ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

Encryption-Based Security Framework for Ensuring Data Privacy and Protection Compliance in Higher Education E-Learning Systems in Uganda

Kavunga Tembo Joseph[1]; Ali Najib[2]; Anthony Bua[3]; David Kakeeto[4]

[1]Postgraduate Student, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda
[2,4]Senior Lecturer, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda
[3]Lecturer, Faculty of Science and Technology, School of Postgraduate Studies and Research, Victoria University, Kampala, Uganda

Publication Date: 2026/08/10

Abstract: Educational institutions increasingly rely on e-learning platforms that store large volumes of sensitive student and staff data, yet many of these platforms continue to lack robust technical safeguards and effective privacy-compliance mechanisms. This study designed and proposed an encryption-based security framework to enhance data privacy and support compliance with Uganda's Data Protection and Privacy Act (DPPA) 2019 in higher education the e-learning system in Uganda, guided by three objectives: assessing the current state of data privacy and DPPA 2019 compliance; establishing the effectiveness of a proposed encryption-based security framework in enhancing confidentiality, integrity, and access control; and determining the degree to which the framework would facilitate regulatory compliance. The study adopted a mixed-methods design combining a quantitative correlational survey and a qualitative case study. A structured questionnaire was self-administered to 120 , and semi-structured interviews were conducted with four key informants from the ICT department. Quantitative data were analysed SPSS using, descriptive statistics, Pearson correlation, and Cronbach's alpha reliability testing; interview data were analysed thematically using Braun and Clarke's six-phase reflexive thematic analysis. The study was theoretically grounded in the Protection Motivation Theory, the CIA Triad, and the NIST Cybersecurity Framework. The study findings revealed moderate data-privacy awareness coupled with high breach anxiety: concern about data breaches and unauthorized use exceeded respondents' confidence in existing protections, while knowledge of who accesses their data of breach-reporting procedures remained low. All inter-objective correlations were statistically significant, with the strongest relationship observed between framework effectiveness and compliance. Reliability across the three objective scales ranged from acceptable. Interviews with ICT staff confirmed that encryption is present but technically opaque, that access controls are undermined by voluntary credential sharing, and that consent is reduced to a click-through formality. Notably, 80.8% of respondents indicated they would increase their e-learning engagement if given greater control over their data. The study concludes that Uganda's higher education data privacy challenges are fundamentally socio-technical, requiring simultaneous technical reinforcement and human-centred governance. It proposes and recommends the urgent deployment of a six-layer encryption-based security framework comprising data collection and consent, data-at-rest and in-transit encryption (AES-256-GCM, TLS 1.3), role-based access control and multi-factor authentication, integrity and audit logging, compliance and governance, and a user-empowerment dashboard, phased over 36 months and anchored in mandatory data-privacy training and a DPPA 2019-aligned institutional policy.

Keywords: *Encryption, Data Privacy, E-Learning Security, Data Protection Compliance, Uganda DPPA 2019, Access Control, Protection Motivation Theory, Higher Education Cybersecurity*.

How to Cite: Kavunga Tembo Joseph; Ali Najib; Anthony Bua; David Kakeeto (2026) Encryption-Based Security Framework for Ensuring Data Privacy and Protection Compliance in Higher Education E-Learning Systems in Uganda. *International Journal of Innovative Science and Research Technology*, 11(7), 3415-3427. https://doi.org/10.38124/ijisrt/26jul1810

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

I. INTRODUCTION

This study examines the design of an encryption-based security framework aimed at enhancing data privacy and ensuring compliance with data protection standards in Uganda's e-learning systems, a higher education institution whose learning management system and e-learning platform mediate the academic, personal, and financial data of students and staff.

➢ *Historical Perspective*

The challenge of ensuring data privacy and protection compliance in e-learning systems has evolved alongside the rapid digitisation of education, with early research focusing on basic access controls and later studies exploring advanced cryptographic solutions. Globally, the proliferation of digital learning platforms has exposed sensitive student and institutional data to increasing risks of breaches, unauthorized access, and regulatory non-compliance (Polydorou, 2023). Regulatory responses such as the GDPR set new standards for privacy compliance globally, and strong legal frameworks drove the adoption of advanced encryption, homomorphic encryption, and blockchain integration for fine-grained access control in Europe and North America (Muhiddinov, 2025). In Asia and the Middle East, hybrid models combining AES, RSA, and elliptic-curve cryptography with machine learning have been explored to balance efficiency with security (Mihailescu et al., 2020.

In Africa, most regions face low ICT adoption rates, low cybersecurity awareness, and limited infrastructure. During COVID-19, Uganda's rapid shift to digital education exposed vulnerabilities such as weak enforcement of data protection laws, reliance on third-party EdTech vendors with unclear privacy practices, and low stakeholder awareness (Ubaka-Okoye, 2020). Despite progress in cryptographic techniques, most existing studies focus on technical controls in isolation rather than an integrated framework that also accounts for regulatory alignment (Mawgoud et al., 2025), and there remains a gap in region-specific solutions that address the infrastructural realities of Africa and Uganda while aligning with international best practice (Ubaka-Okoye, 2020).

➢ *Theoretical Perspective*

This study is theoretically grounded in the Protection Motivation Theory (PMT) (Rogers, 1975), supplemented by the Confidentiality-Integrity-Availability (CIA) Triad and the NIST Cybersecurity Framework (NIST CSF 2.0, 2024). PMT explains how individuals and institutions evaluate a threat through threat appraisal and coping appraisal before adopting protective behaviour (Mou et al., 2022); it is relevant here because it links the design and perceived effectiveness of the encryption framework to actual protective and compliant behaviour among students, staff, and IT personnel. The CIA Triad underpins the technical design of the framework by holding that confidentiality, integrity, and availability must be preserved simultaneously, so that encryption mechanisms protect data without compromising system usability. The NIST CSF supplies a broad governance scaffold, structured around the functions of identify, protect, detect, respond, and recover, that supports proactive risk management and continuity planning. Reviewed together, these frameworks reveal a gap: existing models emphasise threat exposure but offer limited guidance tailored to the resource constraints and regulatory context of e-learning systems in African higher education, a gap this study's proposed framework directly addresses.

➢ *Contextual Perspective*

Educational institutions, particularly universities, collect vast amounts of sensitive student information encompassing demographics, enrolment, academic performance, and financial records, making data privacy a paramount concern (O'Hara & Straus, 2022). Universities have experienced significant data breaches due to inadequate encryption and outdated security procedures, and the adoption of third-party EdTech services exposes institutional systems to unauthorized disclosure and external threats. At the university, the increasing volume of digital data flows through the E-learning platfrom e-learning platform and growing regulatory demands under Uganda's Data Protection and Privacy Act 2019 have created a pressing need for stronger encryption techniques, clearer access governance, and restored confidence and trust in the university's digital ecosystem.

➢ *Conceptual Perspective*

This study is grounded in four key concepts: an encryption-based security framework, data privacy, data protection compliance, and e-learning systems, all within the context of the university. Encryption is a cryptographic process that converts readable data into an unreadable form using a key and an algorithm to preserve the confidentiality and integrity of data in transit and at rest (Stallings, 2017). A security framework is a structured set of policies, controls, and technologies that guide how an organisation protects sensitive information (ISO/IEC 27001); in this study, an encryption-based security framework refers to the structured set of encryption mechanisms, access-control mechanisms, and key-management procedures integrated into the university's e-learning system to protect student and staff data. Data privacy refers to the prevention of unauthorized access, disclosure, and misuse of academic and personal information, while data protection compliance refers to the degree to which the proposed framework aligns with Uganda's national legal framework, institutional ICT policy, and relevant international standards (Bygrave, 2014). E-learning systems, in this study, refer specifically to the electronic learning platforms and related digital services used at the university, including the e-learning platform learning management system, online assessment tools, and student information portals.

➢ *Statement of the Problem*

Despite the growing adoption of e-learning systems in Uganda's higher education institutions, many e-learning systems continue to lack robust technical safeguards and effective privacy-compliance mechanisms for protecting sensitive academic and personal data. Consequently, these systems remain exposed to unauthorized access, data breaches, improper data handling, and non-compliance with applicable data protection requirements. Persistent weaknesses, such as inconsistently encrypted data storage, dependence on legacy systems with insufficient security controls, misalignment

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

between institutional privacy policies and actual practice, limited staff training, and low user awareness of data-protection obligations, further increase the risk of misuse and reputational harm.

The study's baseline findings confirm this pattern in practice: users expressed high anxiety about data breaches (mean=3.68) and unauthorized data use (mean=3.61), while their knowledge of who can access their data (mean=2.98), institutional transparency about data collection (mean=2.96), and awareness of breach-reporting procedures (mean=2.67) all fell below the moderate threshold. Qualitative evidence further confirmed that consent is often reduced to a click-through formality and that voluntary credential sharing among students undermines otherwise tiered access controls. It is upon this basis that this study designed and proposed an encryption-based security framework to strengthen confidentiality, improve key management and access control, and support compliance with national and international data protection regulations at the university.

➢ *Study Objectives*

- *General Objective*

The overall objective of this study was to design and propose an encryption-based security framework to enhance data privacy and ensure compliance with data protection standards and laws in higher education e-learning systems in Uganda.

- *Specific Objectives*

✓ To assess the current state of the higher education e-learning systems in ensuring data privacy and complying with Uganda's Data Protection and Privacy Act 2019.

✓ To establish the effectiveness of the proposed encryption-based security framework in enhancing data confidentiality, integrity, and access control while maintaining acceptable system performance.

✓ To determine the degree to which the implemented encryption-based security framework facilitates compliance with Uganda's data protection and privacy requirements within the higher education sector.

➢ *Study Hypotheses*

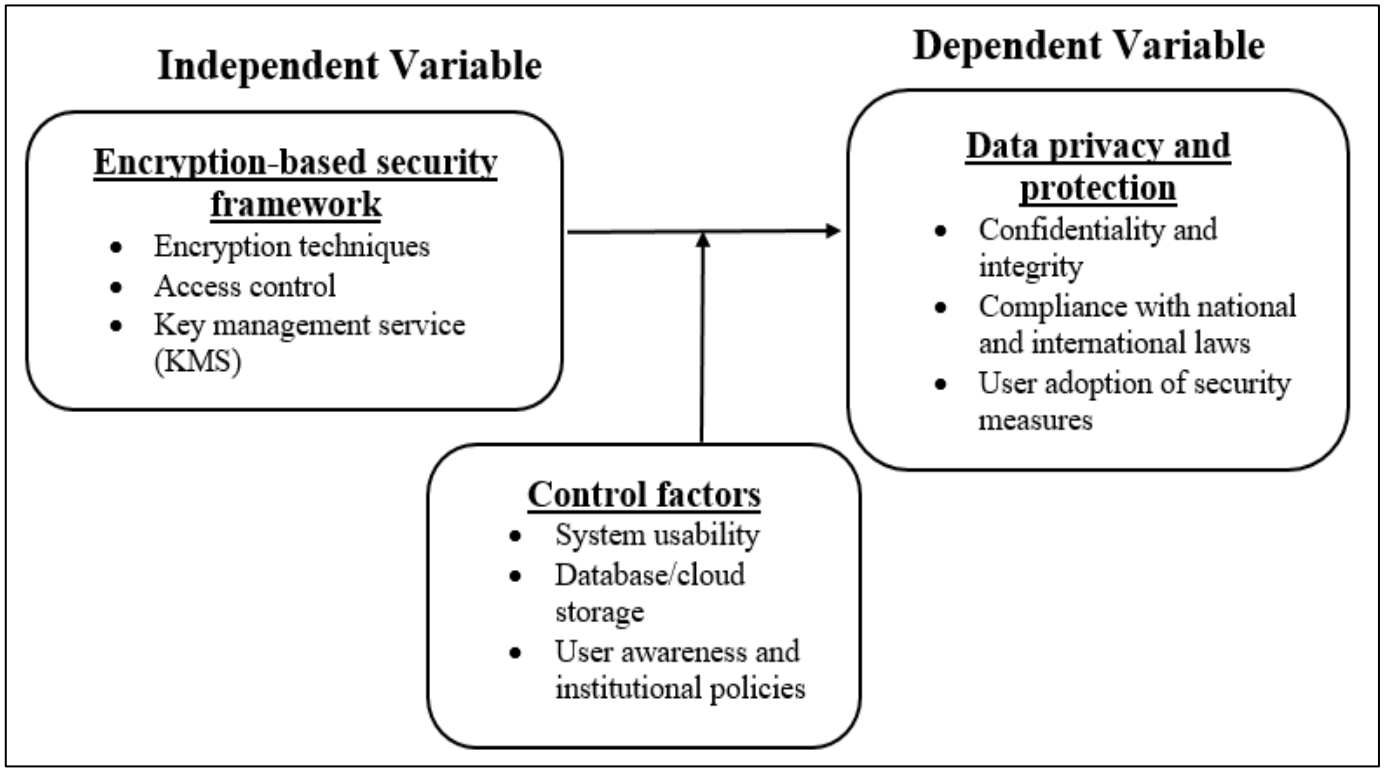
- H_0: The higher education current e-learning systems adequately ensure data privacy and comply with Uganda's Data Protection and Privacy Act 2019.
- H_1: There is a significant improvement in data confidentiality levels following the implementation of the encryption-based security framework.
- H_2: There is an improvement in the level of compliance with Uganda's Data Protection and Privacy Act 2019 following the implementation of the encryption-based security framework.

➢ *Conceptual Framework*

The conceptual framework displays the linkage between the encryption-based security framework (the independent variable) and data privacy and protection compliance (the dependent variable), moderated by institutional and technical factors.

- *Moderating Variables:*

Institutional ICT infrastructure quality, staff and student digital literacy, existing university data-protection policy, and the regulatory enforcement environment under the DPPA 2019.



ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

II. LITERATURE REVIEW

➢ *E-Learning Security and the Human-Technical Divide*

E-learning refers to the use of internet-based platforms to deliver instructional content and class experiences to geographically dispersed learners (Moore et al., 2011). Because e-learning systems depend on network and internet stability, and because the internet has become an environment where malicious actors actively target connected systems, ensuring the confidentiality, integrity, and availability of e-learning data has become an urgent institutional priority (Moore et al., 2011). Empirical studies on encryption-based security frameworks for e-learning show diverse methods and populations but a consistent finding: hybrid cryptographic techniques meaningfully strengthen access control, data confidentiality, and resistance to attack. Combined RSA-AES encryption (Shadmanova et al., 2024), attribute-based encryption integrated with blockchain (Muhiddinov, 2025), elliptic-curve cryptography with searchable encryption (Mihailescu et al., 2020), multi-factor authentication (Daidong-Fa et al., 2025), and homomorphic encryption applied to federated learning (Shen et al., 2024) have all been shown to reduce false-acceptance rates in authentication and improve accuracy in attack detection for cloud-based educational environments (El-Sofany et al., 2024).

The strengths of the existing literature lie in its practical implementation of hybrid encryption methods tailored for e-learning data protection, validated using real or simulated datasets, alongside emerging attention to user-behaviour considerations. However, few studies address user acceptance or policy alignment explicitly, and there is a limited focus on region-specific contexts such as Uganda or East Africa (Mpirirwe et al., 2021), where infrastructural constraints and nascent regulatory enforcement differ markedly from the European and North American contexts in which most cryptographic frameworks were developed and validated (Arsyad et al., 2026; Mihailescu et al., 2020).

➢ *Protection Motivation Theory and Security Behaviour*

Protection Motivation Theory has been applied extensively in the information-systems literature to explain the conditions under which individuals adopt protective security behaviour, holding that adoption depends jointly on threat appraisal (perceived severity and vulnerability) and coping appraisal (perceived response efficacy and self-efficacy) (Rogers, 1975; Mou et al., 2022). Applied to e-learning contexts, PMT predicts that students and staff will engage more fully with security-enhancing features, such as multi-factor authentication and transparent consent mechanisms, when they perceive both a credible threat to their data and confidence that the available protective measures are effective and usable (Rogers, 1975). This theoretical lens directly informs the design priority given, in the proposed framework, to visible and user-controlled security features rather than backend measures alone.

➢ *Regulatory Compliance in African Higher Education*

Uganda's Data Protection and Privacy Act (DPPA) 2019 establishes obligations for data controllers, including lawful processing, purpose limitation, security of processing, and breach notification within a reasonable timeframe (Muhangi, 2019). Comparative assessments of African data-protection regimes note that while legal instruments increasingly mirror international standards such as the GDPR, enforcement mechanisms and institutional champions frequently remain underdeveloped, producing a gap between formal legal compliance and operational reality (Greenleaf, 2021; Blazevic et al., 2021). Studies of Ugandan tertiary institutions similarly report that formalised data-governance structures capable of translating user awareness into systemic protection are often lacking (Mpirirwe et al., 2021), a condition consistent with the empirical findings of the present study at the university.

➢ *Encryption as a Trust and Adoption Mechanism*

Beyond its technical function, encryption and visible data-control mechanisms have been shown to function as trust-building and adoption-driving mechanisms in digital platforms (Ali & Zafar, 2017). Extending the Technology Acceptance Model (Davis, 1989), recent scholarship has proposed data sovereignty and perceived privacy control as an additional, contextually specific determinant of platform engagement alongside the traditional dimensions of perceived usefulness and ease of use (Mtebe & Raisamo, 2014). The privacy-calculus perspective further predicts that users engage more fully with digital platforms when perceived benefits, including security and control, outweigh perceived risks (Dinev & Hart, 2006), implying that investments in encryption and transparency are likely to yield measurable improvements in both compliance behaviour and user engagement.

III. METHODOLOGY

➢ *Research Design*

The study adopted a mixed-methods design, combining a quantitative correlational approach and a qualitative case study. Quantitatively, the design evaluated the perceived effectiveness of encryption mechanisms and compliance levels through a structured questionnaire; qualitatively, a case-study approach explored contextual factors specific to the university through semi-structured interviews with key ICT informants. Integrating the two approaches strengthened the robustness of the findings and supported triangulation between user perceptions and institutional practice.

➢ *Study Population and Sample*

The target population comprised stakeholders at the university directly affected by the implementation of an encryption-based security framework: IT staff and system administrators responsible for deploying and managing encryption measures; academic staff who access student data and upload content through the university's digital platforms; and students, particularly those in computer science, cybersecurity, and information technology-related programmes, who interact daily with the university's e-learning system. Using purposive sampling to obtain information-rich data from respondents most knowledgeable about and affected by the university's encryption practices and regulatory compliance, the study achieved a final sample of 120 questionnaire respondents and four semi-structured interview informants from the ICT department.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

➢ *Data Collection and Analysis*

Primary data were collected through a self-administered structured questionnaire designed in Google Forms and distributed electronically to all 120 respondents, and through semi-structured interviews conducted face-to-face and online with four key ICT informants. Secondary data, comprising university policy documents and relevant national and international regulatory instruments, supported the design of the survey and interview instruments and helped validate the primary findings.

Quantitative data were analysed in IBM SPSS using descriptive statistics (means, standard deviations, frequencies), Pearson correlation coefficients to test the relationships among the three research objectives, and Cronbach's alpha to assess the internal-consistency reliability of each objective's item set. Qualitative interview data were transcribed verbatim, anonymised, and analysed thematically following Braun and Clarke's (2006) six-phase reflexive thematic analysis framework, with an initial deductive coding structure refined inductively as new themes emerged. Quantitative and qualitative findings were triangulated to validate and deepen understanding of how the encryption-based framework would influence data privacy and compliance outcomes.

IV. STUDY FINDINGS

➢ *Demographic Composition of Respondents*

The study gauged the demographic and background characteristics of the 120 respondents. The results are presented in Table 1.

Table 1 Demographic Composition of Respondents (n = 120)

Category	Item	Frequency	Percentage
Respondent category	Students	104	86.7%
	Lecturers	7	5.8%
	Academic staff	5	4.2%
	Academic researchers	2	1.7%
	Security officers	2	1.7%
Gender	Male	82	68.3%
	Female	38	31.7%
Age range	18-25 years	46	38.3%
	26-35 years	63	52.5%
	36-45+ years	11	9.2%
Usage frequency	Daily	51	42.5%
	Weekly	35	29.2%
	Occasionally	24	20.0%
	Rarely	10	8.3%
System duration	Less than 1 year	25	20.8%
	1-2 years	62	51.7%
	3-4 years	7	5.8%
	More than 4 years	26	21.7%

Source: Field Data (2025)

Table 1 shows that the majority of respondents were students (86.7%), reflecting the primary population of e-learning users at the university. Male respondents made up 68.3% of the sample, and 52.5% fell into the 26-35 age group. A notable share (42.5%) used the e-learning system daily, and 51.7% had engaged with the platform for one to two years, indicating a digitally active and experienced respondent base well placed to assess the system's privacy and security posture.

➢ *Descriptive Statistics for Data Privacy and Security Perceptions*

All Likert-scale items were rated on a five-point scale (1 = strongly disagree to 5 = strongly agree), with mean scores interpreted as: 1.00-2.49 (Low), 2.50-3.49 (Moderate), and 3.50-5.00 (High). Table 2 presents the descriptive statistics for the seventeen items, grouped by research objective.

Table 2 Descriptive Statistics for Likert-Scale Items (n = 120)

Item	Construct	Mean	SD	Interpretation
Q1	Understanding of personal data collected	3.51	1.22	Moderate
Q2	Knowledge of who accesses data	2.98	1.28	Low-Moderate
Q3	Concern about unauthorized data use	3.61	1.29	Moderate-High
Q4	Worry about data breaches/leaks	3.68	1.33	Moderate-High
Q5	Privacy adequately protected on e-learning platform	3.48	1.12	Moderate
Q6	University informs about data collection	2.96	1.29	Low-Moderate
Q7	System uses strong technical security	3.57	1.16	Moderate
Q8	MFA available and easy to use	3.33	1.16	Moderate
Q9	Safety of submitting personal work online	3.28	1.26	Moderate
Q10	Training received on data protection	3.01	1.39	Moderate

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

Q11	Ability to change privacy settings	3.32	1.22	Moderate
Q12	Aware of university data protection policy	3.15	1.23	Moderate
Q13	Knowledge of breach-reporting procedures	2.67	1.37	Low-Moderate
Q14	University follows data protection regulations	3.62	1.05	Moderate
Q15	Privacy concerns discourage system use	2.68	1.14	Low-Moderate
Q16	Satisfied with data protection on system	3.46	1.03	Moderate
Q17	Willing to use more features with data control	4.06	1.06	High

Source: Field Data (2025)

Items Q1-Q5 assess awareness of the current state of data privacy within the e-learning platform. Data breaches (Q4: mean=3.68) and unauthorized use of personal data (Q3: mean=3.61) were the greatest concerns, both above the moderate threshold, while knowledge of who can access that data (Q2: mean=2.98) remained below it, indicating a critical gap in access transparency. Items Q6-Q9, addressing the perceived adequacy of technical security features, produced a compound mean of 3.28 (SD=0.90, α=0.719), the highest reliability among the three objectives; Q6 (institutional transparency) was the weakest item (mean=2.96), while Q7 and Q8 were moderate, suggesting technical security is partially perceived but not fully trusted. Items Q10-Q17, addressing compliance awareness, produced a compound mean of 3.25 (SD=0.65, α=0.662); the lowest-scoring items were Q13 (breach-reporting knowledge: mean=2.67) and Q15 (privacy concerns deterring use: mean=2.68), while Q17 (willingness to engage more with better data control: mean=4.06) was the single highest-scoring item in the study.

➢ *Reliability and Correlation Analysis*

Table 3 summarises the reliability statistics for each objective's item set, and Table 4 presents the Pearson correlation results testing the relationships among the three research objectives and selected item pairs.

Table 3 Reliability Statistics by Research Objective (n = 120)

Objective	No. of Items	Composite Mean	SD	Cronbach's α	Reliability
Obj. 1 – Current State	5	3.45	0.81	0.651	Acceptable
Obj. 2 – Framework Effectiveness	4	3.28	0.90	0.719	Acceptable
Obj. 3 – DPPA 2019 Compliance	8	3.25	0.65	0.662	Acceptable

Source: Field Data (2025)

Table 4 Pearson Correlation Coefficients for Key Constructs (n = 120)

Construct Pair	r	p-value	Interpretation
Current State (Obj.1) ↔ Framework Effectiveness (Obj.2)	0.448	< 0.001	Moderate positive
Current State (Obj.1) ↔ Compliance (Obj.3)	0.441	< 0.001	Moderate positive
Framework Effectiveness (Obj.2) ↔ Compliance (Obj.3)	0.544	< 0.001	Moderate-strong positive
Transparency (Q6) ↔ Technical Security (Q7)	0.342	< 0.001	Moderate positive
Technical Security (Q7) ↔ MFA (Q8)	0.525	< 0.001	Moderate-strong positive
Data Awareness (Q1) ↔ Training (Q10)	0.389	< 0.001	Moderate positive
Satisfaction (Q16) ↔ Privacy Deterrence (Q15)	-0.536	< 0.001	Moderate-strong negative

Source: Field Data (2025)

All inter-objective correlations were statistically significant ($p<0.001$). The strongest relationship was observed between framework effectiveness (Objective 2) and compliance (Objective 3) ($r=0.544$), indicating that improvements in the e-learning system's technical security posture are meaningfully associated with enhanced regulatory-compliance perceptions. The correlation between technical security and multi-factor authentication was similarly strong ($r=0.525$), affirming that these two components should be implemented together as complementary controls, consistent with NIST digital-identity guidance. The negative correlation between satisfaction and privacy-deterrence ($r=-0.536$) confirms that privacy anxiety and system satisfaction are inversely related, meaning that investment in encryption and transparency is likely to yield measurable improvements in user engagement and compliance-related behaviour. H_0 is rejected; H_1 and H_2 are supported by the pattern of significant, theoretically consistent relationships across all constructs.

➢ *Qualitative Findings from Key Informant Interviews*

Semi-structured interviews with four ICT department informants (coded VUK001-VUK004) were analysed thematically, yielding themes that corroborate and enrich the quantitative findings, summarised in Table 5.

Table 5 Summary of Interview Themes

Theme	Key Finding	Strength / Gap	Quantitative Link
Encryption architecture	Multi-layer encryption confirmed at rest, in transit, and in storage; specific standards undisclosed	Strength; auditability gap	Q7 M=3.57
Encryption confidence	Internal knowledge gap between informants on system robustness	Gap	Q5 M=3.48

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

Access control & RBAC	Tiered role-based access in place; undermined by voluntary credential sharing	Strength; behavioural gap	Q2 M=2.98
DPPA 2019 compliance	Claimed national alignment; tick-box consent inadequate for meaningful informed consent	Gap	Q6 M=2.96
Incident history	No confirmed technical breaches; phishing app and credential sharing incidents reported	Social-threat gap	Q4 M=3.68; 7.5% incidents
Staff training & awareness	No organised internal training; awareness identified as a critical institutional gap	Gap	Q10 M=3.01; Q12 M=3.15

Taken together, the interview themes establish that encryption is operationally present at the university but technically opaque, that access controls are role-differentiated but behaviourally undermined by voluntary credential sharing, and that compliance with the DPPA 2019 is claimed institutionally but insufficiently demonstrated to the users it is meant to protect. Social engineering and credential exposure, rather than external system breaches, constitute the primary threat vectors, confirming that the university's data-privacy challenges are fundamentally socio-technical in character and require both advanced encryption infrastructure and a robust human-centred governance culture.

V. THE PROPOSED ENCRYPTION-BASED SECURITY FRAMEWORK

Building on the empirical findings above, the study designed a six-layer encryption-based security framework for the university's e-learning system, grounded in the Protection Motivation Theory, the CIA Triad, and the NIST Cybersecurity Framework. Each layer targets a specific empirically identified gap and maps to one or more principles of Uganda's DPPA 2019. Layers 2 and 3 are prioritised for immediate deployment, supported by the two strongest correlations in the study: r=0.544 (the encryption-compliance nexus) and r=0.525 (the security-MFA nexus), both significant at $p<0.001$.

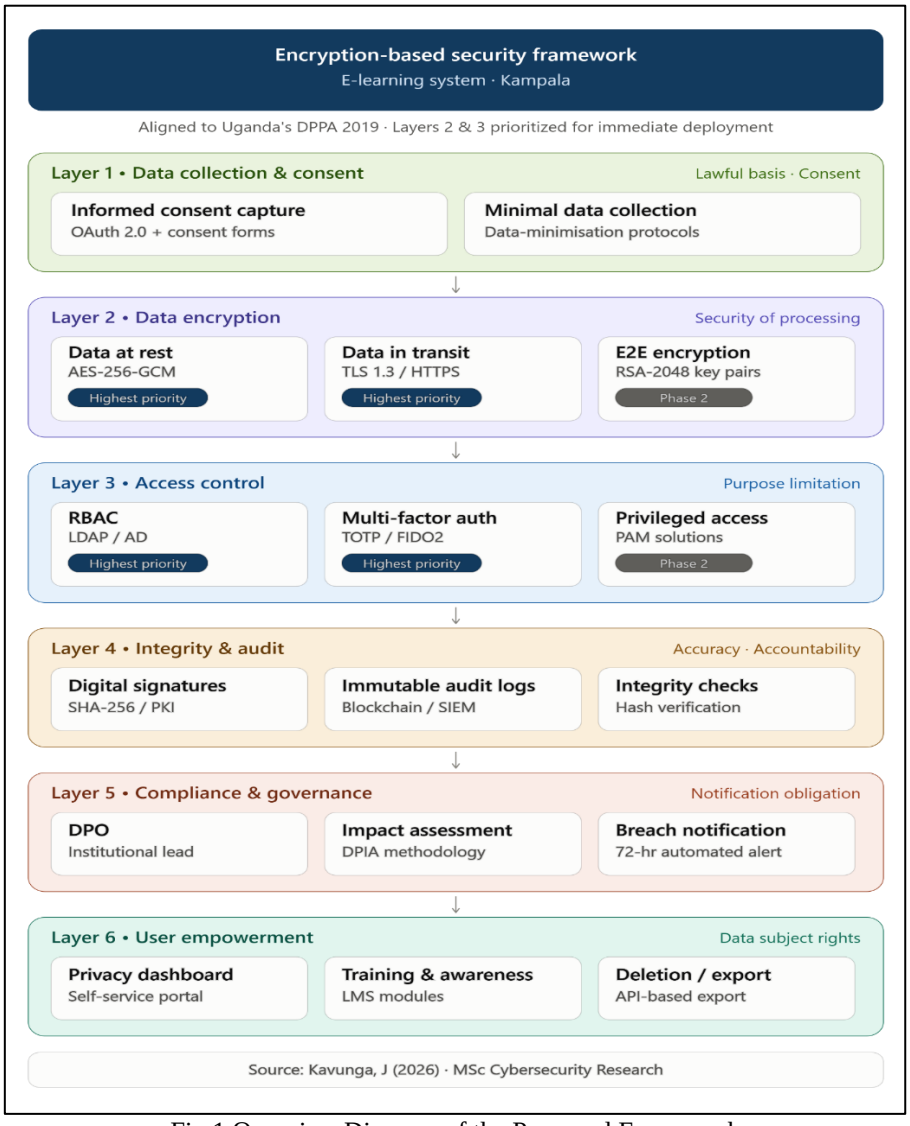


Fig 1 Overview Diagram of the Proposed Framework

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

➢ *Layer 1: Data Collection and Consent*

This layer ensures a lawful basis for all data processing through informed consent capture (OAuth 2.0-based consent forms) and data-minimisation protocols that limit collection to what is strictly necessary, directly addressing the study's finding that institutional transparency about data collection (Q6, mean=2.96) was the weakest item in the entire survey.

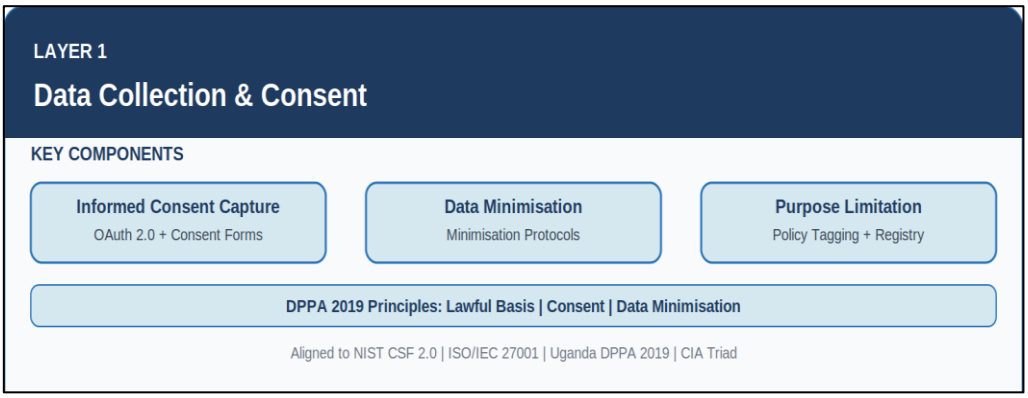


Fig 2 Layer 1 – Data Collection & Consent

➢ *Layer 2 Data Encryption*

This layer protects data at rest using AES-256-GCM encryption, data in transit using TLS 1.3/HTTPS, and end-to-end assignment submissions using RSA-2048 key pairs. It responds directly to the moderate but not fully trusted perception of technical security (Q7, mean=3.57) and is prioritised for deployment within the first six months given its strong correlation with compliance outcomes (r=0.544).

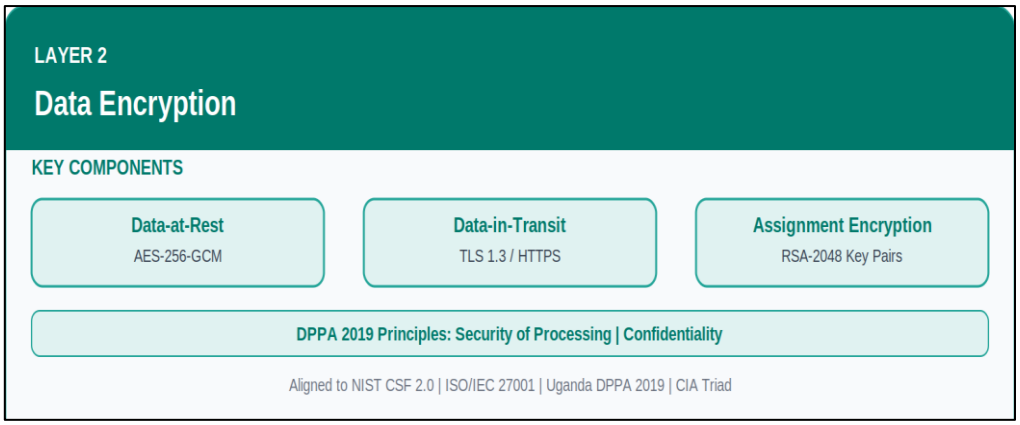


Fig 3 Layer 2 – Data Encryption

➢ *Layer 3: Access Control*

This layer implements role-based access control (RBAC) through LDAP/Active Directory, multi-factor authentication (TOTP/FIDO2), and privileged access management, directly targeting the behavioural vulnerability of voluntary credential sharing identified in the qualitative interviews and the low score on access-transparency (Q2, mean=2.98). It is co-prioritised with Layer 2 for deployment within the first six months, given its strong correlation with technical security perceptions (r=0.525).

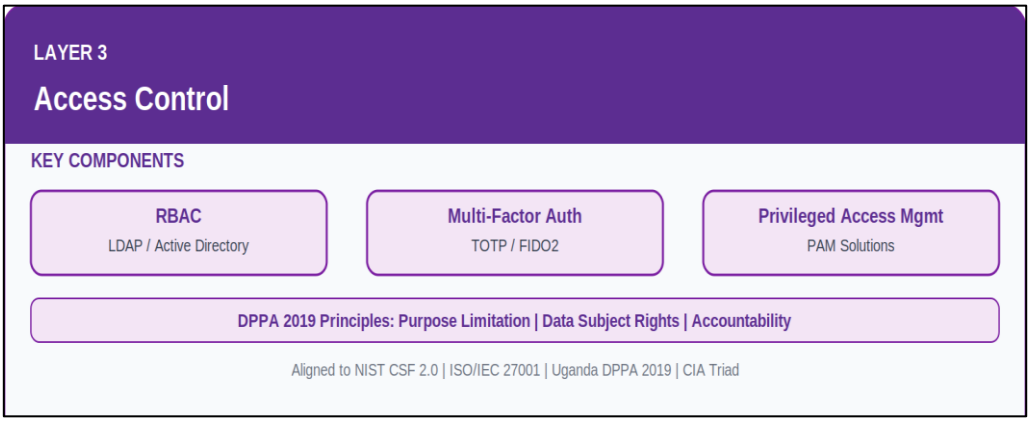


Fig 4 Layer 3 – Access Control

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

➢ *Layer 4: Integrity and Audit*

This layer maintains data accuracy and accountability through digital signatures (SHA-256/PKI), immutable audit logs (blockchain-ledger or SIEM-based), and routine data-integrity checks via hash verification, providing the auditability that Theme 1 of the qualitative findings identified as currently absent from the institution's encryption practice.

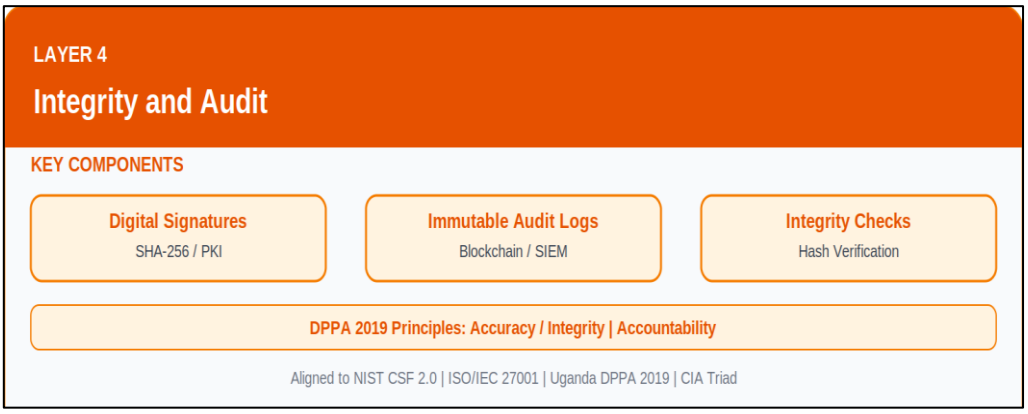


Fig 5 Layer 4 – Integrity & Audit

➢ *Layer 5: Compliance and Governance*

This layer institutionalises DPPA 2019 alignment through the formal designation of a Data Protection Officer (DPO), routine Data Protection Impact Assessments (DPIAs), and an automated 72-hour breach-notification system, directly addressing the study's lowest-scoring compliance item, breach-reporting knowledge (Q13, mean=2.67), and Section 30 of the DPPA 2019's notification obligation.

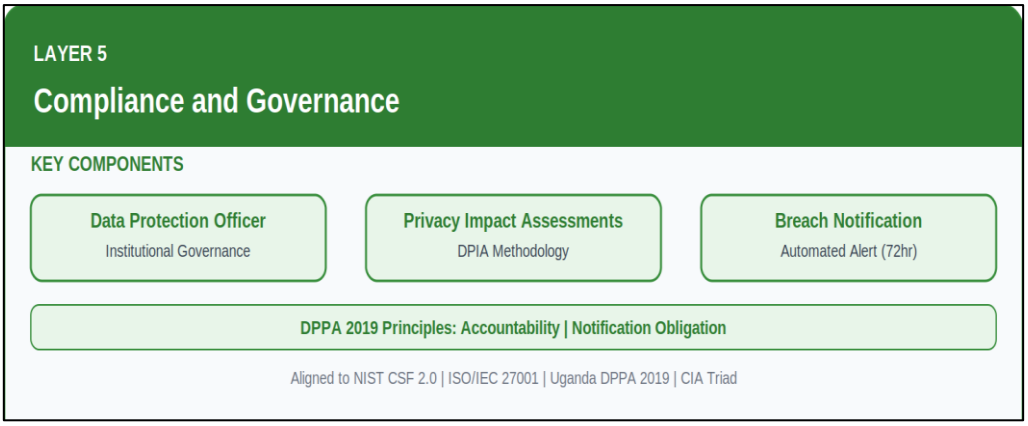


Fig 6 Layer 5 – Compliance & Governance

➢ *Layer 6: User Empowerment*

This layer enables data subjects to exercise their rights through a self-service user data dashboard, LMS-embedded training and awareness modules, and API-based data export that supports deletion and portability requests. It responds to the strongest positive finding of the study: 80.8% of respondents (Q17, mean=4.06) indicated they would engage more fully with e-learning if given greater control over their data, confirming that security investment functions as a driver of platform adoption rather than merely a compliance cost.

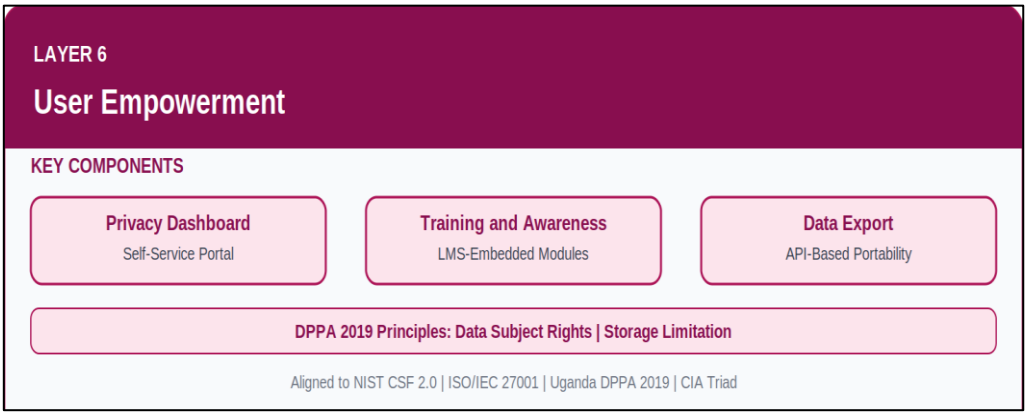


Fig 7 Layer 6 – User Empowerment

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

➢ *Framework Implementation Roadmap*

The six layers are phased for implementation over 36 months, based on empirical priority and institutional feasibility, as presented in Table 6.

Table 6 Six-Layer Framework Implementation Roadmap

Layer	Component	Phase	Timeline	Lead Responsibility
2	Data Encryption	Phase 1 (Priority)	Months 1-6	ICT Department
3	Access Control	Phase 1 (Priority)	Months 1-6	ICT Department
1	Data Collection & Consent	Phase 2	Months 7-12	DPO + ICT Department
4	Integrity & Audit	Phase 2	Months 7-18	ICT Department + DPO
5	Compliance & Governance	Phase 2	Months 7-18	University Senate + DPO
6	User Empowerment	Phase 3	Months 19-36	ICT + Academic Registry + DPO

The framework was benchmarked against existing models, including the NIST CSF 2.0 and the CIA Triad in their generic forms. Neither of these reviewed frameworks, on their own, combines empirically prioritised phased deployment, DPPA 2019-mapped governance, and a dedicated user-empowerment layer within a single model tailored to a resource-constrained East African higher-education context, a combination the proposed framework provides and which the study's key informants independently corroborated through their own forward-looking recommendations for encryption investment, biometric authentication, and data minimisation.

VI. CONCLUSION

This study set out to design and evaluate an encryption-based security framework for ensuring data privacy and protection compliance at the university. The findings confirm that the university's e-learning system faces significant privacy challenges: a transparency deficit, inadequate user training, an insufficient breach-notification system, and a latent but manageable behavioural security risk profile centred on voluntary credential sharing rather than technical compromise. All hypothesised relationships among current-state perceptions, framework effectiveness, and compliance were statistically significant, with the framework-effectiveness-to-compliance relationship the strongest in the study ($r=0.544$, $p<0.001$), confirming that well-implemented and clearly communicated technical security measures function as compliance enablers rather than mere compliance requirements.

The proposed six-layer framework, grounded in empirical evidence and aligned to the DPPA 2019, offers a structured, technically rigorous, and institutionally feasible pathway to closing these gaps. The data reveal a user population that is not resistant to privacy-enhancing technology but rather eager for it: 80.8% of respondents affirmed they would engage more fully with e-learning if given greater control over their data. This finding reframes data protection not as a regulatory burden but as a strategic investment in the quality, trustworthiness, and adoption of digital higher education at the university.

RECOMMENDATIONS

The study recommends that the university's Senate enact a comprehensive data-privacy policy explicitly aligned to the DPPA 2019, specifying data-retention schedules, third-party sharing restrictions, and user-consent mechanisms for the E-learning platfrom platform. In practice, the ICT department should deploy AES-256-GCM encryption for all E-learning platform data at rest and implement TLS 1.3 for all platform communications within twelve months, prioritising student assignment and assessment data, alongside a 72-hour data-breach notification protocol with automated alerting to the Data Protection Officer and affected data subjects.

The study further recommends that a user-facing privacy dashboard be developed, enabling students and staff to view what data is collected, who accesses it, and to request deletion or portability, directly addressing the transparency gap identified in this study (Q6, mean=2.96). Data-privacy literacy should be embedded as a module within all first-year curricula, not limited to the Faculty of Science and Technology, and the Ministry of Education and Sports should develop sector-specific data-protection guidelines for higher-education institutions to operationalise the DPPA 2019 in e-learning environments.

Finally, the study recommends longitudinal research examining whether the proposed six-layer framework reduces the incidence and impact of data breaches following implementation, comparative legal analysis between Uganda's DPPA 2019 and the EU's General Data Protection Regulation in the higher-education context, and experimental evaluation of AES-256 and TLS 1.3 implementation performance on low-bandwidth e-learning systems in rural Uganda.

REFERENCES

[1]. Agbeko, K., A., E., & O.-D., K. (2022). Data privacy awareness among university students in sub-Saharan Africa: An empirical investigation. Journal of African Information Systems.
[2]. Ali, R., & Zafar, H. (2017). A security and privacy framework for e-learning. International Journal for E-Learning Security, 7(2), 556-566.
[3]. Alier, M., Guerrero, M. J. C., Amo, D., Severance, C., & Fonseca, D. (2021). Privacy and e-learning: A pending task. Sustainability, 13(16), 9206.
[4]. Alkalbani, A., Deng, H., & Kam, B. (2016). Investigating the role of socio-organizational factors in the information security compliance in organizations.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

[5]. Bacharach, S. B. (1989). Organizational theories: Some criteria for evaluation. The Academy of Management Review, 14(4), 496.
[6]. Blazevic, A. N., Mugalula, P., & Wandera, A. (2021). Towards operationalizing the Data Protection and Privacy Act 2020: Understanding the draft data protection and privacy regulations, 2020. SSRN Electronic Journal.
[7]. Bygrave, L. A. (2014). Data privacy law. Oxford University Press.
[8]. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.
[9]. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61-80.
[10]. El-Sofany, H., El-Seoud, S., Karam, O., Bouallegue, B., & Ahmed, A. (2024). A proposed secure framework for protecting cloud-based educational systems from hacking. Egyptian Informatics Journal.
[11]. Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines: Revision 3. National Institute of Standards and Technology.
[12]. Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. SSRN Electronic Journal.
[13]. Mihailescu, M., Nita, S., & Pau, V. (2020). E-learning system framework using elliptic curve cryptography and searchable encryption. eLearning and Software for Education.
[14]. Moore, J. L., Dickson-Deane, C., & Galyen, K. (2011). e-Learning, online learning, and distance learning environments: Are they the same? The Internet and Higher Education, 14(2), 129-135.
[15]. Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. Journal of the Association for Information Systems, 23(6).
[16]. Mtebe, J. S., & Raisamo, R. (2014). Investigating students' behavioural intention to adopt and use mobile learning in higher education in East Africa. International Journal of Education and Development Using ICT, 10, 4-20.
[17]. Muhiddinov, M. (2025). Privacy-aware information security for e-learning platforms in history using attribute-based encryption algorithm. Journal of Internet Services and Information Security, 15, 305-315.
[18]. Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. Information Systems Journal, 16(4), 317-342.
[19]. NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology.
[20]. 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.
[21]. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93-114.
[22]. Shadmanova, S., et al. (2024). Ensuring the security of an internet-based e-learning system through the use of integrated encryption methods. Journal of Internet Services and Information Security, 14, 389-400.
[23]. Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, 20(2), 167-196.
[24]. Stallings, W. (2017). Cryptography and network security: Principles and practice. Pearson.
[25]. Ubaka-Okoye, M. (2020). Blockchain framework for securing e-learning system. International Journal of Advanced Trends in Computer Science and Engineering.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

APPENDIX

APPENDIX: QUESTIONNAIRE SURVEY

Topic: Encryption-Based Security Framework for Ensuring Data Privacy and Protection Compliance in Higher Education E-Learning Systems In Uganda.

This questionnaire is designed to collect information on encryption-based security practices in the university's e-learning system and their relationship with data privacy and protection compliance. The information you provide will be used strictly for academic purposes and will be treated with confidentiality. You are kindly requested to answer all questions as honestly as possible.

➢ *Section I: Background Information*

- Respondent category: Student □ Lecturer □ Other: _____
- Gender: Male □ Female □
- Age group: 18-25 □ 26-35 □ 36-45 and above □
- Faculty/Department: _____
- How often do you use the e-learning system? Daily □ Weekly □ Occasionally □ Rarely □
- How long have you used the e-learning system? Less than 1 year □ 1-2 years □ 3-4 years □ More than 4 years □
- Which device do you mainly use to access the e-learning system? Smartphone □ Laptop □ Desktop □ Tablet □

➢ *Section II: Data Privacy and Trust in Learning Management System*

Please indicate your level of agreement with each statement using the scale below: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

No.	Data privacy and Trust in learning management systems	SD	D	N	A	SA
1	I do understand what types of my personal data are collected by the e-learning system.					
2	I know who (lecturers, administrators, third parties) can access my data in the system.					
3	I am concerned that my data could be used for purposes I did not consent to (e.g., analytics, profiling).					
4	I worry about data breaches or leaks of my personal information from the e-learning system.					
5	I feel that my privacy is adequately protected when I use the university e-learning platform.					
6	The university clearly informs me about data collection, storage duration, and sharing practices.					

➢ *Section III: Security Controls and Encryption (Perception)*

Please indicate your level of agreement with each statement using the scale below: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

No.	Security controls and encryption (perception)	SD	D	N	A	SA
1	The e-learning system uses strong technical security measures (e.g., encryption, secure login).					
2	Multi-factor authentication or similar mechanisms are used and easy to use.					
3	I feel safe submitting assignments, exams, and personal information online.					

I have experienced or suspect hacking, unauthorized access, or malware incidents related to the e-learning system: Yes □ No □

If Yes, kindly give a brief of what you have experienced or suspect: _____

➢ *Section IV: Awareness, Training, and Compliance*

Please indicate your level of agreement with each statement using the scale below: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

No.	Awareness, Training, and Compliance	SD	D	N	A	SA
1	I have received training or guidance on how to protect my data and privacy when using the e-learning system.					
2	I know how to change my privacy/security settings in the system.					
3	I am aware of university policies on data protection and acceptable use of the e-learning platform.					
4	I know how to report a suspected data breach or privacy violation.					

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1810

5	The university appears to follow national/international data protection regulations in managing student data.					

➢ *Section V: Satisfaction, Usability, and Willingness to Use*

Please indicate your level of agreement with each statement using the scale below: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

No.	Satisfaction, Usability, and Willingness to Use	SD	D	N	A	SA
1	Concerns about privacy or security discourage me from fully using the e-learning system.					
2	Overall, I am satisfied with how the system protects my personal data.					
3	I would be more willing to use online learning features if I had more control over my data (e.g., consent, visibility).					