Balancing Authenticity and Academic Integrity in the Age of Generative AI: A Constructively Aligned Approach to Cybersecurity Assessment

Ismail Hassan

Department of Computer Science
Oslo Metropolitan University
Oslo, Norway
ismai@oslomet.no

Abstract. The increasing use of generative artificial intelligence (GenAI) presents challenges for assessment in higher education, particularly where unsupervised coursework is used to evaluate practical competence. Although supervised examinations can provide stronger assurance of individual authorship, conventional examination formats may provide limited opportunities for students to demonstrate applied technical skills. This tension is particularly relevant in cybersecurity education, where learning outcomes typically encompass both conceptual understanding and practical competence.

This paper presents a constructively aligned assessment approach implemented in an undergraduate Computer Security course. Intended Learning Outcomes (ILOs), Teaching and Learning Activities (TLAs), and Assessment Tasks (ATs) were connected through a shared browser-based Linux laboratory environment used for practical learning throughout the semester and for a supervised digital final examination. The examination required students to apply previously developed competencies to cybersecurity problems within the same practical environment.

Students' perceptions of the alignment between learning outcomes, teaching activities, and assessment were evaluated through an anonymous post-course questionnaire. The findings indicate that students generally perceived strong alignment across the course and supported the use of the practical environment for assessment.

The study demonstrates how supervised digital examinations can incorporate authentic practical activities while strengthening assurance that assessed work reflects individual student competence.

1 Introduction

The rapid adoption of generative artificial intelligence (GenAI) is reshaping assessment practices in higher education [11, 12]. This development presents a particular challenge for computing education, where projects, programming assignments, reports, and practical exercises have traditionally allowed students

to demonstrate knowledge and skills through activities that resemble professional practice. Such approaches are closely associated with authentic assessment, which emphasizes meaningful tasks requiring the application of knowledge and higher-order skills [1, 4]. The increasing capabilities and accessibility of GenAI complicate the interpretation of evidence produced through such assessments [15]. Students can use GenAI systems to generate code, technical explanations, analyses, and solutions to practical problems with varying degrees of human involvement. When substantial parts of an assessment are completed outside supervised conditions, it may therefore be difficult to determine whether the submitted work provides reliable evidence of the individual student's knowledge and competence [3, 13]. Computing educators consequently face a tension between maintaining authentic assessment of applied disciplinary skills and obtaining sufficient assurance that those skills are demonstrated by the student being assessed.

This tension is especially relevant in cybersecurity education, where conceptual knowledge must be complemented by practical competence. Students are expected not only to understand security principles but also to apply them through interaction with operating systems, networks, security mechanisms, and specialised tools. Assessment that relies primarily on written descriptions may therefore provide only limited evidence of a student's ability to perform the practical activities represented by the learning outcomes.

The work presented in this paper emerged from the progressive development of an undergraduate Computer Security course. Earlier iterations combined terminal-session demonstrations with self-paced practical assignments and preconfigured Linux environments to support the development of command-line cybersecurity skills [6]. The practical infrastructure was subsequently extended into a centrally managed, browser-accessible remote laboratory, providing students with isolated and consistently configured Linux environments [7], followed by its use with practical activities, repeated attempts, and feedback to support competence development [8]. These developments established a flexible environment for authentic hands-on learning, but the widespread availability of GenAI raised a new question: *how can the practical competence developed in such an environment be assessed while retaining confidence that the demonstrated competence belongs to the individual student?*

The approach investigated in this study addresses this question by extending the established practical learning environment into the summative assessment.

Throughout the semester, students develop knowledge and skills through lectures, demonstrations, Canvas-based practical assignments, and hands-on activities in the remote Linux laboratory. They subsequently demonstrate corresponding competencies in a supervised digital examination conducted in a controlled physical environment. Rather than replacing practical assessment with a conventional written examination, the examination retains the browser-accessible Linux environment, technical tools, and practical workflows with which students have worked during the course.

The design is guided by constructive alignment between the intended learning outcomes, teaching and learning activities, and assessment tasks. The objective is therefore not simply to restrict access to GenAI during assessment, but to preserve the relationship between the capabilities students are expected to develop, the activities through which they develop them, and the tasks through which achievement is verified. In this way, formative practical activities provide opportunities for experimentation and skill development, while the supervised digital examination provides controlled conditions for demonstrating individual competence.

This paper presents and evaluates the resulting assessment design. Rather than treating authenticity and assessment integrity as competing objectives, the study investigates how they can be supported together through the alignment of learning outcomes, practical learning activities, technological infrastructure, and supervised summative assessment.

The main contributions of this work are threefold:

- We describe the progression of a practical cybersecurity learning environment into an assessment model that connects browser-accessible laboratory activities with supervised digital assessment.
- We present a constructively aligned assessment design that retains authentic, tool-based cybersecurity tasks while providing controlled conditions for verifying individual student competence in the presence of widely accessible GenAI tools.
- We report experiences from implementing and evaluating the approach in an undergraduate Computer Security course and consider its implications for authentic computing assessment in the age of GenAI.

2 Background and Related Work

2.1 Authentic Assessment and Constructive Alignment

Authentic assessment evaluates students through meaningful tasks reflecting contexts in which knowledge and skills are applied beyond education. Rather than relying exclusively on conventional written examinations, students demonstrate competence through activities resembling professional practice [4,19]. This is particularly relevant in computing, where competence may require configuring systems, using technical tools, diagnosing problems, interpreting output, and developing solutions alongside conceptual understanding.

The value of such assessment depends on both task authenticity and alignment with intended learning outcomes and preceding learning activities. Constructive alignment emphasizes that students should develop the capabilities expressed by the learning outcomes and demonstrate them through corresponding assessment tasks [2]. In practical computing courses, this implies continuity between what students practise and what they demonstrate during assessment.

Previous work has applied these principles to practical computing assessment. In an undergraduate Network and System Administration course, students completed professional system-administration activities and subsequently

demonstrated corresponding competencies through practical tasks under controlled conditions [5]. The same platform and software supported learning and assessment, while predefined scoring criteria and automated feedback provided transparency and opportunities for improvement. Related studies have investigated technology-supported environments for authentic learning and assessment in networking, cybersecurity, and secure software development [10,14,20]. These studies demonstrate the potential of practical environments for assessing applied competence, while GenAI raises new questions about evidence of individual achievement.

2.2 Generative AI and Assessment Validity

Generative AI can generate and revise text and code, explain technical concepts, analyse errors, and propose solutions to computing problems. Although these capabilities support learning, they complicate the interpretation of student work when AI assistance is unrestricted or cannot be reliably determined [12, 15].

This issue extends beyond academic misconduct because assessment provides evidence of achievement of specified learning outcomes. If a solution has been substantially generated, corrected, or guided by an external AI system, the extent to which it represents the student's own competence may be uncertain [3, 13, 16]. This is particularly important when students are expected to demonstrate independent performance of disciplinary tasks.

Supervised examinations can increase confidence in individual authorship by controlling access to external resources, but control alone does not ensure validity. Where learning outcomes concern practical competence, replacing technical activity with written descriptions may measure a different capability. In cybersecurity, describing a security tool is not equivalent to executing it, interpreting its output, and using the results to solve a security problem.

Assessment design in the presence of GenAI therefore requires credible evidence of individual achievement while maintaining alignment with the learning outcomes. This calls for assessment models that combine controlled conditions with practical tasks rather than treating supervision and authenticity as mutually exclusive.

2.3 Practical Cybersecurity Education

Cybersecurity education presents particular infrastructure requirements because practical learning involves interaction with operating systems, networks, security mechanisms, vulnerabilities, and specialised tools [18]. Students therefore require environments in which such activities can be performed safely and repeatedly without compromising institutional systems or interfering with other students .

Virtual machines, containers, and remote laboratories have been used to provide isolated and reproducible environments for cybersecurity exercises [17]. Compared with dedicated physical laboratories or individually configured student computers, centrally managed environments can provide consistent software

and system configurations across a cohort while allowing flexible access. Browser-based environments can further reduce dependencies on local operating systems and hardware while retaining interaction with command-line tools and realistic technical workflows.

The browser-based virtual laboratory used in this study was developed by the author to provide remotely accessible, preconfigured Linux environments for practical computing activities. Initially developed to support cybersecurity teaching [7], it has subsequently been adopted in several courses at both bachelor's and master's levels. The environment therefore represents an established teaching infrastructure rather than a system developed specifically for the assessment examined in this study.

The present study addresses the subsequent assessment problem created by the changing technological context: how practical competencies developed through flexible laboratory activities can be verified as individual achievement when GenAI can provide substantial assistance with unsupervised tasks. The approach connects authentic assessment, constructive alignment, practical laboratory infrastructure, and controlled assessment by using the same browser-based environment for practical learning throughout the course and for the supervised digital final examination.

3 Course Context, Evolution, and Constructive Alignment of the Practical Assessment

3.1 Course Context and Evolution of the Practical Learning Environment

The study was conducted in an undergraduate Computer Security course offered to third-year Computer Science students. The course introduces fundamental and advanced cybersecurity concepts while placing substantial emphasis on their practical application. Topics include security principles, cryptography, identity and authentication, access control, network security, intrusion detection and prevention, software and web security, malware, and privacy.

The intended learning outcomes encompass both conceptual knowledge and applied technical skills. In addition to understanding fundamental and advanced cybersecurity principles, students are expected to use security tools, identify vulnerabilities, apply cryptographic mechanisms, configure access controls and network protection mechanisms, and analyse security events. Practical activities therefore form an integral part of the course, enabling students to translate conceptual knowledge into applied technical skills and develop the analytical thinking required to identify and address security problems. The relationship between the Intended Learning Outcomes (ILOs), Teaching and Learning Activities (TLAs), and Assessment Tasks (ATs) is informed by principles of constructive alignment [2, 9].

The practical learning environment supporting these activities has evolved over successive course iterations while the underlying pedagogical approach has

remained broadly consistent. An earlier implementation combined short terminal-based demonstrations with self-paced practical assignments delivered through Canvas [6]. Students initially performed these activities using a preconfigured Linux virtual machine distributed for local execution through VirtualBox. Although this approach provided access to the required cybersecurity tools, it introduced dependencies on students' hardware, operating systems, and local configurations. The laboratory was subsequently migrated to centrally managed remote infrastructure to provide a more consistent and accessible environment while preserving the established hands-on, terminal-oriented learning model.

A typical practical task presents a technical problem or scenario that requires students to select and execute appropriate commands or security tools, interpret the resulting output, and use the technical evidence obtained to determine or construct an answer in Canvas. For example, students may use a network-scanning tool to identify exposed services and interpret the resulting output. Other activities similarly require the application of tools and techniques associated with the security topics covered during the course. Canvas question banks provide variations of these tasks, allowing parameters or questions to differ between attempts and enabling students to repeat activities while practising the underlying competencies rather than relying on a single fixed solution [7, 8].

During these formative activities, students can consult course resources, investigate errors, repeat procedures, and develop their understanding through continued interaction with the laboratory environment. Across the course, the practical activities support progression from conceptual understanding and instructor demonstration toward increasingly independent application. Students therefore become familiar with the technical environment, relevant cybersecurity tools, interpretation of technical evidence, and security-oriented problem solving before being required to demonstrate these competencies independently in assessment.

The practical learning environment consequently provides continuity across teaching, practice, and assessment. Competencies specified in the ILOs are introduced conceptually through teaching, demonstrated and practised through laboratory activities, and subsequently assessed through tasks requiring increasingly independent application [2, 9]. This alignment concerns the knowledge, skills, and problem-solving capabilities that students are expected to develop and demonstrate rather than the repetition of particular laboratory exercises. Accordingly, the transition from locally executed virtual machines to remotely managed containers represents primarily an infrastructural evolution: the pedagogical emphasis on hands-on application and progressive development of practical cybersecurity competencies has remained consistent.

3.2 Constructive Alignment of the Final Supervised Digital Examination

The culmination of this learning trajectory is the final supervised digital examination which was conducted in a controlled setting, where the students accessed

the Inspera assessment platform and the web-based Linux environment from assigned workstations, as shown in Figures 1(a) and 1(b).



(a) Controlled examination facility (b) Individual examination workstation

Fig. 1. Supervised digital examination setting: (a) the examination facility used as the controlled environment for the Computer Security examination; (b) an individual workstation providing access to the same web-based Linux environment used throughout the course.

Approximately 35% of the examination consisted of practical cybersecurity scenarios requiring students to investigate technical problems, execute relevant tools or commands, interpret the resulting output, and derive answers from the technical evidence.

A central design principle was to preserve continuity between learning and assessment. Students entered the examination already familiar with the Linux environment, its interaction model, and the categories of cybersecurity tools encountered during the course. The examination, however, presented new problems for which students had to determine independently how their conceptual knowledge and practical experience should be applied.

The intended learning outcomes, teaching and learning activities, and assessment tasks were therefore aligned at the level of competence: students learned security concepts, practised their application through technical activities, and were ultimately required to select, apply, and interpret appropriate techniques independently during the final assessment.

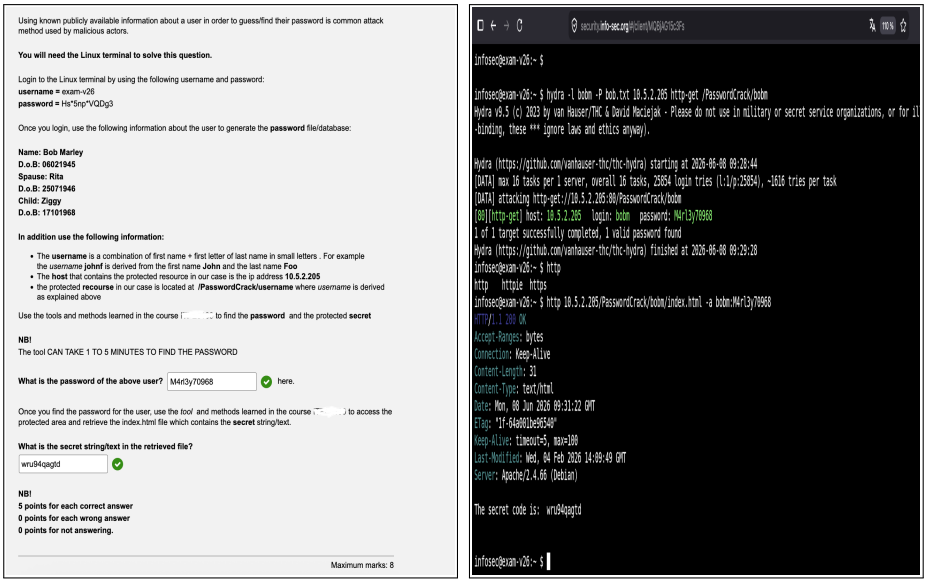
The assessment design thus combines two complementary objectives. First, the practical tasks retain characteristics of authentic cybersecurity activity by requiring students to interact with technical systems, use relevant tools, interpret evidence, and solve security-related problems rather than merely describe these processes theoretically. Second, the supervised setting provides stronger assurance that the observed performance represents the individual student's competence. In this way, constructive alignment extends beyond correspondence between course content and examination questions: the final assessment requires

students to independently demonstrate the forms of practical competence that the preceding learning activities were designed to develop.

3.3 Example of Constructive Alignment in a Practical Assessment Task

One examination task illustrates how this alignment was implemented in practice. Students were presented with a password-security scenario through Inspera and required to investigate the problem using the Hydra password-auditing tool in the Linux laboratory, as illustrated in Figure 2. Although students had developed experience with command-line security tools and related forms of technical investigation during the course, the examination scenario required them to determine and execute the appropriate procedure for the problem presented.

Students had to perform the technical investigation, interpret the resulting output to identify valid credentials, and submit the relevant result through the examination platform. Successful completion therefore depended on more than recalling conceptual knowledge or reproducing a written description of the procedure. It required students to connect their understanding of password security with appropriate tool use, execution of the investigation, and interpretation of technical evidence.



(a) Inspera examination scenario (b) Web-based Linux environment

Fig. 2. Example of a practical cybersecurity examination task: (a) the examination scenario presented through Inspera; and (b) the corresponding technical investigation performed in the web-based Linux environment.

4 Methodology

The evaluation examined students' perceptions of the constructive alignment between the intended learning outcomes, teaching and learning activities, and the final supervised digital examination. The methodology was therefore structured around the same relationships that guided the course and assessment design described in Section 3. In particular, the evaluation considered whether students understood the intended learning outcomes, whether the learning activities supported achievement of those outcomes, whether the practical activities prepared them for the assessment, and whether the examination assessed the competencies specified by the learning outcomes.

4.1 Research Design

The study employed a quantitative survey design to investigate students' perceptions of constructive alignment in an undergraduate Computer Security course. The survey was developed around the principles of constructive alignment [2], according to which intended learning outcomes, teaching and learning activities, and assessment tasks should form a coherent learning system.

Rather than evaluating the final examination in isolation, the study considered the complete learning and assessment process experienced by the students. The survey therefore examined four related dimensions: students' understanding of the intended learning outcomes (ILO), the relationship between teaching and learning activities and those outcomes (TA $\rightarrow$ ILO), the relationship between teaching and learning activities and assessment tasks (TA $\rightarrow$ AT), and the relationship between assessment tasks and the intended learning outcomes (AT $\rightarrow$ ILO). These relationships provide the analytical framework for evaluating the constructive alignment of the implemented course design.

4.2 Participants

Participants were students enrolled in the Computer Security course during the autumn semester of 2025. The course is a mandatory third-year course within a bachelor's degree program in Computer Science. As described in Section 3, students participated throughout the semester in lectures and practical laboratory activities before completing the final supervised digital examination.

The survey was administered after completion of the examination on December 1, 2025. A total of 331 students were enrolled in the course, of whom 41 completed the post-course survey, corresponding to a response rate of 12.4%. Participation was voluntary and anonymous, and no personally identifiable information was collected.

4.3 Survey Instrument

Data were collected using an anonymous online questionnaire consisting of 14 closed-ended items. The questionnaire was designed to measure the four dimensions of constructive alignment identified in the research design. The first three

items (Q1–Q3) addressed students' understanding of the intended learning outcomes. Q4–Q7 examined whether the teaching and learning activities supported achievement of those outcomes. Q8–Q9 addressed the relationship between the semester-long practical activities and the final assessment, while Q10–Q14 examined whether the assessment tasks reflected the intended learning outcomes and enabled students to demonstrate the corresponding practical competencies.

All items were measured using a five-point Likert scale ranging from *Strongly Disagree* (1) to *Strongly Agree* (5). Table 2 in Appendix Appendix A presents the complete questionnaire and the mapping between individual items and the four constructs.

4.4 Data Collection

The questionnaire was administered electronically using Microsoft Forms, with a link distributed through the institution's learning management system immediately after completion of the final supervised digital examination. Administering the survey at this point ensured that respondents had experienced the complete learning and assessment sequence, including lectures, practical laboratory activities, coursework, and the final assessment.

This timing was particularly relevant to the purpose of the study. Students were not being asked to predict whether the practical activities would prepare them for the examination rather, they were able to evaluate this relationship after experiencing both. Similarly, their responses concerning the consistency of the laboratory and examination environments and the relationship between assessment tasks and learning outcomes were based on their completed experience of the course and examination.

4.5 Data Analysis

Survey responses were numerically coded from 1 (*Strongly Disagree*) to 5 (*Strongly Agree*). Descriptive statistics were calculated for each of the 14 items, including response frequencies, percentages, means, and standard deviations. These statistics were used to characterize students' perceptions of individual aspects of the course and assessment design.

To examine the four dimensions of constructive alignment at the construct level, mean scores were calculated by averaging the items associated with each construct: ILO (Q1–Q3), TA $\rightarrow$ ILO (Q4–Q7), TA $\rightarrow$ AT (Q8–Q9), and AT $\rightarrow$ ILO (Q10–Q14). These construct scores were used to examine the perceived relationships among learning outcomes, teaching and learning activities, and assessment tasks.

The internal consistency of the questionnaire was evaluated using Cronbach's alpha. Reliability was examined for the individual multi-item constructs and for the overall instrument. The resulting item-level and construct-level statistics are presented in Section 5.

5 Results

A total of 41 students completed the post-course survey. The results were analyzed at both construct and individual-item levels to examine students' perceptions of constructive alignment between the Intended Learning Outcomes (ILOs), Teaching and Learning Activities (TLAs), and Assessment Tasks (ATs).

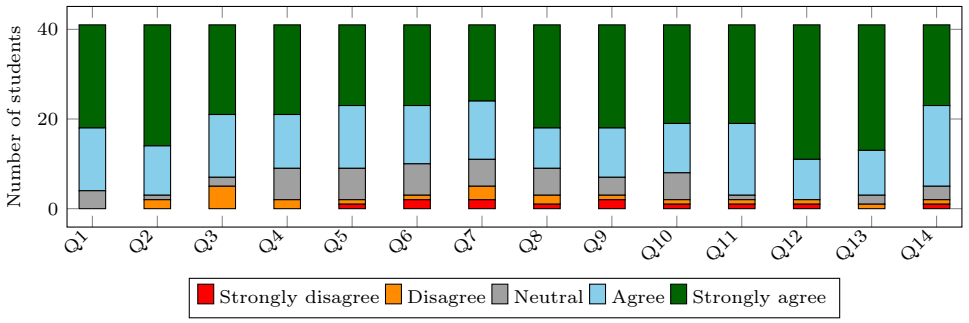


Fig. 3. Response distribution for each survey question.

As shown in Figure 3, responses were predominantly concentrated in the *Agree* and *Strongly Agree* categories. Q12 received the highest individual-item score ($M = 4.61$), followed by Q13 ($M = 4.59$) and Q2 ($M = 4.54$). Q12 concerned the use of the same web-based Linux laboratory environment for practical assignments and the final supervised digital examination, while Q13 concerned whether this environment enabled students to demonstrate the skills described in the learning outcomes. The lowest-rated item was Q7 ($M = 3.98$, $SD = 1.11$), concerning students' confidence that they had achieved the intended learning outcomes.

Table 1 summarizes the construct-level descriptive statistics and internal consistency. All four constructs achieved mean scores above 4.0 on the five-point Likert scale, with an overall alignment score of 4.30 (SD = 0.74).

Table 1. Construct-level descriptive statistics and internal consistency.

Construct	**Mean**	**SD**	**Cronbach's α**
ILO	4.40	0.73	0.854
TLA $\rightarrow$ ILO	4.10	0.92	0.918
TLA $\rightarrow$ AT	4.26	1.00	0.882
AT $\rightarrow$ ILO	4.42	0.74	0.913
Overall Alignment	4.30	0.74	0.954

AT$\rightarrow$ILO received the highest construct-level score ($M = 4.42$, $SD = 0.74$), followed by ILO ($M = 4.40$, $SD = 0.73$) and TLA$\rightarrow$AT ($M = 4.26$, $SD = 1.00$).

TLA→ILO received the lowest construct-level score ($M = 4.10$, $SD = 0.92$), although responses remained positive overall. Cronbach's alpha ranged from 0.854 to 0.918 across the four constructs, while the complete 14-item instrument achieved $\alpha = 0.954$, indicating high internal consistency.

6 Discussion

The results indicate that students generally perceived strong constructive alignment across the course, with particularly strong alignment between the assessment tasks and intended learning outcomes. This supports the principle of constructive alignment, in which learning activities and assessment should enable students to develop and demonstrate the capabilities specified by the intended learning outcomes [2].

A particularly important finding concerns the role of the shared browser-based Linux laboratory environment. The strong responses to Q12 and Q13 indicate that students recognized both the continuity of the technical environment from practical learning to assessment and its role in enabling them to demonstrate the intended practical skills. The laboratory therefore functioned not merely as infrastructure for practical exercises, but as a common technical environment connecting the development and assessment of practical competence.

The approach also addresses a tension between supervised assessment and opportunities to demonstrate practical competence. Supervision provides stronger assurance of individual authorship, which has become increasingly relevant as GenAI complicates attribution in unsupervised coursework. Conventional examinations, however, may provide limited opportunities to demonstrate applied cybersecurity skills. Providing the laboratory during the supervised examination enabled students to investigate technical problems, use cybersecurity tools, and interpret technical evidence under controlled conditions. The study does not independently establish assessment authenticity or academic integrity, but the findings indicate that students perceived the resulting assessment as aligned with the competencies they were expected to develop.

The comparatively lower response to Q7 suggests a distinction between students' perceptions of course structure and their confidence in their own competence. Students could perceive the learning outcomes, activities, and assessment as well aligned while being less certain that they personally had achieved all intended outcomes. As Q7 concerns self-assessment rather than structural alignment alone, it should be interpreted cautiously, but the result suggests that future course development could make evidence of individual achievement more explicit.

Several limitations should be considered. The study measures student perceptions rather than objective learning gains or assessment validity, and only 41 of 331 enrolled students completed the questionnaire (12.4%), creating potential self-selection and nonresponse bias. The study was also conducted in a single undergraduate cybersecurity course, limiting generalizability. Future work should

examine additional courses and cohorts and complement perception data with objective measures of learning and assessment performance.

7 Conclusion

This study examined a constructively aligned approach in which Intended Learning Outcomes (ILOs), Teaching and Learning Activities (TLAs), and Assessment Tasks (ATs) were connected through a shared browser-based Linux laboratory environment. Students used the same environment to develop practical cybersecurity competencies during the course and to demonstrate them through new problems in a supervised digital examination.

Among the students who participated in the survey, the findings indicate a high perceived degree of constructive alignment, particularly between the assessment tasks and the intended learning outcomes. However, the low survey response rate introduces a risk of non-response bias and limits the extent to which these perceptions can be considered representative of the full cohort.

The main contribution is the integration of a shared practical environment into the learning and assessment design rather than the environment itself. The approach illustrates how supervised digital examinations can retain authentic technical activities while providing stronger assurance of individual authorship, an increasingly relevant consideration in the context of GenAI. Future work should evaluate the approach across additional cohorts and computing courses, seek higher participation rates, and complement student perceptions with objective measures of learning and assessment performance.

References

1. Ashford-Rowe, K., Herrington, J., Brown, C.: Establishing the critical elements that determine authentic assessment. Assessment & Evaluation in Higher Education, https://doi.org/10.1080/02602938.2013.819566 **39**(2), 205–222 (2014)
2. Biggs, J.: Enhancing teaching through constructive alignment. Higher education **32**(3), 347–364 (1996). https://doi.org/10.1007/BF00138871
3. Brattli, H., Utne, A., Lynch, M.: Assessment validity in the age of generative ai: A natural experiment. In: Informatics. vol. 13, p. 56. MDPI (2026). https://doi.org/10.3390/informatics13040056
4. Gulikers, J.T., Bastiaens, T.J., Kirschner, P.A.: A five-dimensional framework for authentic assessment. Educational technology research and development **52**(3), 67–86 (2004). https://doi.org/10.1007/BF02504676
5. Hassan, I.: Automated authentic assessment: Applied to an undergraduate course in network and system administration. In: 2020 IEEE Global Engineering Education Conference (EDUCON). pp. 183–191. IEEE (2020). https://doi.org/10.1109/EDUCON45650.2020.9125320
6. Hassan, I.: Teaching cybersecurity to computer science students utilizing terminal sessions recording software as a pedagogical tool. In: 2020 IEEE Frontiers in Education Conference (FIE). pp. 1–8. IEEE (2020). https://doi.org/10.1109/FIE44824.2020.9274268

7. Hassan, I.: Levereging apache guacamole, linux lxd and docker containers to deliver a secure online lab for a large cybersecurity course. In: 2022 IEEE Frontiers in Education Conference (FIE). pp. 1–9. IEEE (2022). https://doi.org/10.1109/FIE56618.2022.9962510
8. Hassan, I.: Fostering motivation in cybersecurity education: A self-determination theory approach to student-centered learning. In: 2026 IEEE Global Engineering Education Conference (EDUCON). pp. 1–9. IEEE (2026). https://doi.org/10.1109/EDUCON67543.2026.11574402
9. Hristov, S., Nakov, D., Miočinović, J.: Constructive alignment between objectives, teaching and learning activities, student competencies and assessment methods in higher education. Journal of Agriculture and Plant Sciences **21**(2), 21–36 (2023). https://doi.org/10.46763/JAPS23212021h
10. Lo, D.C.T., Qian, K., Chen, W., Shahriar, H., Clincy, V.: Authentic learning in network and security with portable labs. In: 2014 IEEE Frontiers in Education Conference (FIE) Proceedings. pp. 1–5. IEEE (2014). https://doi.org/10.1109/FIE.2014.7043995
11. Lye, C.Y., Lim, L.: Generative artificial intelligence in tertiary education: Assessment redesign principles and considerations. Education Sciences **14**(6), 569 (2024). https://doi.org/10.3390/educsci14060569
12. Mao, J., Chen, B., Liu, J.C.: Generative artificial intelligence in education and its implications for assessment. TechTrends **68**(1), 58–66 (2024). https://doi.org/10.1007/s11528-023-00911-4
13. Moorhouse, B.L., Yeo, M.A., Wan, Y.: Generative ai tools and assessment: Guidelines of the world's top-ranking universities. Computers and Education Open **5**, 100151 (2023). https://doi.org/10.1016/j.caeo.2023.100151
14. Qian, K., Lo, D., Parizi, R., Wu, F., Agu, E., Chu, B.T.: Authentic learning secure software development (ssd) in computing education. In: 2018 IEEE Frontiers in Education Conference (FIE). pp. 1–9. IEEE (2018). https://doi.org/10.1109/FIE.2018.8659217
15. Scarfe, P., Watcham, K., Clarke, A., Roesch, E.: A real-world test of artificial intelligence infiltration of a university examinations system: A "turing test" case study. PloS one **19**(6), e0305354 (2024). https://doi.org/10.1371/journal.pone.0305354
16. Shepherd, C.: Generative ai misuse potential in cyber security education: A case study of a uk degree program. In: Computing Conference. pp. 448–467. Springer (2026). https://doi.org/10.1007/978-3-032-24807-7_29
17. Švábenskỳ, V., Weiss, R., Cook, J., Vykopal, J., Čeleda, P., Mache, J., Chudovskỳ, R., Chattopadhyay, A.: Evaluating two approaches to assessing student progress in cybersecurity exercises. In: Proceedings of the 53rd ACM Technical Symposium on Computer Science Education-Volume 1. pp. 787–793 (2022). https://doi.org/10.1145/3478431.3499414
18. Towhidi, G., Pridmore, J.: Aligning cybersecurity in higher education with industry needs. Journal of Information Systems Education **34**(1), 70–83 (2023)
19. Villarroel, V., Bloxham, S., Bruna, D., Bruna, C., Herrera-Seda, C.: Authentic assessment: Creating a blueprint for course design. Assessment & Evaluation in Higher Education **43**(5), 840–854 (2018). https://doi.org/10.1080/02602938.2017.1412396
20. Willems, C., Meinel, C.: Online assessment for hands-on cyber security training in a virtual lab. In: Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON). pp. 1–10. IEEE (2012). https://doi.org/10.1109/EDUCON.2012.6201149

Appendix A Post-Course Questionnaire

Table 2 presents the 14 items used to evaluate students' perceptions of constructive alignment. Responses were recorded on a five-point Likert scale ranging from 1 (*Strongly Disagree*) to 5 (*Strongly Agree*).

Table 2. Survey questions and construct mapping.

Construct	Item	Survey Question
ILO	Q1	The learning outcomes of the course were clearly stated at the start of the course.
	Q2	At the beginning of each module, the lecture clearly stated the intended learning outcomes for that module.
	Q3	I understood what knowledge and skills I was expected to develop in each module.
TA → ILO	Q4	The teaching activities focused on the same skills and knowledge described in the learning outcomes.
	Q5	The module lab assignments helped me achieve the intended learning outcomes of the course.
	Q6	The progression of module assignments supported gradual achievement of the learning outcomes.
	Q7	By the end of the course, I felt confident that I had achieved the course intended learning outcomes.
TA → AT	Q8	The module lab assignments prepared me well for the final supervised digital exam.
	Q9	The lab environment used during the semester was consistent with the environment used in the final supervised digital exam.
AT → ILO	Q10	The tasks in the final supervised digital exam directly reflected the stated learning outcomes.
	Q11	The practical aspects of the final supervised digital exam accurately assessed what I had learned through the course's practical lab activities.
	Q12	The web-based Linux lab environment used in the final supervised digital exam was the same as the environment used in the course's practical assignments.
	Q13	Using the same lab environment in the final supervised digital exam allowed me to demonstrate the skills described in the learning outcomes.
	Q14	Overall, the final supervised digital exam was a fair measure of the course's intended learning outcomes.