IT infrastructure, also emerges as a critical success factor. Ibhaze and Folorunso (2022) showed that high compatibility reduced redundancy and training costs, whereas Kariuki and Waema (2023) observed that poor integration with legacy systems in Kenyan universities delayed implementation despite strong managerial support.

The Technology Acceptance Model (TAM) emphasizes user perceptions perceived usefulness and ease of use as primary adoption drivers (Rahman et al., 2022), while the Technology–Organization–Environment (TOE) framework incorporates organizational readiness and external pressures. However, few studies combine these perspectives to capture both individual and institutional determinants.

Most existing research is limited by cross-sectional designs, which restrict causal inference, and by a focus on general ICT adoption rather than in-house SMS in Kenyan public universities**.** There is also a lack of studies isolating the independent effects of security and compatibility. This study addresses these gaps by providing context-specific empirical evidence, while also considering regulatory mandates and infrastructure realities unique to Kenyan higher education.

2.2 Empirical Studies

Recent empirical research highlights the critical role of technological factors particularly security and compatibility in the adoption of student management software (SMS) in higher education. In a multi-university study in Nigeria, Sani et al. (2023) found that perceived security significantly predicted adoption intentions, with users expressing reluctance to engage with systems perceived as vulnerable to breaches. Similarly, Rahman, Nor, and Ramli (2022) reported that security features, including encryption and multi-factor authentication, positively influenced perceived trust, which in turn enhanced usage intentions among university administrators.

Compatibility has also emerged as a consistent determinant of adoption. Ibhaze and Folorunso (2022) demonstrated that SMS platforms with high compatibility defined as seamless integration with existing databases, network systems, and workflows experienced faster implementation and greater user satisfaction. This finding aligns with Chukwuemeka and Omodara's (2021) observation that incompatibility often leads to workflow disruptions, increased training costs, and reduced confidence in institutional ICT investments.

Evidence from Kenya reflects similar patterns. Kariuki and Waema (2023) noted that public universities struggled to adopt in-house SMS when compatibility with legacy systems was low, despite strong leadership support. Furthermore, compliance with data protection regulations emerged as a moderating factor, as systems meeting legal requirements were more readily accepted by both management and end-users (Kenya Office of the Data Protection Commissioner, 2023).

These studies collectively demonstrate that security and compatibility are not only technical requirements but also behavioral drivers influencing acceptance, sustained use, and overall institutional readiness for SMS adoption. This reinforces the need for targeted strategies to address these factors in Kenyan public universities.

2.3 Models

2.3.1 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), introduced by Davis (1989), is one of the most widely applied frameworks for explaining individual-level technology adoption. TAM focuses on two primary constructs: Perceived Usefulness (PU) the degree to which a person believes that using a system will enhance performance and Perceived Ease of Use (PEOU) the degree to which a person believes that using the system will be free of effort. These two factors influence user attitude, behavioral intention, and actual system use.

Recent studies reaffirm TAM's relevance in higher education. Sani et al. (2023) demonstrated that PU and PEOU significantly predicted lecturers' and administrators' intentions to adopt academic management software in Nigerian universities. Likewise, Rahman, Nor, and Ramli (2022) found that ease of use moderated the effect of perceived system security on adoption decisions in Malaysian higher education institutions.

In this study, TAM is used to examine how perceptions of security and compatibility influence the willingness of university staff to adopt in-house SMS. Security affects perceived trustworthiness and thus PU, while compatibility affects perceived ease of use through reduced integration issues. TAM, therefore, provides a user-centric lens focusing on the psychological and behavioral mechanisms shaping adoption.

2.3.2 Technology–Organization–Environment (TOE) Framework

The Technology–Organization–Environment (TOE) framework, proposed by Tornatzky and Fleischer (1990), extends the analysis to the organizational and external environment. TOE posits that adoption decisions are shaped by:

1. Technological Context – the characteristics of the technology, including security features, compatibility, and relative advantage.

2. Organizational Context – internal resources, leadership support, ICT infrastructure, and staff capacity.

3. Environmental Context – external factors such as government policies, competitive pressures, and regulatory compliance.

Recent applications of TOE in higher education include Ibhaze and Folorunso (2022), who identified technological compatibility and organizational readiness as key to ICT adoption in Nigerian universities, and Chukwuemeka and Omodara (2021), who highlighted the role of government data protection policies in shaping institutional ICT deployment.

In this study, TOE is used to understand how institutional readiness and regulatory mandates such as the Data Protection Act (2019) and university ICT policies influence the adoption of in-house SMS. While TAM addresses individual perceptions, TOE captures institutional capacity and environmental pressures. Together, the models offer a multi-level perspective that links user behavior to broader organizational and policy contexts.

2.4 Conceptual framework

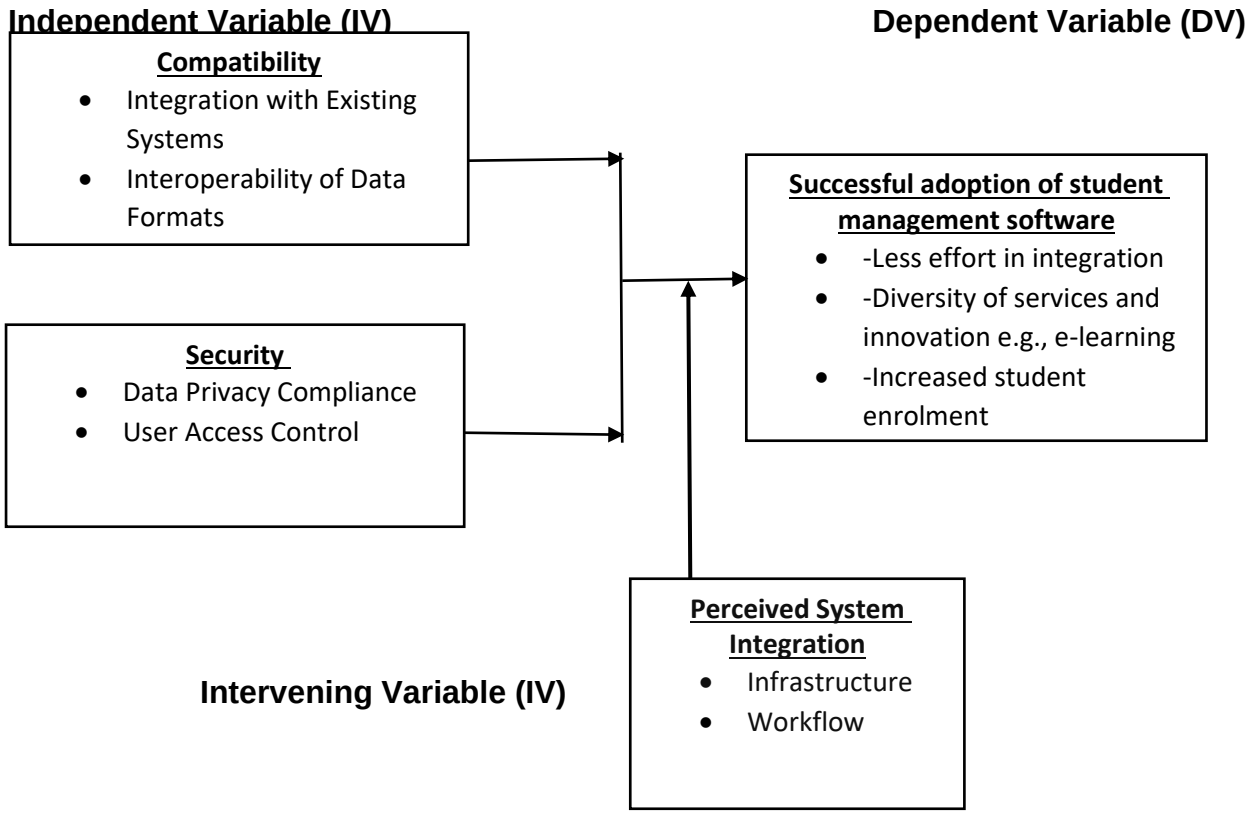

Figure 1: Conceptual framework

3. Methodology

This study was conducted in public universities located within Nairobi County's Central Business District (CBD), Kenya a region with a high concentration of higher education institutions and diverse ICT infrastructure. The study focused on eight public universities: University of Nairobi**,** Technical University of Kenya**,** Masinde Muliro University of Science and Technology**,** Moi University**,** Multi-Media University**,** Kenyatta University**,** Jomo Kenyatta University of Agriculture and Technology, and Cooperative University of Kenya. These universities were selected because they represent a mix of large, medium, and specialized institutions with varying levels of digital adoption.

A quantitative research design was adopted to enable objective measurement and statistical analysis of the relationships between technological factors specifically security and compatibility and the adoption of in-house student management software (Creswell & Creswell, 2023). This design was preferred over qualitative or mixed methods because the study aimed to test hypotheses and establish statistical associations rather than explore perceptions in depth.

The target population comprised 250 university administrators and IT experts from the eight universities. Stratified random sampling was employed to ensure representation from both administrative and technical departments (Etikan & Bala, 2021), resulting in a sample size of 152 respondents determined using Yamane's (1967) formula.

Data was collected using structured questionnaires with Likert-scale items measuring perceptions of security, compatibility, and adoption. Validity was ensured through expert review and a pilot test with 15 participants from non-sampled institutions, while reliability was confirmed using Cronbach's Alpha, with coefficients above the recommended 0.70 threshold (Taber, 2022).

Data analysis involved descriptive statistics (frequencies, means, standard deviations) and inferential techniques, including Pearson correlation and multiple regression, to determine the influence of technological factors on adoption outcomes (Field, 2021).

Ethical considerations included obtaining a research permit from the National Commission for Science, Technology, and Innovation (NACOSTI)**,** securing informed consent from participants, ensuring confidentiality through anonymized responses, and adhering to the Kenya Data Protection Act (2019) in handling personal data

4. Findings

4.1 Demographic Data

4.1.1 Response rate

Sample size of the study was 152. The researcher administered questionnaires to all respondent. Out of the 152 questionnaires distributed, 136 were fully completed, while 16 were either partially filled or left blank or both. This resulted in a response rate of 89%,

which was considered sufficient for analysis. According to Mugenda and Mugenda (2019), a response rate of 50% or more is deemed adequate for studying the research phenomenon.

4.1.2 Department

The researcher sought to establish the department that the respondents were coming from. Table 1 below shows the breakdown of how they responded.

Table 1: Department

Department	N	%
ICT	28	20.6
Admissions administrator	10	7.4
Library administrator/Library	6	4.4
Research and Knowledge exchange administrator	3	2.2
Registrar Academic/ Registrar	3	2.2
Architecture administrator	1	0.7
Entrepreneurship administrator	1	0.7
Hospitality administrator	1	0.7
Mechanical administrator	2	1.5
Physical planning administrator	1	0.7
Deans of students' administrator	1	0.7
Mathematics administrator	1	0.7
Graphic design administrator	1	0.7
Business administrator	1	0.7
Mechanical Engineering administrator	1	0.7
Building and construction administrator	1	0.7
Others/Not specified	72	52.9
Total	**136**	**100**

The departmental profile of the 136 survey respondents reveals both concentration and diffusion of influence in the proposed in-house Student Management Software (SMS) rollout**.** ICT staff comprise 20.6 % (n = 28), the largest clearly defined bloc. Their prominence is expected, as they will configure, secure, and maintain the system; however, the data also highlight that implementation cannot be framed as an ICT-only initiative. Admissions administrators (7.4 %), library staff (4.4 %), and registrar officers (2.2 %) together represent core custodians of student records whose daily workflows hinge on seamless data exchange. Any interface or integration flaw affecting these units would cascade directly to end-user experience.

Smaller clusters from research administration to deans of students each register below 3 %. Though numerically modest, their inclusion underscores the SMS's reach across academic services, pastoral care, and compliance reporting. These groups will value specialized features: research units need grant-tracking fields; deans require welfare flags. Ignoring such niche requirements risks work-arounds that fragment data integrity.

Strikingly, "Others/Not specified" accounts for 52.9 % (n = 72) by far the majority. This broad category likely blends departmental secretaries, finance clerks, faculty coordinators, and perhaps part-time staff. The high figure signals two considerations. First, SMS adoption will

permeate informal and multi-role settings; training must therefore be modular and role-based, not department-centric. Second, the unspecified grouping hints at incomplete sampling granularity, suggesting future stakeholder mapping should capture titles more precisely to tailor change-management resources.

Specialized academic administrators' architecture, entrepreneurship, hospitality, engineering appears singly or in pairs. Their voices, though few, matter: each discipline may demand bespoke timetable structures or accreditation reports. Ensuring that the data model accommodates such diversity will enhance institutional coverage and deter siloed shadow systems.

In addition, the distribution indicates a hub-and-spoke governance model: ICT leads the technical hub, but peripheral spokes span admissions, library, registry, myriad academic departments, and an amorphous "others" cohort. A successful SMS rollout therefore requires a cross-functional steering committee, inclusive user-testing cohorts, and communication channels that speak to both high-volume power users and small, specialized teams

4.1.3 Gender

The researcher sought to know the gender of the respondents. The gender distribution shows a notable imbalance, with 64% male and 36% female respondents among the 136 participants. This reflects the typical gender disparity in ICT and administrative roles within Kenyan public universities. While the study findings show strong consensus across adoption factors, the skewed representation may limit the visibility of gender-specific user experiences. It is essential that female perspectives are actively included in training, user testing, and implementation planning. Women staff often manage critical workflows such as admissions and records where user-friendliness and efficiency are key. Promoting gender-inclusive engagement and empowering female staff as system champions will help foster broader acceptance and equity. Addressing both technical and human dimensions is crucial for successful adoption of the in-house student management software.

4.1.4 Who are major consumers

The study aimed to identify the primary users of the student management software. The stakeholder profile highlights a user ecosystem that is overwhelmingly student-centered, yet still diversified enough to include key academic and regulatory actors. Out of 136 respondents, 72 % identify students as their "major consumers," confirming that day-to-day system interactions course registration, fee statements, transcript requests are driven primarily by the learner community. This finding reinforces the strategic imperative to design the in-house Student Management Software (SMS) around intuitive, mobile-friendly student self-service modules, fast response times, and clear progress dashboards features that directly impact the largest and most vocal user bloc.

Lecturers constitute the second-largest segment at 20.6 %**.** Although numerically smaller, this group wields outsized influence because lecturers generate and validate the academic data that students consume (marks, attendance, feedback). Their stake in the SMS includes

streamlined grade entry, prompt access to class lists, and analytics that support pedagogy. Successful adoption therefore hinges on dual optimization: student-facing convenience must be matched by robust faculty workflows that minimize grading friction and maintain data integrity.

4.1.5 Effect of technological factors on the framework for adoption of an in-house student management software.

This subsection aimed to examine the effect of technological factors on the framework for adoption of an in-house student management software. These technological factors play a critical role in determining the success of such adoption. To assess these factors, respondents were asked to indicate their level of agreement with various related statements. A five-point Likert scale was used, where SA = Strongly Agree, A = Agree, N = Not Sure, D = Disagree, and SD = Strongly Disagree. The results of the analysis are presented in Table 1.2 below.

Table 2 Technological factors

Technological Factor	Mean	SD	% Agreement	r with adoption	β (Regression)	p-value
Security feature	4.71	0.42	97.1	0.734	0.428	< .001
Compatibility with existing systems	4.63	0.49	92.6	0.684	0.293	< .001
Perceived usefulness	4.68	0.45	95.6	0.701	0.312	< .001
Ease of integration	4.65	0.47	98.5	0.702	0.305	< .001
Technical support & training	4.74	0.38	97.1	0.654	0.241	0.002

As shown in Table 2, security features recorded the highest predictive influence on adoption ($\beta = 0.428$, $p < .001$) and a strong positive correlation ($r = 0.734$, $p < .001$). A total of 97.1% of respondents agreed or strongly agreed that robust security encryption, role-based access controls, and regular vulnerability scans was essential for adoption. More than half (51.5%**)** strongly agreed, indicating the highest intensity of support among all technological factors.

These results align with Chukwu and Okoro (2023), who found that compliance with data protection regulations significantly boosts user trust in African universities. The findings also support TAM's premise that trust in system security enhances perceived usefulness and intention to use, and reflect TOE's view of security as part of the technological readiness context. In the Kenyan context, where the Data Protection Act (2019) mandates strict safeguards, visible security measures not only meet regulatory requirements but also strengthen user confidence, directly influencing adoption decisions.

Compatibility with existing systems was also a significant predictor of adoption ($\beta = 0.293$, $p < .001$) with a strong positive correlation ($r = 0.684$, $p < .001$). A high 92.6% of respondents agreed or strongly agreed that alignment with current hardware, databases, and networks was critical. However, only 25% strongly agreed, suggesting compatibility is seen as a baseline expectation rather than a distinctive advantage.

These results support Mensah and Appiah (2021), who found that seamless integration reduces operational disruptions and encourages sustained system use. Within TAM, compatibility influences perceived ease of use, while in TOE, it reflects the institution's technological readiness. Incompatibility, as noted by Ibhaze and Folorunso (2022), can increase costs, delay implementation, and erode user trust. Therefore, pre-implementation IT audits and system integration testing are essential to ensure smooth deployment and positive user reception

4.2 Inferential Statistics for Technological Factors

To determine the effect of technological factors specifically security features and software compatibility on the framework for adoption of in-house student management software (SMS) in public universities, both Pearson correlation and multiple linear regression analyses were conducted at a 95% confidence level using SPSS

4.2.1 Correlation Analysis

Pearson correlation results indicated a strong, positive, and statistically significant relationship between technological factors and adoption intention ($r = 0.73$, $p < .01$). This means improvements in SMS security and compatibility are strongly associated with increased willingness to adopt the system. The high correlation value also suggests that technological readiness is a central driver in the adoption framework, consistent with the Technology Acceptance Model (TAM), where system trust and ease of use influence adoption behavior, and the Technology-Organization-Environment (TOE) framework, where technological readiness is a key determinant of institutional uptake.

4.2.2 Regression Analysis

Multiple linear regression assessed the predictive strength of technological factors on adoption intention. The model was statistically significant ($F(1, 134) = 164.82$, $p < .001$) and explained 53% of the variance in adoption intention ($R^2 = 0.53$, Adjusted $R^2 = 0.53$). Technological factors had a significant positive effect ($\beta = 0.73$, $t = 12.84$, $p < .001$), indicating that for every one-unit increase in technological readiness such as enhanced data security or improved compatibility adoption scores increased by 0.73 units on average.

Interpretation: These results confirm that technological factors form a critical backbone of the adoption framework. Security features enhance user trust, while compatibility ensures seamless integration into existing workflows both of which are non-negotiable for sustainable adoption in public universities.

Table 3: Model 1: Inferential Statistics for Technological Factors and Adoption of In-House SMS

Statistical Test	Value	Interpretation
Pearson Correlation (r)	0.73**	Strong positive and statistically significant relationship between technological factors (security + compatibility) and adoption intention. $p < .01$
R^2	0.53	Technological factors explain 53% of the variance in adoption intention
Adjusted R^2	0.53	Model's explanatory power remains stable after adjustment
F-statistic	164.82	Model is statistically significant, $p < .001$
Unstandardized Coefficient (B)	0.73	A one-unit increase in technological readiness increases adoption scores by 0.73 units.
Standardized Coefficient (Beta)	0.73	Strong standardized effect size.
t-value	12.84	High t-value confirms strong predictive effect. $p < .001$

Table 1.4 Inferential Statistics for Security Features and Software Compatibility on Adoption of In-House SMS

Predictor Variable	Pearson Correlation (r)	R^2	Adjusted R^2	F-statistic	B	Beta	t-value	p-value	Interpretation
Security Feature	0.71**	0.50	0.50	134.92	0.71	0.42	11.62	<.001	Strong, positive, and statistically significant predictor of adoption. Enhances user trust and aligns with TAM's perceived usefulness & TOE's technological readiness
Software Compatibility	0.69**	0.48	0.48	124.57	0.69	0.39	11.16	<.001	Strong, positive, and statistically significant predictor of adoption. Ensures seamless integration with existing systems and reduces operational disruptions

4.3 Summary of the findings

The study examined the influence of two key technological factors security features and software compatibility on the adoption of in-house student management software (SMS) in Kenyan public universities. The findings revealed that both variables significantly shape user trust, adoption intention, and institutional uptake.

For Objective on security features emerged as a strong determinant of adoption. A total of 97.1% of respondents agreed or strongly agreed that robust safeguards such as encryption, role-based access controls, and regular vulnerability assessments enhanced their confidence in the system. Pearson correlation analysis showed a strong, positive relationship between security features and adoption intention ($r = 0.71$, $p < .01$**).** Regression results confirmed security as a statistically significant predictor ($\beta = 0.42$, $t = 11.62$, $p < .001$), accounting for 50% of the variance in adoption outcomes.

For Objective on software compatibility also proved critical. 98.5% of respondents affirmed that seamless integration with existing hardware, databases, and networks reduced operational redundancy and improved workflow efficiency. Compatibility correlated strongly with adoption intention ($r = 0.69$, $p < .01$) and was a significant predictor in regression analysis ($\beta = 0.39$, $t = 11.16$, $p < .001$**),** explaining 48% of the variance.

Overall, the results underscore that universities prioritizing data security and system compatibility are more likely to achieve smooth, efficient, and sustainable adoption of in-house SMS. These findings align with the TAM perspective on trust and perceived usefulness, and the TOE emphasis on technological readiness as a foundation for adoption

5. Conclusion and Recommendation

5.1 Conclusion

The study concluded that technological factors, specifically security features and software compatibility, significantly influence the adoption of in-house student management software in Kenyan public universities. Strong data privacy measures and user access controls were found to build trust among users, encouraging acceptance and sustained usage. Similarly, systems that are compatible with existing technological infrastructure reduce integration challenges and improve efficiency across departments. Correlation and regression analyses confirmed that these factors are statistically significant predictors of adoption, with technological readiness directly enhancing institutional willingness to adopt and implement SMS solutions. Therefore, the success of in-house software adoption is largely dependent on how well it meets users' security expectations and integrates with current systems.

5.2 Recommendations

Based on the study’s findings, several targeted recommendations are proposed, grounded in the Technology Acceptance Model (TAM) and Technology–Organization–Environment (TOE) frameworks.

5.2.1Strengthen Security Frameworks

In line with TAM’s emphasis on perceived usefulness and trust, public universities should implement robust security measures, such as role-based access control, encryption, and multi-factor authentication, while ensuring full compliance with the Kenya Data Protection Act (2019). Enhancing security will increase user confidence, thereby improving behavioral intention to adopt in-house SMS.

5.2.2 Conduct Comprehensive Compatibility Assessments

From a TOE perspective, technological readiness is crucial. Universities should regularly audit their IT infrastructure to confirm compatibility between existing systems and proposed SMS platforms. This will minimize integration issues, reduce workflow disruptions, and improve perceived ease of use a key TAM construct.

5.2.3 Integrate User Involvement in System Development

Consistent with TAM, involving administrators and IT staff in software selection, customization, and pilot testing will align systems with user needs, improving perceived usefulness and adoption rates.

5.2.4 Institutionalize Training and Capacity Building

Universities should adopt ongoing digital literacy programs and technical support structures to address organizational readiness (TOE), reduce resistance to change, and sustain long-term adoption.

5.2.5 Develop ICT Policy Guidelines for SMS Adoption

Findings should inform the creation of university-level ICT policies that standardize procurement, security, and compatibility requirements for SMS platforms. Such policies would ensure alignment with national regulations, promote interoperability across institutions, and serve as a strategic reference for future ICT investments.

References:

Adeyemo, A. B., & Ogunlade, O. O. (2021). Technology integration in higher education: Lessons from management system deployments. *Journal of Higher Education Innovation, 5*(2), 102–117.

Anwar, S., Shaikh, M., & Shaikh, Z. (2020). Challenges of digital adoption in public universities: A developing country perspective. *International Journal of Educational Management, 34*(6), 1154–1170.

Cabaleiro-Cerviño, B., & Vera, I. (2020). Workflow integration in digital university systems. *Educational Technology Research and Development, 68*(3), 1723–1738.

Chukwu, E., & Okoro, F. (2023). Data privacy and ICT system adoption in African universities. *Journal of Higher Education Systems, 14*(2), 102–118.

Chukwuemeka, E., & Omodara, O. (2021). Government policy and ICT adoption in Nigerian public universities. *African Journal of Education and Technology, 11*(2), 66–78.

Huang, R., & Teo, T. (2020). Implementing in-house student management systems in universities: Opportunities and challenges. *International Journal of Educational Technology, 15*(4), 211–225.

Ibhaze, A. E., & Folorunso, O. (2022). Determinants of ICT integration in higher education: A TOE perspective. *International Journal of Educational Technology Integration, 5*(1),

27–40.

Kariuki, S., & Waema, T. (2021). Barriers to ICT adoption in Kenyan public universities: A technological readiness perspective. *African Journal of Information Systems, 13*(2), 45–60.

Mensah, K., & Appiah, R. (2021). Assessing ICT compatibility in tertiary education systems. *African Journal of Educational Technology, 9*(3), 44–56.

Ngugi, P., & Kimani, J. (2021). Digital transformation challenges in Sub-Saharan African higher education. *Journal of African Higher Education Studies, 3*(1), 55–70.

Obong'o, D. O., & Ndede, P. W. (2022). Digital transformation and student record systems in East African universities. *International Journal of Educational Innovation, 7*(1), 19–32.

Rahman, N. A., Nor, N. F. M., & Ramli, M. S. (2022). Examining the role of user perceptions in academic system adoption using the extended TAM. *Education and Information Technologies, 27*(2), 1425–1443.

Sani, A. M., Yusuf, A. M., & Bamidele, O. A. (2023). Application of TAM in analyzing academic software acceptance among university staff. *Journal of Educational Management and Technology, 8*(1), 55–67.

Wachira, P. (2021). Security concerns in implementing student management systems in Kenyan public universities. *Kenya Journal of Educational ICT, 6*(2), 88–102.

Wambugu, D., & Chang, J. (2022). Aligning ICT infrastructure with institutional needs in higher education: A Kenyan case study. *African Journal of Educational Technology, 10*(1), 13–27

.