Generative AI Adoption in Higher Education: Examining Faculty Readiness, Trust and Institutional Support

Shakhnoza Norkulova
Department of Uzbek Language and Literature, Termez University of Economics and Service, Termez, Uzbekistan.
Email: shaxnoza_norkulova@tues.uz
ORCID: 0009-0008-7546-7613

Otaxanova Umida
Teacher of Finance
Alfraganus University
Tashkent, Uzbekistan
Email: u.otaxanova@afu.uz
ORCID: 0009-0001-1456-7169

Rajabov Khabibullo
DSc, Associate Professor in the Department of Social Sciences
Tashkent State Transport University
Temiryolchilar Str., Tashkent, 100167, Uzbekistan. Telefon; +99871 299-02-36
ORCID: 0009-0009-6698-1589
Email: rajabov_x@tstu.uz

Abstract

Generative artificial intelligence (GenAI) is reshaping higher education, yet sustainable adoption depends on more than access to tools. This study develops an integrated framework explaining how faculty readiness, trust in AI systems, institutional support, perceived usefulness, and perceived risk jointly influence faculty intention to adopt GenAI in teaching and academic work. Drawing on technology acceptance, organizational support, trust calibration, and AI literacy research, the paper specifies a cross-sectional survey design and a structural model suitable for empirical validation. To demonstrate the analysis pipeline without misrepresenting uncollected evidence, a fully disclosed synthetic dataset of 300 hypothetical faculty responses is used for illustrative tables and charts. Illustrative estimates suggest positive relationships for readiness, trust, and institutional support and a negative association for perceived risk. These numbers are pedagogical examples, not observed effects. The study contributes a reproducible instrument blueprint, construct operationalizations, mediation and moderation hypotheses, an ethics

protocol, and actionable institutional recommendations. Empirical data collection and preregistered testing are necessary before any causal or generalizable claims can be made.

Keywords: generative artificial intelligence; faculty readiness; trust; institutional support; higher education; technology acceptance; AI literacy; structural equation modeling

DOI: 10.21590/ijhit.05.04.27

1. Introduction

Generative artificial intelligence has moved from a specialist research topic to an everyday academic resource. Conversational models, code assistants, image generators, and document tools can support lesson planning, formative feedback, research discovery, accessibility, and administrative drafting. Their presence raises an institutional question that is fundamentally social as well as technical: under what conditions do faculty members choose to incorporate these systems into professional practice, and when is such adoption educationally responsible?

Higher education institutions have historically experienced uneven diffusion of educational technology. Investments in learning management systems, virtual laboratories, and online assessment platforms have not automatically produced consistent classroom use. Faculty differ in digital confidence, disciplinary expectations, time availability, professional autonomy, and exposure to training. GenAI intensifies these differences because it can generate fluent but incorrect material, obscure source provenance, reproduce bias, and complicate authorship and assessment. Adoption therefore cannot be interpreted simply as a binary decision to use a tool.

Faculty readiness describes the practical and psychological capacity to engage with GenAI. It includes baseline digital competence, understanding of model limitations, prompt design ability, critical evaluation of outputs, awareness of privacy obligations, and willingness to redesign pedagogical activities. A faculty member may be enthusiastic yet unprepared to validate AI-generated citations or protect student data. Conversely, a technically skilled instructor may decline adoption when benefits are unclear or the governance environment is unstable. Readiness is therefore distinct from behavioral intention and actual use.

Trust is another central determinant. Appropriate trust involves confidence that a system can provide useful assistance within clearly defined boundaries, together with awareness of uncertainty and failure. Excessive trust can encourage unverified outputs and automation bias,

while insufficient trust may prevent faculty from using genuinely beneficial tools. Trust should be calibrated through transparency, verification practices, and experience. In higher education, trust also extends beyond the technology to the institution that selects, licenses, governs, and supports it.

Institutional support provides the enabling conditions for responsible experimentation. Support may include access to approved tools, professional development, clear data protection rules, workload recognition, disciplinary communities of practice, help desks, and transparent assessment policies. Faculty are more likely to experiment when guidance is consistent and when institutional leaders acknowledge the time needed to redesign coursework. Support can also reduce perceived risk by clarifying acceptable uses and providing escalation routes for errors or misconduct.

Existing acceptance theories help explain technology adoption, but GenAI presents distinctive challenges. The technology acceptance model emphasizes usefulness and ease of use; unified acceptance approaches consider social influence and facilitating conditions; trust and risk frameworks foreground uncertainty. A combined model is needed because a faculty member can perceive a tool as useful while distrusting its outputs, or trust its technical performance while lacking permission or resources to deploy it in a course.

This paper focuses on three primary explanatory variables: faculty readiness, trust, and institutional support. Perceived usefulness and perceived risk are incorporated as mechanisms that may transmit or constrain their influence. Adoption intention is the principal outcome; self-reported use is treated as a secondary, behaviorally closer outcome. The study distinguishes pedagogical uses from research and administrative uses because risk, governance, and expected value may differ across tasks.

The research addresses four questions. First, how strongly are readiness, trust, and institutional support associated with adoption intention? Second, does perceived usefulness mediate readiness and trust effects? Third, does institutional support strengthen the readiness-to-intention relationship? Fourth, how do perceived risks and disciplinary differences shape the pattern of associations? These questions guide a survey instrument and an analytical workflow designed for institutional replication.

The proposed design is explanatory but observational. Cross-sectional responses can estimate associations and test consistency with a theory, yet they cannot establish temporal precedence or rule out unobserved confounding. A subsequent longitudinal or intervention study would be needed to evaluate whether training, governance changes, or access programs cause adoption to increase. This distinction matters when translating findings into policy recommendations.

The contribution is methodological as well as substantive. The paper provides explicit constructs, item examples, equations, quality checks, and a stepwise analysis plan. It also demonstrates how numeric reporting should be presented using a synthetic example that is clearly separated from empirical evidence. The resulting framework can help higher education researchers design a defensible faculty study while helping university leaders identify measurable prerequisites for responsible GenAI adoption.

2. Literature Review

Technology acceptance research establishes that perceived usefulness and perceived ease of use are important predictors of technology-related attitudes and intentions (Davis, 1989). Later unified models incorporated facilitating conditions, social influence, and individual differences (Venkatesh et al., 2003). These perspectives remain relevant for GenAI, but educational use involves professional judgment, academic integrity, and obligations to learners that exceed conventional productivity-tool adoption.

Faculty readiness draws on digital competence and self-efficacy. Bandura (1997) characterizes self-efficacy as beliefs about capability to organize and execute actions. For GenAI, capability is multidimensional: faculty must formulate requests, scrutinize generated answers, detect fabricated sources, decide when automation is inappropriate, and communicate transparent use expectations. Readiness may therefore predict adoption directly and indirectly through usefulness judgments.

AI literacy research has emphasized understanding what AI can do, evaluating its outputs, and interacting critically with AI applications. Long and Magerko (2020) proposed competencies that inform AI literacy design. In university contexts, professional learning should move beyond tool demonstrations toward assessment design, disciplinary validation, bias

evaluation, accessibility, and privacy-safe workflows. An instructor who can produce an attractive teaching resource but cannot verify its factual basis is not fully prepared.

Trust in automation has long been understood as a determinant of reliance under uncertainty. Lee and See (2004) argue for appropriate reliance rather than indiscriminate confidence. GenAI complicates trust because polished linguistic presentation can mask errors. Faculty may evaluate reliability through firsthand experience, explanations of model limitations, peer recommendations, institutional endorsement, and the feasibility of human review. Trust is best modeled as a calibrated belief, not an assumption that AI outputs are authoritative.

Perceived risk can counterbalance usefulness. Potential harms include inaccurate explanations, biased feedback, leakage of sensitive student information, intellectual property uncertainty, unequal student access, and reduced authenticity of assessment. UNESCO (2023) recommends human-centered governance and attention to privacy, inclusion, and educational integrity. Risk perceptions are expected to vary by discipline, assessment stakes, and institutional rules.

Organizational support theory suggests that employees respond to the degree to which their institution values contributions and supports well-being (Eisenberger et al., 1986). In a university setting, GenAI support includes more than licensing. Faculty need policy clarity, workload allowances, technical assistance, peer learning opportunities, and recognition that adoption should be critically evaluated rather than mandated. Support can reduce uncertainty and increase the feasibility of experimentation.

Facilitating conditions in unified acceptance models overlap with institutional support but do not fully capture its governance dimension. A campus may provide internet access and software while withholding guidance on permissible student data or authorship disclosure. Consequently, this study measures institutional support through access, training, technical help, policy clarity, and leadership responsiveness. These facets can be analyzed as a composite or as correlated first-order dimensions.

Perceived usefulness concerns anticipated gains in teaching quality, efficiency, feedback timeliness, and research or administrative workflows. Usefulness should be task-specific: a system may help create quiz variants while being unsuitable for grading high-stakes examinations without review. It is also important to distinguish perceived time savings from

verified performance improvements. Faculty self-reports can indicate expectations but cannot substitute for measured student learning outcomes.

Empirical educational discussions have highlighted both opportunities and concerns surrounding large language models. Kasneci et al. (2023) examine implications for learning and teaching, while Tlili et al. (2023) discuss educational applications and challenges of ChatGPT. These works support a balanced conceptual approach but do not imply that the coefficients in the present illustrative analysis have been established by their findings.

An integrated framework is therefore warranted. Readiness should facilitate experimentation and strengthen usefulness perceptions; trust should increase willingness to rely on outputs; institutional support should make responsible use feasible; risk should inhibit intention; and usefulness should connect capability with motivation. Institutional support may also moderate the effect of readiness: skills can be translated into practice more readily when tools, policies, and help are available.

Important gaps remain. Many studies rely on convenience samples, self-reported intention, or single-institution data; construct definitions and tool types vary; and rapid changes in model capability make results time-sensitive. Cross-sectional models are particularly vulnerable to common-method bias and reverse causality. A rigorous study should therefore predefine constructs, report uncertainty, examine alternative models, and separate observed results from illustrative calculations.

3. Research Methodology

3.1 Research design and hypotheses

The proposed study uses an explanatory, cross-sectional faculty survey followed by confirmatory measurement analysis and structural equation modeling. The target population comprises full-time and part-time faculty in accredited higher education institutions. The unit of analysis is the individual faculty member. The protocol should be approved by an appropriate ethics committee before recruitment. The following hypotheses are directional associations, not assertions of causality.

H1: Faculty readiness is positively associated with GenAI adoption intention.

H2: Trust is positively associated with adoption intention.

H3: Institutional support is positively associated with adoption intention.

H4: Perceived risk is negatively associated with adoption intention.

H5: Perceived usefulness mediates the readiness–intention association.

H6: Institutional support positively moderates the readiness–intention association.

3.2 Sampling and recruitment

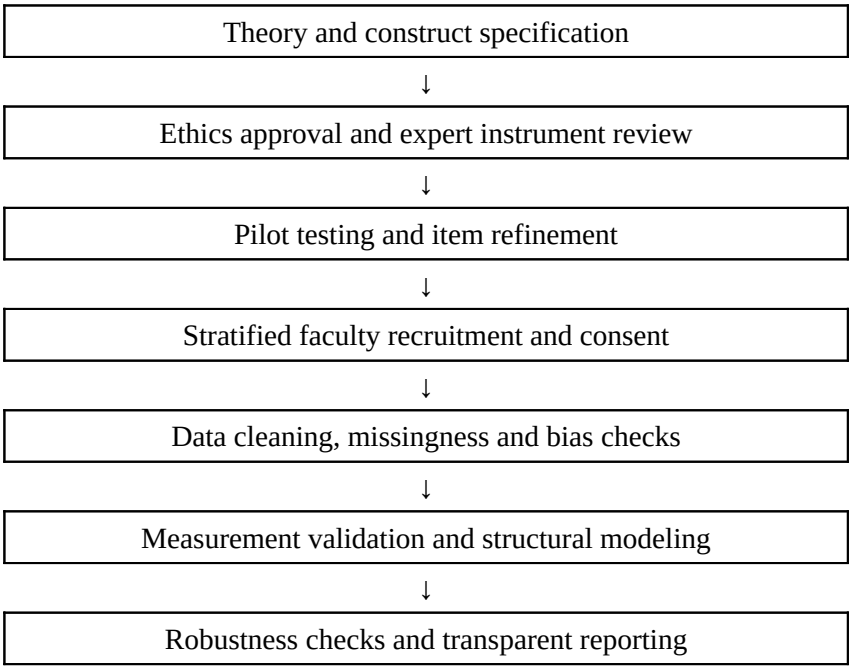
A multi-institution, stratified sampling plan should cover public and private institutions, academic disciplines, faculty ranks, and prior AI-use levels. Invitations should be distributed through neutral institutional channels, with no pressure from supervisors. The planned minimum sample is 300 complete responses, subject to a formal power analysis for the intended model and expected effect sizes. Researchers should record invitations, responses, exclusions, and institutional clusters, and report nonresponse patterns. No faculty participants were recruited for this manuscript; the numeric illustration below uses synthetic observations only.

3.3 Instrument and construct operationalization

Construct	Example survey item (5-point agreement scale)	Items
Readiness	I can critically verify content generated by AI tools.	4
Trust	I can rely on GenAI for appropriate tasks after verification.	4
Institutional support	My institution provides clear GenAI use guidance.	5
Usefulness	GenAI can improve efficiency in my academic tasks.	4
Risk	Using GenAI could expose sensitive academic data.	4
Adoption intention	I intend to use approved GenAI tools in future work.	3

Response anchors range from 1 (strongly disagree) to 5 (strongly agree). Collect background variables including institution type, discipline, years of teaching, academic rank, prior training, and prior use frequency. Use expert review and a pilot study of approximately 20–30 faculty to assess item clarity, content validity, and response burden. Reverse-keyed items should be minimized and documented. Avoid collecting student-identifiable information or actual prompts containing confidential material.

3.4 Conceptual flowchart



3.5 Data screening and scoring

Predefine exclusion rules for duplicate submissions, implausibly fast completion, excessive missingness, and failed attention checks. Inspect item distributions and missing-data mechanisms. When missingness is limited and plausibly missing at random, full-information maximum likelihood or multiple imputation may be considered; complete-case analysis should be compared as a sensitivity check. Compute descriptive construct means only after checking item direction and scale quality.

$$X = (1/k) \sum_{i=1}^{k} x_i$$

Here X is the participant-level construct score, k is the number of valid items in that construct, and x_i is the response to item i. The equation is an editable Word equation object. Report means, standard deviations, observed ranges, and the percentage of missing values for each item.

3.6 Measurement model

A confirmatory factor analysis should establish whether the six theoretical constructs are distinguishable. Standardized loadings should be inspected alongside substantive item content. Composite reliability, Cronbach alpha, and average variance extracted may be reported, but rigid cutoffs should not replace judgment. Discriminant validity can be evaluated using the heterotrait–monotrait ratio and factor correlations.

$$x_i = \lambda_i \eta + \varepsilon_i$$

In this measurement equation, x_i denotes an observed survey indicator, λ_i its factor loading, η the latent construct, and ε_i measurement error. Each construct is estimated using multiple indicators. Model identification, estimator selection for ordinal items, and residual diagnostics must be reported.

$$AVE = (\sum_{i=1}^{k} \lambda_i^2)/k$$

AVE is average variance extracted, λ_i represents standardized loading i, and k is the number of indicators. A high AVE indicates that indicators share substantial variance with their intended latent factor; interpretation also depends on the model and measurement quality.

3.7 Structural model and mediation

$$I = \beta_0 + \beta_1 R + \beta_2 T + \beta_3 S + \beta_4 U + \beta_5 K + \varepsilon$$

I represents adoption intention; R readiness; T trust; S institutional support; U perceived usefulness; K perceived risk; β_0 the intercept; β_1 through β_5 regression paths; and ε residual variation. Positive coefficients are expected for readiness, trust, support, and usefulness; a negative coefficient is expected for risk. Standardize variables for comparable effect sizes and use robust standard errors clustered by institution when appropriate.

$$U = \alpha_0 + \alpha_1 R + \alpha_2 T + \alpha_3 S + \zeta$$

The usefulness model estimates paths from readiness, trust, and support to perceived usefulness. The indirect association from readiness through usefulness equals the product $\alpha_1\beta_4$. Use bootstrap confidence intervals to evaluate uncertainty rather than relying only on normal-theory tests.

$$Indirect\ effect = \alpha_1 \times \beta_4$$

3.8 Moderation, controls, and estimation

$$I = \theta_0 + \theta_1 R + \theta_2 S + \theta_3 (R \times S) + \theta_4 T + \theta_5 U + \theta_6 K + \xi$$

The interaction R × S tests whether institutional support changes the readiness–intention slope. θ_3 is the moderation coefficient, and ξ is residual variation. Center continuous predictors before creating the interaction. Probe estimated slopes at low, average, and high support, and report confidence intervals rather than treating a nominal significance threshold as definitive.

Control variables should be theoretically justified rather than included mechanically. Plausible covariates are academic discipline, institution type, teaching experience, and prior GenAI exposure. Multicollinearity should be assessed using correlations and variance inflation factors. Because the survey is observational, estimated paths are conditional associations and must not be interpreted as intervention effects.

3.9 Validity, bias, and robustness

Procedural remedies for common-method bias include anonymous responses, separating predictor and outcome sections, neutral wording, and clear assurances that responses will not affect employment. Statistical sensitivity analyses can compare the primary model with an alternative factor specification or an unmeasured method-factor model. Measurement invariance should be examined before comparing disciplines or institutional types. Missingness and influential cases should be reported transparently.

Preregister primary hypotheses, construct scoring, exclusions, and analysis choices. Use two-sided confidence intervals and adjust interpretation for multiple exploratory tests. For external validation, collect a later wave of actual usage measures, such as voluntarily reported approved-tool frequency, while avoiding invasive monitoring. Qualitative interviews can explain why faculty perceive specific support or risks.

3.10 Ethical safeguards and reproducibility

Provide a plain-language consent statement, allow withdrawal, minimize personal data, and store deidentified responses in access-controlled repositories. Report the AI systems and versions in use during data collection, since model behavior and campus policies can change rapidly. Release a deidentified codebook, analysis script, and synthetic demonstration data where permissions allow. Any eventual publication must distinguish observed data, simulations, and illustrative numbers.

3.11 Illustrative analysis procedure

The numerical example in Section 4 is deliberately synthetic. It assumes 300 hypothetical observations and prespecified summary statistics to demonstrate a publication-style results layout. The coefficients are illustrative teaching values, not fitted estimates from real faculty responses. Therefore, inferential claims, confidence intervals, p-values, and causal interpretations

are intentionally omitted. A real study would replace the entire section with estimates generated from collected and audited data.

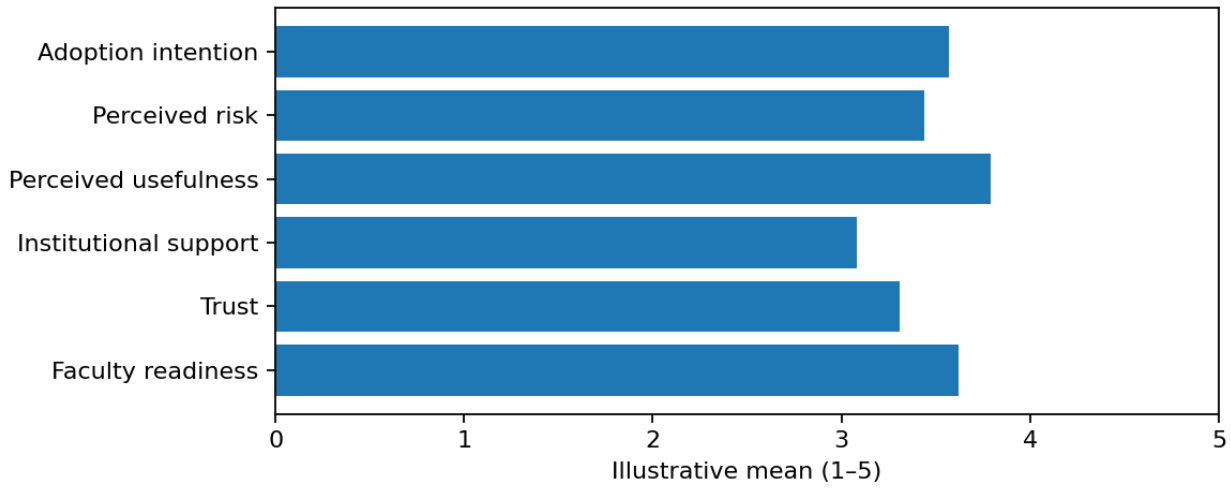
4. Results and Discussion — Synthetic Illustration Only

IMPORTANT: All numbers and graphs in this section are fabricated for methodological illustration, not empirical findings. They must not be represented as evidence about faculty in any institution.

4.1 Hypothetical descriptive statistics

Construct	Hypothetical N	Mean / 5	SD
Faculty readiness	300	3.62	0.71
Trust	300	3.31	0.76
Institutional support	300	3.08	0.84
Perceived usefulness	300	3.79	0.68
Perceived risk	300	3.44	0.73
Adoption intention	300	3.57	0.77

In this illustrative scenario, perceived usefulness is assigned the highest mean (3.79), whereas institutional support has the lowest (3.08). The difference is a designed demonstration of how unmet institutional conditions might coexist with favorable usefulness perceptions; it is not a measured gap. Standard deviations illustrate moderate response dispersion on five-point scales.

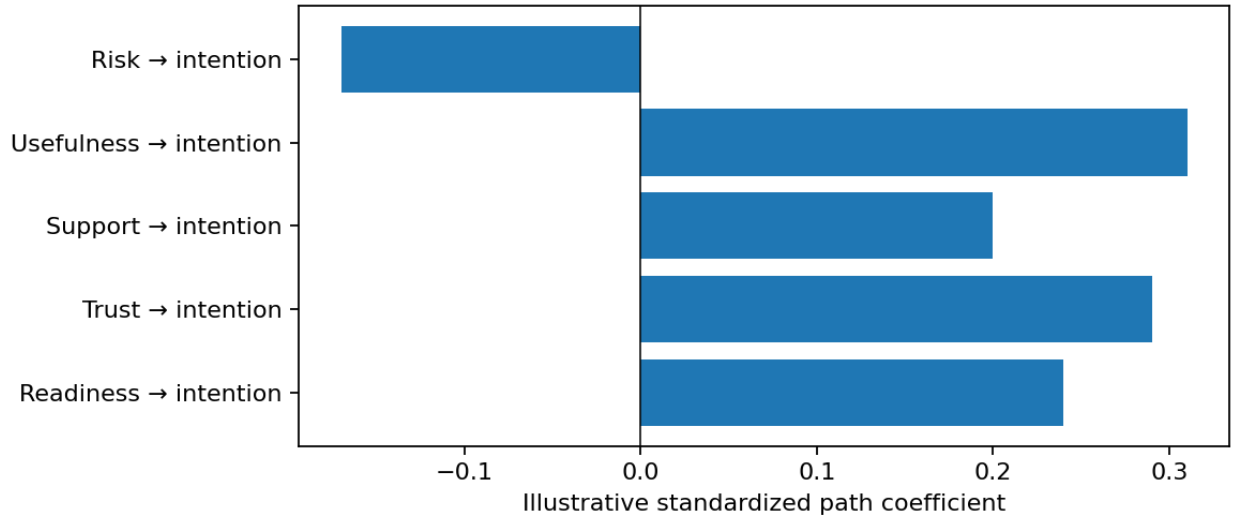


4.2 Hypothetical standardized structural paths

Illustrative relationship	Standardized coefficient	Direction
Readiness → intention	0.24	Positive
Trust → intention	0.29	Positive
Support → intention	0.2	Positive
Usefulness → intention	0.31	Positive
Risk → intention	-0.17	Negative
Readiness → usefulness	0.35	Positive
Readiness × support → intention	0.1	Positive

The example assigns the largest direct coefficient to usefulness (0.31), followed by trust (0.29). Risk is negative (−0.17), indicating how a model could represent reluctance under perceived uncertainty. The interaction value of 0.10 demonstrates the reporting of moderation but should not be read as a statistically supported interaction.

4.3 Hypothetical path comparison



4.4 Illustrative mediation calculation

Assume a hypothetical readiness-to-usefulness path of 0.35 and usefulness-to-intention path of 0.31. Their product is 0.1085. This is an arithmetic illustration of an indirect effect, not a bootstrapped estimate or a statistically demonstrated mediation mechanism.

$$0.35 \times 0.31 = 0.1085$$

4.5 Interpretation and institutional implications

The conceptual pattern suggests that interventions should address skills, trust calibration, and institutional infrastructure together. Training alone may not translate into use when policy is ambiguous or approved tools are unavailable. Similarly, providing software without professional development can produce shallow or unsafe adoption. Institutions should evaluate practical competencies through authentic tasks rather than attendance at a one-off workshop.

Trust should be cultivated through demonstrations of both strengths and failure modes. Faculty can practice checking citations, comparing generated material against primary sources, auditing bias, and documenting human review. Clear boundaries for sensitive data and high-stakes grading are necessary. Institutional guidance should distinguish permitted assistance, prohibited disclosure, and required attribution without assuming that one policy fits every discipline.

A responsible implementation program can combine baseline AI literacy assessment, tiered workshops, access to approved platforms, peer mentors, disciplinary exemplars, and regular policy revision. Monitoring should focus on educational quality, faculty workload, equitable access, and incidents requiring remediation, not merely the count of AI logins. The synthetic example is useful for planning measurement, but it cannot establish which intervention would work.

5. Conclusion

This paper proposes an integrated account of faculty GenAI adoption based on readiness, trust, institutional support, usefulness, and perceived risk. The model treats adoption as a situated professional decision requiring both individual capability and organizational safeguards. It offers a survey blueprint, editable mathematical specifications, a measurement-validation strategy, and a transparent analytic workflow. Its numerical results are explicitly synthetic and do not substantiate claims about real faculty behavior. Future research should collect representative multi-institution data, assess actual rather than solely intended use, test changes over time, and evaluate the effects of training and governance interventions. Responsible institutional adoption requires calibrated trust, critical AI literacy, clear policies, and continuing human accountability.

References

Gupta, N., Jain, A., Vaisla, K. S., Kumar, A., & Kumar, R. (2021). Performance analysis of DSDV and OLSR wireless sensor network routing protocols using FPGA hardware and machine learning. Multimedia Tools and Applications, 80(14), 22301–22319. https://doi.org/10.1007/s11042-021-10820-4

Khan, S. (2022). The use of artificial intelligence in ESG (environmental, social, and governance) investing: A study on AI models for sustainability analytics in asset and wealth management. International Journal of Multidisciplinary and Scientific Emerging Research, 10(1), 431–439. https://doi.org/10.15662/IJMSERH.2022.1001046

Chatrath, A. (2018). The impact of containerization on DevSecOps: Security considerations for Docker, Kubernetes, and microservices architectures in continuous deployment pipelines. International Journal of Advanced Research in Education and Technology, 5(6). https://doi.org/10.15680/IJARETY.2018.0506019

Talasila, D. (2018). Implementation of versioned configuration management in DevSecOps for preventing misconfigurations and ensuring environmental consistency through GitOps automation. International Journal of Innovative Research in Computer and Communication Engineering, 6(2), 1731–1739. https://doi.org/10.15680/IJIRCCE.2018.0602134

Khan, S. (2018). The role of zero-trust models in database security: Eliminating implicit trust and enforcing continuous verification in enterprise data access systems. International Journal of Research in Electronics and Computer Engineering, 6(1), 1622–1628.

Chatrath, A. (2019). DevSecOps in Agile and Lean development: Examining the alignment of security, speed, and scalability in rapid iteration and continuous delivery environments. International Journal of Multidisciplinary and Scientific Emerging Research, 7(3), 1506–1513. https://doi.org/10.15662/IJMSERH.2019.0703046

Devulapalli, N. (2020). The evolution of database security from centralized architectures to distributed cloud-native systems: A comparative and historical perspective. Turkish Online Journal of Qualitative Inquiry, 11(4), 2954–2963. https://doi.org/10.69980/j1064z97

Ahuja, R. (2020). Database security in smart cities: Protecting interconnected infrastructure data, ensuring citizen privacy, and managing large-scale IoT data streams. International Journal of Multidisciplinary and Scientific Emerging Research, 8(1), 410–418. https://doi.org/10.15662/IJMSERH.2020.0801047

Dwivedi, D. (2023). Integration of secure file upload mechanisms in user-facing applications for preventing malware injections and file-based exploits through content-type validation. International Journal on Recent and Innovation Trends in Computing and

Communication, 11(6), 768–775. https://www.ijritcc.org/index.php/ijritcc/article/view/11940

Rangappa, A. S. (2021). Database security in cloud environments: Exploring multi-tenant risks, data isolation challenges, and compliance mechanisms in hybrid and public clouds. International Journal on Recent and Innovation Trends in Computing and Communication, 9(2), 50–57. https://www.ijritcc.org/index.php/ijritcc/article/view/11921

Aggarwal, A. (2018). Application of federated learning in medical IoT devices for preserving patient privacy and preventing data breaches through decentralized cyber defense models. International Journal of Innovative Research in Computer and Communication Engineering, 6(3), 2654–2660. https://doi.org/10.15680/IJIRCCE.2018.0603167

Ghai, D., Gianey, H. K., Jain, A., & Uppal, R. S. (2020). Quantum and dual-tree complex wavelet transform-based image watermarking. International Journal of Modern Physics B, 34(4), Article 2050009. https://doi.org/10.1142/S0217979220500095

Ahuja, R. (2019). A comparative study of traditional DevOps and DevSecOps: Examining the cultural, technical, and organizational shifts required to embed security into software engineering practices. International Journal of Innovative Research in Science, Engineering and Technology, 8(8), 8561–8569. https://doi.org/10.15680/IJIRSET.2019.0808096

Khan, S. (2019). Sales force security compliance: An in-depth study of GDPR, HIPAA, and PCI-DSS enforcement in cloud-based CRM systems and their implications for global enterprises. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 8(9), 2211–2219. https://doi.org/10.15662/IJAREEIE.2019.0809010

Rangappa, A. S. (2020). Integration of behavioral analytics in developer workflows for detecting insider threats and malicious activities through activity monitoring and contextual profiling. International Journal of Innovative Research in Science, Engineering and Technology, 9(1), 13375–13383. https://doi.org/10.15680/IJIRSET.2020.0901064

Dwivedi, D. (2022). Application of AI-powered vulnerability scanners in legacy applications for identifying unpatched security flaws and weak dependencies through semantic code analysis. International Journal on Recent and Innovation Trends in Computing and Communication, 10(12), 617–623. https://www.ijritcc.org/index.php/ijritcc/article/view/11918

Chatrath, A. (2019). A multi-layered DevSecOps framework: Integrating secure coding, automated testing, vulnerability scanning, and incident response into end-to-end software development lifecycles. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 8(3). https://doi.org/10.15662/IJAREEIE.2019.0803102

Kumar, S., Jain, A., Shukla, A. P., Singh, S., Raja, R., Rani, S., Harshitha, G., AlZain, M. A., & Masud, M. (2021). A comparative analysis of machine learning algorithms for detection of organic and nonorganic cotton diseases. Mathematical Problems in Engineering, 2021, Article 1790171. https://doi.org/10.1155/2021/1790171

Bhaskara Raju Rallabandi. (2022). SYNC-ADAPTIVE RESOURCE SCHEDULING IN PRIVATE 5G FOR TIME-CRITICAL APPLICATIONS. International Journal of Data Science and IoT Management System, 1(2), 40–45. https://doi.org/10.64751/ijdim.2022.v1.n2.pp40-45

Jain, J., Jain, A., Srivastava, S. K., Verma, C., Raboaca, M. S., & Illés, Z. (2022). Improved security of e-healthcare images using hybridized robust zero-watermarking and hyper-chaotic system along with RSA. Mathematics, 10(7), Article 1071. https://doi.org/10.3390/math10071071

Bhaskara Raju Rallabandi. (2019). Enhancing 5G NSA Performance with Lightweight Network Data Analytics Loops. International Journal of Engineering Research and Science & Technology, 15(4), 57–61. https://doi.org/10.62643/ijerst.2019.v15.n4.pp57-61

Anchala, S. (2018). Deployment of container image scanning in DevSecOps pipelines for mitigating open-source vulnerabilities and ensuring runtime safety through CVE-based detection mechanisms. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 7(3), 1546–1554. https://doi.org/10.15662/IJAREEIE.2018.0703058

Bhanushali, B. (2019). Graph-based network analysis for identifying complex money laundering typologies, detecting suspicious transaction chains, and tracing illicit financial flows. International Journal of Multidisciplinary and Scientific Emerging Research, 7(4), 2007–2014. https://doi.org/10.15662/IJMSERH.2019.0704047

Talasila, D. (2019). DevSecOps in e-governance platforms: Safeguarding public data, ensuring transparency, and enhancing trust in cloud-based government applications. International Journal of Innovative Research in Science, Engineering and Technology, 8(2), 1561–1570. https://doi.org/10.15680/IJIRSET.2019.0802107

Bhaskara Raju Rallabandi. (2020). PRIVATE 5G SLICING DRIVEN BY INTENT USING MEC AND SD-WAN FOR SUPPORTING MULTITNTARY COMMUNICATIONS. International Journal of Engineering Research and Science & Technology, 16(4), 49–54. https://doi.org/10.62643/ijerst.2020.v16.n4.pp49-54

Jain, A., Kumar, A., & Sharma, S. (2015). Comparative design and analysis of mesh, torus and ring NoC. Procedia Computer Science, 48, 330–337. https://doi.org/10.1016/j.procs.2015.04.190

Ahuja, R. (2020). Adoption of secure API development practices in microservice architectures for preventing unauthorized access and data leakage through OAuth2 and input throttling. Journal of Critical Reviews, 7(9), 4063–4069. https://doi.org/10.69980/jcr.v7:i9.13404

Mahadasu, S. S., & Rallabandi, B. R. (2023). Federated learning for privacy-preserving RAN optimization across multi-site enterprise 5G networks. International Journal of Engineering Science and Advanced Technology, 23(4), 53–57. https://doi.org/10.64771/ijesat.2023.v23.i04.pp3847

Anchala, S. (2019). Database security challenges in cross-border data flows: Analysing compliance, privacy, and risk in international data transfers. International Journal of Advanced Research in Education and Technology, 6(3), 831–838. https://doi.org/10.15680/IJARETY.2019.0603016

Bhanushali, B. (2018). Risk-based approaches in anti-money laundering for balancing regulatory compliance costs and maximizing detection of high-risk financial activities. International Journal of Innovative Research in Computer and Communication Engineering, 6(11), 9006–9014. https://doi.org/10.15680/IJIRCCE.2018.0611081

Talasila, D. (2018). Integration of identity federation in multi-cloud access management for streamlining user authentication and reducing credential sprawl through centralized SSO protocols. International Journal of Multidisciplinary and Scientific Emerging Research, 6(4), 2017–2025. https://doi.org/10.15662/IJMSERH.2018.0604046

Jain, A., Gupta, A., Sengar, A. S., Shukla, R. K., & Jain, A. (2021). Application of deep learning for image sequence classification. In 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART) (pp. 280–284). IEEE. https://doi.org/10.1109/SMART52563.2021.9676200

Chatrath, A. (2020). The role of policy-as-code in DevSecOps: Automating compliance, governance, and risk management in cloud-native and hybrid IT environments. International Journal of Innovative Research in Computer and Communication Engineering, 8(1). https://doi.org/10.15680/IJIRCCE.2020.0801020

Talasila, D. (2018). Utilization of runtime application self-protection (RASP) in production environments for real-time vulnerability mitigation and behavioral enforcement through embedded monitoring agents. International Journal of Advanced Research in Education and Technology, 5(3), 831–840. https://doi.org/10.15680/IJARETY.2018.0503017

Jain, J., & Jain, A. (2022). Securing e-healthcare images using an efficient image encryption model. Scientific Programming, 2022, Article 6438331. https://doi.org/10.1155/2022/6438331

Bhaskara Raju Rallabandi. (2019). Comprehensive Design and Field Performance Assessment of Early 5G NSA Private Networks for Industrial IoT Campuses. International Journal of Engineering Research and Science & Technology, 15(1), 22–26. https://doi.org/10.62643/ijerst.2019.v15.n1.pp22-26

Jain, A., Gahlot, A. K., Dwivedi, R., Kumar, A., & Sharma, S. K. (2018). Fat tree NoC design and synthesis. In R. Singh, S. Choudhury, & A. Gehlot (Eds.), Intelligent communication,

control and devices (Advances in Intelligent Systems and Computing, Vol. 624, pp. 1749–1756). Springer. https://doi.org/10.1007/978-981-10-5903-2_180

Gupta, A. (2021). Application of cyber deception strategies in military networks for enhancing operational security and misleading attackers through adaptive honeypots and decoy systems. NeuroQuantology, 19(4), 317–333. https://doi.org/10.48047/nq.2021.19.4.NQ21068

Jain, A., & Kumar, A. (2021). Desmogging of still smoggy images using a novel channel prior. Journal of Ambient Intelligence and Humanized Computing, 12(1), 1161–1177. https://doi.org/10.1007/s12652-020-02161-1

Ahuja, R. (2023). The role of artificial intelligence and machine learning in DevSecOps: Leveraging predictive analytics, automated threat detection, and anomaly identification for secure software delivery pipelines. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 381–389. https://www.ijritcc.org/index.php/ijritcc/article/view/11946

Aggarwal, A. (2019). Application of secure Virtual Private Cloud (VPC) architectures in public cloud infrastructure for strengthening network isolation and segmenting trust zones through fine-tuned routing. International Journal of Multidisciplinary and Scientific Emerging Research, 7(1), 423–431. https://doi.org/10.15662/IJMSERH.2019.0701048

Bhanushali, B. (2020). Effective sanctions screening and false positive identification. International Journal of Innovative Research in Science, Engineering and Technology, 9(4), 8306–8313. https://doi.org/10.15680/IJIRSET.2020.0904179

Jain, A., Dwivedi, R., Kumar, A., & Sharma, S. (2017). Scalable design and synthesis of 3D mesh network on chip. In R. Singh & S. Choudhury (Eds.), Proceeding of International Conference on Intelligent Communication, Control and Devices (Advances in Intelligent Systems and Computing, Vol. 479, pp. 661–666). Springer. https://doi.org/10.1007/978-981-10-1708-7_75

Aggarwal, A. (2018). Implementation of quantum cryptography in financial transactions for enhancing data confidentiality and resisting future quantum attacks through secure key distribution mechanisms. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 7(7), 3196–3204. https://doi.org/10.15662/IJAREEIE.2018.0707016

Devulapalli, N. (2018). Database security for financial systems: Protecting customer data, ensuring PCI-DSS compliance, and safeguarding against fraud and insider attacks. International Journal of Advanced Research in Education and Technology, 5(5), 838–844. https://doi.org/10.15680/IJARETY.2018.0505018

Gupta, A. (2021). Deployment of advanced endpoint detection in remote work environments for preventing malware intrusions and data exfiltration through behavioral analytics and AI-

driven responses. NeuroQuantology, 19(9), 1206–1224. https://doi.org/10.48047/nq.2021.19.9.NQ21199

Devulapalli, N. (2020). Implementation of compliance-as-code in regulated DevSecOps environments for automating audit readiness and reducing human error through scripted control validation. Journal of Critical Reviews, 7(1), 2651–2657. https://doi.org/10.69980/jcr.v7:i1.13405

Rangappa, A. S. (2018). Deployment of immutable infrastructure in Dev Sec Ops practices for minimizing configuration drift and recovery time through ephemeral build environments. International Journal of Multidisciplinary and Scientific Emerging Research, 6(4), 2026–2034. https://doi.org/10.15662/IJMSERH.2018.0604047

Anchala, S. (2018). Adoption of infrastructure as code security validation in cloud-native environments for reducing configuration drifts and compliance violations through automated template scanning. International Journal of Innovative Research in Science, Engineering and Technology, 7(10), 8305–8313. https://doi.org/10.15680/IJIRSET.2018.0710087

Gupta, A. (2020). Utilization of homomorphic encryption in healthcare data sharing for ensuring confidentiality and compliance through secure computation without data exposure. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 3(10). https://doi.org/10.15680/IJMRSET.2020.0310011

Aggarwal, A. (2018). Implementation of cloud security automation in continuous integration pipelines for accelerating DevSecOps adoption and minimizing manual misconfigurations through security-as-code. International Journal of Innovative Research in Science, Engineering and Technology, 7(11). https://doi.org/10.15680/IJIRSET.2018.0711083

Mahadasu, S. S. (2022). Cross-domain service assurance for private 5G networks using streaming telemetry and dependency-aware event correlation. International Journal of Data Science and IoT Management System, 1(3), 51–56. https://doi.org/10.64751/ijdim.2022.v1.n3.1290

Kumar, A., & Jain, A. (2021). Image smog restoration using oblique gradient profile prior and energy minimization. Frontiers of Computer Science, 15(6), Article 156706. https://doi.org/10.1007/s11704-020-9305-8

Bhanushali, B. (2019). Integration of biometric authentication with AML systems for strengthening know-your-customer (KYC) processes and reducing identity fraud in financial institutions. International Journal of Advanced Research in Education and Technology, 6(5), 853–860. https://doi.org/10.15680/IJARETY.2019.0605019

Jain, A., Dwivedi, R. K., Alshazly, H., Kumar, A., Bourouis, S., & Kaur, M. (2022). Design and simulation of ring network-on-chip for different configured nodes. Computers, Materials & Continua, 71(2), 4085–4100. https://doi.org/10.32604/cmc.2022.023017

Dwivedi, D. (2020). Adoption of secure software updates in application lifecycle for preventing supply chain tampering and maintaining trust through cryptographically signed patches. Journal of Critical Reviews, 7(10), 6974–6980. https://doi.org/10.69980/jcr.v7:i10.13406