ISSN: 2181-3337 | SCIENTISTS.UZ VOLUME 5 ISSUE 7 JULY 2026

ENHANCING DIGITAL COMPETENCE IN NETWORK TECHNOLOGIES EDUCATION THROUGH RULE-BASED ADAPTIVE LEARNING AND WEB-BASED LEARNING ANALYTICS

Yuldashev Shadiyor
Tashkent State University of Economics
shyuldashev@tsue.uz

DOI: 10.67620/sai.57b0014

ABSTRACT

This exploratory quasi-experimental study examined a rule-based adaptive learning and web-based learning analytics framework in a university Network Technologies course. The framework combined diagnostic assessment, structured digital content, virtual network laboratories, automated feedback, activity monitoring, and competency-based evaluation. Over one academic semester, 124 undergraduate students were assigned to a control group and an experimental group of 62 students each. The reported pretest means were comparable (58.6 and 59.0), whereas the posttest means were 71.2 for the control group and 84.1 for the experimental group. The experimental group also showed fewer laboratory errors, shorter task-completion time, more independently completed tasks, and a higher proportion of on-time submissions. These results are interpreted descriptively because participant-level data, dispersion estimates, and validated measurement evidence were not available in the reported dataset. The framework should therefore be regarded as a promising instructional design rather than a validated artificial-intelligence system or a definitive causal intervention. Its practical value lies in linking repeated network practice with transparent, instructor-supervised feedback and early support. Future multisite studies should validate the assessment rubric, document implementation fidelity, and report effect sizes, confidence intervals, and ethical data-governance procedures.

ACCEPTED

02.08.26

Keywords: *digital competence; network technologies; learning analytics; adaptive learning; virtual laboratory; automated feedback; cybersecurity; responsible AI use.*

CC BY

Introduction

Digital competence extends beyond the ability to operate devices. It includes the confident, critical, safe, and responsible use of digital technologies for learning, work, communication, information management, and problem-solving (Vuorikari et al., 2022). In higher education, this competence is increasingly connected with students' capacity to learn independently, evaluate digital information, collaborate in online environments, and transfer technical knowledge to authentic professional tasks. Educators therefore need learning designs that connect knowledge acquisition with practice, reflection, and responsible technology use (Redecker, 2017).

Network Technologies is especially suitable for developing observable forms of digital competence because students must combine conceptual knowledge with configuration, testing, diagnosis, and security decisions. Typical course content includes network architecture, topologies, the OSI and TCP/IP models,

IPv4 and IPv6 addressing, switching, routing, network services, wireless communication, monitoring, virtualization, and cybersecurity (Cisco Networking Academy, 2020). Success in these areas depends not only on knowing terminology but also on identifying faults, testing alternative explanations, and documenting technical choices.

Adaptive educational systems use information about learners' performance or activity to modify content, task difficulty, sequencing, or feedback (Brusilovsky, 2001; Brusilovsky & Millán, 2007). Learning analytics can complement this process by making patterns of engagement, delay, repeated error, and help-seeking more visible to students and instructors (Ferguson, 2012; Ifenthaler & Yau, 2020). However, the educational value of analytics depends on the validity of the indicators, the transparency of decisions, and appropriate safeguards for student data (Pardo & Siemens, 2014; Slade & Prinsloo, 2013).

Artificial intelligence is often used as a broad label for automated educational technology, even when a system relies only on predetermined rules. Reviews of artificial intelligence in higher education have repeatedly called for clearer descriptions of the underlying technology, stronger evaluation designs, and greater educator involvement (Bond et al., 2024; Zawacki-Richter et al., 2019). The present study therefore describes the implemented mechanism as rule-based adaptive learning. It did not train or validate a machine-learning model. The term artificial intelligence is retained only when discussing students' responsible evaluation of AI-generated advice as part of digital competence.

The purpose of the study was to explore whether an integrated web-based framework could support digital competence development more effectively than conventional instruction in a university Network Technologies course. The evaluation focused on reported changes in overall competence scores, practical performance, task completion, independent work, and student perceptions. A second objective was to examine how transparent activity and error indicators could support instructor-supervised identification of students who might need additional assistance.

Methods

Research design and participants

The study used an exploratory quasi-experimental pretest–posttest design over one academic semester. A total of 124 undergraduate students enrolled in a university-level Network Technologies course participated. The control group and experimental group each included 62 students. Because the study record did not document random allocation, the design is treated as quasi-experimental rather than randomized. The control group received conventional instruction, while the experimental group used the web-based framework described below. Demographic covariates, attrition, instructor equivalence, and implementation-fidelity measures were not included in the reported analysis; these omissions are considered in the limitations.

Structure of the web-based framework

The framework integrated six components across the learning cycle: diagnostic assessment, structured content delivery, virtual network laboratories, rule-based adaptation, automated feedback, and instructor-facing learning analytics. The diagnostic component identified initial theoretical and practical readiness. The content component organized resources by module. The practical component enabled students to create, test, and revise network configurations. The analytics component summarized activity and error patterns. The adaptive component selected predefined forms of support or challenge according to recent performance. The evaluation component combined several course indicators into an operational Digital Competence Index.

Course content was divided into ten modules: network fundamentals; the OSI and TCP/IP models; IPv4, IPv6, and subnetting; switching; routing; network services; wireless networking; cybersecurity; monitoring and troubleshooting; and network design. Each module included an introduction, conceptual explanation, visual material, formative questions, a practical task, feedback, and reflection. The final module required students to design and justify a complete network solution.

ISSN: 2181-3337 | SCIENTISTS.UZ

Table 1

Digital Competence Assessment Criteria

No.	Criterion	Main indicators	Weight
1	Theoretical knowledge	Models, protocols, terminology, and standards	15%
2	Network configuration	Correct setup of routers, switches, and services	25%
3	Problem-solving	Detection and correction of network failures	20%
4	Cybersecurity	Secure configuration and risk awareness	15%
5	Independent learning	Task completion with limited support	10%
6	Collaboration	Contribution to group tasks and technical discussion	5%
7	Responsible AI use	Verification and appropriate use of AI-generated output	10%
	Total		**100%**

Operational measures

The Digital Competence Index (DCI) was calculated from seven indicators converted to a 0–100 scale:

$$DCI_i = 0.15K_i + 0.25C_i + 0.20P_i + 0.15S_i + 0.10I_i + 0.05G_i + 0.10A_i$$

where K is theoretical knowledge, C network configuration, P problem-solving, S cybersecurity, I independent learning, G group collaboration, and A responsible AI use. Scores below 56 were categorized as basic, 56–70 as developing, 71–85 as proficient, and above 85 as advanced. These weights and thresholds were operational design choices for this course. They were not derived from psychometric validation and should not be interpreted as universal competence standards.

The platform also generated an activity score from login regularity (L), task completion (T), module engagement (M), deadline compliance (D), and participation in collaborative activities (G):

$$AS_i = 0.20L_i + 0.25T_i + 0.25M_i + 0.15D_i + 0.15G_i$$

The activity score was used as a monitoring indicator rather than a replacement for academic assessment. It helped distinguish, for example, a low-performing but active student from a low-performing student with limited activity and repeated missed deadlines.

Rule-based adaptation and feedback

The adaptive mechanism used predefined decision rules rather than a trained artificial-intelligence model. Recommendations were based on test performance, laboratory performance, error patterns, task-completion time, and requests for assistance. A module score below 60% triggered a concise explanation, visual support, and a simplified laboratory task. Scores from 60% to 79% triggered reinforcement activities at the same level. Scores of 80% or higher triggered a more complex troubleshooting or project-based task. The learner profile was updated after each major task, so students were not permanently assigned to fixed ability groups.

A learning-state score combined theoretical performance (T), practical performance (P), activity (A), and independence (R):

$$LS_i = 0.30T_i + 0.40P_i + 0.15A_i + 0.15R_i$$

ISSN: 2181-3337 | SCIENTISTS.UZ

Practical performance received the largest weight because the course emphasized configuration, testing, and troubleshooting. Feedback was provided in levels: an initial prompt or reminder, a more specific hint, and, when necessary, a complete explanation reviewed by the instructor.

Learning analytics and risk flags

The platform recorded login frequency, time spent on modules, viewed resources, task-completion time, attempts, laboratory errors, hint requests, forum participation, and submission punctuality. The system used these indicators to produce a rule-based risk flag:

$$RS_i = 0.35(1 - Perf_i) + 0.25E_i + 0.20(1 - Act_i) + 0.20D_i$$

where Perf is current performance, E normalized error frequency, Act activity, and D the proportion of delayed tasks. Scores below 0.30 were categorized as low risk, 0.30–0.59 as moderate risk, and 0.60 or higher as high risk. These categories were heuristic alerts, not validated predictions. A high-risk flag prompted instructor review and possible additional practice, a simplified learning path, or individual consultation. The instructor retained responsibility for any intervention.

Statistical analysis

The analysis reported here was limited to descriptive statistics: group means, absolute change, relative change, task-process indicators, and frequency percentages. Relative change was calculated as:

$$\text{Relative change (\%)} = [(\text{posttest} - \text{pretest}) / \text{pretest}] \times 100$$

Participant-level scores, standard deviations, confidence intervals, and the full output required to reproduce an inferential test were not reported in the consolidated results. Accordingly, no causal or statistically significant group difference is claimed in this revised report. The findings should be interpreted as descriptive evidence from a pilot evaluation.

Results

Overall outcomes

The control and experimental groups began with similar reported pretest means of 58.6 and 59.0, respectively. At the end of the semester, the control-group mean was 71.2 and the experimental-group mean was 84.1. This represented an absolute increase of 12.6 points in the control group and 25.1 points in the experimental group. Relative change was 21.5% and 42.5%, respectively. Because measures of dispersion were unavailable, the difference is presented descriptively.

Table 2

Comparison of Main Reported Outcomes

No.	Indicator	Control group	Experimental group
1	Pretest mean score	58.6	59.0
2	Posttest mean score	71.2	84.1
3	Absolute change	12.6	25.1
4	Relative change	21.5%	42.5%
5	Average laboratory errors	4.4	2.2
6	Average task-completion time	45.1 min	35.7 min
7	Independently completed tasks	63.0%	86.2%
8	On-time submissions	68.4%	90.1%
9	Students at the advanced level	11.3%	35.5%
10	Students remaining at the basic level	12.9%	3.2%

ISSN: 2181-3337 | SCIENTISTS.UZ

Note. The table reports aggregate descriptive values. Standard deviations, confidence intervals, and participant-level data were not available for reproducible inferential analysis.

Competence dimensions and process indicators

The largest reported differences were in network configuration and problem-solving. The mean network-configuration score was 86.7 in the experimental group and 69.4 in the control group. The corresponding problem-solving means were 85.2 and 68.8. Cybersecurity scores were 82.9 and 70.3. The experimental group also showed a reported 14.2-point advantage in independent learning, although the two underlying group means were not provided.

Process indicators followed the same descriptive pattern. The experimental group averaged 2.2 laboratory errors compared with 4.4 in the control group, completed tasks in 35.7 minutes compared with 45.1 minutes, and recorded higher percentages of independent completion and on-time submission. These measures suggest more efficient task performance, but the study did not report the distribution of these indicators or whether task difficulty and exposure were equivalent between groups.

Error patterns

The learning-analytics log classified more than 3,000 laboratory events. Common errors involved IP addressing, subnet masks, routing entries, inactive interfaces, VLAN mismatches, and incomplete security settings. The study record reported decreases in the experimental group of 47% for IP-addressing errors, 43% for routing errors, and 39% for security-related errors. Exact baseline and follow-up counts were not supplied, so these values are interpreted as descriptive platform summaries rather than independently reproducible rates.

The framework distinguished isolated errors from repeated patterns. An isolated error triggered a brief reminder, whereas repeated errors triggered additional explanatory material and practice. This distinction was intended to separate occasional inattention from a possible conceptual gap.

Student perceptions

The end-of-semester questionnaire indicated generally positive perceptions. Approximately 91% of respondents reported that the platform made progress easier to follow, about 88% considered the adaptive tasks appropriate for their level, and more than 85% believed that the system increased their independence. Some students expressed concern about the quantity of activity data collected, and some considered the feedback too general. The item wording, response scale, respondent count, and reliability evidence were not included in the reported materials; therefore, these percentages should be treated as indicative rather than as a validated attitude measure.

Discussion

The descriptive outcomes suggest that integrating virtual laboratories, structured feedback, and visible learning indicators may support digital competence development in a practical Network Technologies course. The strongest reported differences concerned configuration, troubleshooting, cybersecurity, independent completion, and task efficiency. These outcomes are educationally plausible because the framework increased opportunities for repeated practice, immediate error information, and differentiated follow-up. Adaptive systems can be useful when they connect learner information to specific instructional actions rather than merely displaying data (Brusilovsky & Millán, 2007; Ifenthaler & Yau, 2020).

The contribution of the framework lies less in technological novelty than in pedagogical integration. Content, practice, feedback, monitoring, and instructor review were placed in one workflow. A student with weak conceptual understanding could receive a different response from a student who understood the concept but made a syntax or configuration error. This distinction is difficult to maintain consistently through manual monitoring in larger classes. Nevertheless, the mechanism remained rule-based. Describing fixed thresholds as artificial intelligence would overstate the technology and make the study difficult to reproduce.

ISSN: 2181-3337 | SCIENTISTS.UZ

The virtual laboratory appears central to the reported pattern. Network education requires students to configure systems, observe consequences, test alternatives, and correct errors. Physical laboratories remain important, but virtual environments can provide additional opportunities to repeat tasks and explore failure conditions without disrupting production equipment. The framework's staged feedback was designed as temporary scaffolding: students first received a prompt, then a more explicit hint, and only later a complete explanation. The reported decrease in errors and increase in independent completion are consistent with that instructional purpose, although the available data do not establish causation.

Learning analytics also created a more detailed view of the learning process. A correct final configuration may conceal many failed attempts or extensive assistance, whereas another student may reach the same result independently. Process indicators can therefore enrich assessment, but they should not be treated as direct measures of competence without validation. Activity can be affected by connectivity, device access, disability, work obligations, and other circumstances. Ethical learning analytics requires proportional data collection, understandable explanations, and meaningful human oversight (Pardo & Siemens, 2014; Sclater, 2016; Slade & Prinsloo, 2013).

Responsible AI use remained relevant as a competence outcome even though the adaptive platform itself was rule-based. Students increasingly encounter generative systems that can produce fluent but inaccurate technical explanations. A competent learner should compare automated advice with documentation, simulation output, and security requirements before applying it. Current guidance on AI in education similarly emphasizes critical evaluation, transparency, and educator responsibility (European Commission, 2022; Holmes et al., 2019).

The findings should be interpreted cautiously. First, the study involved one course in one institutional context and lasted one semester. Second, random assignment, demographic comparability, attrition, instructor equivalence, and implementation fidelity were not documented. Third, the competence weights and cut scores were not psychometrically validated. Fourth, standard deviations, confidence intervals, effect sizes, and participant-level data were unavailable, preventing reproducible inferential analysis. Fifth, the questionnaire lacked reported item and reliability information. Sixth, the risk score was a heuristic rule rather than a validated predictive model. Finally, formal ethics approval, consent procedures, data retention, and access-control details must be documented before publication. These limitations prevent definitive claims of effectiveness but do not eliminate the framework's value as a testable instructional design.

Future research should use multisite samples, preregistered outcomes, validated competence measures, and clearly documented control conditions. Baseline-adjusted models or group-by-time analyses should report exact test statistics, effect sizes, and confidence intervals. The risk-flag mechanism should be evaluated for calibration, sensitivity, specificity, and potential subgroup bias before it is used for consequential decisions. Qualitative interviews could also examine how students interpret feedback and monitoring. Such work would allow the framework to move from a promising pilot design toward a reproducible and ethically governed educational intervention.

Conclusion

This study developed and descriptively evaluated a web-based, rule-based adaptive learning framework for Network Technologies education. The framework combined diagnostic assessment, modular content, virtual laboratories, automated feedback, activity monitoring, and instructor-supervised risk flags. Across the reported aggregate indicators, the experimental group achieved a higher posttest mean, fewer laboratory errors, shorter completion time, more independent task completion, and more on-time submissions than the control group. The pattern suggests that integrated practice and feedback may support technical digital competence, particularly in configuration, troubleshooting, and cybersecurity.

The evidence does not yet justify a definitive causal claim or the classification of the platform as a validated artificial-intelligence system. The principal contribution is a transparent instructional framework

ISSN: 2181-3337 | SCIENTISTS.UZ

that can be tested and improved. Its responsible use requires validated measures, complete statistical reporting, human oversight, explainable rules, and documented protection of student data. With these conditions and stronger multisite evaluation, the framework may offer a practical model for technology courses in which competence depends on repeated performance, diagnosis, reflection, and responsible use of automated assistance.

REFERENCES

1. Alam, A. (2021). Possibilities and apprehensions in the landscape of artificial intelligence in education. In 2021 International Conference on Computational Intelligence and Computing Applications (ICCICA) (pp. 1–8). IEEE. https://doi.org/10.1109/ICCICA52458.2021.9697272
2. Bond, M., Khosravi, H., De Laat, M., Bergdahl, N., Negrea, V., Oxley, E., Pham, P., Chong, S. W., & Siemens, G. (2024). A meta systematic review of artificial intelligence in higher education: A call for increased ethics, collaboration, and rigour. International Journal of Educational Technology in Higher Education, 21, Article 4. https://doi.org/10.1186/s41239-023-00436-z
3. Brusilovsky, P. (2001). Adaptive hypermedia. User Modeling and User-Adapted Interaction, 11, 87–110. https://doi.org/10.1023/A:1011143116306
4. Brusilovsky, P., & Millán, E. (2007). User models for adaptive hypermedia and adaptive educational systems. In P. Brusilovsky, A. Kobsa, & W. Nejdl (Eds.), The adaptive web (pp. 3–53). Springer. https://doi.org/10.1007/978-3-540-72079-9_1
5. Chen, L., Chen, P., & Lin, Z. (2020). Artificial intelligence in education: A review. IEEE Access, 8, 75264–75278. https://doi.org/10.1109/ACCESS.2020.2988510
6. Cisco Networking Academy. (2020). Introduction to networks companion guide (CCNAv7). Cisco Press.
7. European Commission. (2022). Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators. Publications Office of the European Union. https://doi.org/10.2766/153756
8. Ferguson, R. (2012). Learning analytics: Drivers, developments and challenges. International Journal of Technology Enhanced Learning, 4(5–6), 304–317. https://doi.org/10.1504/IJTEL.2012.051816
9. Holmes, W., Bialik, M., & Fadel, C. (2019). Artificial intelligence in education: Promises and implications for teaching and learning. Center for Curriculum Redesign.
10. Ifenthaler, D., & Yau, J. Y.-K. (2020). Utilising learning analytics to support study success in higher education: A systematic review. Educational Technology Research and Development, 68, 1961–1990. https://doi.org/10.1007/s11423-020-09788-z
11. Pardo, A., & Siemens, G. (2014). Ethical and privacy principles for learning analytics. British Journal of Educational Technology, 45(3), 438–450. https://doi.org/10.1111/bjet.12152
12. Redecker, C. (2017). European framework for the digital competence of educators: DigCompEdu (Y. Punie, Ed.). Publications Office of the European Union. https://doi.org/10.2760/159770
13. Sclater, N. (2016). Developing a code of practice for learning analytics. Journal of Learning Analytics, 3(1), 16–42. https://doi.org/10.18608/jla.2016.31.3
14. Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. American Behavioral Scientist, 57(10), 1510–1529. https://doi.org/10.1177/0002764213479366
15. Vuorikari, R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The digital competence framework for citizens—with new examples of knowledge, skills and attitudes. Publications Office of the European Union. https://doi.org/10.2760/115376

ISSN: 2181-3337 | SCIENTISTS.UZ