

Modeling University Professors' Trust in the "Progress" Platform: Effects of Service Quality and Information Security on Scientific Performance (Higher Education, 2025)

Meriem Merabet^{1*}, Nadjoua Bouzourine²

¹Laboratory of Public Policies and Developmental and Security Challenges in Maghreb Countries, Higher School of Political Science (ENSSP), Algeria

²Member, Laboratory of Public Policies and Developmental and Security Challenges in Maghreb Countries, Higher School of Political Science (ENSSP), Algeria

DOI: <https://doi.org/10.47772/IJRISS.2026.100400062>

Received: 29 March 2026; Accepted: 03 April 2026; Published: 29 April 2026

ABSTRACT

This study examines the determinants of university professors' digital trust in the Progress platform in Algerian higher education. Using a PLS-SEM approach and data from 382 professors, the study analyzes the effects of service quality, ease of use, security and information protection, technical stability and support, and academic suitability.

The results indicate that security and information protection have the strongest and most significant effect on digital trust ($\beta = 0.394$, $p < 0.001$), followed by technical stability and support ($\beta = 0.143$, $p = 0.045$). In contrast, service quality and academic suitability show positive but non-significant effects, while ease of use has no significant impact.

The model explains 46.4% of the variance in digital trust ($R^2 = 0.464$) and demonstrates strong predictive relevance ($Q^2 = 0.385$). The findings highlight that digital trust in institutional platforms is primarily driven by security and system reliability, emphasizing the importance of data protection and stable digital infrastructure in supporting higher education digital transformation.

Keywords: Digital trust; Higher education; Progress platform; PLS-SEM; Technical stability.

INTRODUCTION

The digital transformation of higher education has become a central pillar of public-sector modernization, particularly in developing countries seeking to enhance efficiency, transparency, and service quality. In Algeria, the Progress platform, introduced in 2017, serves as the primary digital infrastructure supporting academic, administrative, and pedagogical processes. Despite its strategic importance, concerns persist regarding university professors' trust in the platform, particularly in relation to technical reliability, institutional support, and data protection.

Research on technology adoption has traditionally relied on models such as the Technology Acceptance Model (TAM), the Unified Theory of Acceptance and Use of Technology (UTAUT), and the SERVQUAL framework. These models emphasize perceived usefulness, ease of use, and service quality as key determinants of system adoption. However, they often overlook digital trust as a broader and multidimensional construct shaped not only by user perceptions, but also by institutional reliability, data security, and system stability. In mandatory institutional platforms, such as those used in higher education, trust may therefore depend more on structural and governance-related factors than on usability alone.

Empirical research on digital trust in Algerian universities remains limited, particularly in terms of integrating technical, organizational, and academic dimensions within a unified analytical framework. Existing studies

have rarely examined how security, technical stability, and institutional support interact with classical adoption variables to shape trust in a compulsory digital environment. This gap is especially significant given the increasing reliance on the Progress platform for core academic operations.

Accordingly, this study addresses the following research question: What are the key determinants of university professors' digital trust in the Progress platform? To answer this question, the study develops an extended TAM-based model, complemented by SERVQUAL, UTAUT, and security–trust perspectives, and empirically tests the proposed relationships using the PLS-SEM method based on survey data collected from 382 university professors.

By positioning digital trust as a central construct, this study aims to provide a more comprehensive understanding of the institutional, technical, and academic factors shaping trust in higher education digital platforms, and to contribute to the design of more reliable and sustainable digital transformation policies.

Importance of the study

The importance of this study lies in its contribution to understanding the determinants of digital trust among university professors within the context of Algeria's ongoing digital transformation strategy. Given the central role of the Progress platform as the primary tool for academic, administrative, and pedagogical management, identifying the factors that shape trust in this system is essential for improving the overall effectiveness of digital initiatives in higher education.

Despite the strategic relevance of the platform, empirical research exploring trust formation in Algerian universities remains scarce. This study addresses this gap by examining how key dimensions—such as service quality, technical stability and support, security and information protection, and academic suitability—collectively influence professors' trust in the platform. By adopting a comprehensive conceptual model that integrates theoretical insights from the Technology Acceptance Model (TAM), the SERVQUAL framework, and organizational trust theory, the study provides a deeper understanding of the institutional and technical requirements necessary to enhance digital trust.

From a practical standpoint, the study offers evidence-based insights for policymakers at the Ministry of Higher Education and Scientific Research. These insights underscore the importance of strengthening data protection mechanisms, ensuring continuous system stability, and reinforcing technical support structures to enhance user confidence. Theoretically, the study contributes to the literature by contextualizing TAM within an institutional environment characterized by regulatory complexity and evolving digital infrastructures, thereby highlighting digital trust as a critical element for sustaining long-term digital transformation in the Algerian higher education sector.

LITERATURE REVIEW

Theoretical Models Related to the Study

Research on technology adoption in higher education commonly relies on frameworks such as TAM, UTAUT, and SERVQUAL, which focus on user perception, acceptance, and intention to use digital technologies. However, these models often overlook digital trust as a broader construct encompassing organizational reliability, data security, service continuity, and compatibility with academic culture.

This study primarily builds on TAM (Davis, 1989) by integrating perceived usefulness and ease of use, while extending the model to include institutional factors specific to Algerian higher education, such as regulatory constraints and digital readiness. Elements from UTAUT (Venkatesh et al., 2003) are incorporated through facilitating conditions, operationalized as technical stability and institutional support. The SERVQUAL model (Parasuraman et al., 1988) is adapted by treating security and information protection as independent determinants, reflecting their critical role in safeguarding academic data. Finally, Diffusion of Innovations Theory (Rogers, 2003) is considered through academic suitability, referring to the alignment between digital platforms and academic practices.

Accordingly, digital trust is conceptualized as a central construct, with TAM as the primary framework, complemented by technical, institutional, and cultural dimensions relevant to digital transformation in higher education.

However, prior studies have rarely examined these dimensions jointly within a unified institutional trust framework, particularly in developing higher education systems.

Objective of the study

The main objective of this study is to analyze the determinants of university professors' digital trust in the Progress platform by examining the influence of key quality dimensions: perceived usefulness, ease of use, security and information protection, technical stability and institutional support, and academic suitability. By integrating these factors into a single analytical framework, the research aims to provide a comprehensive understanding of the technical, organizational, and academic determinants that shape trust in digital systems within Algerian higher education.

To empirically test the proposed model, the study employs Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 4. This method is suitable for analyzing complex relationships between latent variables and evaluating predictive models in emerging digital contexts. It allows the study to assess the relationships between platform quality dimensions and digital trust while generating insights that can support effective digital transformation policies in higher education institutions.

Previous studies and hypothesis development

Digital trust is widely recognized as a key determinant in the effective adoption of digital platforms within higher education institutions. It is shaped through the interaction of technical performance, organizational reliability, perceived usefulness, and users' confidence in system security. Based on established theoretical frameworks in technology adoption and service quality, this study synthesizes prior research to formulate a set of testable hypotheses regarding university professors' trust in the Progress platform.

According to the SERVQUAL model (Parasuraman, Zeithaml, & Berry, 1988), service quality—reflected in operational accuracy, responsiveness, and system reliability—plays a central role in shaping positive user evaluations of digital environments. In the academic context, high service quality enhances trust by ensuring the smooth execution of essential pedagogical and administrative tasks. Therefore:

H1: Service quality of the Progress platform positively influences users' digital trust.

Within the Technology Acceptance Model (TAM) (Davis, 1989), perceived ease of use reduces the cognitive effort required to interact with a system, thereby facilitating continued engagement. A digital platform perceived as easy to use is thus more likely to be trusted by its users. Hence:

H2: Ease of use of the Progress platform positively influences users' digital trust.

Literature on digital security highlights the importance of data protection, privacy mechanisms, and user perceptions of safety as foundational components of digital trust (Martin & Murphy, 2017). In university settings, where sensitive academic and administrative information is processed, security becomes a decisive factor in building trust. Thus:

H3: Security and information protection of the Progress platform positively influence users' digital trust.

The UTAUT model (Venkatesh et al., 2003) identifies facilitating conditions—such as technical stability, continuous system support, and institutional assistance—as essential in enhancing system reliability and user confidence. In this light, technical reliability and effective support services contribute directly to strengthening digital trust. Accordingly:

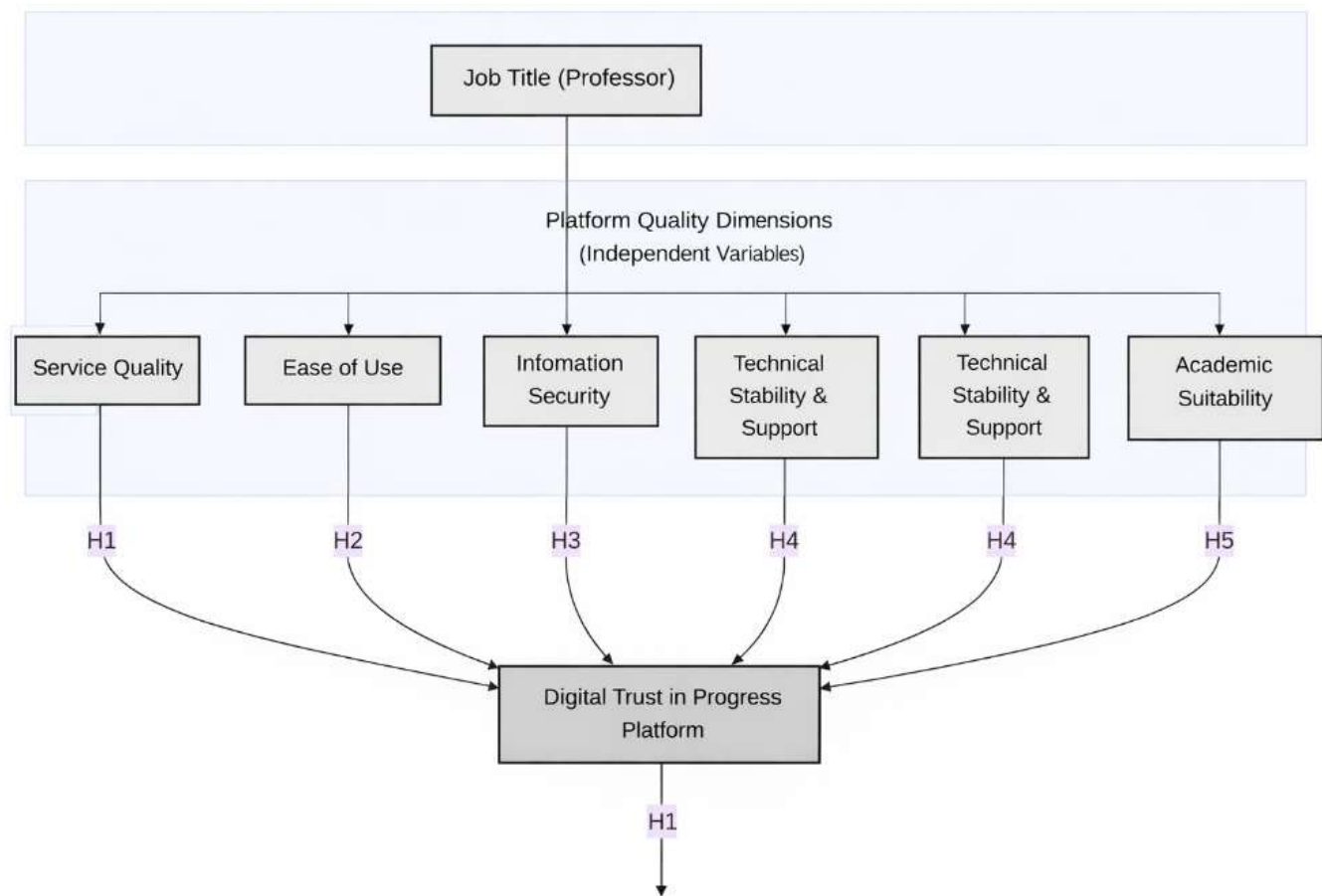
H4: Technical stability and institutional technical support positively influence users' digital trust.

Drawing from Rogers’s (2003) Diffusion of Innovations Theory, the concept of compatibility (or academic suitability) suggests that technologies aligned with users’ professional practices and institutional culture are more likely to be trusted and adopted. Within the Progress platform, alignment with academic workflows and pedagogical responsibilities is therefore expected to reinforce trust. Thus:

H5: Academic suitability of the Progress platform positively influences users’ digital trust.

Although prior literature acknowledges that individual characteristics may shape perceptions of technology, the present study does not include job title as a moderating variable due to the lack of categorical variation within the sample. Therefore, no moderating hypothesis is proposed.

Fig.1. Research framework



Research design

This study adopts a quantitative research design to examine the impact of the Progress platform’s quality dimensions on digital trust among university professors in Algerian higher education. The target population consists of university professors, estimated at 63,652 individuals nationwide; estimated at approximately 63,000 professors nationwide (Ministry data)

The sample size was determined using the Krejcie and Morgan (1970) formula with finite population correction. At a 95% confidence level, a 0.50 population proportion, and a 5% margin of error, the recommended minimum sample was 382 respondents. Accordingly, 382 valid questionnaires were collected and used for analysis, meeting the statistical requirements for structural equation modeling.

The questionnaire was developed based on an extensive literature review on service quality, technology acceptance, digital trust, and information security, and was evaluated by academic experts to ensure content validity and clarity.

Data collection was conducted through two methods

Electronic distribution via official institutional email channels.

Direct distribution with an explanation of the study's objectives and confidentiality assurances.

The questionnaire contained a structured section measured using a five-point Likert scale. It included five independent constructs: Service Quality (SQ), Ease of Use (EU), Security and Information Protection (SIP), Technical Stability and Support (TST), and Academic Suitability (AS), in addition to the dependent construct Digital Trust (DT). Each construct was measured using items adapted from validated scales.

This design provides methodological rigor for analyzing causal relationships using PLS-SEM and supports evidence-based recommendations to strengthen digital trust in higher education digital platforms.

PLS-SEM analysis

Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 4 was applied to analyze the relationships between the Progress platform's quality dimensions and digital trust among university professors. This method is suitable for predictive and exploratory research, for analyzing complex models with multiple latent constructs, and for handling relatively large samples ($N = 382$).

SmartPLS 4 was selected due to its suitability for complex predictive models and its robustness in handling non-normal data.

The analysis followed two main stages

Measurement Model Assessment The first stage evaluated the reliability and validity of the reflective measurement model. Internal consistency was assessed using Cronbach's Alpha and Composite Reliability (CR), while convergent validity was measured through the Average Variance Extracted (AVE). Discriminant validity was verified using the Heterotrait–Monotrait Ratio (HTMT) to ensure that each construct represented a distinct conceptual dimension. Most indicator loadings exceeded 0.70, and indicators with slightly lower values were retained when CR exceeded 0.70 and discriminant validity conditions were satisfied, consistent with PLS-SEM guidelines for exploratory research.

Structural Model Assessment The second stage tested the hypothesized relationships between platform quality dimensions and digital trust. Path coefficients were estimated and their significance assessed using the bootstrapping procedure. The model's explanatory power was evaluated using R^2 , while effect sizes (f^2) and predictive relevance (Q^2) were calculated to assess predictive accuracy and the contribution of each independent construct.

This analysis enabled the testing of five hypotheses linking Service Quality, Ease of Use, Security and Information Protection, Technical Stability and Support, and Academic Suitability to Digital Trust. No moderating variables were included because the sample consisted solely of university professors.

Overall, PLS-SEM provided a robust framework for integrating theoretical constructs with empirical evidence and for identifying the determinants of digital trust in higher education platforms.

Analysis

Professors' confidence in the Progress platform

The analysis shows that professors' trust in the Progress platform varies across the evaluated quality dimensions. Overall perceptions are generally positive, but trust remains uneven and closely related to

technical reliability, procedural clarity, and compatibility with academic workflows.

1. Service Quality

Perceptions of service quality were moderately positive. Professors recognized that the platform facilitates key academic and administrative tasks such as course management, grade submission, and student monitoring. However, the lack of standardized operational guidelines across institutions created inconsistencies in procedures (e.g., deadlines and record visibility), which reduced perceived transparency and stability.

2. Information Security

Confidence in data security was relatively strong, as most professors trusted the platform's ability to protect institutional and personal data. Nevertheless, some uncertainty remained regarding data confidentiality and long-term storage, mainly due to limited communication about security protocols and insufficient institutional awareness regarding data protection mechanisms.

3. Technical Stability and Support

Technical stability appeared as a weaker dimension of trust. Although support channels exist, professors reported delays in problem resolution and uneven responsiveness across institutions. These issues were linked to limited specialized technical staff and centralized system management, particularly during high-demand periods such as enrollment and grade processing.

4. Academic Suitability

Academic suitability recorded the highest level of confidence. Professors emphasized that the platform effectively integrates administrative, pedagogical, and documentation functions, aligning well with academic needs. However, several features remain underused due to limited training and insufficient user guidance.

5. Overall Assessment

In general, professors' trust in the Progress platform can be described as positive but conditional. Stronger trust is associated with academic suitability and service facilitation, while weaker confidence relates to technical responsiveness, procedural clarity, and limited communication about security measures. Strengthening digital trust therefore requires continuous training, transparent communication, improved technical support, and stronger institutional coordination in digital governance.

These descriptive insights are further validated by the structural model results, which confirm the dominant role of security and technical stability in shaping trust

Results of PLS-SEM analysis

Measurement Model Analysis

The measurement model was evaluated using SmartPLS 4, and the results indicate acceptable psychometric quality across all constructs. Indicator reliability was first examined through outer loadings, where most indicators exceeded the recommended 0.70 threshold. A few items showed slightly lower values but were retained because their constructs demonstrated adequate composite reliability and discriminant validity, consistent with PLS-SEM guidelines for exploratory research.

Multicollinearity was assessed using the Variance Inflation Factor (VIF). The values ranged from 1.107 to 1.534, remaining well below the recommended threshold of 5.0 (Hair et al., 2019). The highest values were recorded for PSAAW4 (1.534) and UCPP5 (1.406), confirming that multicollinearity is not a concern.

Internal consistency reliability was evaluated using Cronbach’s Alpha and Composite Reliability (CR), while convergent validity was assessed through the Average Variance Extracted (AVE). All constructs showed CR values above 0.70, indicating satisfactory reliability. Although some AVE values were slightly below 0.50, they remain acceptable in PLS-SEM when composite reliability is adequate and constructs are theoretically supported.

Discriminant validity was examined using the Fornell–Larcker criterion, where the square root of AVE for each construct exceeded its correlations with other constructs, confirming discriminant validity. This result was further supported by the Heterotrait–Monotrait Ratio (HTMT), with all values below the 0.90 threshold.

Overall, the measurement model demonstrates acceptable reliability, convergent validity, and discriminant validity, with VIF values below 3, confirming the absence of collinearity issues. These results indicate that the measurement instrument is psychometrically sound and suitable for structural model evaluation in the Algerian higher education context.

Although some AVE and Cronbach’s Alpha values fall slightly below recommended thresholds, this is acceptable in exploratory PLS-SEM studies, particularly in emerging research contexts. However, these results suggest potential limitations in indicator reliability and highlight the need for future refinement of measurement scales.

Structural Model Analysis

After confirming the reliability and validity of the measurement model, the structural model was evaluated using the bootstrapping procedure in SmartPLS 4 to estimate path coefficients and test the significance of the hypothesized relationships.

The results show that Security and Information Protection (SIP) had the strongest positive effect on digital trust ($\beta = 0.394, p < 0.001$). This indicates that data confidentiality, integrity, and system security play a central role in professors’ trust toward institutional digital platforms. Technical Stability and Technical Support (TST) also showed a significant positive effect ($\beta = 0.143, p = 0.045$), suggesting that consistent system performance and responsive support contribute to trust formation.

In contrast, Service Quality (SQ) and Academic Suitability (AS) had positive but statistically non-significant effects ($p \approx 0.081$ and $p = 0.082$). Likewise, Ease of Use (EU) did not show a significant direct impact on digital trust ($p = 0.174$), indicating that system usability alone is not a decisive factor in this mandatory institutional platform context.

The structural model explained 46.4% of the variance in digital trust ($R^2 = 0.464$), reflecting moderate explanatory power. The model also demonstrated strong predictive relevance ($Q^2 = 0.385$), confirming its predictive capability.

Overall, the findings suggest that digital trust in Algerian universities is primarily driven by security and technical reliability, rather than interface simplicity or service efficiency. This aligns with methodological recommendations emphasizing the importance of system stability and data protection in trust formation. However, these results should be interpreted within the Algerian institutional context, where centralized governance and strong expectations for data protection may increase the importance of security and reliability compared with other platform quality dimensions.

Table 1. Multicollinearity Statistics (VIF) for Indicators Collinearity statistics (VIF)

		AS 1	1,393	SQ4	1,186	TST4	1,353
EU1	1,144	AS 2	1,254	SIP 1	1,260	DT1	1,467

EU2	1,292	AS 3	1,182	SIP 2	1,226	DT2	1,283
EU3	1,369	AS 4	1,303	SIP3	1,349	DT3	1,260
EU4	1,199	AS 5	1,534	SIP 5	1,201	DT4	1,278
EU5	1,215	SQ1	1,179	TST1	1,107	DT5	1,406

Note: SQ = Service Quality; EU = Ease of Use; SIP = Security and Information Protection; TST = Technical Stability and Technical Support; AS = Academic Suitability; DT = Digital Trust.

Higher degree compositions

The evaluation of higher-order constructs shows that the main platform quality dimensions—Ease of Use (EU), Platform Suitability for Academic and Administrative Work (PSAAW), Service Quality (SQ), Security and Information Protection (SIP), and Technical Stability and Technical Support (TST)—demonstrate acceptable psychometric properties according to PLS-SEM standards. Composite reliability (ρ_c) values exceeded the recommended 0.70 threshold, ranging from 0.786 (TST) to 0.806 (PSAAW), confirming adequate internal consistency.

However, some constructs showed Cronbach’s Alpha values slightly below 0.70, including Ease of Use (0.673), Service Quality (0.593), and Security and Information Protection (0.656). Similarly, Average Variance Extracted (AVE) values for Ease of Use (0.433), Platform Suitability (0.454), and Security and Information Protection (0.492) were marginally below the recommended 0.50 threshold. Despite this, these deviations do not compromise the overall measurement model.

Within the PLS-SEM framework, composite reliability is considered more robust than Cronbach’s Alpha, particularly for reflective constructs with a limited number of indicators. In this study, satisfactory composite reliability values support construct reliability. Discriminant validity was also confirmed using the Fornell–Larcker criterion and HTMT (< 0.90), indicating clear conceptual distinctions among constructs. Additionally, multicollinearity diagnostics showed no issues, with VIF values below 3, confirming the absence of indicator redundancy.

In exploratory or context-specific research, especially in studies of emerging digital infrastructures in higher education, minor deviations from strict AVE or Cronbach’s Alpha thresholds are generally acceptable when theoretical justification and other validity criteria are satisfied. Therefore, all higher-order constructs were retained for structural model evaluation. Future research may improve measurement precision by refining weaker indicators or expanding item sets to strengthen convergent validity and internal consistency.

Table 2. Construct Reliability and Validity

Construct	Cronbach’s Alpha	Dijkstra–Henseler’s reliability coefficient (ρ_A)	Composite Reliability (CR)	Average Variance Extracted (AVE)	VIF	f^2	$Q^2_{predict}$
Ease of Use (EU)	0.673	0.674	0.792	0.433	1.500	0.010	0.214
Academic Suitability (AS)	0.701	0.701	0.806	0.454	1.891	0.028	0.237
Quality of Service (SQ)	0.593	0.596	0.795	0.551	1.340	0.022	0.105

Security and Information Preservation (SPI)	0.656	0.661	0.795	0.492	1.229	0.190	0.163
Technical Stability and Technical Support (TST)	0.721	0.601	0.786	0.551	—	0.031	0.179

Table 3. Fornell–Larcker Criterion

Construct	EU	PSAAW	QS	SIP	TST	DT
EU	0.658					
AS	-0.006	0.674				
SQ	0.009	0.418	0.742			
SIP	-0.013	0.554	0.281	0.702		
TST	0.082	0.346	0.221	0.372	0.742	
DT	0.385	-0.003	0.530	0.378	0.600	0.688

Note: Diagonal elements (in bold) represent the square roots of the Average Variance Extracted (AVE) Off-diagonal elements represent the correlations between constructs.

Discriminant validity is established when the square root of AVE for each construct exceeds its correlations with other constructs.

Table 4. Heterotrait–Monotrait Ratio (HTMT) – Matrix

	EU	AS	SQ	SIP	TST	DT
EU						
AS	0,066					
SQ	0,705	0,632				
SIP	0,468	0,807	0,457			
TSTS	0,386	0,571	0,377	0,578		
DT	0,541	0,727	0,572	0,858	0,593	

Note: HTMT values below the conservative threshold of 0.90 indicate adequate discriminant validity between constructs.

Although the HTMT value between SIP and DT (0.858) approaches the upper bound, it remains within

acceptable limits, reflecting a theoretically coherent and substantively meaningful relationship rather than construct redundancy.

Analyzing direct effects in the structural model (Path Coefficients)

The analysis of the direct path coefficients confirms that Security and Information Protection (SIP) exerted the strongest direct effect on university professors’ digital trust in the Progress platform ($\beta = 0.394, p < 0.001$), as reported in Table 5. This result highlights the central role of data confidentiality, information integrity, and perceived system security in shaping trust toward institutional digital platforms.

Technical Stability and Technical Support (TST) also demonstrated a statistically significant positive effect on digital trust ($\beta = 0.143, p = 0.045$), indicating that system reliability, continuity of service, and the availability of effective technical support contribute meaningfully to professors’ confidence in the platform.

In contrast, Service Quality (SQ) and Academic Suitability (AS) exhibited positive but statistically non-significant effects at the 0.05 level, suggesting that while these dimensions enhance platform functionality and contextual alignment, they do not independently determine trust within the examined institutional setting. Similarly, Ease of Use (EU) showed no statistically significant direct effect on digital trust, indicating that perceived usability alone is insufficient to explain trust formation in a mandatory higher education platform environment.

Overall, the pattern of direct effects indicates that digital trust is driven primarily by institutional assurances of security and technical reliability, rather than by interface simplicity or perceived operational efficiency. These findings reinforce the hierarchical nature of trust formation in public-sector digital platforms, where structural and governance-related factors precede functional considerations.

Table 5. Path Coefficients

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (O/STDEV)	P values	Significance
EU -> DT	0,088	0,100	0,065	1,360	0,174	n.s.
AS -> DT	0,169	0,165	0,097	1,737	0,082	n.s.
SQ -> DT	0,126	0,127	0,073	1,745	0,081	n.s.
SIP -> DT	0,394	0,396	0,080	4,922	< 0.001	<i>Significant</i>
TST -> DT	0,143	0,153	0,071	2,002	0,045	Significant

Note: DT = Digital Trust; EU = Ease of Use; AS = Academic Suitability; SQ = Service Quality; SIP = Security and Information Protection; TST = Technical Stability and Technical Support. Significance was assessed using bootstrapping in SmartPLS 4 (two-tailed test).

Table 5 presents the results of the structural model analysis conducted using the PLS-SEM approach to test the study hypotheses regarding the influence of the Progress platform’s quality dimensions on digital trust (DT) among university professors.

All estimated path coefficients exhibited positive signs consistent with the theoretical framework; however, their levels of statistical significance varied across constructs. The results indicate that Security and Information Protection (SIP → DT) constitutes the most influential determinant of digital trust ($\beta = 0.394, t = 4.922, p < 0.001$), thereby supporting Hypothesis H3 and reinforcing prior research that identifies digital security as a cornerstone of trust in institutional and public-sector platforms.

Similarly, Technical Stability and Technical Support (TST → DT) demonstrated a positive and statistically significant effect ($\beta = 0.143$, $t = 2.002$, $p = 0.045$), confirming Hypothesis H4 and highlighting the importance of system reliability, continuity of service, and responsive technical assistance in sustaining users' trust.

In contrast, Academic Suitability (AS → DT) showed a positive but statistically non-significant relationship ($\beta = 0.169$, $t = 1.737$, $p = 0.082$), as did Service Quality (SQ → DT) ($\beta = 0.126$, $t = 1.745$, $p = 0.081$). These findings suggest that while these dimensions contribute to overall platform perceptions, they play a supportive rather than decisive role in the formation of digital trust, leading to the rejection of Hypotheses H1 and H5 at the 0.05 significance level.

Moreover, Ease of Use (EU → DT) exhibited no statistically significant direct effect on digital trust ($\beta = 0.088$, $p = 0.174$), resulting in the rejection of Hypothesis H2. This outcome indicates that usability alone does not independently explain trust formation within the Algerian higher education context, particularly in a mandatory institutional platform.

Overall, the results reported in Table 5 confirm that security-related and infrastructural factors—namely information protection and technical stability—constitute the primary drivers of digital trust in the Progress platform. In contrast, service quality and academic suitability exert complementary yet secondary effects, while ease of use, although behaviorally relevant, does not directly shape trust perceptions. These findings underscore the necessity of adopting a multidimensional and institutionally grounded analytical approach that integrates technical, security, and governance-related factors when examining digital trust in higher education platforms.

Fig.2. Structural equation modeling using PLS-SEM

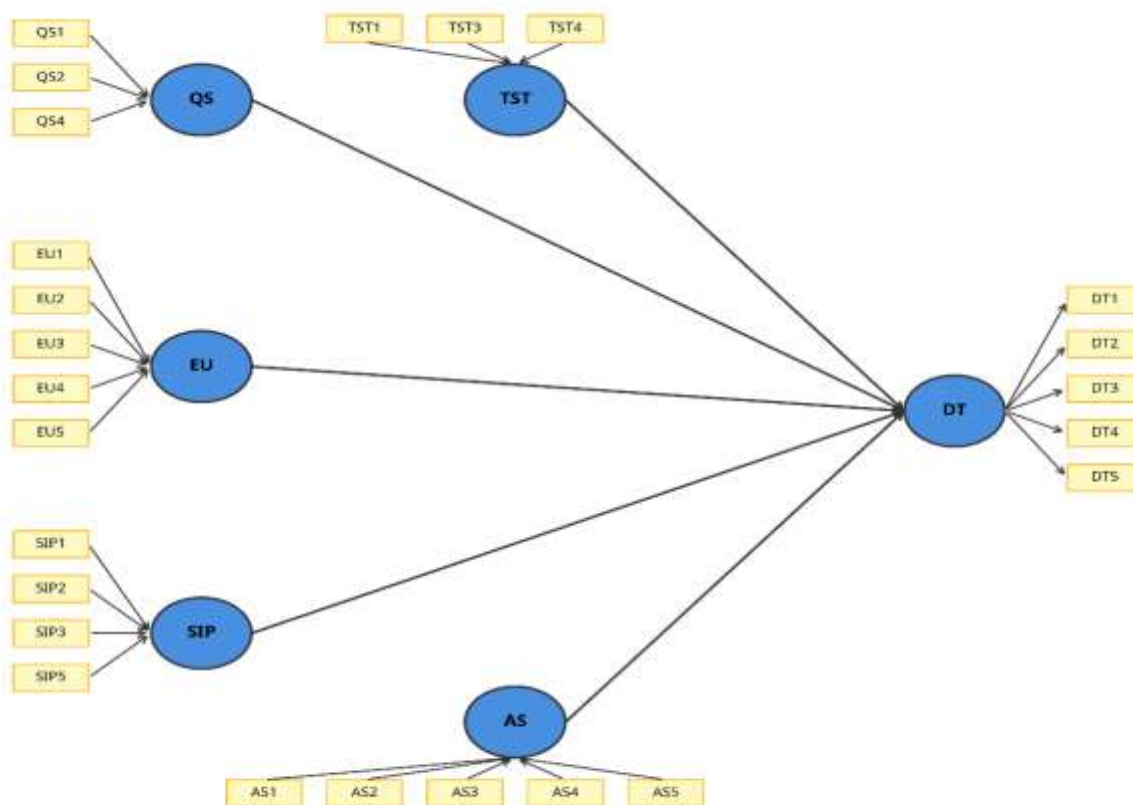


Figure 2 illustrates the structural model estimated using the Partial Least Squares Structural Equation Modeling (PLS-SEM) approach. The blue circles represent the latent constructs, while the arrows indicate the hypothesized relationships between the quality dimensions of the Progress platform—Service Quality (SQ),

Ease of Use (EU), Security and Information Protection (SIP), Technical Stability and Technical Support (TST), and Academic Suitability (AS)—and the endogenous construct, Digital Trust (DT).

As shown in Figure 2, Security and Information Protection (SIP) emerged as the strongest determinant of digital trust ($\beta = 0.394$, $t = 4.922$, $p < 0.001$), underscoring the central role of data protection, confidentiality, and system security in shaping professors' trust in a mandatory national digital platform. Technical Stability and Technical Support (TST) also demonstrated a statistically significant positive effect on digital trust ($\beta = 0.143$, $p = 0.045$), indicating that system reliability and the availability of effective technical assistance contribute meaningfully to trust formation.

In contrast, Service Quality (SQ) and Academic Suitability (AS) exhibited positive but statistically non-significant effects ($p > 0.05$), while Ease of Use (EU) showed no significant direct influence on digital trust. These results suggest that, within an institutional and compulsory usage context, trust is not primarily driven by usability or perceived functional efficiency, but rather by structural assurances related to security and technical reliability.

The structural model explained 46.4% of the variance in digital trust ($R^2 = 0.464$) and demonstrated satisfactory predictive relevance ($Q^2 = 0.385$), indicating moderate explanatory and predictive power. Overall, the pattern of results depicted in Figure 2 confirms that digital trust in higher education platforms follows a hierarchical logic, in which security-related and infrastructural dimensions take precedence over interface-related considerations.

DISCUSSION

The findings indicate a clear reordering of digital trust determinants in mandatory institutional platforms. In contrast to TAM, which emphasizes ease of use and perceived usefulness, digital trust in the Progress platform is primarily driven by Security and Information Protection (SIP) and Technical Stability and Support (TST). This underscores that trust in public-sector digital systems is grounded more in institutional guarantees, data protection, and system reliability than in interface usability.

The non-significant effects of Service Quality (SQ) and Academic Suitability (AS) suggest that these dimensions play a complementary role by enhancing overall platform perception rather than directly shaping trust. Likewise, the absence of a significant effect for Ease of Use (EU) indicates that usability may operate indirectly, consistent with studies distinguishing digital trust from technology acceptance.

These results align with prior research emphasizing the central role of security and institutional reliability in trust formation, while diverging from classical adoption models. The model demonstrates moderate explanatory power ($R^2 = 0.464$) and strong predictive relevance ($Q^2 = 0.385$), supporting its robustness. Overall, the study highlights that strengthening digital trust in higher education requires prioritizing security, system stability, and transparent digital governance over usability improvements alone.

This finding contrasts with TAM-based studies where ease of use is typically a primary determinant (Davis, 1989).

Implications

Theoretical Implications

This study contributes to the literature on digital trust and technology adoption in several ways.

First, it conceptualizes digital trust as a hierarchical construct, where security and technical reliability play a primary role, challenging traditional models such as TAM that prioritize ease of use.

Second, it expands technology adoption frameworks by incorporating institutional and infrastructural factors, particularly security and technical stability, which are critical in developing digital ecosystems.

Third, the study positions digital trust as an institutional construct rather than solely an individual perception. In mandatory public-sector platforms, trust is shaped by governance quality, institutional credibility, and data protection policies, aligning digital trust research with broader discussions in public administration and digital governance.

Practical Implications

The findings provide several practical insights for policymakers, university administrators, and platform developers.

First, universities should prioritize information security, including standardized data protection protocols across institutions.

Second, the importance of technical stability highlights the need for decentralized technical support units capable of responding quickly to system failures, particularly during critical academic periods.

Third, professional training programs should move beyond technical instruction and link platform use to academic and administrative productivity.

Finally, implementing real-time feedback mechanisms for reporting technical and security issues can improve system responsiveness, transparency, and long-term trust in digital platforms.

Limitations and Future Research

Despite its methodological rigor, this study has several limitations.

First, the cross-sectional design limits causal interpretation and the analysis of trust evolution over time. Future studies could adopt longitudinal approaches.

Second, the sample included only university professors, which limits generalization to other stakeholders such as students, administrative staff, and ICT specialists. Future research could adopt a multi-stakeholder perspective.

Third, the reliance on self-reported perceptions may introduce common method bias. Future studies could integrate objective system indicators, such as system uptime, response latency, and security incident records.

Fourth, although the model explains a significant portion of digital trust ($R^2 = 0.464$), additional variables such as perceived risk, digital literacy, institutional transparency, and trust in government could further enhance explanatory power.

Finally, comparative studies across institutions or countries, particularly within the Maghreb or Global South, could provide deeper insights into how governance and cultural contexts influence digital trust.

CONCLUSION

Using PLS-SEM, this study examined the determinants of digital trust in the Progress platform among university professors in Algerian higher education. The results indicate that digital trust is primarily driven by security and information protection, followed by technical stability and support, while ease of use, service quality, and academic suitability do not exert significant direct effects.

The study contributes by reconceptualizing digital trust as an institutional construct shaped by security assurances, system reliability, and governance quality, rather than by usability factors emphasized in traditional adoption models. These findings highlight the need for higher education institutions to prioritize

data protection, infrastructure stability, and transparent digital governance to sustain effective digital transformation.

Scientific and practical contribution and recommendations

Scientific Contribution

The study provides a new institutional interpretation of digital trust in higher education. Rather than extending TAM at the individual level, it demonstrates that trust in mandatory academic platforms is hierarchically structured and driven primarily by security and institutional reliability.

The dominance of Security and Information Protection over usability factors challenges traditional acceptance models and emphasizes that trust should be understood as an institutional construct shaped by governance, infrastructure, and reliability. This perspective contributes to research on digital governance and technology adoption in developing digital ecosystems.

Practical Contributions and Recommendations

Based on the empirical results, several recommendations can be proposed

1. Institutionalize information security standards, including encryption, privacy protection policies, and formal data governance procedures.
2. Strengthen decentralized technical support units, especially during critical academic periods such as registration and examinations.
3. Redesign digital training programs to connect platform usage with academic productivity and administrative efficiency.
4. Implement multidimensional evaluation frameworks assessing digital trust, security perception, technical stability, and support responsiveness.
5. Establish formal feedback systems allowing professors to report technical problems and security concerns.
6. Conduct post-update system evaluations to monitor the impact of technical upgrades on system performance and reliability.

REFERRALS AND REFERENCES

1. Hair J. F., Hult G. T. M., Ringle C. M., & Sarstedt M. (2019), *A primer on partial least squares structural equation modeling (PLS-SEM)*, SAGE Publications, United States.
2. Hair J. F., Hult G. T. M., Ringle C. M., & Sarstedt M. (2022), *Partial least squares structural equation modeling (PLS-SEM): Guidelines for using SmartPLS*, SAGE Publications, United States.
3. Rogers E. M. (2003), *Diffusion of innovations*, Free Press, United States.
4. Al-Hujran O., Al-Debei M. M., Chatfield A., & Migdadi M. (2015), The imperative of influencing citizen attitude toward e-government adoption and use, *Computers in Human Behavior*, Volume 53, pp.189–203.
5. Davis F. D. (1989), Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, Volume 13, No.3, pp.319–340.
6. Falciola J., Riva S., & Zanaboni P. (2020), Factors influencing the adoption of digital technologies in healthcare: A systematic review, *International Journal of Medical Informatics*, Volume 141, Article 104242.
7. Krejcie R. V., & Morgan D. W. (1970), Determining sample size for research activities, *Educational and Psychological Measurement*, Volume 30, pp.607–610.
8. Li H., Wu J., Zhang X., & Yang F. (2022), Examining information security and digital trust in online environments, *Information & Management*, Volume 59, No.1, Article 103118.

9. Martin K. D., & Murphy P. E. (2017), The role of data privacy in digital trust, *Journal of Business Ethics*, Volume 143, pp.1–13.
10. Parasuraman A., Zeithaml V. A., & Berry L. L. (1988), SERVQUAL: A multiple-item scale for measuring consumer perceptions of service quality, *Journal of Retailing*, Volume 64, No.1, pp.12–40.
11. Venkatesh V., Morris M. G., Davis G. B., & Davis F. D. (2003), User acceptance of information technology: Toward a unified view, *MIS Quarterly*, Volume 27, No.3, pp.425–478.
12. Sarstedt M., Ringle C. M., & Hair J. F. (2016), Partial least squares structural equation modeling, *Handbook of Market Research*, Springer, pp.1–40.
13. Samia A. (2021), Digital transformation in Algerian universities: A case study of the Progress platform, *Journal of Educational Technology Studies*, Volume 5, No.3, pp.88–102.
14. Senadjki A. (2025), Enhancing organizational research models through moderating and mediating variables: A PLS-SEM perspective, *International Journal of Organizational Analysis*, Volume 33, No.1, pp.112–128.
15. Pisarska A., Kryczka S., & Castellone A. (2025), Institutional digital trust: The interplay of technical and organizational factors, *Journal of Digital Governance*, Volume 7, No.2, pp.45–63.
16. Ministry of Higher Education and Scientific Research (n.d.), National strategy for digital transformation in higher education, Government of Algeria. OnLine: <http://www.mesrs.dz> (consulted on: 06.03.2026).