Security, Privacy Protection, and Trust in Learning Management System Continuance: Evidence from Sri Lankan Higher Education

Nivashinie Gopalaakrishnan[1]*, Anuradha Jayakody[2]
Faculty of Graduate Studies, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka[1]
Department of Computer Systems Engineering-Faculty of Computing,
Sri Lanka Institute of Information Technology, Malabe, Sri Lanka[2]

***Abstract*—Learning Management Systems (LMSs) are integral to higher education, yet understanding the factors associated with users' intentions to continue using these platforms remains important. While previous continuance research has emphasized functional and experiential factors, the combined relationships among perceived security, perceived privacy protection, trust, and LMS continuance intention warrant further examination. This study investigates these relationships in Sri Lankan higher education, distinguishing security and privacy protection as separate information-assurance perceptions and examining their direct and indirect associations with continuance intention through trust. Data were collected through a cross-sectional questionnaire survey of 101 students, lecturers, and academic staff selected using purposive sampling and analyzed using partial least squares structural equation modeling (PLS-SEM). The results indicate that perceived security ($\beta = 0.458$, $p < 0.001$) and perceived privacy protection ($\beta = 0.372$, $p < 0.001$) were positively associated with trust, which was positively associated with continuance intention ($\beta = 0.367$, $p = 0.002$). Perceived security also showed a significant direct association with continuance intention ($\beta = 0.365$, $p = 0.016$), whereas the direct association for privacy protection was not statistically significant ($\beta = 0.059$, $p = 0.718$). Significant indirect associations through trust were identified for both security ($\beta = 0.168$, $p = 0.003$) and privacy protection ($\beta = 0.137$, $p = 0.042$). Overall, six of the seven hypotheses were supported. The findings highlight the relevance of information-assurance perceptions and trust in LMS continuance research, while the cross-sectional design and sampling approach limit causal interpretation and generalizability.**

***Keywords*—Learning management systems; continuance intention; perceived security; perceived privacy protection; institutional platform trust; higher education; Sri Lanka**

I. Introduction

Learning Management Systems (LMSs) have become important components of higher education, supporting teaching, learning, assessment, communication, and the management of academic information. Their use expanded during the COVID-19 pandemic as universities adopted online and blended learning arrangements to maintain educational continuity. As LMS platforms remain embedded in institutional activities, understanding users' intentions to continue using them has become an important post-adoption research concern. Previous studies have examined online learning continuance in the post-pandemic period [1], learners' continuance intentions [2], and the roles of habit, performance, and other experiential factors in continued digital learning engagement [3], [4].

Information systems continuance research has traditionally emphasized expectation confirmation, perceived usefulness, satisfaction, and related post-adoption evaluations [5]. These factors provide an established foundation for understanding continued technology use. However, institutional LMS platforms also process personal and academic information, including user identities, assessment records, grades, learning activities, and communications. Consequently, users' confidence in the security of these systems and the protection of their information may be relevant to their willingness to maintain engagement. Examining these information-assurance perceptions provides a complementary perspective to established continuance research rather than replacing its existing explanations.

Security is a significant concern in educational information systems. Previous studies have investigated vulnerabilities in modern LMS platforms [6], security risks in university-level LMS environments [7], and security issues associated with Moodle deployment in higher education [8]. A systematic review by Ulven and Wangen [9] further documented cybersecurity risks affecting higher education institutions. Although these studies establish the importance of technical and organizational safeguards, identifying security vulnerabilities does not directly explain how users' perceived LMS security is associated with their trust in institutional platforms or their continuance intention.

Privacy protection represents a related but conceptually distinct consideration. Perceived LMS security concerns users' confidence in safeguards against unauthorized access, misuse, and other security threats. In contrast, perceived LMS privacy protection concerns confidence in how personal and academic information is collected, accessed, processed, disclosed, and protected. Previous research has examined privacy-related evaluations in online learning [10], privacy concerns in online teaching [11], and the protection of LMS users' rights [12]. These studies demonstrate the relevance of privacy considerations in digital education, but privacy concerns, initial technology acceptance, and the governance of users' information are not equivalent to positive perceptions of

*Corresponding author.

privacy protection or post-adoption LMS continuance intention.

Trust offers a potential connection between information-assurance perceptions and continued LMS engagement. Users may not be able to observe the technical safeguards or institutional information-management practices underlying an LMS. Their confidence in the platform may therefore be associated with perceived security and privacy protection, while trust itself may be associated with their intention to continue using the system. Examining direct and specific indirect relationships through trust allows these associations to be assessed simultaneously. Nevertheless, because the present study uses cross-sectional survey data, such indirect relationships are interpreted statistically rather than as evidence of causal mediation.

The reviewed literature thus provides valuable but distinct perspectives on LMS continuance, technical security, privacy, and trust. The research gap is not that these topics have been overlooked individually. Rather, the available evidence provides a more limited basis for understanding how perceived LMS security and perceived LMS privacy protection are jointly associated with institutional platform trust and continuance intention, including their respective indirect associations through trust. A focused empirical model can help clarify these relationships without assuming that security and privacy protection are interchangeable constructs or that their associations with continuance intention are necessarily identical.

Sri Lankan higher education provides a relevant setting for investigating this issue. Yang et al. [13] examined online higher education during university closures in Sri Lanka, highlighting the importance of digital learning provision during institutional disruption. As LMS platforms continue to support academic activities, users' perceptions of information protection and institutional trust warrant investigation. However, the post-pandemic setting is treated as contextual background rather than as a measured cause of current continuance intention, and the study does not presume that the relationships are unique to Sri Lanka.

Accordingly, this study examines the relationships among perceived LMS security, perceived LMS privacy protection, trust in institutional LMS platforms, and LMS continuance intention. Specifically, it investigates the associations of perceived security and privacy protection with trust, their direct associations with continuance intention, the association between trust and continuance intention, and the specific indirect associations of security and privacy protection with continuance intention through trust. A quantitative, cross-sectional survey was conducted with 101 students, lecturers, and academic staff recruited through purposive sampling in Sri Lankan higher education. The proposed relationships were evaluated using partial least squares structural equation modeling (PLS-SEM).

The study makes three contributions. First, it integrates perceived security and perceived privacy protection as conceptually distinct information-assurance constructs within a focused LMS continuance model. Second, it examines trust alongside the direct and specific indirect relationships linking these perceptions to continuance intention, providing a more differentiated assessment of the proposed associations. Third, it contributes context-specific empirical evidence from a heterogeneous sample of LMS users in Sri Lankan higher education. These contributions complement established continuance research and are interpreted within the limitations of the study's sampling strategy, cross-sectional design, and measurement model.

II. Related Work

A. LMS Continuance and Post-Adoption Theoretical Foundations

Learning Management Systems (LMSs) support teaching, assessment, communication, and the management of academic information in higher education. While initial adoption is important, continuance intention concerns users' willingness to maintain engagement with a system after gaining experience with it. Bhattacherjee's Information Systems Continuance Model [5] identifies confirmation, perceived usefulness, and satisfaction as central post-adoption considerations. Subsequent studies have examined additional determinants of continued engagement in online learning and related environments, including habit, system performance, and users' experiences [1]–[4].

Research focusing specifically on institutional LMS platforms provides a relevant foundation. Rabaa'i et al. [14] examined Moodle continuance intention among 387 university students in Kuwait using partial least squares structural equation modeling (PLS-SEM). Their findings identified significant relationships involving performance expectancy, effort expectancy, satisfaction, attitude, self-efficacy, and facilitating conditions, whereas subjective norms were not a significant predictor. This evidence demonstrates that continued LMS engagement is associated with multiple functional and experiential considerations.

Nevertheless, the explanatory scope of existing continuance studies differs from that of the present research. Studies of MOOCs and general online learning do not necessarily reflect the institutional arrangements of university-managed LMS platforms, which support academic records, assessments, and potentially sensitive user information. Furthermore, the Moodle continuance model examined by Rabaa'i et al. [14] did not explicitly incorporate perceived LMS security, perceived privacy protection, and institutional platform trust as the combined explanatory constructs considered here. The present study therefore complements established post-adoption frameworks by investigating information-assurance perceptions and trust without assuming that these factors replace usefulness, satisfaction, or other established determinants.

B. Perceived Security and Privacy Protection in LMS Environments

Perceived LMS security and perceived LMS privacy protection represent related but conceptually distinct information-assurance perceptions. Security concerns users' confidence in safeguards against unauthorized access, information misuse, and other threats. Privacy protection concerns confidence in how personal and academic

information is collected, accessed, processed, disclosed, and protected. A platform perceived as technically secure may not necessarily inspire equivalent confidence in institutional information-handling practices.

Previous research has established the importance of technical security in educational systems. Scerbakov et al. [6] examined vulnerabilities in modern LMS platforms; Secaira et al. [7] investigated risks in a university-level LMS environment, and Ally [8] studied vulnerabilities associated with Moodle deployment in Tanzanian higher education. Ulven and Wangen [9] reviewed cybersecurity risks across higher education institutions. More recent work by Mawgoud et al. [15] examined a blockchain-based access-control protocol for cloud educational systems, emphasizing technical information protection. Although these studies establish the relevance of cybersecurity safeguards, technical assessments do not directly measure users' perceptions of platform security, trust, or continuance intention.

A complementary user-centered perspective is provided by Xu et al. [16], who examined educational information and communication technology (ICT) usage among 382 university students in China. Their findings indicated a positive association between perceived security and perceived trust ($\beta = 0.358$, $p < 0.001$). This supports examining security perceptions in relation to trust, although the study concerned broader educational ICT usage rather than institutional LMS continuance.

Privacy-related research has investigated different aspects of information handling in digital education. Jiang et al. [10] examined online learning decisions through a privacy calculus perspective; Xiao et al. [11] considered privacy concerns in teachers' adoption of live online teaching, and Kabata [12] discussed users' legitimate rights in an institutional Blackboard LMS environment. These studies establish the relevance of privacy-related evaluations but do not necessarily measure positive perceptions of privacy protection. Privacy concern, which reflects apprehension about information-related risks, should therefore be distinguished from confidence in protective practices.

Anwar [17] discussed privacy, trust, and personalization in online learning, including privacy preferences, identity management, and appropriate information flows. This work provides a conceptual rationale for considering responsible information handling in trustworthy online learning environments. However, it does not empirically test the relationship between perceived LMS privacy protection and institutional platform trust. Taken together, these studies support examining security and privacy protection as distinct user perceptions while recognizing that the empirical boundaries between them require assessment.

C. Trust and Continuance Intention in Digital Learning

Trust is relevant to institutional LMS engagement because users depend on platforms whose technical operations and information-management practices may not be fully observable. In the present study, trust refers to confidence in the institutional LMS platform rather than interpersonal trust among students, lecturers, or academic staff. Such confidence may be associated with users' willingness to continue relying on the platform for academic activities.

Xu et al. [16] reported positive associations between perceived trust and intentions to use educational ICT for information-related activities ($\beta = 0.645$, $p < 0.001$) and interaction ($\beta = 0.508$, $p < 0.001$). These findings indicate the relevance of trust to educational technology engagement, although intention to use ICT for specific activities is not equivalent to post-adoption LMS continuance.

Evidence from another digital-service context further supports examining trust in relation to continuance intention. Rashidov and Park [18] investigated 410 mobile-payment application users in Uzbekistan and reported a positive trust–continuance association ($\beta = 0.413$, $p < 0.001$). Satisfaction was also positively associated with continuance intention. However, mobile-payment applications differ from institutional LMS platforms in their functions, governance arrangements, and information risks; their findings therefore cannot be generalized directly to higher education.

These studies provide complementary support for investigating trust as an intervening construct. Educational ICT research links security perceptions with trust, conceptual work connects privacy-preserving practices with trustworthy online learning, and research in another digital-service setting associates trust with continuance intention [16]–[18] Nevertheless, these sources do not establish the complete security–trust–continuance or privacy protection–trust–continuance relationships within a single institutional LMS model. The present study evaluates those proposed direct and indirect associations empirically, while recognizing that cross-sectional statistical mediation does not establish causal mechanisms.

D. Critical Synthesis, Research Gap, and Sri Lankan Context

The reviewed literature can be grouped into four complementary research streams. First, information systems and online learning continuance studies emphasize post-adoption evaluations, including usefulness, satisfaction, confirmation, habit, performance, and facilitating conditions [1]–[5], [14]. Second, LMS cybersecurity research examines technical vulnerabilities, institutional risks, and protective mechanisms [6]–[9], [15]. Third, privacy-related studies address disclosure decisions, privacy concerns, users' rights, and privacy-preserving practices [10]–[12], [17]. Fourth, research on educational ICT and other digital services investigates associations involving security perceptions, trust, and technology-use or continuance intentions [16], [18].

These streams offer different forms of evidence. Technical security investigations do not directly explain user perceptions; privacy concern is not interchangeable with perceived privacy protection; and relationships observed in general educational ICT or mobile-payment services cannot automatically be assumed to apply to institutional LMS continuance. Consequently, the research gap is not that security, privacy, trust, or continuance intention have been ignored individually. Rather, the reviewed evidence provides a limited basis for understanding their combined associations in a model that distinguishes perceived LMS security from perceived LMS

privacy protection and examines both direct relationships with continuance intention and indirect relationships through institutional platform trust.

Sri Lankan higher education provides the empirical setting for examining this gap. Yang et al. [13] discussed inclusive online higher education through lessons from Sri Lanka's university closures, highlighting the importance of digital learning provision during institutional disruption. However, this contextual evidence does not establish distinctive national effects or demonstrate that pandemic-related experiences determine current perceptions of security, privacy, or trust.

Accordingly, the present study examines perceived LMS security, perceived LMS privacy protection, institutional platform trust, and continuance intention among students, lecturers, and academic staff in Sri Lankan higher education. Its contribution lies in evaluating these relationships jointly and providing context-specific evidence from a heterogeneous user sample. The findings are interpreted within the limitations of purposive sampling, cross-sectional self-report data, and the exclusion of other established continuance determinants.

III. Research Model and Hypotheses

The proposed research model examines four constructs: Perceived LMS Security (PS), Perceived LMS Privacy Protection (PP), Trust in Institutional LMS Platforms (PT), and LMS Continuance Intention (CI). PS and PP represent conceptually distinct information-assurance perceptions, while PT is proposed as an intervening construct associated with CI. Building on information systems continuance research and literature concerning security, privacy, and trust, the model specifies five direct relationships and two specific indirect relationships through trust, as illustrated in Fig. 1.

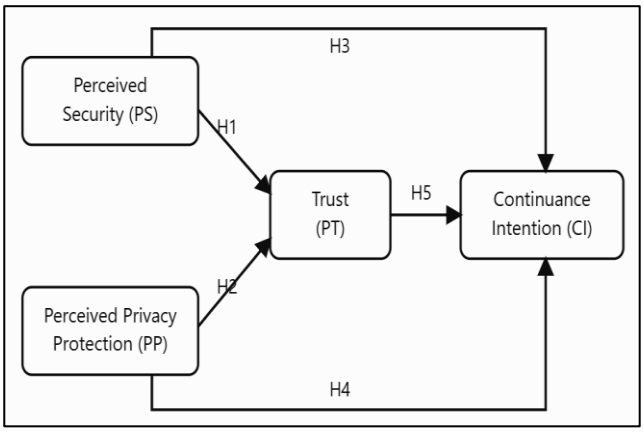

Fig. 1. Proposed research model and hypothesized relationships.

The framework complements established continuance models, which emphasize perceived usefulness, satisfaction, confirmation, and other post-adoption evaluations [5], [14]. It focuses specifically on whether users' perceptions of institutional LMS security and privacy protection are associated with platform trust and their intention to continue using the system. The proposed paths represent theoretically motivated associations rather than predetermined causal effects.

A. Perceived LMS Security, Privacy Protection, and Trust

Perceived LMS security refers to users' confidence that an institutional platform provides appropriate safeguards against unauthorized access, information misuse, and security threats. Such confidence may reduce uncertainty about the dependability of the LMS environment. Although technical investigations have established the importance of cybersecurity risks and protective mechanisms in educational systems [6]–[9], [15], these studies do not directly demonstrate how users' security perceptions relate to institutional platform trust.

More relevant empirical evidence is provided by Xu et al. [16], who reported a positive relationship between perceived security and perceived trust in educational ICT usage ($\beta = 0.358$, $p < 0.001$). Although their study did not investigate institutional LMS continuance, it supports examining whether users who perceive stronger LMS security also report greater platform trust.

H1: Perceived LMS Security is positively associated with Trust in Institutional LMS Platforms.

Perceived LMS privacy protection concerns users' confidence in the responsible collection, access, processing, disclosure, and protection of personal and academic information. It differs from perceived security because technical safeguards do not necessarily establish confidence in institutional information-handling practices. Privacy-related studies have highlighted the relevance of information disclosure, privacy concerns, and users' rights in digital education [10]–[12]. Anwar [17] further discussed how privacy-preserving practices and appropriate information flows may support trustworthy online learning environments.

These sources provide a conceptual basis for expecting a positive privacy protection–trust association, although they do not establish that relationship empirically among institutional LMS users. Accordingly, the present study evaluates the following hypothesis.

H2: Perceived LMS Privacy Protection is positively associated with Trust in Institutional LMS Platforms.

B. Perceived LMS Security, Privacy Protection, and Continuance Intention

LMS continuance intention refers to users' stated willingness to maintain engagement with an institutional LMS following prior experience. Established post-adoption research identifies users' evaluations of a system as important considerations in continuance intention [5]. Within institutional LMS environments, Rabaa'i et al. [14] identified several significant correlates of Moodle continuance, including performance expectancy, satisfaction, attitude, self-efficacy, and facilitating conditions.

Information-assurance perceptions may represent additional considerations because institutional LMS platforms support assessment submissions, academic communications, and access to personal and educational records. Users who perceive stronger security safeguards may also express greater willingness to continue relying on these functions. However, the technical security studies reviewed earlier do not directly

establish this relationship [6]–[9], [15]. The proposed association is therefore tested empirically.

H3: Perceived LMS Security is positively associated with LMS Continuance Intention.

Perceived privacy protection may likewise be relevant to continuance intention because repeated LMS engagement involves the generation, storage, and processing of personal and academic information. Privacy calculus research indicates that privacy-related evaluations can be relevant to online learning decisions [10], while Anwar [17] provides a conceptual discussion of privacy-preserving practices in trustworthy online learning.

Nevertheless, evidence concerning initial technology-use decisions should not be equated with evidence concerning post-adoption continuance. Privacy protection may be associated with continuance intention directly or through other constructs, including trust. Its direct relationship is therefore evaluated separately rather than assumed to follow from the proposed privacy protection–trust relationship.

H4: Perceived LMS Privacy Protection is positively associated with LMS Continuance Intention.

C. Trust and LMS Continuance Intention

Trust in an institutional LMS refers to users' confidence in the platform as a dependable environment for academic activities and information handling. Because users cannot directly observe every aspect of an LMS's technical operation or institutional information-management practices, platform trust may be relevant to their willingness to maintain engagement.

Xu et al. [16] reported positive associations between perceived trust and intentions to use educational ICT for information-related activities ($\beta = 0.645$, $p < 0.001$) and interaction ($\beta = 0.508$, $p < 0.001$). These findings support the relevance of trust to educational technology engagement, although the measured outcomes were not equivalent to LMS continuance intention. In another digital-service context, Rashidov and Park [18] reported a positive relationship between trust and mobile-payment continuance intention ($\beta = 0.413$, $p < 0.001$).

Together, these findings provide a rationale for examining trust in relation to institutional LMS continuance, while recognizing the differences between educational ICT use, mobile-payment services, and university-managed learning platforms.

H5: Trust in Institutional LMS Platforms is positively associated with LMS Continuance Intention.

D. The Proposed Mediating Role of Trust

In addition to the proposed direct relationships, perceived LMS security and perceived LMS privacy protection may exhibit indirect associations with continuance intention through trust. Such relationships are theoretically plausible when information-assurance perceptions are associated with platform trust and trust is, in turn, associated with continuance intention.

For perceived security, Xu et al. [16] provide empirical evidence of a positive security–trust association in educational ICT. Rashidov and Park [18] provide complementary evidence of a positive trust–continuance association in mobile-payment services. Although these findings arise from different contexts and do not establish the complete indirect pathway within an institutional LMS, they provide a rationale for evaluating that pathway in the proposed model.

H6: Perceived LMS Security has a positive indirect association with LMS Continuance Intention through Trust in Institutional LMS Platforms.

For perceived privacy protection, Anwar [17] provides conceptual support for the relevance of responsible information handling to trustworthy online learning. Privacy-related studies also demonstrate the importance of information-handling evaluations in digital education [10]–[12]. Considered alongside evidence linking trust with continuance intention [18], these perspectives motivate the examination of an indirect privacy protection–continuance relationship through institutional platform trust. However, the supporting evidence is less direct than that available for the security–trust association.

H7: Perceived LMS Privacy Protection has a positive indirect association with LMS Continuance Intention through Trust in Institutional LMS Platforms.

The two proposed indirect relationships are evaluated alongside the corresponding direct relationships to distinguish their estimated patterns of association. Because the study uses cross-sectional survey data, statistically significant indirect effects cannot establish temporal precedence or causal mediation. The analysis therefore evaluates indirect associations consistent with the proposed framework rather than demonstrating that security or privacy perceptions causally produce trust or continued LMS use.

IV. Methodology

A. Research Design

This study employed a quantitative, cross-sectional survey design to examine associations among perceived LMS security (PS), perceived LMS privacy protection (PP), trust in institutional LMS platforms (PT), and LMS continuance intention (CI) in Sri Lankan higher education. Data were collected through a structured, self-administered questionnaire completed by respondents with prior experience using institutional LMS platforms.

The proposed model comprised four reflective latent constructs, five direct hypotheses, and two specific indirect hypotheses through trust. Partial least squares structural equation modeling (PLS-SEM) was employed to evaluate the measurement and structural models using SmartPLS 4 [19]. This approach enabled the simultaneous estimation of the specified relationships, but the cross-sectional design does not establish causal effects or changes in LMS engagement over time.

B. Population, Sampling, and Sample Size

The target population comprised students, lecturers, and academic staff with experience using institutional LMS platforms in Sri Lankan higher education. Purposive non-probability sampling was used to recruit respondents relevant to the research objectives.

The final sample included 101 valid responses: 51 students (50.5%), 30 lecturers (29.7%), and 20 academic staff members (19.8%). These respondent categories represent different institutional LMS roles, but their responsibilities, usage patterns, and information-assurance expectations may differ. All respondents were analyzed as one pooled sample; measurement invariance and group-specific structural relationships were not established. The sampling method also limits statistical generalizability to the wider higher education population.

An a priori sample-size calculation was performed using G*Power 3.1.9.7 [20]. The calculation specified a linear multiple regression F-test, a medium effect size ($f^2 = 0.15$), a significance level of 0.05, statistical power of 0.80, and three predictors. These assumptions yielded a minimum estimated sample size of 77, which was exceeded by the 101 valid responses. However, this calculation does not establish adequate power for every structural coefficient or for detecting the two specific indirect effects, particularly if their true magnitudes are small.

C. Questionnaire Design and Measurement

Data were collected using a structured electronic questionnaire comprising five sections: respondent characteristics, perceived LMS security, perceived LMS privacy protection, institutional LMS trust, and continuance intention. The demographic and contextual questions covered respondent role, age group, gender, institution type, LMS platform, usage frequency, and duration of LMS experience.

The construct statements used a five-point Likert response scale ranging from 1 (strongly disagree) to 5 (strongly agree). Perceived LMS security was assessed using five items (PS1–PS5), trust using five items (PT1–PT5), and continuance intention using five items (CI1–CI5).

The questionnaire included 11 privacy-related items. Eight positively framed privacy-protection indicators (PP1–PP5, PP8, PP9, and PP11) were included in the primary PP construct. Three negatively worded privacy-concern items (PP6R, PP7R, and PP10R) were treated as supplementary measures and excluded from the primary reflective PP construct. These items addressed privacy concerns rather than positive confidence in privacy protection and were therefore not combined with the eight primary indicators in the reported structural model. Consequently, the final primary measurement model comprised 23 reflective indicators: five PS, eight PP, five PT, and five CI indicators.

The items were contextualized for institutional LMS use. Nevertheless, contextual adaptation and construct-level reliability do not by themselves establish the validity of every indicator. The measurement results are therefore interpreted with attention to comparatively weak item loadings and the distinction between privacy protection and privacy concern.

D. Data Collection and Preparation

The questionnaire was distributed electronically to respondents with experience using LMS platforms in Sri Lankan higher education. Participation was voluntary, and respondents were informed that the information collected would be used for academic research purposes.

Following data collection, questionnaire responses were coded numerically according to the five-point response scale. The final dataset contained 101 valid cases. SPSS was used for descriptive and preliminary analyses, while SmartPLS 4 was used to estimate the reflective measurement and structural models.

All four constructs were measured using the same self-report questionnaire at one point in time. Consequently, the analysis was potentially susceptible to common method bias and response-related measurement error. The available evidence does not establish that these sources of bias were eliminated.

E. Measurement Model Assessment

The reflective measurement model was evaluated before interpreting the structural relationships. Indicator reliability was assessed using standardized outer loadings. Internal consistency reliability was examined using Cronbach's alpha, rho_A, and composite reliability (rho_C), while convergent validity was evaluated using average variance extracted (AVE) [19].

Conventional benchmarks of 0.70 for composite reliability and 0.50 for AVE were used to guide interpretation. Individual indicator loadings were also examined because acceptable construct-level reliability and AVE do not necessarily imply that every item performs satisfactorily.

Discriminant validity was assessed using the heterotrait–monotrait ratio of correlations (HTMT) [21]. The commonly used 0.90 threshold and the more conservative 0.85 threshold were considered when interpreting construct distinctiveness, particularly between perceived security and perceived privacy protection.

The final model retained the reported 23 indicators, including indicators with comparatively weak outer loadings. These limitations were considered when evaluating measurement quality rather than treating satisfaction of construct-level thresholds as evidence of uniformly strong indicator validity.

F. Structural Model Assessment and Hypothesis Testing

The structural model was evaluated using standardized path coefficients (β), coefficients of determination (R^2), effect sizes (f^2), and inner-model variance inflation factors (VIF) [19]. Collinearity was considered using the commonly applied VIF threshold of 5, while recognizing that values above more conservative benchmarks may indicate meaningful overlap among predictors.

Statistical significance was assessed through nonparametric bootstrapping in SmartPLS 4 using 10,000 subsamples, two-tailed testing, and a significance level of 0.05. Percentile

bootstrap confidence intervals were calculated at the 95% confidence level.

The five direct hypotheses (H1–H5) were evaluated using standardized path estimates, t-statistics, and p-values. The two specific indirect hypotheses (H6 and H7) were assessed using the estimated indirect effects and their 95% bootstrap confidence intervals [22]. An indirect association was considered statistically supported when its confidence interval excluded zero.

The direct and indirect relationships were interpreted as statistical associations within the specified model. Significant indirect effects were not treated as proof of causal mediation because the study did not establish temporal ordering, experimentally manipulate the predictors, or observe subsequent LMS usage.

V. Results

A. Respondent Profile and Descriptive Statistics

A total of 101 valid questionnaire responses were analyzed, comprising 51 students (50.5%), 30 lecturers (29.7%), and 20 academic staff members (19.8%). The results represent the pooled sample and do not establish whether the relationships differ across respondent categories.

Table I presents the construct-level descriptive statistics. Perceived LMS privacy protection had the highest mean (M = 3.020, SD = 0.577), followed by perceived LMS security (M = 2.947, SD = 0.663) and trust (M = 2.943, SD = 0.640). Continuance intention had the lowest mean (M = 2.711, SD = 0.497). The means were relatively close to the midpoint of the five-point scale, indicating that respondents did not report uniformly strong agreement with the measured statements.

TABLE I. Descriptive Statistics

Construct	Mean	SD
Perceived LMS Security (PS)	2.947	0.663
Perceived LMS Privacy Protection (PP)	3.020	0.577
Trust (PT)	2.943	0.640
Continuance Intention (CI)	2.711	0.497

B. Measurement Model Assessment

The reflective measurement model comprised 23 indicators across four constructs: PS (five), PP (eight), PT (five), and CI (five). Indicator loadings, internal consistency reliability, convergent validity, and discriminant validity were assessed before interpreting the structural relationships.

Most indicators demonstrated satisfactory outer loadings. However, PP5 (0.465), PP9 (0.620), CI2 (0.602), and CI3 (0.555) were below the commonly recommended threshold of 0.708. PP5 was particularly weak. These indicators remained in the reported final model, but their retention does not eliminate the associated measurement limitations.

Table II presents construct reliability and convergent validity. Cronbach's alpha ranged from 0.742 to 0.925, composite reliability (rho_C) ranged from 0.831 to 0.944, and AVE ranged from 0.501 to 0.770. All constructs met the conventional composite reliability and AVE benchmarks. Nevertheless, CI recorded an AVE of 0.501, indicating borderline convergent validity. Thus, acceptable construct-level statistics should not be interpreted as evidence of uniformly strong indicator quality.

TABLE II. Construct Reliability And Convergent Validity

Construct	Cronbach's α	rho_A	rho_C	AVE
CI	0.742	0.767	0.831	0.501
PP	0.909	0.943	0.927	0.622
PS	0.910	0.921	0.933	0.736
PT	0.925	0.926	0.944	0.770

Discriminant validity was examined using HTMT [21]. As shown in Table III, HTMT values ranged from 0.749 to 0.879. The highest value, between PS and PP (0.879), was below 0.90 but exceeded the more conservative 0.85 threshold. This indicates substantial empirical overlap between security and privacy protection, requiring caution when interpreting their distinctiveness and structural relationships.

TABLE III. HTMT Discriminant Validity

Construct pair	HTMT
PP–CI	0.749
PS–CI	0.824
PS–PP	0.879
PT–CI	0.821
PT–PP	0.789
PT–PS	0.830

C. Structural Model Assessment

The structural model was assessed using inner-model VIF values, coefficients of determination (R^2), and effect sizes (f^2). As shown in Table IV, VIF values ranged from 2.720 to 3.837. Although none exceeded 5, the values for PS and PP as predictors of CI exceeded 3.3, suggesting meaningful predictor overlap. Accordingly, individual path estimates should be interpreted with caution.

TABLE IV. Inner-Model Collinearity Statistics

Relationship	VIF
PP → CI	3.644
PS → CI	3.837
PT → CI	2.720
PP → PT	3.267
PS → PT	3.267

The model explained 63.2% of the variance in PT (R^2 = 0.632; adjusted R^2 = 0.625) and 54.7% of the variance in CI (R^2 = 0.547; adjusted R^2 = 0.533). These values describe in-sample explanatory performance rather than out-of-sample predictive accuracy.

The individual effect sizes (f^2) were 0.174 for PS → PT, 0.116 for PP → PT, 0.077 for PS → CI, 0.002 for PP → CI,

and 0.109 for PT → CI. The PP → CI relationship exhibited a negligible incremental effect size within the estimated model.

D. Direct Relationships and Hypothesis Testing

The five direct relationships were evaluated using the final SmartPLS 4 bootstrapping analysis with 10,000 subsamples, two-tailed testing, and a significance level of 0.05. Table V presents the standardized path coefficients, t-statistics, p-values, and hypothesis decisions.

TABLE V. DIRECT RELATIONSHIPS AND HYPOTHESIS TESTING

Hypothesis	Path	β	t	p	Decision
H1	PS → PT	0.458	4.693	<0.001	Supported
H2	PP → PT	0.372	3.833	<0.001	Supported
H3	PS → CI	0.365	2.408	0.016	Supported
H4	PP → CI	0.059	0.361	0.718	Not supported
H5	PT → CI	0.367	3.066	0.002	Supported

Perceived LMS security was positively associated with trust (β = 0.458, p < 0.001), supporting H1. Perceived LMS privacy protection was also positively associated with trust (β = 0.372, p < 0.001), supporting H2.

Perceived LMS security was positively associated with continuance intention (β = 0.365, p = 0.016), supporting H3. In contrast, the direct relationship between privacy protection and continuance intention was small and statistically nonsignificant (β = 0.059, p = 0.718); therefore, H4 was not supported. This finding does not establish that privacy protection has no relevance to continuance intention, but indicates that its estimated direct coefficient was not statistically distinguishable from zero after accounting for the other predictors.

Trust was positively associated with continuance intention (β = 0.367, p = 0.002), supporting H5. These results indicate that security and trust were significant direct correlates of continuance intention in the specified model, whereas privacy protection did not exhibit a statistically significant direct association.

E. Specific Indirect Effects through Trust

The two hypothesized indirect relationships were assessed using specific indirect-effect estimates and 95% percentile bootstrap confidence intervals. Table VI presents the results.

TABLE VI. SPECIFIC INDIRECT EFFECTS

Hypothesis	Indirect path	β	t	p	95% CI
H6	PS → PT → CI	0.168	2.937	0.003	[0.055, 0.280]
H7	PP → PT → CI	0.137	2.036	0.042	[0.031, 0.292]

Both specific indirect effects were statistically significant at the 0.05 level. The indirect association between perceived LMS security and continuance intention through trust was positive and statistically significant (β = 0.168, t = 2.937, p = 0.003). Its 95% bootstrap confidence interval [0.055, 0.280] excluded zero, supporting H6. The corresponding direct security–continuance relationship was also positive and significant.

The indirect association between perceived LMS privacy protection and continuance intention through trust was likewise positive and statistically significant (β = 0.137, t = 2.036, p = 0.042), with a 95% bootstrap confidence interval of [0.031, 0.292]. Thus, H7 was supported despite the nonsignificant direct PP → CI relationship.

The H7 finding warrants particular caution because its p-value was close to 0.05, the sample was relatively small, and the data were cross-sectional. Both indirect effects represent statistically estimated associations consistent with the proposed model, not evidence that trust causally transmits the influence of security or privacy protection on subsequent LMS usage.

F. Summary of Hypothesis Testing

Overall, six of the seven hypotheses were supported. Perceived LMS security and perceived LMS privacy protection were positively associated with trust. Security was associated with continuance intention both directly and indirectly through trust, whereas privacy protection showed a statistically significant indirect association through trust but no significant direct relationship with continuance intention (Fig. 2).

These results demonstrate different statistical association patterns within the estimated model. They do not establish that security is inherently more influential than privacy protection, that the corresponding coefficients differ significantly from one another, or that the observed relationships are causal.

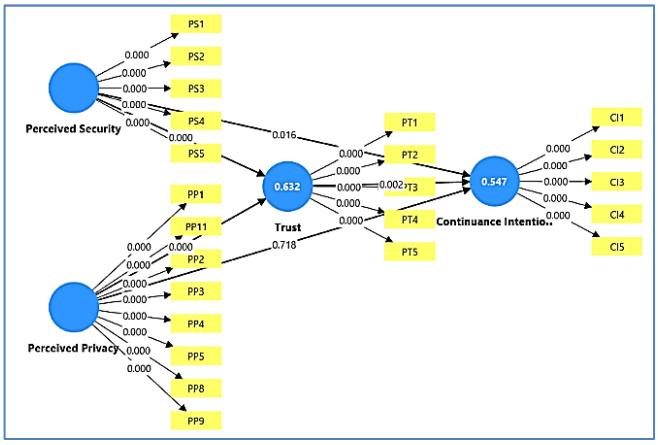

Fig. 2. SmartPLS export.

VI. DISCUSSION

A. Security, Privacy Protection, and Trust in LMS Continuance

The findings reveal different patterns of association for perceived LMS security and perceived LMS privacy protection. Both constructs were positively associated with institutional platform trust, whereas only perceived security demonstrated a statistically significant direct association with continuance intention. This distinction suggests that information-assurance perceptions should not automatically be treated as interchangeable predictors of continued LMS engagement.

The positive security–trust association (β = 0.458, p < 0.001) is consistent with Xu et al. [16], who identified a

positive relationship between perceived security and trust in educational ICT. The present study extends the examination of this relationship to users of institutional LMS platforms in Sri Lankan higher education. Perceived security was also positively associated with continuance intention ($\beta = 0.365$, $p = 0.016$). This finding suggests that confidence in platform safeguards is relevant not only to trust but also to users' stated willingness to continue using an LMS. However, because the study measured perceptions rather than actual security performance, the results do not establish that technically more secure platforms necessarily generate stronger continuance intention.

Perceived privacy protection was positively associated with trust ($\beta = 0.372$, $p < 0.001$). This result is consistent with the conceptual relevance of responsible information handling to trustworthy online learning environments discussed by Anwar [17] and complements privacy-related research in digital education [10]–[12]. Nevertheless, the direct privacy protection–continuance relationship was not statistically significant ($\beta = 0.059$, $p = 0.718$), and its incremental effect size was negligible ($f^2 = 0.002$).

One possible interpretation is that confidence in privacy protection is more closely associated with users' trust evaluations than with their stated continuance intention after security and trust are considered simultaneously. However, this interpretation remains tentative. The relatively high HTMT value between security and privacy protection (0.879) and elevated VIF values for these predictors indicate overlapping explanatory information. The nonsignificant direct privacy coefficient may also reflect limited statistical precision, omitted continuance determinants, or the characteristics of the sampled respondents. The findings therefore do not establish that privacy protection is unimportant or that its direct relationship is absent in the wider population.

Trust itself was positively associated with continuance intention ($\beta = 0.367$, $p = 0.002$). This finding is consistent with the positive trust–continuance relationship reported by Rashidov and Park [18] in mobile-payment applications, although the institutional LMS context differs substantially from consumer financial services. The result also complements established LMS continuance research emphasizing satisfaction, performance expectations, and other post-adoption evaluations [5], [14]. Trust may therefore be considered alongside these established constructs rather than as a replacement for them.

B. Interpretation of the Indirect Relationships

The analysis identified positive specific indirect associations between both information-assurance constructs and continuance intention through trust. The security–trust–continuance association was statistically significant ($\beta = 0.168$, $p = 0.003$; 95% CI [0.055, 0.280]). Because the corresponding direct security–continuance coefficient was also positive and significant, the estimated model exhibited both direct and trust-related indirect associations involving perceived security.

The privacy protection–trust–continuance association was also statistically significant ($\beta = 0.137$, $p = 0.042$; 95% CI [0.031, 0.292]), despite the nonsignificant direct privacy protection–continuance coefficient. This pattern is consistent with an indirect-only statistical association through trust within the specified model. It demonstrates why examining only direct coefficients could overlook relationships represented by the proposed indirect pathways.

However, the privacy-related indirect finding requires particular caution. Its statistical significance was close to the conventional 0.05 threshold, and the sample comprised only 101 respondents. Furthermore, the cross-sectional design cannot establish whether security and privacy perceptions preceded trust or whether trust preceded continuance intention. The indirect results therefore support the specified statistical relationships but do not demonstrate causal mediation.

The different significance patterns also should not be interpreted as proof that security is inherently more influential than privacy protection. A significant coefficient and a nonsignificant coefficient are not necessarily significantly different from one another. Establishing such a difference would require a direct statistical comparison, which was not part of the reported analysis.

C. Contribution to LMS Continuance Research

The study contributes to LMS continuance research by jointly examining perceived security, perceived privacy protection, institutional platform trust, and continuance intention. Established continuance models have emphasized perceived usefulness, satisfaction, expectation confirmation, habit, and other post-adoption factors [1]–[5], [14]. The present model addresses a complementary question concerning the associations between information-assurance perceptions, trust, and continued LMS engagement.

A central contribution is the distinction between security and privacy protection. Although both constructs were positively associated with trust, their estimated direct relationships with continuance intention differed. This finding provides a basis for investigating them separately rather than automatically combining them into a single information-assurance construct. Nevertheless, their substantial empirical overlap, reflected in the HTMT value of 0.879, indicates that further validation of their distinctiveness is necessary.

The second contribution concerns the simultaneous examination of direct and specific indirect associations. In particular, the positive privacy protection–trust–continuance association was statistically significant despite the nonsignificant direct privacy protection–continuance relationship. This finding illustrates the additional information provided by testing indirect paths while retaining appropriate caution about causal interpretation.

Finally, the study connects user-centered LMS continuance research with technical cybersecurity and privacy literature. Previous investigations have examined LMS vulnerabilities, institutional cybersecurity risks, and information-protection mechanisms [6]–[9], [15]. The present study does not assess the effectiveness of such mechanisms; instead, it investigates users' perceptions of security and privacy protection. These perspectives are complementary, and perceived information assurance should not be equated with verified technical security or regulatory compliance.

D. Interpretation in the Sri Lankan Higher Education Context

The Sri Lankan higher education setting provides a relevant context for examining institutional LMS engagement. Previous research has documented challenges associated with online higher education during university closures in Sri Lanka [13]. Against this background, the present findings provide evidence that perceived security, perceived privacy protection, and trust are associated with stated LMS continuance intention among the sampled users.

The mean continuance-intention score (M = 2.711) was lower than the corresponding means for security, privacy protection, and trust. This suggests that strong willingness to continue using LMS platforms should not be assumed merely because such systems have become established in higher education. However, the survey did not measure changes before and after the pandemic, subsequent LMS usage, or whether respondents had meaningful alternatives to their institutional platforms. The findings therefore cannot establish a pandemic-related change in continuance behavior.

Including students, lecturers, and academic staff responded to different institutional roles. Nevertheless, these groups may differ in their LMS responsibilities, usage patterns, and information-protection expectations. Because the analysis pooled all 101 respondents without establishing measurement invariance or testing group-specific relationships, the findings should not be assumed to apply equally across the three categories.

Accordingly, the study offers context-specific evidence from a purposively selected Sri Lankan higher education sample rather than nationally representative estimates. Its contribution is the identification of information-assurance and trust relationships that merit further investigation within institutional LMS environments, not the demonstration of effects unique to Sri Lanka.

VII. Theoretical and Practical Implications

A. Theoretical Implications

This study contributes to LMS continuance research by integrating perceived security, perceived privacy protection, and institutional platform trust into a focused post-adoption model. Established continuance research has emphasized usefulness, satisfaction, expectation confirmation, habit, and other experiential factors [1]–[5], [14]. The present findings complement these explanations by identifying associations involving users' perceptions of information protection and their intention to continue using institutional LMS platforms.

The first theoretical implication concerns the distinction between perceived security and perceived privacy protection. Both constructs were positively associated with trust, but only perceived security showed a statistically significant direct association with continuance intention. This supports examining security and privacy protection separately rather than assuming that they have identical relationships with post-adoption outcomes. Nevertheless, their relatively high HTMT value (0.879) indicates substantial empirical overlap, and further research is required to establish their discriminant validity more conclusively.

The second implication concerns the role of trust. Trust was positively associated with continuance intention, and both security and privacy protection exhibited statistically significant specific indirect associations through trust. Notably, the privacy-related indirect association was significant despite the nonsignificant direct privacy protection–continuance relationship. This demonstrates the analytical value of examining indirect relationships alongside direct paths. However, the findings identify statistical associations rather than establishing that trust causally mediates the influence of information-assurance perceptions.

Third, the study contributes empirical evidence from Sri Lankan higher education by examining students, lecturers, and academic staff within a common model. This broadens the institutional user roles represented in the investigation. Nevertheless, the purposive sampling procedure and pooled analysis do not establish whether the relationships differ across respondent categories or are distinctive to Sri Lanka.

Overall, the theoretical contribution lies in extending the examination of LMS continuance intention to include information-assurance perceptions and trust while recognizing the continuing relevance of established post-adoption determinants. The proposed model should therefore be viewed as complementary to, rather than a replacement for, existing continuance frameworks.

B. Practical Implications

The findings suggest that higher education institutions should consider users' perceptions of security, privacy protection, and trust alongside the functional performance of their LMS platforms. Because perceived security was positively associated with both trust and continuance intention, institutions may benefit from combining effective technical safeguards with clear communication that helps users understand the protections in place.

Relevant practices include reviewing authentication and role-based access controls, maintaining software updates, providing accessible security guidance, and establishing clear procedures for reporting suspected security incidents. These measures are consistent with broader concerns about cybersecurity risks in higher education [9]. However, the present study did not assess the effectiveness of individual security controls or test whether implementing them increases continuance intention.

The positive association between privacy protection and trust also highlights the importance of transparent information-handling practices. Institutions should consider communicating what personal and academic information is collected through the LMS, why it is needed, who is authorized to access it, how it is protected, and how long it is retained. Accessible privacy notices and appropriate channels for raising concerns may help users understand institutional information-management practices.

Importantly, the nonsignificant direct privacy protection–continuance relationship does not justify deprioritizing privacy safeguards. Responsible information handling remains an institutional obligation regardless of whether privacy perceptions are directly associated with stated continuance

intention. The significant indirect association through trust suggests that privacy protection and platform trust are relevant considerations to examine together, although it does not establish that privacy communication will causally increase LMS usage.

Institutions may also consider periodically gathering user feedback on perceived security, privacy protection, and confidence in LMS platforms. Such feedback could help identify concerns that technical assessments alone may not capture. However, perception surveys should complement rather than replace independent security evaluations, privacy-governance reviews, and established institutional procedures.

Finally, security and privacy protection should form part of broader LMS governance and user-support strategies. Continuance intention may also depend on usability, accessibility, educational usefulness, satisfaction, institutional requirements, and other factors not examined in this study. Consequently, information-assurance measures should be integrated with wider efforts to maintain reliable and effective digital learning environments rather than treated as standalone solutions for increasing LMS engagement.

VIII. Limitations and Future Work

Several limitations should be considered when interpreting the findings. First, the study employed purposive non-probability sampling and analyzed 101 respondents from Sri Lankan higher education. Although the sample exceeded the minimum size estimated using G*Power under the specified regression assumptions, this does not establish adequate statistical power for all structural relationships, particularly smaller indirect effects. The sampling strategy also limits generalizability to the wider higher education population. Future studies should recruit larger, more diverse samples across multiple institutions and consider probability-based sampling where feasible.

Second, the analysis combined students, lecturers, and academic staff into a single sample. These groups may differ in their LMS responsibilities, usage patterns, and expectations concerning information security and privacy. Measurement invariance and group-specific relationships were not established. Future research should examine these differences using adequately sized subsamples, measurement invariance assessment, and multigroup analysis.

Third, the cross-sectional design limits causal interpretation because security perceptions, privacy protection perceptions, trust, and continuance intention were measured at one point in time. Consequently, the significant indirect associations through trust do not establish temporal precedence or causal mediation. Longitudinal research could investigate whether changes in information-assurance perceptions precede changes in trust and subsequent LMS engagement.

Fourth, all primary constructs were measured through a common self-report questionnaire, creating the possibility of common method bias, social desirability effects, and response-related measurement error. The available analysis does not demonstrate that these influences were eliminated. Future studies could separate predictor and outcome measurements over time and incorporate independently obtained indicators, including institutional LMS usage records collected with appropriate privacy safeguards.

Fifth, several measurement results warrant caution. The outer loadings of PP5 (0.465), PP9 (0.620), CI2 (0.602), and CI3 (0.555) were below the commonly recommended threshold of 0.708. The AVE for continuance intention was marginally above the minimum criterion (0.501), while the HTMT value between security and privacy protection (0.879) exceeded the conservative 0.85 benchmark. Some inner-model VIF values also exceeded 3.3, indicating overlapping explanatory information. Future studies should refine and independently validate the measurement items, examine the distinctiveness of security and privacy protection, and assess the robustness of the structural findings under theoretically defensible alternative measurement specifications.

Sixth, the model focused on perceived security, perceived privacy protection, and trust without incorporating several established determinants of LMS continuance, including perceived usefulness, satisfaction, expectation confirmation, usability, facilitating conditions, and habit. Their omission limits the explanatory scope of the model and leaves open the possibility of omitted-variable influences. Future research could integrate information-assurance perceptions with established continuance frameworks and assess their additional explanatory contribution.

Finally, the study measured stated continuance intention rather than actual subsequent LMS usage. It also did not directly measure changes associated with the COVID-19 pandemic. Therefore, the findings cannot establish whether the observed relationships reflect pandemic-related transitions or predict sustained LMS engagement over time. Future studies could combine longitudinal surveys with observed usage data and compare institutional platforms, user groups, and educational settings.

Addressing these limitations would strengthen the measurement quality, explanatory scope, and generalizability of future research on information assurance, trust, and LMS continuance intention.

IX. Conclusion

This study examined the relationships among perceived LMS security, perceived LMS privacy protection, trust, and continuance intention in Sri Lankan higher education. Using cross-sectional survey data from 101 students, lecturers, and academic staff, the study evaluated five direct relationships and two specific indirect relationships through trust using partial least squares structural equation modeling (PLS-SEM). Six of the seven hypotheses were supported. Both perceived security and perceived privacy protection were positively associated with trust, while trust was positively associated with continuance intention. Perceived security also demonstrated a significant direct association with continuance intention, whereas the corresponding direct association for privacy protection was not statistically significant.

The principal contribution lies in identifying different patterns of direct and indirect association within a common information-assurance framework. Security was associated with continuance intention both directly and indirectly through

trust, while privacy protection exhibited a statistically significant indirect association through trust despite its nonsignificant direct relationship. These findings highlight the relevance of examining security and privacy protection as conceptually distinct perceptions and considering trust alongside established post-adoption determinants. For higher education institutions, the results suggest that users' confidence in LMS security and information-handling practices deserves attention alongside platform functionality and educational value.

The findings should be interpreted in light of the purposive sample, pooled respondent groups, cross-sectional design, self-reported measurements, and identified measurement limitations. Consequently, the results establish statistical associations rather than causal relationships and cannot be generalized to all Sri Lankan higher education institutions. Future research involving larger and more diverse samples, longitudinal designs, refined measurement instruments, and observed LMS usage could provide stronger evidence concerning these relationships. Overall, the study contributes context-specific empirical evidence to understanding the roles of information-assurance perceptions and trust in institutional LMS continuance intention.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support provided by the Sri Lanka Institute of Information Technology (SLIIT) in facilitating this research. The authors also sincerely thank the students, lecturers, and academic staff who voluntarily participated in the study and contributed their valuable responses. Their participation and cooperation were instrumental in the successful completion of this research.

DECLARATIONS

Competing Interests: The authors declare that there are no financial or non-financial competing interests relevant to the content of this article.

Funding: The authors declare that they have no financial or non-financial competing interests relevant to this article.

Informed Consent: Informed consent was obtained from all participants prior to their participation in the study. Participation was voluntary, and participants were informed of the purpose of the research before data collection.

Data Availability: The data supporting the findings of this study are available from the corresponding author upon reasonable request, subject to applicable ethical and privacy considerations.

Use of GenAI: Generative artificial intelligence tools were used during manuscript preparation solely to assist with language editing, grammar correction, and improvement of clarity and readability. The author reviewed and revised the resulting text and takes full responsibility for the accuracy, integrity, and final content of the manuscript. Generative AI was not used to generate research data or perform the statistical analysis.

REFERENCES

[1] M. Cocosila, H. Trabelsi and G. Farrelly, "An empirical investigation of student online learning continuance intention in the post-COVID-19 pandemic era," Journal of Systems and Information Technology, vol. 26, no. 3, pp. 447-472, 2024.

[2] Y. Li, N. Nishimura, H. Yagami and H. S. Park, "An Empirical Study on Online Learners' Continuance Intentions in China," Sustainability, vol. 13, no. 2, 2021.

[3] H. M. Dai, T. Teo and N. A. Rappa, "Understanding continuance intention among MOOC participants: The role of habit and MOOC performance," Computers in Human Behavior, vol. 112, 2020.

[4] I. S. Rekha, J. Shetty and S. Basri, "Students' continuance intention to use MOOCs: Empirical evidence from India," Education and Information Technologies, vol. 28, pp. 4265-4286, 2023.

[5] A. Bhattacherjee, "Understanding information systems continuance: An expectation-confirmation model," MIS Quarterly, vol. 25, no. 3, pp. 351–370, 2001.

[6] A. Scerbakov, F. Kappe and N. Scerbakov, "Security Vulnerabilities in Modern LMS," in IADIS International Conference e-Learning 2019, 2019.

[7] J. M. Secaira, R. D. Ocampo and E. S. Mena, "Analysis of Risks and Vulnerabilities in a University-Level LMS System," Migration Letters, vol. 20, no. S8, 2023.

[8] S. Ally, "Secure Software Deployment: Investigating the Security Vulnerabilities of Moodle LMS in Public Higher Learning Institutions in Tanzania," International Journal of Advanced Information Science and Technology, vol. 47, pp. 53-61, 2016.

[9] J. B. Ulven and G. Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," Future Internet, vol. 13, no. 2, 2021.

[10] X. Jiang, T.-T. Goh and M. Liu, "On Students' Willingness to Use Online Learning: A Privacy Calculus Theory Approach," Frontiers in Psychology, vol. 13, p. 880261, 2022.

[11] W. Xiao, M. Wang and J. Mo, "Factors influencing college teachers' adoption of live online teaching: A conditional process model of technology acceptance, user satisfaction and privacy concerns," Frontiers in Psychology, vol. 14, 2024.

[12] V. Kabata, "Towards safeguarding users' legitimate rights in Learning Management Systems (LMS): A case study of the Blackboard LMS at Sorbonne University Abu Dhabi," International Journal of E-Learning & Distance Education, vol. 37, no. 1, 2022.

[13] D. Yang, Y. M. Tang, S. Ra and R. Hayashi, "Supporting inclusive online higher education in developing countries: Lessons learnt from Sri Lanka's university closure," Education Sciences, vol. 12, no. 7, p. 494, 2022.

[14] A. A. Rabaa'i, S. A. AlMaati and X. Zhu, "Students' Continuance Intention to Use Moodle: An Expectation-Confirmation Model Approach," Interdisciplinary Journal of Information, Knowledge, and Management, vol. 16, pp. 397-434, 2021.

[15] A. A. Mawgoud, M. H. N. Taha, M. Loey, M. H. Malik and N. E. Khalifa, "Enhancing Data Privacy and Trust in E-Learning: A Blockchain-Based Access Control Protocol for Cloud Educational Systems," Concurrency and Computation: Practice and Experience, vol. 37, no. 18, July 2025.

[16] S. Xu, K. I. Khan and M. F. Shahzad, "Examining the Influence of Technological Self-Efficacy, Perceived Trust, Security, and Electronic Word of Mouth on ICT Usage in the Education Sector," Scientific Reports, vol. 14, 2024.

[17] M. Anwar, "Supporting Privacy, Trust, and Personalization in Online Learning," International Journal of Artificial Intelligence in Education, vol. 31, pp. 769-783, 2021.

[18] A. Rashidov and S. Park, "Continuance Usage Intention in Mobile Payment Applications: The Mediating Roles of User Satisfaction and Trust—Evidence from Uzbekistan," Asian Journal of Business Environment, vol. 16, no. 2, pp. 9-20, 2026.

[19] J. F. Hair Jr., G. T. M. Hult, C. M. Ringle and M. Sarstedt, A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 3 ed., Thousand Oaks, CA: SAGE Publications, 2022.

[20] F. Faul, E. Erdfelder, A.-G. Lang and A. Buchner, "G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences," Behavior Research Methods, vol. 39, no. 2, pp. 175-191, 2007.

[21] J. Henseler, C. Ringle and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," Journal of the Academy of Marketing Science, vol. 43, no. 1, pp. 115-135, 2015.

[22] C. Nitzl, J. L. Roldán and G. Cepeda, "Mediation analysis in partial least squares path modeling: Helping researchers discuss more sophisticated models," Industrial Management & Data Systems, vol. 116, no. 9, pp. 1849-1864, 2016.