Challenge-Based Learning in Cybersecurity Fundamental Studies

Algimantas Venčkauskas[1,*], Ignas Plauska[1] and Nerijus Šatkauskas[1]

[1] *Kaunas University of Technology, Studentų g. 50, Kaunas, Lithuania*

Abstract

A considerable shortage of qualified cybersecurity professionals has pushed higher education institutions under growing pressure to produce graduates who are skilled enough to fill these positions. Conventional lecture-centered delivery of introductory cybersecurity courses are efficient for knowledge transmission. However, it struggles to develop inquiry, collaboration, and transferable competencies that national and foreign policies now identify as essential. This paper examines Challenge-Based Learning (CBL) as a pedagogical method for a cybersecurity fundamentals course. As the voluntary anonymous survey suggests, students of little to moderate experience considered CBL integration as a useful, helpful and contributive method.

Keywords

Challenge-Based Learning, CBL, Cybersecurity Education, Higher Education, Active Learning

1. Introduction

A cybersecurity workforce shortage is becoming an ever-growing concern for universities, industries, and national security agencies. (ISC)² as the world's largest non-profit organization of certified cybersecurity professionals has completed their 2022 Cybersecurity Workforce Study [1] where they highlighted that the global workforce shortage grew by 26% on annual basis to leave approximately 3.4 million unfilled positions. The workforce availability itself expanded at less than half of that speed. Over the last decades, substantial investments have been directed to cybersecurity disciplines, certification platforms, and online training environments. As it is noted, universities are too slow to react to cybersecurity needs in education. A computer science student will often get a four or five years training without getting a single up-to-date class on cybersecurity [2]. And if students are offered any cybersecurity training modules, these courses tend to be theoretical which do any comply with the real-world problems.

Cybersecurity master's studies provide a lot of theoretical knowledge but lack practical skills. Master's programs develop practical cybersecurity skills through hands-on, immersive methods, including virtual cyber ranges, Capture The Flag (CTF) competitions, capstone projects and case studies. These programs emphasize learning by doing virtualized, industry-standard labs and comprehensive, team-based, real-world case study projects. The Challenge-Based Learning (CBL) methodology is beneficial to teaching cybersecurity education [2].

2. Related Literate Review

CBL is different from other active-learning methods in four respects. First, unlike problem-based learning, CBL begins with a Big Idea rather than with a pre-specified problem. Second, unlike project-based learning, the solution options in CBL are countless since "the challenge is stated broadly enough to allow for a variety of solutions" as per Challenged Based Learning white paper. Due to this,

*IVUS 2026: Information Society and University Studies 2026, May 12, Kaunas, Lithuania

[1,*] Corresponding author.

algimantas.venckauskas@ktu.lt (A. Venčkauskas); ignas.plauska@ktu.lt (I. Plauska); nerijus.satkauskas@ktu.lt (N. Šatkauskas)

0000-0002-4567-5023 (A. Venčkauskas); 0000-0001-7029-2035 (N. Šatkauskas)

Copyright © 2026 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-06

CEUR-WS.org/Vol-4317/paper5.pdf

different approaches across teams are expected. Third, CBL requires authentic external stakeholders to be part of that learning cycle. Fourth, documentation, reflection, and sharing are not just deliverables but an ongoing collection for learning [3].

Integrating CBL scenarios into a university study process raises some issues. Based on literature, it is possible to identify three integration modes. *Extra-curricular* integration practice typically treats scenarios as certain competitions, CTF events, or hackathons which are offered in addition to regular curriculum; this approach is globally popular in cybersecurity education [4,5]. *Intra-curricular* integration adds one or some scenarios to a formally approved course, aligning them with the learning outcomes and assessment scheme; this approach is most commonly supported in recent reviews [6] as beneficial, valuable and promising. *Program-level* integration incorporates scenarios in multiple courses and years. Big Ideas are just a starting point for an engagement and Challenges are a call for their actions as highlighted by the ECIU consortium's challenge-based programs [7].

Four integration issues are observed across studies. First, alignment with competency frameworks requires an explicit mapping from each scenario based on Challenge and Guiding Questions. When scenarios are not aligned, students may practice irrelevant skills, competencies cannot be reliably assessed, and the scenario collapses into an activity with no curricular or industry value. Misalignment may damage both the learning process and the credibility of the assessment [8]. Second, assessment in regular lectures is easier than in CBL courses: team-based results may not reveal any individual learning progress, external feedback to evaluators can inflate grades, and experienced students may dominate in the team-work while other ones would be left with nothing useful to do. Third, scaffolding and infrastructure availability which allows determine the set of feasible scenarios. Usually, open CTF infrastructure is needed. As per Mukherjee et al. [9], this issue is assessed in the perspective of scaffolding (how much pedagogical support the institution can provide) versus barriers (material, regulatory, or resource constraints on what can be done). In that framing, the third integration issue will define which scenarios are therefore feasible. Fourth, scalability remains a significant limitation. It can be easy to use a scenario with small cohorts. But it can be difficult to structure a self-directed learning with increasingly diverse cohorts. It can be challenging for a single educator to develop more complex problems with multiple information sources [10].

3. Fundamentals of Cybersecurity module with CBL integration

Module Fundamentals of Cybersecurity is part of the Kaunas University of Technology master's degree studies program Information and Information Technology Security. This module is also provided as a non-formal learning module through KTU's open learning Moodle environment (https://open.ktu.edu).

CBL is an integral part of the study module, the study process is transformed from "listening and doing tasks" to "researching, solving and implementing". CBL integration turns the study module not into a static set of knowledge, but into a dynamic ecosystem. At the master's level, such a model is extremely effective, because it simulates a real professional environment, where an expert must not only "know", but also "act" in the face of uncertainty. The developed model of the study module with CBL integration shows how each part complements each other.

3.1. Structure of the module with CBL integration

The purpose of the module is the synthesis of competencies. Here, theoretical knowledge, practical skills and analytical thinking merge to solve a complex challenge.

1. **The Foundation**
    - Purpose: To provide the student with a "toolbox" and scientific context.
    - Content: In a master's degree, it is not only facts, but also formal models, standards and algorithms.
    - Role of CBL: Theory is not an end in itself. During lectures, the teacher emphasizes how a specific theory (e.g. Zero Trust architecture) can be applied to solve the big challenge of the module.

- Result: The student understands the "why" (principles), not just the "what" (definitions).

2. **Seminars (The Research & Critique)**
   - Purpose: To develop critical thinking, the ability to research and argue.
   - Content: Analysis of scientific articles, studies of best practices (Case Studies) and the Challenge Investigation (Investigate) phase.
   - Role of CBL: During seminars, student groups present their intermediate research on the chosen challenge. Peer-review takes place – colleagues criticize and suggest improvements.
   - Outcome: Ability to base their future solution on scientific evidence.
3. **Lab work (The Skillset)**
   - Purpose: Technical readiness and mastery of tools.
   - Content: Working with specific software, simulations, programming, or security testing.
   - Role of CBL: Lab work becomes a "sandboxing". If the challenge requires securing a network, during the lab students test specific configurations that they will later include in their final solution.
   - Outcome: Technical confidence in implementing the solution.
4. **Solving specific challenges (CBL scenarios: The Synthesis / Act)**
   - Purpose: Real impact and implementation of the solution.
   - Content: This is the culmination of the module. Student teams work on an authentic challenge presented by a business partner or university.
   - Process: Based on theory, seminars and laboratory experience, students develop a product, strategy, or prototype.
   - Result: Presentation of the solution (Pitch) and defence before a committee consisting not only of lecturers but also of challenge owners (practitioners).

Table 1 summarizes the introduction of the CBL scenario in the Fundamentals of Cybersecurity module.

Table 1
The introduction of the CBL scenario in the Fundamentals of Cybersecurity module

Study method	General aims	CBL activities
The Foundation (lectures)	Establish a theoretical foundation in cybersecurity: this involves exploring the fundamental concepts, models, and frameworks that guide cybersecurity thinking and practice	
Seminars	Analyze security problems from a theoretical perspective: This involves understanding the underlying causes of security vulnerabilities and developing theoretical solutions	Introduction to CBL scenarios
Lab works	Provide practical experience, enabling familiarity with industry-standard tools	Lab work becomes a "sandboxing". During the lab students master cybersecurity tools and methods that they will later include in their final solution.
Solving specific challenges	Develop practical cybersecurity skills. CBL projects aim to provide hands-on experience in applying cybersecurity knowledge and techniques to solve real-world problems.	The learners are suggested to use and or be inspired to use material from the Principles (key material) and Use Cases (examples) in their challenge-based solutions

	Enhance problem-solving and critical thinking abilities. By confronting complex challenges, learners develop their ability to analyse situations, identify vulnerabilities, devise solutions, and evaluate their effectiveness.

The study module addresses various challenges. Below we will present one of the challenges, Security of smart home systems, and its implementation using the CBL methodology.

3.2. CBL scenario - Security of smart home systems

The Internet of Things (IoT) is an emerging concept where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. In the context of "Smart Home Environments" both IoT and traditional devices and services integrate in a home to enhance the quality of life of citizens. This allows improvements in several domains such as energy efficiency and health monitoring… New Smart Home devices and services appear at a fast pace, from various manufacturers which may have limited experience of cyber security. Yet, it is often necessary to integrate these devices in the "Home Area Network" in order to provide connectivity for data exchange and to perform their operations[2].

The challenge "Security of smart home systems" addresses the problems of secure communication in home systems.

3.2.1. Big Idea Background

The Big Idea of the scenario is *security of smart home systems*. Making a choice of this Big Idea was defined for three reasons. First, smart-home deployments present a dense cluster of real security problems - weak commissioning, unauthenticated messaging, insecure cloud APIs, privacy-leaking radio broadcasts etc. These vulnerabilities can be examined at a level accessible to fundamental stage students. Second, the topic is widely relevant. Every student has encountered some smart-home devices, and the consequences of any compromise can be devastating. Third, the topic connects explicitly to three United Nations Sustainable Development Goals — SDG 9 (Industry, Innovation and Infrastructure), SDG 11 (Sustainable Cities and Communities), and SDG 16 (Peace, Justice and Strong Institutions). It allows our scenario to be framed not purely as a technical exercise but as a contribution to resilient digital infrastructure.

The stakeholders of this challenge span across smart-home device manufacturers and installers, owners and end-users, and, to some extent, any wider community, the well-being of which depends on reliability of their digital infrastructure. This stakeholder diversity is important because it discourages narrow, purely technical framings of the challenge. It forces students to consider usability, on-boarding, and communication constraints alongside cryptographic and protocol-level decisions.

3.2.2. Core Challenge

Our scenario is designed as a mini challenge for four weeks. This duration is long enough to accommodate the full Engage–Investigate–Act cycle of CBL, but short enough to be embeddable inside a single semester-long fundamentals module without eliminating the foundational content that the rest of the module must cover. The core challenge is stated as follows: Connected homes offer convenience but also introduce significant security risks. How can we design systems that remain secure even if an attacker gains internal network access?

[2]https://www.enisa.europa.eu/sites/default/files/publications/Security%20and%20Resilience%20of%20Smart%20Home%20Environments.pdf

Specific security problems related to the most common smart home communication protocols are as follows:

Topic 1: MQTT ACL Enforcement. This challenge continues the previous lab work on securing MQTT communication. It focuses on implementing fine-grained access control for an IoT system that already uses mutual TLS (mTLS) for secure connections. Learners design and enforce topic-level permissions to prevent unauthorized actions by authenticated clients.

Specific Problem: Even with mTLS, all authenticated devices can publish or subscribe to any topic. This lack of authorization creates a risk of cross-device control and data leakage.

The Goal of the CBL Solution: Create and apply ACLs that restrict devices to their own topics, enforce role-based permissions, and validate these controls through negative testing and log analysis while documenting an onboarding policy for new devices.

Topic 2: MQTT Security Validation & Attack Simulation. This challenge builds on the previous lab work by performing a comprehensive security validation of an MQTT-based IoT system secured with mTLS. Learners simulate attacks and stress conditions to evaluate the robustness of encryption and broker configuration.

Specific Problem: Even with encryption and authentication, systems may remain vulnerable to replay attacks, brute-force attempts, or denial-of-service (DoS) scenarios. Without validation, these risks go unnoticed.

The Goal of the CBL Solution: Conduct penetration tests, verify TLS handshake and cypher strength, simulate stress conditions, and produce an audit report with evidence and automated scripts to confirm MQTT security resilience.

Topic 3: Insecure (not sufficient) Wi-Fi communication via MQTT, CoAP, HTTP protocols. While Wi-Fi is standard, security often breaks down where a device communicates with the internet via application layer protocols such as MQTT, CoAP or HTTP, as these protocols do not implement security measures. Additional protocols or solutions are required to provide security.

Specific Problem: Insecure Cloud API Design. Smart device data is usually sent to the manufacturer's cloud server. If the manufacturer's Application Programming Interface (API) endpoints are poorly secured, an attacker could exploit simple flaws (e.g., lack of proper authorization checks) to access data streams or send commands to devices belonging to other users on the same cloud service.

The goal of the CBL solution: Improve Insecure Cloud API Design, which is based on MQTT, CoAP or HTTP protocols, by using additional security levels implemented using DTLS or similar solutions.

Topic 4: Protocol Zigbee: Weak or Absent Device Commissioning Security. Zigbee is a low-power, mesh network protocol widely used in smart lighting, sensors, and utility monitoring.

Specific Problem: Insecure Key Exchange during commissioning. During the initial device pairing process, many older or poorly implemented Zigbee devices use a well-known default key (a publicly known password). If an attacker is within radio range during this short window, they can capture the network key and join the entire mesh network, compromising all connected devices.

The goal of the CBL solution: Design a "zero-touch" secure commissioning model that uses technologies like QR codes or Near-Field Communication (NFC) for initial authentication, ensuring the network key is never transmitted over the air in an easily crackable format.

Topic 5: Bluetooth Low Energy (BLE): Tracking and Spoofing. BLE is used for short-range communication, often for setup or local control (e.g., smart light bulbs, fitness trackers).

Specific Problem: Device Tracking via Static MAC Addresses. Many BLE devices use a static Media Access Control (MAC) address for their broadcasts, meaning anyone can track the location and activity of the device (and thus the user) over time by simply monitoring the BLE signals.

CBL Solution Focus: Develop a local gateway service or phone application that detects and alerts the user when a BLE device is broadcasting a static MAC address and proposes a solution (if supported by the device) or recommends switching to a device that supports MAC address randomization.

Table 2
Challenge implementation measures and prerequisites for students

Challenge	Challenge Implementation Measures	Student Prerequisites
Topic 1: MQTT ACL Enforcement	Mosquitto MQTT broker with ACL suport Smart home simulation environment (Home Assistant + IoT device containers) Linux environment with VS Code or terminal access Tools: mosquitto.conf, ACL files, MQTT Explorer for testing	Understanding of MQTT topic structure Basic Linux and Docker/Podman skills Familiarity with mTLS and broker configuration Ability to edit config files and restart services
Topic 2: MQTT Security Validation & Attack Simulation	Smart home lab environment secured with mTLS Wireshark for traffic analysis Kali Linux container for attack simulation Stress testing tools (mosquitto_pub, custom scripts) OpenSSL for TLS handshake verification	Knowledge of TLS/mTLS concepts Ability to use Wireshark filters and interpret packet captures Familiarity with penetration testing basics Understanding the MQTT protocol and broker logs
Topic 3: Insecure Wi-Fi Communication via MQTT, CoAP, HTTP	IoT devices or simulated containers using MQTT, CoAP, HTTP Test environment with insecure API endpoints DTLS or TLS libraries for securing protocols Network monitoring tools	Understanding of application-layer protocols (MQTT, CoAP, HTTP) Basics of API security and common vulnerabilities Familiarity with DTLS/TLS configuration Ability to analyse traffic and implement secure endpoints
Topic 4: Zigbee – Weak or Absent Device Commissioning Security	Zigbee coordinator and end devices (or Zigbee simulation tools) Sniffer hardware/software (e.g., TI CC2531, Wireshark with Zigbee plugin) NFC or QR code generator for secure onboarding prototype	Knowledge of Zigbee protocol and commissioning process Basics of cryptographic key exchange Familiarity with NFC or QR-based authentication concepts
Topic 5: BLE – Tracking and Spoofing	BLE-enabled devices (smart bulbs, fitness trackers) or BLE simulators Smartphone or gateway with BLE scanning capability BLE sniffing tools (e.g., nRF Connect, Wireshark BLE plugin) Development environment for mobile app or gateway service	Understanding of BLE advertising and MAC addressing Basics of privacy features like MAC randomization Ability to develop or configure BLE scanning and alerting applications

Implementation follows a standard actionable-steps pattern: configure the MQTT broker and IoT devices to support DTLS/TLS or mTLS as appropriate; develop scripts or firmware updates for BLE MAC randomisation; integrate packet-level security fields where relevant; deploy the resulting solution in a simulated smart-home environment built on Docker or Podman stacks; and perform penetration tests and traffic analysis using Wireshark and custom scripts.

See table 3 for evaluation metrics.

Table 3
Evaluation metrics

Metrics	Requirements
Confidentiality	Verify encryption using Wireshark (no plaintext credentials or data)
Integrity	Confirm packet modifications, prevent replay attacks
Authentication	Validate mutual TLS and ACL enforcement
Privacy	BLE MAC randomization confirmed via scanning tools
Performance	Measure latency and resource overhead introduced by security enhancements
Resilience	Stress test broker under high connection load and log error rates

Each team produces a written solution report with a five-criteria structure. See table 3 for criteria:

Table 4
CBL solution report structure

Criteria	Requirements
Challenge and Context Definition	This section grounds the project, ensuring the reader understands the problem's scope and relevance
Investigation and Research Summary	This section details the knowledge acquisition phase, showing the foundation of the proposed solution
Solution Design and Development	This section focuses on the creative and engineering phase, detailing the deliverable
Testing, Results, and Evaluation	This critical section provides evidence of the solution's impact and effectiveness
Reflection and Next Steps	This section concludes the report by assessing the learning process and charting the future course

4. CBL Implementation Feedback

This study was conducted within the Fundamentals of Cybersecurity course during the 2025 academic year. A Challenge Based Learning (CBL) project was integrated into the course for the first time as part of the instructional design. Participants were students enrolled in the course, predominantly at the graduate level, with smaller representations of undergraduate students, postgraduate researchers, educators, and other professional roles. Participation in all surveys was voluntary and conducted in accordance with institutional guidelines for course evaluation.

4.1. Data Collection Instruments

Three complementary data sources were employed to examine the integration and perceived impact of the CBL project. Two of these instruments were teacher-created questionnaires administered via the course Moodle environment, while the third was a standardized institutional survey.

1. **Course evaluation survey (Moodle-based)** – This teacher-developed questionnaire was administered at the end of the semester through the course Moodle environment and focused on students' perceptions of the course as a whole. The survey included items addressing clarity of learning outcomes, use of active and independent learning methods, instructional design, assessment alignment, and overall course coherence. Responses were collected using Likert-type scales, enabling aggregation of frequencies and percentages for descriptive analysis. The purpose of this survey was to capture students' overall evaluation of the course structure and learning environment after the introduction of the CBL project (N = 26).

2. **CBL integration evaluation survey (Moodle-based)** – This teacher-developed questionnaire was also administered at the end of the semester via Moodle and focused specifically on the design and implementation of the Challenge-Based Learning project. Survey items addressed perceived alignment between the CBL activities and course learning objectives, contribution of CBL to engagement and depth of understanding, clarity of instructions and structure, use of collaboration tools, and perceived difficulty or disorientation during the CBL process. Like the course evaluation survey, responses were collected using Likert-type scales. This instrument was designed to isolate students' perceptions of the CBL component itself rather than the course as a whole (N = 20).

3. **Standardized university satisfaction survey (institutional system)** – The study module and lecturer evaluation survey is a voluntary and anonymous questionnaire administered to students at the end of each semester. Respondents are automatically selected through the Academic Information System based on the study modules they attended, and each eligible student receives an individually generated online survey link. Quantitative evaluations are collected using a 5-point Likert scale ranging from −2 ("strongly disagree") to +2 ("strongly agree"), complemented by open-ended questions that allow respondents to provide qualitative feedback; responses marked as "cannot answer" are excluded from the analysis. In this study, the item "I am satisfied with this study module" was used as the primary indicator of overall module quality and student satisfaction, while other items served as supplementary diagnostic indicators. At the institutional level, survey results are processed by calculating mean scores after removing statistical outliers, defined as responses deviating by more than two standard deviations from the mean, and are routinely used for module improvement and quality assurance. For the purposes of this study, aggregated results from this survey were used to compare student satisfaction in the academic year prior to CBL implementation (2024; 30 responses out of 36 eligible students) with the year in which CBL was introduced (2025; 26 responses out of 30 eligible students).

4.2. Data Analysis

Data were analysed descriptively using frequencies, percentages, and arithmetic means. Only survey items explicitly selected for analysis were included, in order to focus the study on questions directly aligned with the research objectives related to Challenge-Based Learning and course design. Survey items addressing administrative aspects, general demographics, or elements not directly relevant to the evaluation of CBL integration were excluded to ensure analytical clarity, reduce redundancy, and avoid over-interpretation of exploratory data. Horizontal bar charts were generated for all included survey questions and are referenced in the Results section. The two Moodle-based surveys yielded different numbers of responses (course evaluation: N = 26; CBL integration evaluation: N = 20) because participation was voluntary. Consequently, the datasets represent partially overlapping but non-identical respondent groups. The standardized university satisfaction survey was analysed separately and is characterised by near-census participation in both academic years. No inferential statistical analyses were conducted; findings are therefore interpreted as descriptive and indicative rather than causal.

4.3. Results

This section presents results derived from the course evaluation survey, the CBL integration evaluation survey, and the standardized university satisfaction survey. The findings are organised into four thematic areas: respondent context, perceived educational value of the CBL project, instructional design and assessment alignment, and changes in overall student satisfaction following the introduction of CBL.

Respondent Context and Prior Experience. The respondent profile provides context for interpreting students' perceptions of Challenge-Based Learning. Most respondents identified as

graduate students, with smaller proportions reporting undergraduate status, postgraduate research roles, educational roles, or other professional backgrounds (Figure 1). Prior exposure to CBL was limited, with most respondents reporting novice or intermediate ("journeyman") experience (Figure 2). Self-assessed prior knowledge of cybersecurity fundamentals was likewise predominantly at the novice or intermediate level (Figure 3).

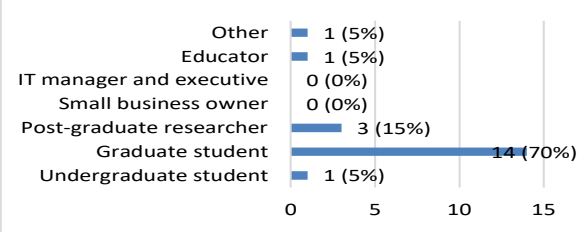


Figure 1. Distribution of respondents by academic or professional

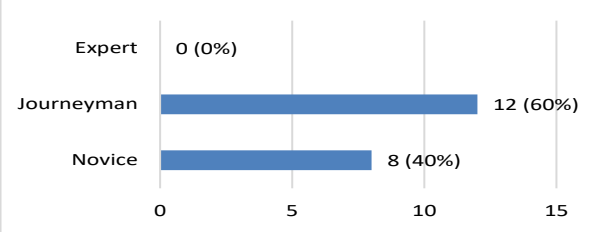


Figure 2. Students' prior experience with Challenge-Based Learning courses

Students' evaluations of the CBL module are presented in (Figure 3).

Perceived Alignment and Educational Value of the CBL Project. A clear majority of respondents agreed that participation in the CBL project supported achievement of the course learning objectives. Students also perceived the overall course design as aligned with the stated learning objectives, suggesting that the CBL project was an integral component of the course structure.

Student Engagement and Cognitive Impact of CBL. Most respondents indicated that the CBL activities supported engagement and attention throughout the course and contributed to a deeper understanding of the subject matter. Responses to a negatively worded item showed that most students did not feel lost during the CBL process, suggesting that the challenges were manageable and clearly structured.

Learning Methods and Instructional Design in the CBL-Enhanced Course. Students perceived learning outcomes as clear for individual topics (Figure 9) and reported extensive use of active learning methods alongside structured independent study activities. Collaborative learning was supported through virtual collaboration tools, and methodological diversity was observed across assignments.

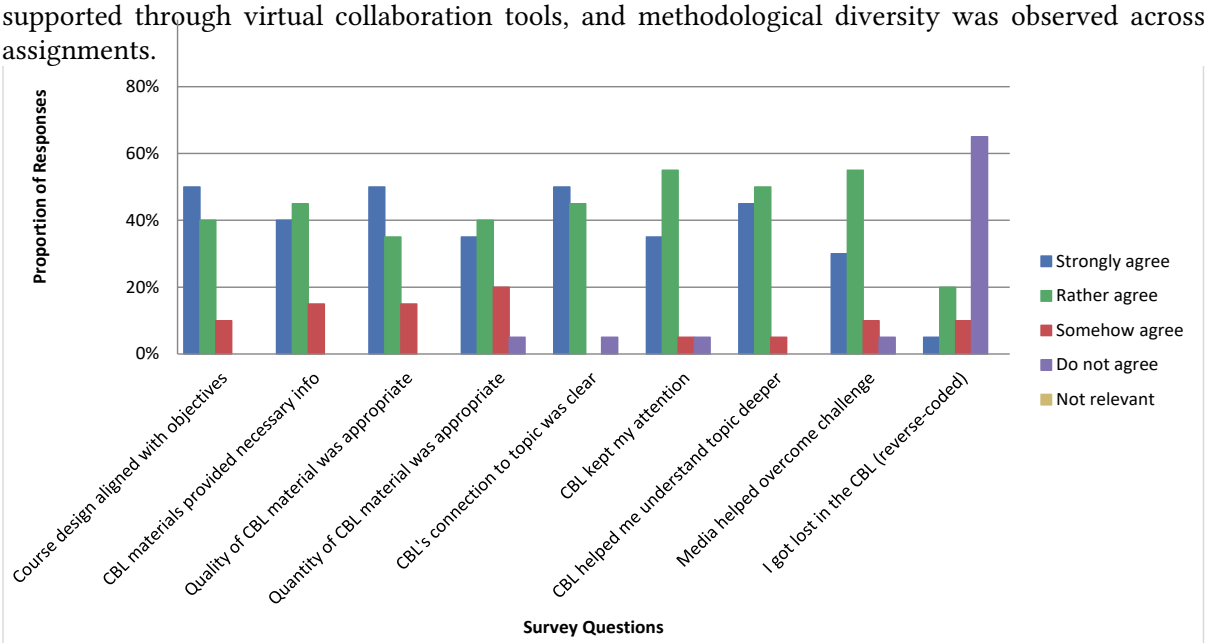


Figure 3: Students' evaluations of the CBL module

Changes in Overall Student Satisfaction Following CBL Introduction. Participation in the standardized university satisfaction survey increased slightly from 83.33 % in 2024 to 86.67 % in 2025 (Figure 4). The mean score for the statement "I am satisfied with this study module" increased from 4.19 to 4.52, while survey reliability remained constant (Cronbach's $\alpha = 0.93$), coinciding temporally with the introduction of CBL (Figure 5).

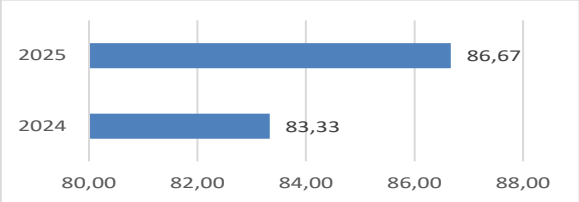


Figure 4. Participation rates in the standardized course evaluation survey (2024 vs. 2025).

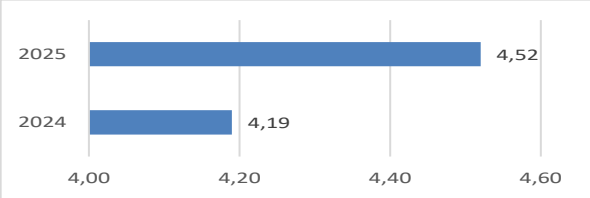


Figure 5. Average student satisfaction with the study module before and after CBL introduction.

5. Discussion and Conclusions

The introduction of a Challenge-Based Learning project into a cybersecurity fundamentals course was associated with positive student perceptions across multiple dimensions, including engagement, perceived learning depth, and alignment with learning objectives. These outcomes are consistent with prior work on problem-centred pedagogies in applied ICT domains. Importantly, students did not report widespread confusion, suggesting that appropriate instructional scaffolding mitigated potential challenges associated with open-ended learning approaches.

This study examined the integration of a CBL project into a Fundamentals of Cybersecurity course. The results indicate that the approach was well received and coincided with increased student satisfaction. For educators and curriculum designers, the findings highlight the importance of structured integration, alignment between activities and assessment, and pedagogical scaffolding when adopting CBL in technical courses.

6. Declaration on Generative AI

The authors have not employed any Generative AI tools.

7. References

1. (ISC)2 (ISC)² Research Reveals the Cybersecurity Profession Needs to Grow by 3.4 Million People to Close Global Workforce Gap Available online: https://www.prnewswire.com/news-releases/isc-research-reveals-the-cybersecurity-profession-needs-to-grow-by-3-4-million-people-to-close-global-workforce-gap-301654730.html (accessed on 22 April 2026).
2. Cheung, R.S.; Lo, H.Z. Challenge Based Learning in Cybersecurity Education. *Proceedings of the International Conference on Security and Management (SAM).*
3. Nichols, M.; Cator, K.; Torres, M. Challenge Based Learning Guide.
4. Bravo, E.; Bayram, D.; Van Der Veen, J.T.; Reymen, I. Students' Learning Gains in Extracurricular Challenge-Based Learning Teams. *European Journal of Engineering Education* **2025**, *50*, 342–359, doi:10.1080/03043797.2024.2386108.
5. Švábenský, V.; Celeda, P.; Vykopal, J.; Brisakova, S. Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges. *Computers & Security* **2020**, *102*, 102154, doi:10.1016/j.cose.2020.102154.
6. Doulougeri, K.; Vermunt, J.D.; Bombaerts, G.; Bots, M. Challenge-Based Learning Implementation in Engineering Education: A Systematic Literature Review. *Journal of Engineering Education* **2024**, *113*, 1076–1106, doi:10.1002/jee.20588.
7. Ambrosi, G.; Hermsen, E. IMPLEMENTING CHALLENGE-BASED LEARNING FOR UNIVERSITY TEACHERS.
8. Ghosh, T.; Francia, G. Assessing Competencies Using Scenario-Based Learning in Cybersecurity. *Journal of Cybersecurity and Privacy* **2021**, *1*, 539–552, doi:10.3390/jcp1040027.
9. Mukherjee, M.; Le, N.T.; Chow, Y.-W.; Susilo, W. Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information* **2024**, *15*, 117, doi:10.3390/info15020117.

10. English, R. Designing and Developing a Scenario-Based Curriculum for Cyber Education in HE. In *Cybersecurity Teaching in Higher Education*; Sikos, L.F., Haskell-Dowland, P., Eds.; Springer: Cham, 2023; pp. 59–77 ISBN 978-3-031-24215-1.