ISSN: 2182-2069 / E-ISSN: 2182-2077

A Comprehensive Analysis of Risk and Trust in Using GPT-Style Models for E-Learning Systems

María Fernanda Moya Puente[1], Augusto Oswaldo Benavides Medina[2],
Eddy Miguel Aguirre Reyes[3], Carlos Alberto Lamadrid Vela[4], Jimmy Frank Silva Urcia[5],
José Daniel Montano Amador[6], and Ronald M. Hernández[7*]

[1]Universidad Nacional de Tumbes, Perú. m.moyampuente@posgradountumbes.edu.pe,
https://orcid.org/0000-0002-5824-9939

[2]Universidad Nacional de Tumbes, Perú. abenavidesm@untumbes.edu.pe,
https://orcid.org/0000-0002-3017-7945

[3]Universidad Nacional de Tumbes, Perú. eaguirrer@untumbes.edu.pe,
https://orcid.org/0000-0003-1304-7601

[4]Universidad Nacional de Tumbes, Perú. c.lamadrid.vela@posgradountumbes.edu.pe,
https://orcid.org/0000-0003-4011-3301

[5]Universidad Nacional de Tumbes, Perú. jsilvau@untumbes.edu.pe,
https://orcid.org/0000-0001-5188-2144

[6]Universidad Nacional de Tumbes, Perú. jmontanoa@untumbes.edu.pe,
https://orcid.org/0000-0003-3500-6165

[7*]Universidad Señor de Sipán, Perú. ronald.hernandez@outlook.com.pe,
https://orcid.org/0000-0003-1263-2454

Received: September 29, 2025; Revised: November 05, 2025; Accepted: December 29, 2025; Published: February 27, 2026

Abstract

The incorporation of GPT-style LLMs (Large Language Models) into e-learning mechanisms has changed digital means of teaching by allowing the generation of content in a personalised manner, smart tutoring, and automated evaluation. But despite this, concerns regarding trust as well as risk, data privacy, bias, reliability of content, and dependence of the learners are continuing to be observed from a methodical and experiential point of view, which is often insufficient. This study offers a detailed exploration of trust-risk interaction in connection with adopting GPT-style frameworks in e-learning settings. A hybrid research mechanism is implemented, bringing together an extensive survey conducted on 412 instructors as well as students through experimental evaluation in three main e-learning approaches, which are the generation of content, adaptive tutoring, and acquiring feedback through automation. Statistical evaluation, in addition to checking the reliability, correlation analysis, and regression modeling, is utilised to calculate trust and risk indicators. This survey denotes robust underlying consistency with a value of 0.87 Cronbach's alpha. The results acquired show that the subjective adequacy with $\beta = 0.42$ and $p < 0.01$, as well as explainability with $\beta = 0.31$ and $p < 0.05$, impact the reliability of consumers in a positive manner, whilst risk of data privacy with $\beta = -0.38$ and $p < 0.01$, and content generated via AI significantly reduce the levels of

DOI: *10.58346/JISIS.2026.I1.024*

* Corresponding author: Universidad Señor de Sipán, Perú.

trust. Preliminary findings denote that learning via the assistance of GPT has increased the percentage of task completion activities by 23%, but despite that, there was a reduction in accuracy by 14% as spotted during evaluation in risky scenarios without human surveillance. On the basis of these evaluations, this paper presents a risk-trust mechanism that combines transparency frameworks, validation through HITL (Human-in-the-loop), and surveillance controls. The research summarizes that GPT-style mechanisms also provide trustworthy benefits in e-learning environments, fostering it in a sustainable manner requires reducing risks and fortifying trust in a systematic manner via supervision, technical, and moral protection.

Keywords: GPT-Style Models, Large Language Models, E-Learning Systems, Trust Assessment, Risk Analysis, Data Privacy, Explainable AI.

1 Introduction

The incorporation of GPT-style LLMs (Large Language Models) into e-learning mechanisms has increasingly improved in recent times, offering profitable benefits in personalized Education, feedback automation, and adaptive generation of content. These generative mechanisms, illustrated with the support of the GPT series of OpenAI, offer striking potential in comprehending and providing human-like content, allowing cognitive tutoring frameworks that can respond to the requirements of learners in real-time. These statistics recommend that such frameworks, which are driven by AI, can improve the efficiency of learning as well as engagement when they are incorporated into pedagogy in a proper manner (Singh et al., 2023; García-López & Trujillo-Liñán, 2025). Nevertheless, along with these advantages, there are rising problems like risks and trust while implementing GPT-style mechanisms in educational environments. A review of literature indicates that generative AI causes risks with regard to integrity in educational settings, combined with the possibility of inappropriate utilisation during examinations and the potential to create outcomes generated by AI, reducing trust in educational environments (Kasneci et al., 2023; Lee et al., 2024). Many educationalists have stressed that inappropriate utilisation of LLMs can cause superficial learning, decreasing the potential of critical questioning and leading to cognitive reliance amongst university students (Lee et al., 2024; Chen, 2024). In addition to that, there are issues like misinformation, bias, and ethical problems. One major problem is the privacy of a student regarding their student data, and hence there is a need for a more responsible employment of AI in educational settings (Zhui et al., 2024; Yan et al., 2024).

In parallel to these risk issues, fostering LLMs and bringing them into use heavily relies on trust. Statistical research denotes that trust is impacted by utilising factors like accuracy of data, relevant content, safety with respect to privacy, and delivery of content that is non-malicious. Along with that, trust also relies on certain rules formed by universities and the guidance offered to faculty as well as students (Batista et al., 2024; Đerić et al., 2025). It is significant for educators as well as beginners to comprehend the balance in trusting AI frameworks, as it may result in over-reliance on such frameworks or lead to not fostering an advantageous technology for the long run.

Given the benefits of GPT-style frameworks with regard to e-learning, a detailed introspection of every risk and trust indicator is significant. This research aims to offer a detailed scrutiny of the way in which these frameworks can be beneficially incorporated into e-learning mechanisms in such a way that they are accountable whilst also protecting the learner's as well as the educator's trust.

Key Contributions

- This paper offers a systematic architecture that together evaluates risk as well as considers fostering GPT-style frameworks in e-learning mechanisms, alleviating a significant gap in current generative AI, which frequently considers those dimensions in an independent manner.
- A statistical analysis is implemented on a dataset consisting of survey responses from large-scale consumers as well as structured e-learning studies, enabling both subjective assessment of trust as well as objective assessment of risks in many learning environments.
- The research quantitatively explores the interaction between risks and trust through statistical indicators as well as regression analysis, offering valuable information on the efficiency of explainability, issues of privacy, user benefits, and risk factors that have an impact on learners' trust.
- A demonstrated risk–trust mechanism incorporating explainability mechanisms as well as HITL validation is presented, showing advanced trust ranges and decreased risk impact in GPT-based e-learning deployments.

The remaining sections of the paper are structured in the following way. Section 2 offers a comprehensive outline of trending literature in relation to GPT-style frameworks, risk indicators, and trust concerns in e-learning frameworks. Section 3 explains the presented methodological architecture, which includes the framework of the device, the algorithm of the overall methodology, and a mathematical demonstration. Section 4 offers an overview of the experimental results, features of the dataset utilised, and evaluation metrics. Section 5 offers an overall conclusion of the research by summarizing significant insights and underlining the scope for future research.

2 Literature Review

Recent literature reviews on generative AI as well as GPT-style frameworks in educational environments underline that it increases the opportunity to enhance learning and teaching, but at the same time, there are concerning issues like risks and trust that demand responsible fostering of these frameworks (Rajendran & Vij, 2025). A structured evaluation of tutoring mechanisms through generative AI suggests that AI features can improve creativity as well as independent learning, whilst also assisting in creating mechanisms to reframe curriculum and assessment methods to protect against inaccurate or misused data (Kazimova et al., 2025). Statistical studies indicate that recommendations from educationalists and popularity amongst them create a trust in utilising the features of AI, such as ChatGPT, and significantly have an impact on their deployment in educational institutions, as trust is a crucial indicator of determining its benefits and readiness to incorporate them in such institutions (Amin et al., 2025). Similar to that, trust gained by educationalists does not only depend on their personal choices, but also on the support they gain from institutions, their policy frameworks, as well as ethical concerns. This shows that there is complexity involved in trusting generative AI and relies on indicators that are based on technical and social aspects and not just on the performance of the framework (Ogalo & Mtenzi, 2025).

In addition to this, studies have included verified mechanisms to assess the trust of a student and their reliance on the usage of AI in Education, indicating that there are numerous factors of trust that revolve around the benefits and readiness of fostering AI frameworks (Ittefaq et al., 2025).

Research targeted at newbies' behavioural responses suggests that trust interacts with reliance and resistance behaviours, which in turn affect real AI utilization and self-directed learning consequences

(Alotaibi, 2025). Systematic opinions further become aware of ethical and regulatory challenges, including equity, duty, bias, and statistical privacy, that have to be addressed to ensure accountable and equitable integration of generative AI in training (Poroohan & Reshadatjoo, 2019; García-López & Trujillo-Liñán, 2025).

There have been other studies that support these claims, which assess the fostering of Generative AI in educational institutions, and they underline the importance of connecting trending AI features with current academic procedures and governance frameworks to reduce risks in authenticity and aid in promoting transparency (Jin et al., 2025). Statistical studies of educationalists, students, as well as researchers indicate that the amount of trust in the accuracy of data, zero maliciousness, and protection of privacy are influenced by the purpose of organisations to foster them, indicating the requirement for trustworthy mechanisms in educational environments (Samala et al., 2025). Experiments with regard to feedback show that students tend to trust feedback acquired by a combination of both human and AI instead of entirely relying on AI feedback. This indicates the complexity of trust in educational settings and relies on the method in which utilization of AI is carried out (Swist et al., 2024). In conclusion, simulation frameworks and structured data review indicate that student's behaviour and their perception about generative AI play a much higher role in determining the outcomes of learning than a mere indicator of trust. This offers an insight into the significance of the perception of generative AI and its role in academic goals (Girón et al., 2024).

Inference

Overall, these studies over the past years present to us the detailed insights about risks, trust, and effectiveness while fostering GPT-style frameworks in e-learning. Trust and perception amongst users have a major impact on adopting these frameworks (Amin et al., 2025; Ittefaq et al., 2025), and ethical issues, institutional guidelines, as well as data privacy influence the overall benefits of such frameworks (Ogalo & Mtenzi, 2025; García-López & Trujillo-Liñán, 2025). These studies enhance the requirement for a structured trust-risk mechanism that holds responsibility for social, technical, and tutoring aspects, thus forming the foundation of the approach of this research.

3 Methodology

This section details the flow of methodology along with the analysis of trust as well as risk in relation to the utilization of GPT-style frameworks in e-learning. This approach incorporates statistical data, regulated by experimental evaluation, as well as the development of the framework, in order to ensure robust analysis and practicality of the framework.

3.1 Overall Methodological Flow and Architecture Description

The presented approach follows an architectural, multi-degree procedure as depicted in Figure 1, and it indicates the entirety of the framework's pipeline. The approach starts by defining the identification of trust as well as risk indicators in GPT-style frameworks utilised in e-learning mechanisms. Two methods of statistical analysis were conducted: a detailed consumer survey of educationalists as well as students, and assessments carried out via simulated interactions in e-learning settings. These two experiments combine into an integrated assessment layer, in which primary utilities of GPT are evaluated in all three procedures, especially content generation, feedback through automation, and adaptive teaching methods.

The outputs obtained via these assessment procedures can have an impact directly due to the level of trust and risk scrutiny. Hence, empirical approaches that constitute regression and correlation are used to indicate relationships among trust and risk elements. On the basis of statistical impacts, a structured framework for risk-trust evaluation is employed, including suggestions for mitigation, validation frameworks, and control mechanisms for deploying a GPT-style Framework that is accountable and efficient in nature. Figure 1 depicts the end-to-end procedure, entirely demonstrating the transformation from data to architecture enhancement.

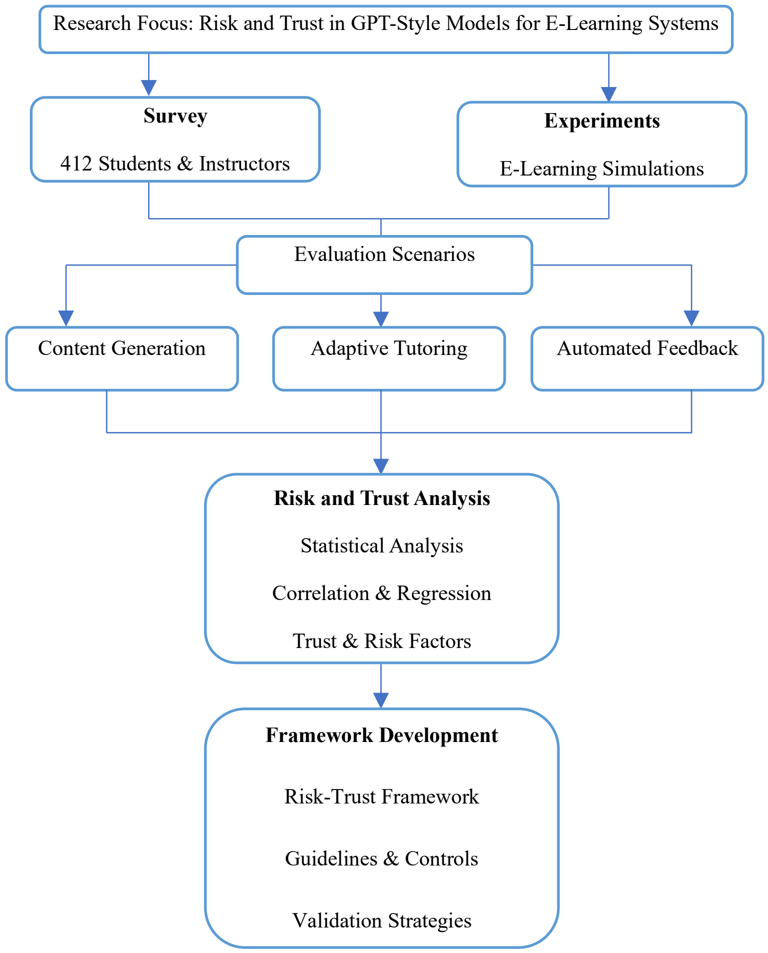

Figure 1: Methodological framework for risk and trust evaluation in GPT-based e-learning systems

3.2 Algorithmic Workflow for Risk–Trust Evaluation

To demonstrate the flow of methodology, an algorithm is depicted to assess the trust and risk involved in various e-learning settings using GPT-style frameworks

Algorithm 1: Risk–Trust Evaluation Workflow for GPT-Based E-Learning Systems

Input:

$S = \{s_1, s_2, \dots s_n\}$: Survey responses

$L = \{l_1, l_2, \dots l_m\}$: Interaction logs from e-learning scenarios

$G = \{g_1, g_2, \dots g_m\}$: GPT outputs for generation, tutoring, and feedback

Output:

T: Quantified trust scores

R: Identified risk indicators

F: Validated risk–trust framework for e-learning deployment

Pseudocode:

Initialize survey dataset S and experimental interaction data L

Preprocess responses to eliminate inconsistencies and incomplete records

Execute GPT-based tasks $g_i \epsilon\ G$ for content generation, adaptive tutoring, and automated feedback

For each interaction instance k do

Measure trust-related factors T and risk indicators R_k

End for

Implement statistical correlation as well as regression scrutiny on gathered metrics

Aggregate results for acquiring dominant trust as well as risk patterns

Develop and authenticate an organised risk–trust framework F

Return finalized framework F as well as evaluation outputs.

Algorithm 1 incorporated the data of perception of humans and observation of systems to assess the risks in GPT-style e-learning settings. Data related to surveys show subjective indicators in addition to perceived benefits, dependency, and transparency, despite the fact that experimental observations provide objective proof in relation to the overall occurrence of errors as well as the consistency in performance. By scrutinizing these datasets, the algorithm makes sure that trust is not evaluated in separating itself from risks. The iterative analytical procedure permits major influencing elements to present themselves, forming the basis for the very last risk–trust framework that helps knowledgeable and managed fostering of GPT-style models in instructional structures.

3.3 Mathematical Description of the Methodology

To quantitatively represent trust and risk relationships, three mathematical formulations are defined. First, the overall user trust score is modelled as a weighted aggregation of individual trust factors, as shown in Equation (1).

$$T = \sum_{i=1}^{n} w_i . f_i \quad (1)$$

Where f_i represents individual trust factors such as perceived usefulness and explainability, and w_i denotes their corresponding weights.

Second, the perceived risk score is expressed as a composite function of multiple risk indicators, including data privacy concerns, bias, and inaccuracy frequency, as defined in Equation (2).

$$R = \frac{1}{m} \sum_{j=1}^{m} r_j \quad (2)$$

Where r_j represents individual risk indicators contributing to the overall risk perception.

Finally, the relationship between trust and risk is modelled using a linear regression formulation to quantify their interaction within the e-learning context, as shown in Equation (3).

$$T = \alpha - \beta R + \epsilon \tag{3}$$

Where α is a constant term, β represents the influence of risk on trust, and ϵ denotes the residual error

4 Results and Discussion

This segment gives the experimental evaluation of the proposed risk– trust evaluation framework for GPT-style models in e-learning structures. The outputs are discussed in terms of executional procedure, characteristics of the dataset, initialization of parameters, performance assessment with the use of more than one metric, and ablation analysis to evaluate the effectiveness of the presented method.

4.1 Software and Implementation Details

The execution of the presented architecture altered the utilization of Python-based statistics analysis and machine learning. Preprocessing of survey data, statistical assessment, and regression modeling were executed along with the usage of Python libraries such as NumPy, Pandas, and Scikit-learn. Experimental interaction details acquired from the e-learning simulation environment have been processed utilising Python scripts. The depiction of overall performance was aided by Matplotlib for producing analytical plots. All the experiments were executed on a device with an Intel i7 processor, 16 GB RAM, and an operating system of Windows 11. This software program configuration ensured consistent implementation and reproducibility of results across all evaluation situations.

4.2 Dataset Description

A structured dataset, which includes survey responses as well as experimental information acquired from GPT-enabled e-learning, was utilized. The dataset details are summarized in Table 1.

Table 1: Dataset characteristics used for experimental evaluation

Dataset Component	Size	Source	Key Features
Survey Dataset	412 samples	Students & instructors	Trust perception, usability, privacy concern, explainability
Experimental Logs	1,236 interactions	E-learning simulations	Response accuracy, latency, feedback quality, error frequency
Scenario Labels	3 categories	Derived	Content generation, adaptive tutoring, automated feedback

The dataset integrates subjective user perceptions with objective system behaviour, enabling a holistic risk–trust assessment.

4.3 Parameter Initialization

Various parameters have been incorporated to standardize the overall experimental evaluation. An initialisation of trust indicators has been carried out to avert bias in the entire assessment and later make use of regression coefficients. Normalisation of risk indicators was scaled as [0,1] to permit comparison amongst different indicators, which have risk of privacy as well as frequency of inaccuracy. The threshold of trust for the acquired outputs within the HITL layer became 0.75, balancing automation performance as well as reliability.

4.4 Performance Metrics and Formulae

The performance of the presented architecture was assessed by making use of various metrics. Two crucial metrics utilized in comparative scrutiny are shown in equations 4 and 5.

Equation (4): Trust Score (TS)

$$TS = \frac{1}{n}\sum_{i=1}^{n} f_i \tag{4}$$

Equation (5): Risk Impact Score (RIS):

$$RIS = \frac{\sum_{j=1}^{m} r_j}{m} \tag{5}$$

These metrics denote overall levels of trust and total risk impact, respectively, and are used throughout the experimental assessment.

4.5 Performance Comparison

The comparative performance of GPT-based e-learning mechanisms across assessment scenarios is depicted in Table 2.

Table 2: Performance comparison across evaluation scenarios

Scenario	Trust Score	Risk Impact Score	Accuracy (%)	Response Time (s)	User Satisfaction (%)
Content Generation	0.81	0.29	86.4	1.8	84.7
Adaptive Tutoring	0.85	0.24	89.2	2.1	88.9
Automated Feedback	0.78	0.33	82.5	1.5	80.3

4.6 Graphical Performance Evaluation

To denote the experimental outputs, two trends of representative performance are scrutinised by making use of graphs obtained through the tabulated data.

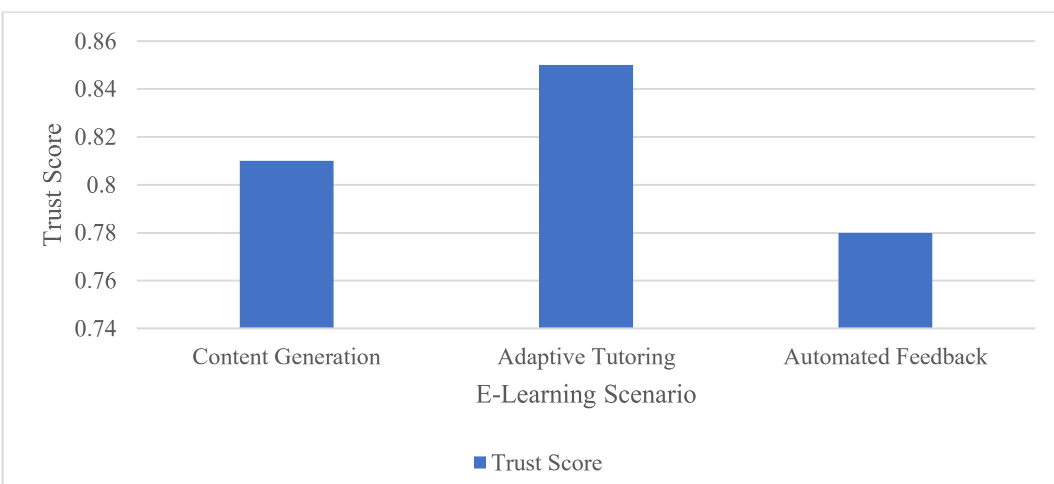

Figure 2: Trust score comparison across GPT-based e-learning scenarios

Figure 2 underlines that adaptive tutoring achieves larger trust tiers in a consistent manner in comparison to content generation as well as automated feedback, showing that consumers trust GPT outputs more when its responses are interactive.

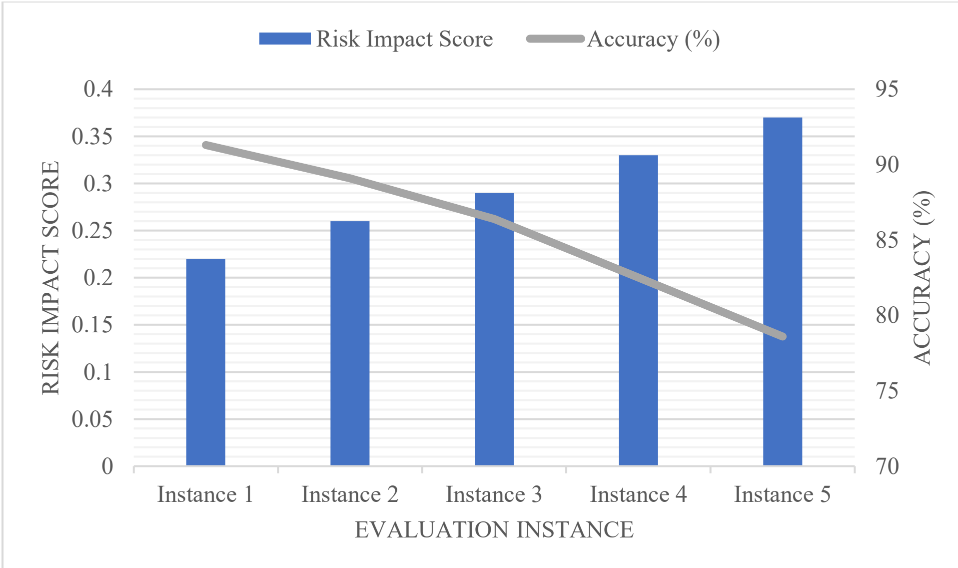

Figure 3: Relationship between risk impact score and response accuracy

Figure 3 shows an inverse relationship between perceived risk and response accuracy, indicating that higher risk indicators decrease the dependency of systems on significant learning functionalities.

4.7 Ablation Study

An ablation study was carried out to assess the role of important functionalities of the framework. When the explainability module was removed, the overall trust score decreased by 12% approximately. Similarly, disabling the HITL authentication caused a 15% increase in the risk impact score, especially due to inaccurate content material in automated feedback scenarios. These effects verify that every module plays an important role in maintaining balanced trust and managing risk within the system.

Discussion

The results acquired through the experiment divulged that GPT-style models can efficiently aid in e-learning when risk and trust are properly assessed. Amongst the evaluated scenarios, adaptive tutoring indicated the best rating in trust and response accuracy, indicating that contextual, interactive AI results in robust learner trust. This study indicates that trust is not entirely dependent on accuracy of output, but additionally by relevance of content and continuity of AI responses in the learning system. In assessment, computerized feedback showed comparatively better risk impact scores, underlining learner sensitivity to false responses and decreased transparency in evaluation-related outcomes

The inverse relationship of risk impact rankings and accuracy similarly shows the significance of risk mitigation mechanisms educational institutions that use AI. As risk indicators like bias as well as an increase in the uncertainty of generated contents, overall functionality of the system and learner trust lower correspondingly. The ablation study assesses this by demonstrating a measurable reduction in trust when explainability elements are removed and am increase in risk when HITL evaluation is inhibited. These results demonstrate that architectural components structured to improve transparency as well as oversight should not be considered as optional elements. Instead, they must be considered as significant components for trustworthy GPT-based learning mechanisms.

Overall, the findings suggest that fostering GPT-style frameworks in a sustainable manner in e-learning relies on regulating a proper stability between automation functionalities as well as governance controls. While the models demonstrate effective ability in enhancing learning as well as personalization, improper deployment result in significant risks which can pose a threat to academic integrity. The presented risk – trust framework addresses this issue by incorporating architectural, analytical as well as procedural protection, thereby enabling responsible utilisation of generative AI while maintaining trust, responsibility as well as learning ability.

5 Conclusion and Future Work

This study presented an entire scrutiny of risk as well as trust in relation with using GPT- style frameworks in e-learning mechanisms, incorporating statistical data of surveys as well as regulated experimental reviews. The findings divulge that e-learning mechanisms enabled by GPT can offer wide range of advantages regarding performance, flexibility, as well as learner outcomes while aided by risk–trust assessment mechanisms. Statistical analysis of data gathered from 412 students as well as instructors found out strong inherent consistency in trust-associated functions, and regression results confirmed that perceived usefulness as well as explainability are extensively advantageous predictors of trust, while concerns regarding privacy of data and inaccuracy risks tend to have negative outcomes. Experimental assessment across content generation, adaptive tutoring, as well as automated feedback further assessed these observations. Adaptive tutoring had the highest trust rating (0.85) and response accuracy (89.2%), indicating that interactive as well as context-aware use-cases are better aligned with learner expectations.

In the evaluation, automated feedbacks showed a higher risk impact rating (0.33) and lower accuracy, underlining its vulnerability in evaluation-intensive situation. The acquired inverse relationship among risk impact scores as well as accuracy depicts the significance of reducing risk factors to maintain overall performance as well as user trust. In addition to this, outcomes in the ablation study showed that removing explainability reduced overall trust by approximately 12%, whereas removing HITL validation increased the impact of risk by nearly 15%, underlining the crucial role of these components. Future studies can extend these innovations by means of incorporating longitudinal research to assess the evolution of trust in the upcoming years, comparing learning outcomes that are domain-specific, and exploring adaptive trust and risk elements by using advanced learning models. Further investigation into regulatory compliance and cross-cultural trust perceptions will also be valuable for large-scale adoption of generative AI in international e-learning environments.

References

[1] Alotaibi, S. M. F. (2025). Determinants of Generative Artificial Intelligence (GenAI) adoption among university students and its impact on academic performance: the mediating role of trust in technology. *Interactive Learning Environments*, 1-30. https://doi.org/10.1080/10494820.2025.2492785

[2] Amin, M. A., Kim, Y. S., & Noh, M. (2025). Unveiling the drivers of ChatGPT utilization in higher education sectors: The direct role of perceived knowledge and the mediating role of trust in ChatGPT. *Education and Information Technologies*, *30*(6), 7265-7291. https://doi.org/10.1007/s10639-024-13095-y

[3] Batista, J., Mesquita, A., & Carnaz, G. (2024). Generative AI and higher education: Trends, challenges, and future directions from a systematic literature review. *Information*, *15*(11), 676. https://doi.org/10.3390/info15110676
[4] Chen, H. (2024). The ethical challenges of educational artificial intelligence and coping measures: A discussion in the context of the 2024 World Digital Education Conference. *Science Insights Education Frontiers*, *20*(2), 3263-3281. https://doi.org/10.15354/sief.24.re339
[5] Đerić, E., Frank, D., & Milković, M. (2025). Trust in generative AI tools: A comparative study of higher education students, teachers, and researchers. *Information*, *16*(7), 622. https://doi.org/10.3390/info16070622
[6] García-López, I. M., & Trujillo-Liñán, L. (2025). Generative Artificial Intelligence in Education: Ethical Challenges, Regulatory Frameworks and Educational Quality in a Systematic Review of the Literature. In *Frontiers in Education* (Vol. 10, p. 1565938). Frontiers. https://doi.org/10.3389/feduc.2025.1565938
[7] García-López, I. M., & Trujillo-Liñán, L. (2025, September). Correction: Ethical and regulatory challenges of Generative AI in Education: a systematic review. In *Frontiers in Education* (Vol. 10, p. 1681252). Frontiers. https://doi.org/10.3389/feduc.2025.1681252
[8] Girón, D. C. A., Rodriguez, W. J. M., Rosas, J. S., Cisneros, E. C., Ramirez, E. T. S., Rojas, M. Z., ... & Torres, H. O. V. (2024). Generative artificial intelligence in higher education learning: A review based on academic databases. *Iberoamerican Journal of Science Measurement and Communication*, *4*(1), 1-16. https://doi.org/10.47909/ijsmc.101
[9] Ittefaq, M., Zain, A., Arif, R., Ahmad, T., Khan, L., & Seo, H. (2025). Factors influencing international students' adoption of generative artificial intelligence: The mediating role of perceived values and attitudes. *Journal of International Students*, *15*(7), 127-154. https://doi.org/10.32674/fnwdpn48
[10] Jin, Y., Yan, L., Echeverria, V., Gašević, D., & Martinez-Maldonado, R. (2025). Generative AI in higher Education: A global perspective of institutional adoption policies and guidelines. *Computers and Education: Artificial Intelligence*, *8*, 100348. https://doi.org/10.1016/j.caeai.2024.100348
[11] Kasneci, E., Seßler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., ... & Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. *Learning and individual differences*, *103*, 102274. https://doi.org/10.1016/j.lindif.2023.102274
[12] Kazimova, D., Tazhigulova, G., Shraimanova, G., Zatyneyko, A., & Sharzadin, A. (2025). Transforming University Education with AI: A Systematic Review of Technologies, Applications, and Implications. *International Journal of Engineering Pedagogy*, *15*(1).
[13] Lee, D., Arnold, M., Srivastava, A., Plastow, K., Strelan, P., Ploeckl, F., ... & Palmer, E. (2024). The impact of generative AI on higher education learning and teaching: A study of educators' perspectives. *Computers and Education: Artificial Intelligence*, *6*, 100221. https://doi.org/10.1016/j.caeai.2024.100221
[14] Lee, J., Hicke, Y., Yu, R., Brooks, C., & Kizilcec, R. F. (2024). The life cycle of large language models in Education: A framework for understanding sources of bias. *British Journal of Educational Technology, 55*(5), 1982-2002. https://doi.org/10.1111/bjet.13505
[15] Ogalo, E. O., & Mtenzi, F. (2025). Leveraging Artificial Intelligence Tools for Learning: Academic Integrity and Ethics in Higher Education in Kenya. In *Artificial Intelligence, Digital Learning, and Leadership: Redefining Higher Education* (pp. 1-36). IGI Global. https://doi.org/10.4018/979-8-3373-0025-2.ch001
[16] Poroohan, R., & Reshadatjoo, H. (2019). Determining the Contribution of Factors Affecting Faculties' Satisfaction with E-learning in Islamic Azad University-Virtual Branch. *International Academic Journal of Organizational Behavior and Human Resource Management*, *6*(1), 24-31. https://doi.org/10.9756/IAJOBHRM/V6I1/1910002

[17] Rajendran, M., & Vij, P. (2025, August). Covert Text Communication Using GPT-Based Language Models and Semantic Similarity Constraints. In *2025 International Conference on Next Generation Computing Systems (ICNGCS)* (pp. 1-7). IEEE. https://doi.org/10.1109/ICNGCS64900.2025.11183393

[18] Samala, A. D., Rawas, S., Wang, T., Reed, J. M., Kim, J., Howard, N. J., & Ertz, M. (2025). Unveiling the landscape of generative artificial intelligence in Education: a comprehensive taxonomy of applications, challenges, and future prospects. *Education and Information Technologies*, *30*(3), 3239-3278. https://doi.org/10.1016/j.caeai.2024.100348

[19] Singh, H., Tayarani-Najaran, M. H., & Yaqoob, M. (2023). Exploring computer science students' perception of ChatGPT in higher Education: A descriptive and correlation study. *Education Sciences*, *13*(9), 924. https://doi.org/10.3390/educsci13090924

[20] Swist, T., Buckingham Shum, S., & Gulson, K. N. (2024). Co-producing AIED ethics under lockdown: An empirical study of deliberative democracy in action. *International Journal of Artificial Intelligence in Education*, *34*(3), 670-705. https://doi.org/10.1007/s40593-023-00380-z

[21] Yan, L., Sha, L., Zhao, L., Li, Y., Martinez-Maldonado, R., Chen, G., ... & Gašević, D. (2024). Practical and ethical challenges of large language models in Education: A systematic scoping review. *British Journal of Educational Technology*, *55*(1), 90-112. https://doi.org/10.1111/bjet.13370

[22] Zhui, L., Fenghe, L., Xuehu, W., Qining, F., & Wei, R. (2024). Ethical considerations and fundamental principles of large language models in medical Education. *Journal of Medical Internet Research*, *26*, e60083. https://doi.org/10.2196/60083

Authors Biography

María Fernanda Moya Puente PhD candidate in Public and Private Planning, Master's degree in Business Administration with a specialization in Marketing and Human Resources. Full Professor at the University of Guayaquil, Marketing Degree Program Manager.

Augusto Oswaldo Benavides Medina Doctor of Administration, Master of Economics with a specialization in business management, Certified Public Accountant, Dean of the Faculty of Economic Sciences at the National University of Tumbes, Senior Lecturer at the School of Administration.

Eddy Miguel Aguirre Reyes Doctor in Educational Administration. Master's degree in Education with a specialization in Teaching and Educational Management and Master's degree in Public Management.

Carlos Alberto Lamadrid Vela Master's degree in Business Administration and Management, PhD candidate in Public and Private Planning, with over 23 years of work experience in the Peruvian financial system, business consultant, university professor.

Jimmy Frank Silva Urcia Doctor in Public Management and Governance, Master's Degree in Public Management. University professor at the undergraduate and graduate levels. Specialist in Government Contracting and Procurement and Compliance Officer for Management Systems.

José Daniel Montano Amador Master's degree in Public Management. Experience in private companies and public administration, served as Director of the Legal Advisory Office of the Regional Government of Tumbes, and the Legal Advisory Office of the Regional Health Directorate.

Ronald M. Hernández PhD candidate in Education. Master's degree in Education with a specialization in Computer Science and Educational Technology. Experience in innovation, educational quality, and the strategic use of ICT applied to research. Continuous training in bibliometrics, evaluation, and scientific writing.