frontiers | Frontiers in Computer Science

TYPE Systematic Review
PUBLISHED 16 December 2024
DOI 10.3389/fcomp.2024.1499490

OPEN ACCESS

EDITED BY
Juan J. García-Machado,
University of Huelva, Spain

REVIEWED BY
James Harold Davenport,
University of Bath, United Kingdom
Abdallah Qusef,
Princess Sumaya University for Technology, Jordan

*CORRESPONDENCE
Ali Ahmed
✉ ali.aa@gust.edu.kw

†These authors have contributed equally to this work

RECEIVED 20 September 2024
ACCEPTED 22 November 2024
PUBLISHED 16 December 2024

CITATION
Ahmed A, Watterson C, Alhashmi S and Gaber T (2024) How universities teach cybersecurity courses online: a systematic literature review.
Front. Comput. Sci. 6:1499490.
doi: 10.3389/fcomp.2024.1499490

How universities teach cybersecurity courses online: a systematic literature review

Ali Ahmed[1,2]*, Craig Watterson[2†], Saadat Alhashmi[3†] and Tarek Gaber[4†]

[1]Center for Applied Mathematics and Bioinformatics (CAMB), Computer Science Department, Gulf University for Science and Technology, Hawally, Kuwait, [2]School of Engineering and Computer Science, Faculty of Engineering, Victoria University of Wellington, Wellington, New Zealand, [3]Department of Information Systems, College of Computing and Informatics, University of Sharjah, Sharjah, United Arab Emirates, [4]School of Science, Engineering, and Environment, University of Salford, Salford, United Kingdom

Introduction: Distance learning has seen a significant increase as educational institutions have shifted toward offering online courses. Although some institutions quickly adapted, many struggled to modify traditional materials for online learners. Time was crucial for institutions lacking experience in remote teaching. Designing engaging online cybersecurity modules for diverse students is a major challenge. With the growing popularity of online courses, it is necessary to examine the teaching methods used. This paper presents a systematic literature review on the current state of online cybersecurity education at universities. Using the PRISMA approach, the study identifies prevalent themes and addresses key research questions. This study aims to analyze academic articles to highlight key findings on how universities teach cybersecurity courses online.

Methods: The authors conducted a systematic review of scholarly articles, adhering to the PRISMA approach for the period from January 2010 to August 2024. PRISMA offers a structured approach to planning, executing, and reporting systematic reviews in various fields, including healthcare and social sciences.

Results: The review revealed several key findings on the design of online cybersecurity courses. Learner-centered approaches were commonly used, featuring active learning and practical applications. Effective instructional methods included collaborative learning, case studies, and simulations, which promoted student engagement and critical thinking. Universities emphasize practical skills evaluation and knowledge acquisition through project-based assessments. The role of IT tools was highlighted, with virtual laboratories, gamification, and simulations providing hands-on experiences, enhancing motivation, and facilitating active learning.

Discussion: This systematic review provides a comprehensive overview of the current online cybersecurity education practices in online universities. As a pioneering effort, it offers educators and curriculum developers valuable insight into designing effective online cybersecurity programmes to enhance teaching and learning practices. The review of online cybersecurity education highlighted several key findings. Learner-centered approaches, which incorporate active learning practices and practical applications, were prevalent. Effective instructional methods included collaborative learning, case studies, and simulations, which fostered student engagement and critical thinking. Assessments focused on the acquisition of practical skills and knowledge, using project-based tasks, practical exercises, and online quizzes. IT tools

played a significant role, with virtual laboratories, gamification, and simulation environments that enhanced hands-on experiences, motivation, and active learning.

KEYWORDS

cybersecurity, gamification, online education, systematic literature review, teaching, computer science

1 Introduction

Distance learning especially in computer science has seen a significant increase as educational institutions have shifted toward offering online courses. In the USA, 98% of universities have transitioned to online courses. Although some institutions quickly adapted, many struggled to modify traditional materials for online learners. Time was crucial for institutions lacking experience in remote teaching. Even before the shift, adult students (andragogical learners) preferred online programmes, and now, we anticipate a substantial increase in younger learners. For example, 63% of US students engage in online learning daily. The COVID-19 pandemic further accelerated this trend, highlighting the need for effective online education solutions.

Designing engaging online cybersecurity modules for diverse students is a major challenge. With the growing popularity of online courses, it is necessary to examine the teaching methods used. The quality of online programmes has been questioned (Wright et al., 2023) reporting that students who participate in in-person classes at least once a week reported higher satisfaction and engagement compared to those exclusively in online settings, suggesting potential quality concerns in fully online education. This paper provides the first systematic literature review (SLR) of the existing literature on this topic. The primary objectives are to review articles on university-level cybersecurity teaching methodologies, providing insight into current practices, challenges, and potential improvements. The research questions guiding this investigation include the following.

- **RQ1.** How are online cybersecurity courses designed in universities?
- **RQ2.** What IT Tools are used to teach online cybersecurity courses in universities?

This systematic review provides a comprehensive overview of current online cybersecurity education practices in universities. The insights from this study offer educators and curriculum developers actionable guidance on incorporating learner-centered strategies and leveraging IT tools, such as simulations and gamification, to enhance student engagement, motivation, and the overall effectiveness of online cybersecurity programmes. As a pioneering effort, it aims to support the development of robust online curricula tailored to meet the evolving demands of cybersecurity education.

2 Methods

2.1 Systematic literature reviews: PRISMA

In general, systematic reviews of the literature are crucial for several reasons. They provide a rigorous approach to summarizing existing knowledge on a specific topic by systematically searching, selecting, and analyzing relevant studies. In addition, systematic reviews help identify research gaps, guide future research directions, and ensure reproducibility. This research employs the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Liberati et al., 2009), a widely recognized methodology for conducting systematic literature reviews. PRISMA offers a structured approach to planning, executing, and reporting systematic reviews in various fields, including healthcare and social sciences. The guidelines outline steps for conducting a systematic review, such as identifying research questions, searching and selecting relevant studies, extracting data, assessing the quality of the study, and synthesizing the findings.

2.2 Database selection

A careful selection of databases was carried out for this systematic review of the literature (SLR) to ensure a complete and thorough review of the literature. The databases chosen were (1) IEEE, ACM, Springer, and Google Scholar. Each of these databases offers a unique collection of scholarly articles and publications, which makes them suitable for capturing a broad range of research relevant to this study.

2.3 Search terms

We combined keywords related to the teaching of cybersecurity courses in tertiary education. Below are the search terms we have used:

1. IEEE: "(University OR tertiary) AND (Cybersecurity OR "digital forensics" OR "ethical hacking") AND (online OR distance) AND (education OR teaching OR Learning) NOT ("K-12")." We then filtered the result for the period 01/01/2010 TO 01/08/2024.
2. ACM: "[[All: university] OR [All: tertiary]] AND [[All: cybersecurity] OR [All: "digital forensics"] OR [All: "ethical

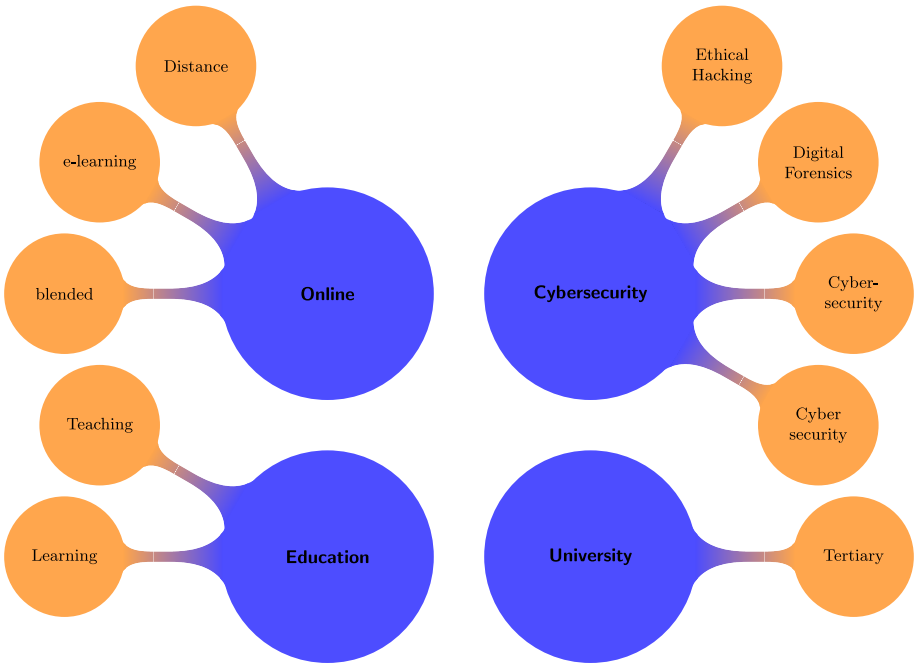

FIGURE 1
Searching terms: word synonyms.

hacking"]] AND [[All: online] OR [All: distance]] AND [[All: education] OR [All: teaching] OR [All: learning]] AND NOT [All: k-12] AND [E-Publication Date: (01/01/2010 TO 01/08/2024)]."

3. Springer: "(university OR tertiary) AND (cybersecurity OR "digital forensics" OR "ethical hacking") AND (online OR distance) AND (education OR teaching OR learning)." We then filtered the result for the period 01/01/2010 TO 01/08/2024.
4. Google Scholar: "Online, distance, e-learning Education, learning, teaching University, tertiary Cyber security, cybersecurity, cyber-security, digital forensics, and ethical hacking."

2.4 Inclusion and exclusion criteria

To ensure the selection of appropriate measurements for the review, several further criteria were established as follows:

1. The search was limited to articles published between January 2010 and end of April 2024 as this period marked significant changes in how cybersecurity is taught.
2. University Cybersecurity online (i.e., distance learning) education.
3. Papers from peer-reviewed conferences, journals, and book chapters are included.

Figure 1 shows the synonyms used for the search terms discussed in the previous subsection.

This SLR study has excluded the following:

1. Papers not written in English.
2. K-12 Cybersecurity teaching courses and cybersecurity training courses for teachers.
3. Cybersecurity awareness training.
4. Non-online courses (or courses without online provision).
5. Articles not reviewed by a peer review process.
6. Massive Open Online Courses (MOOCs).
7. Science, Technology, Engineering, and Mathematics (STEM) Courses.

Our inclusion and exclusion criteria focused exclusively on peer-reviewed research articles that contribute empirical evidence to online cybersecurity education. Experience reports and practical implementations, though valuable in computer science education, were excluded. This strategic decision aimed to ensure a rigorous examination of research findings, maintaining a clear distinction between claims supported by empirical evidence and those from practical experience.

To the authors' knowledge, the only work investigating cybersecurity education using a PRISMA SLR is Salam et al. (2023). However, that study focuses on cybersecurity education for children under 18 years of age, which differs from our objectives. Another related work, Švábenský et al. (2020), addresses broad cybersecurity education but differs in its focus on distance and online education. Finally, it is limited to papers published in SIGCSE[1] and ITiCSE.[2]

The PRISMA protocol was followed to conduct the literature search as seen in Figure 2. The findings reveal significant variation

1 https://www.sigcse.org/ (accessed November 4, 2022).
2 https://iticse.acm.org/ (accessed November 4, 2022).

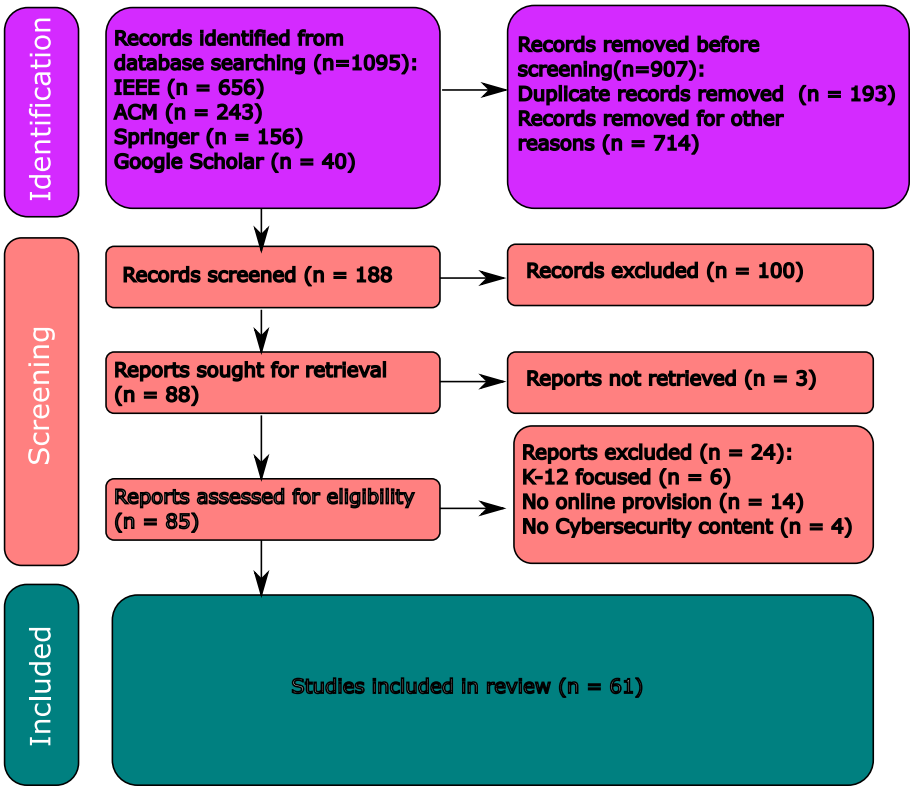

FIGURE 2
PRISMA selection process flow diagram.

in cybersecurity education content across nations, highlighting inconsistencies and gaps.

2.5 Selection process

The article review process, as depicted in Figure 2, encompassed the period from January 2010 to the end of April 2024, during which the search criteria specified produced 1,075 articles in all the databases mentioned. The first author systematically screened the article title, abstract, and conclusion sections. From the initial pool, 188 articles were selected after eliminating 907 due to irrelevance to this research project (i.e., exclusion criteria) or duplicates resulting from multiple searches. Subsequently, 100 more articles were excluded after carefully considering the articles, resulting in 88 articles being sought for retrieval. Of those 88 articles, 3 could not be recovered. Only 85 articles are assessed for eligibility. Furthermore, 24 articles are excluded, resulting in 61 articles in this review.

It is worth mentioning that Google Scholar was also used as a quality control in case some studies were missed during our IEEE, ACM, and Springer searches. For example, once all papers are tagged and common themes are generated, those themes are run against Google Scholar to check whether any related paper is missing. We identified about 10 more papers in this category (that is, included in the 61 articles under review).

It should be noted that, in addressing concerns about the potential inclusion of low-quality sources from Google Scholar, the authors of this article have implemented rigorous quality control measures to ensure the scholarly integrity of our literature review. Recognizing that Google Scholar aggregates articles from a wide range of journals and conferences, some of which may lack academic rigor, we have adhered to the following stringent criteria: (a) only journals and conferences indexed in recognized academic databases were considered, (b) all selected venues were vetted to ensure that they do not appear on established lists of predatory publishers such as those on Beall's List,[3] and (c) additional quality indicators, such as impact factors and the robustness of the peer review process, were also evaluated. These measures ensure that the sources incorporated into our study are of high academic quality and contribute significantly to the rigor and validity of our research.

Figure 3 shows the yearly distribution of relevant articles on online cybersecurity education. An observable increase in the number of publications appears from approximately 2020, potentially reflecting an accelerated shift toward online education, likely influenced by the COVID-19 pandemic. This trend, however, should be interpreted cautiously, as the data post-2020 only weakly support a positive slope (confidence level of 60%, $p = 0.4$). Interestingly, a modest upward trend in publications can also be identified in the pre-2020 data, suggesting that online approaches in cybersecurity education were gaining traction even before the

3 https://beallslist.net (accessed September 15, 2024).

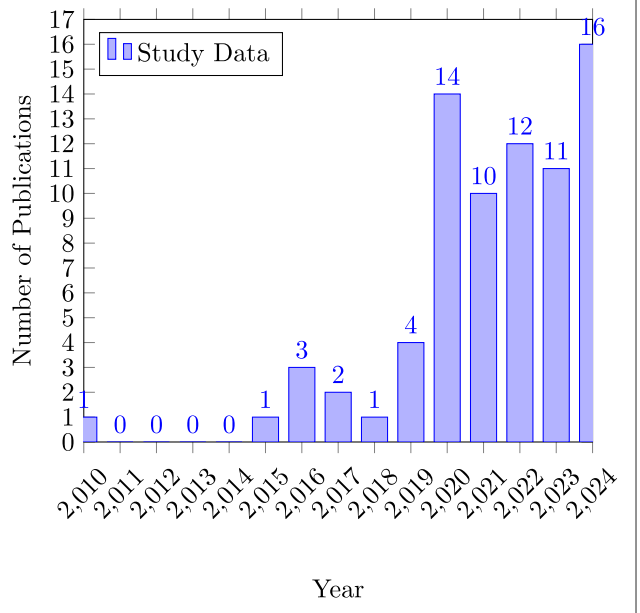

FIGURE 3
Distribution of literature survey papers from January 2010 to end of April 2024.

pandemic. Consequently, while the post-2020 surge aligns with the timing of COVID-19, overall growth may reflect a broader and ongoing interest in refining and advancing online cybersecurity teaching practices.

2.6 Thematic analysis

To identify and categorize themes such as gamification, virtual labs, collaborative learning, and project-based assessments within the articles reviewed, a thematic analysis was conducted. This process involved several structured stages to ensure consistency and accuracy.

1. Initial Coding:
   Following the inclusion of relevant articles, the first author conducted an initial reading of each article to identify recurrent patterns, terminology, and topics discussed within the context of online cybersecurity education. Descriptive codes were assigned to segments of text, capturing key elements of each article (e.g., "hands-on practice," "learner engagement," and "simulation tools").
2. Identification of Themes:
   After initial coding, related codes were grouped to form preliminary themes. For example, codes such as "gamification," "virtual labs," and "simulations" were categorized under a broader theme of "Interactive Learning Tools." This phase aimed to develop a cohesive structure by grouping similar instructional approaches and technologies relevant to online cybersecurity education.
3. Validation of Themes:
   To validate the robustness of these themes, the other authors reviewed the initial themes, where the coding structure is examined. Feedback is provided on the clarity, coherence, and relevance of the theme. Discrepancies or suggestions were discussed collaboratively, and adjustments were made to ensure that each theme accurately represented its underlying codes.
4. Refinement of Themes:
   After validation, a final iteration was conducted where themes were refined for clarity. Some broad themes were split into subthemes where necessary. For example, gamification is separated from the Information Technology Tools theme.
5. Final Thematic Framework:
   The validated and refined themes were used to synthesize findings across articles, highlighting recurring strategies and tools in online cybersecurity education. These themes inform the discussion on best practices and suggest practical approaches for educators and curriculum developers.

3 Discussion

Based on the extensive SLR conducted, numerous significant themes have emerged and are presented in the form of a visual representation in Figure 4. In the subsequent subsections, each of these themes will be examined, analyzed, and discussed in detail to shed light on their relevance to the field of study. By delving into these identified themes, a deeper understanding of how universities teach cybersecurity courses online is achieved, allowing meaningful interpretations and valuable insights to be gained.

It is essential to note that our primary goal is not to independently verify the claims presented in each surveyed paper. Instead, our emphasis lies on synthesizing diverse perspectives within the field to gain a holistic understanding of the current state of knowledge.

3.1 Course design

3.1.1 Active learning

Designing a cybersecurity course for online university students poses significant challenges that encompass various aspects. The process entails carefully considering pedagogical strategies and content delivery methods and integrating interactive learning experiences. Ensuring student engagement and motivation in a purely online environment, characterized by diverse educational backgrounds, requires the development of captivating and practical modules (Ahmed et al., 2020a,b). In addition, maintaining the quality of distance learning degree education and the expertise of teaching staff becomes a critical concern.

The work in Chung (2017) highlighted the lack of readily available curricular materials, pedagogical research, and cybersecurity courses that specifically address the challenges posed by the data deluge. The research introduces a contextual active learning approach for developing curricular modules in online informatics education to address this gap. This approach prioritizes active and contextual learning throughout the design and deployment of the module. It utilizes techniques such as student participation, problem-based thinking, case studies, and interactive question-answering and discussions, students participate in the research.

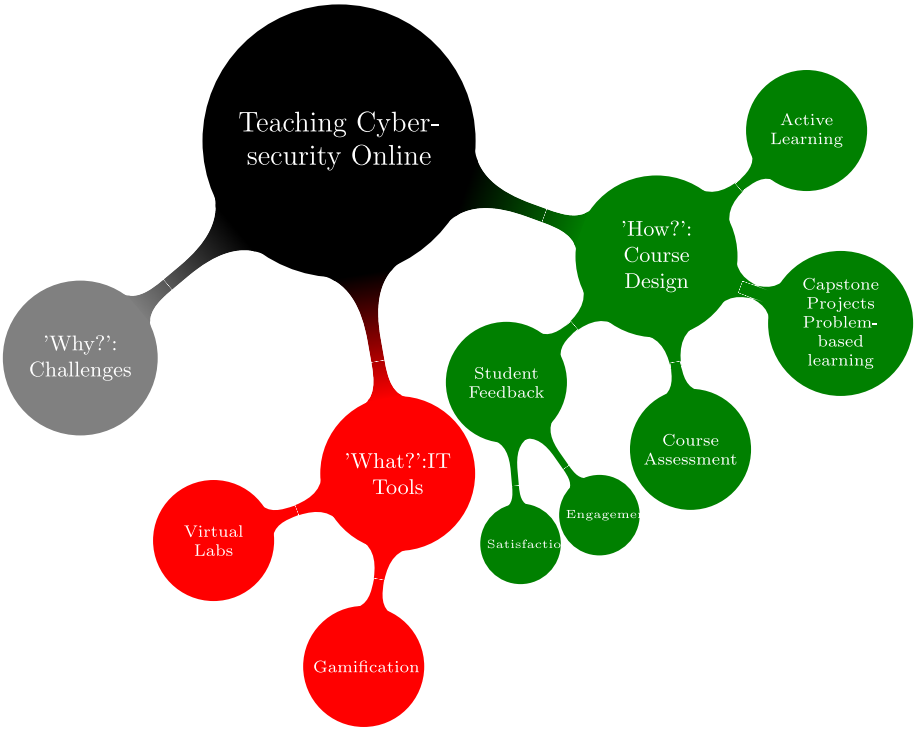

FIGURE 4
Cybersecurity online teaching literature survey: themes.

The work in Taladriz (2021) discussed the implementation of the flipped learning methodology, precisely the flipped mastery approach, which offered the advantage of ensuring deep understanding and learning of the subject matter rather than mere surface-level comprehension. It should be noted that the methodology incorporated some gamification elements, such as badges, points, and the Escape Room activity, which proved to be effective in enhancing student motivation. However, adjustments had to be made to accommodate the team-based nature of in-person classes. The use of breakout rooms during online sessions facilitated group work. Remote sessions and examinations yielded positive academic results and high student satisfaction with the methodology. Along the same line is the work of Chandrasekaran and KV (2023) that focused on the customized instructional design of the information security course, its impact on learning outcomes, student engagement, and satisfaction, providing insights into the effectiveness of online course delivery in the context of cybersecurity education. The course syllabus has been carefully designed in collaboration with industrial experts, considering the job market demands skilled cybersecurity professionals. The student satisfaction index, assessed through course end surveys and informal feedback, was found to be significantly high. The work in Troja et al. (2023) highlighted the impact of the COVID-19 pandemic on teaching strategies, the challenges faced in designing gamified cybersecurity courses, the potential of Metaverse as a solution, and the intention of investigating the effectiveness of Metaverse in remote learning. The work in Affia et al. (2022) highlighted the need for innovative ways to teach cybersecurity in online classes. The work proposed using hackathons as a practical learning approach in cybersecurity education. The study explores the integration of a series of online hackathon events into an online cybersecurity course. The objective is to address issues associated with online education by fostering collaboration and enhancing students' practical understanding through solving real-world challenges. The findings suggest that the interventions introduced, which support teamwork and collaboration, maintain student participation and interest, and promote learning-by-doing, are attributed to learning benefits by students.

The work in Srivatanakul and Annansingh (2022) focused on designing and developing a degree course in software and web security at York College of the City University of New York (CUNY), using active learning strategies. The rationale for the design of the course is discussed considering the knowledge and skills selected in cybersecurity. Active learning activities such as think-pair-share, buzz group, and role-play enhanced technical security and non-technical skills required in cybersecurity. The results indicate that active learning approaches contribute to the student's problem-solving abilities, solution proposal skills, and effective communication through writing and discussion, which are crucial skills in the field of cybersecurity. The work in Chung (2017) focused on developing a contextual active learning approach to create curricular modules in online informatics education. The approach emphasizes active and contextual learning in module design and deployment, incorporating student participation, problem-based thinking, case studies, and interactive question-answering and discussion. The results of an expert evaluation demonstrate strongly positive feedback and significant innovation in active learning.

The work in Whitman and Mattord (2023) examined the importance of flexible curriculum design in the context of limited faculty resources. The study focused on a Master's programme in cybersecurity that maximized faculty productivity and incorporated part-time staff to deliver a fully online programme. This new dimension has not been studied extensively before (that is, faculty resources to teach the cybersecurity programme due to lack of expertise in the field, for example). In addition, the research highlighted the need to adapt the curriculum to meet the needs of specialized groups of employers and students when faced with resource constraints.

By prioritizing a human-centered approach, active learning in cybersecurity education programmes empowers students to effectively tackle cyber risks through problem-solving and decision-making. The work in Waddell (2024) underscored the need to integrate human-centered approaches into cybersecurity education, particularly within healthcare settings. It advocates for educating and training staff to effectively mitigate cyber risks alongside technical safeguards. Inspired by practices in industries such as aviation, the paper outlines a customized cybersecurity education programme for healthcare, focussing on dynamic delivery options, social engineering simulations, role-based training, and engagement with stakeholders.

There is a need for education in AI security, recognizing its significance in today's society. Although the work in Mamatnabiyev et al. (2024) is not entirely designed for cybersecurity courses, it introduced a holistic approach to using educational robots in Computer Science education, showcasing the feasibility of employing an open-source robot, FOSSbot, for various courses including cybersecurity ones. By integrating multiple sensors and actuators, FOSSbot supports customization and extension across different course requirements. The results demonstrate improved student performance and engagement, both in formal university settings and in informal educational contexts, validating the effectiveness of employing FOSSbot. The work in Arai et al. (2024) design REN-A.I., a video game aimed at educating users about AI security, filling the gap in educational resources in this domain. Through hypotheses focused on simulating AI attacks and countermeasures in a video game environment, the paper explores the effectiveness of REN-A.I. in improving users' awareness of AI security, particularly through episodic memory.

3.1.1.1 Capstone projects

The work in Ahmed et al. (2020a,b) highlighted that online classes require specific infrastructure and may have varying hardware requirements, adding to the complexity. Another hurdle is designing a course that caters to students with diverse educational backgrounds while being pedagogically effective, engaging, and enjoyable. The work in Ahmed et al. (2020a,b) introduced an innovative approach to designing capstone projects and examined their impact on retention, completion, and success rates. The work involving students in the design process has shown promising outcomes. This approach reduces instances of plagiarism, improves the selection of diverse project topics, allows flexibility in module coverage by less experienced staff, and facilitates meeting feedback deadlines. The new approach has yielded positive results, including decreased academic integrity breaches, higher retention and completion rates, and improved overall success rates. Under the same umbrella comes the work of Carthy et al. (2018), emphasizing the advantages of international collaboration in creating teaching material and sharing knowledge in digital forensics. The work in Carthy et al. (2018) proposes an alternative approach that involves international collaboration between students from Norway and the United States. Students work together to create forensic investigation scenarios and develop educational tools for other student groups. By documenting the case, establishing a realistic evidence trail, and addressing potential errors, such as server crashes or email typographical errors, the students gain a deeper understanding of digital evidence, root cause analysis, and file provenance. This collaborative experience offers a unique learning opportunity and presents more complex assessment scenarios due to the involvement of different time zones and cultural norms. The work in Olagunju (2019) provided practical demonstrations of hands-on case-based projects to enhance understanding and learning of security risk assessments. The purpose of this project is to engage the audience by showcasing the application of theoretical concepts in real-world contexts and promoting active learning approaches in cybersecurity education.

The work in Fernández-Caramés and Fraga-Lamas (2020) proposed a methodology for teaching the Industrial Internet of Things (IIoT) and industrial cybersecurity through practical use cases and audits. The described teaching approach is blended and successfully implemented at the authors' University. Feedback from students indicates the usefulness of the proposed methodology, and the teaching results demonstrate the achievement of the course learning outcomes.

The work in Phuong (2022) combined project-based learning (PBL) and guided inquiry collaborative learning (GICL), a comprehensive framework was developed to teach a Cybersecurity Biometrics class. The framework incorporated various activities, including lab assignments, guided inquiry questions, and a semester-long project where students designed an optical fingerprint reader using specific components. The work in Gonzalez et al. (2022) highlighted a collaborative effort that led to curriculum modifications and research opportunities, including sponsored capstone projects and support for graduate teaching assistants specializing in cybersecurity education. Specialized teaching assistants have provided cybersecurity awareness training to cohorts of senior students, focussing on designing and building cybertrainer devices used by the army. The collaboration has also facilitated student internship experiences and potential job opportunities in the field while opening avenues for additional research funding in cybersecurity. The work in Andriessen et al. (2022) introduced the COLTRANE Methodology to enhance cybersecurity education by incorporating scenario-based and problem-oriented learning by presenting students with realistic situations. This approach helps bridge the gap between theory and practice and prepares students for real-world cybersecurity scenarios. Problem-based learning is essential in the instructional design of the online course on information security (Chandrasekaran and KV, 2023).

Including industry-oriented components in cybersecurity teaching in universities is crucial to bridge the gap between academic knowledge and real-world practices. It allows students to gain practical skills, understand industry challenges, and become better prepared for the dynamic and evolving cybersecurity

landscape. An industry component in teaching cybersecurity would enhance the learning experience of students, especially if workshops featuring industry experts are organized as part of the curriculum, as highlighted by Hölbl and Welzer (2017). The work in Hölbl and Welzer (2017) is interesting as it also resulted in high student satisfaction. In some programmes such as those mentioned by Ahmed et al. (2022), capstone projects are sources of industry, which improves both the learning of students and the knowledge of industrial practices. The work in Yankson et al. (2024) underscored the imperative of industry-academia partnerships in fortifying cybersecurity training and awareness to combat the pervasive threat of cybercrime. Through secondary research, it explored the impact of such collaborations on cybersecurity education and identified areas for improvement. The study proposed innovative strategies for collaboration between industry, academia, and government, highlighting the crucial role of academia in raising national cybersecurity awareness. It highlights the need for practical hands-on training to bridge competency gaps and advocates for robust strategic partnerships to review educational curricula and meet the growing demand for cybersecurity expertise.

3.1.1.2 Course assessment

Assessing cybersecurity courses, particularly in online delivery, is of paramount importance due to the critical nature of the subject matter. The effective assessment ensures that students have acquired the knowledge and skills necessary to protect information systems and networks from cyber threats. However, evaluating cybersecurity courses in an online setting presents unique challenges. Unlike traditional face-to-face classes, online courses require innovative methods to evaluate practical skills and hands-on experiences (Ahmed et al., 2020a,b). In addition, ensuring the integrity and security of assessments is crucial to maintaining the credibility and validity of the results. Addressing these challenges requires the development of robust assessment strategies that leverage technology, simulate real-world scenarios, and provide opportunities for active engagement and feedback.

Designing an innovative personalized group-based assessment in cybersecurity teaching is crucial as it enhances students' practical cybersecurity skills and fosters the development of transferable skills needed in the workplace. The work in Moldovan and Ghergulescu (2020) discussed designing and implementing an innovative personalized group-based assessment in a post-graduate network security and penetration testing module. It highlights how cybersecurity platforms can enhance students' practical cybersecurity skills and transferable skills needed in the workplace. The results of the student survey indicate that the personalized assessment approach received significantly higher ratings than a traditional non-personalized assessment.

Although the work in Crick et al. (2020) is not exclusively for online cybersecurity courses, it is an important piece of research that discusses the challenges of teaching cybersecurity in UK Computer Science degree programmes. The work examined progress, challenges, and opportunities in cybersecurity education in the UK, focussing on assessment. They addressed concerns about the quality and availability of educational resources, faculty competencies in pedagogy, progression, and assessment, and the necessary technical resources to deliver rigorous cybersecurity content. The study presented recommendations for policy and practice, including the development of effective teaching practices, faculty recruitment and professional development, and the support of diverse pathways to cybersecurity education and careers.

The work in Churi and Rao (2021) discussed the implementation of new pedagogy and assessment practices in a cybersecurity course. The aim is to design a practical curriculum rather than relying on rote learning methods. The study evaluates the effectiveness of different assessment tools, finding that the Viva voce assessment methodology[4] is not suitable for evaluating technical details and concepts in cybersecurity.

The work in Boubeta-Puig et al. (2022) described a teaching innovation experience using information and communication technologies (ICT) to enhance the evaluation and self-assessment activities in Security in Computer Systems and Risk Analysis and Management. The experience incorporated badge-based gamification strategies to engage students and encourage their interest in the subjects. The use of badges is a well-known technique in gamification (Boubeta-Puig et al., 2022). As demonstrated by Boubeta-Puig et al. (2022), the results demonstrated increased student participation and reinforced knowledge through self-assessment activities. The work in Scripcariu and Mătăsaru (2022) focused on planning online teaching activities that maintain students' interest and motivation in the studied content. The aim is to overcome challenges such as reduced focus and motivation during online learning. Short-time activities, student competitions, self-evaluation, time limits, and gaming elements are proposed as strategies to engage students and encourage active participation.

The work in Švábenský et al. (2022) addressed the challenge of assessing practical skills in cybersecurity education by proposing a method to model and visualize student progress during hands-on exercises. Two types of graph models were implemented and evaluated using data from 46 students across two universities. The findings demonstrate the benefits of graph models in assessing student progress and provide recommendations to instructors. In another work, Švábenský et al. (2022) employed data mining and machine learning techniques, specifically pattern mining and clustering, to gain insight into trainee behavior, mistakes, solution strategies, and challenging stages. This work demonstrated the suitability of data mining methods for analyzing cybersecurity training data and suggested their application in the evaluation of students, the support, and the improvement of course design.

The work in Ahmad et al. (2023) implemented a new approach to online learning called Peer Online Training (POT). The students were assigned a mini project related to ISMS, risk analysis, and incident management, involving information search, practical exercises, and industry communications. Physical training sessions and self/peer assessments were conducted, and feedback surveys and personal interviews were used to evaluate student performance. The results indicate a high student satisfaction rate that improved their understanding and skill in audit activities. The increasing demand for computer science education and the shift to online learning have highlighted the importance of online learning platforms and automatic grading. Jupyter notebooks are commonly used to teach coding skills, but auto-grading them poses challenges.

4 https://www.csu.edu.au/division/learning-teaching/assessments/assessment-types/viva-voce (accessed September 5, 2024).

To address this, Malone et al. (2023) presented a custom grading system for Jupyter notebooks integrated into a gamified learning platform for a cybersecurity course. The system focusses on design, feedback, and security, allowing students to exploit vulnerabilities while protecting the system.

Tabletop exercises represent a pioneering instructional approach applied in real-world scenarios to train teams to respond to incidents and evaluate emergency plans (Švábenský et al., 2024). INJECT Exercise Platform (IXP) supports such an innovative approach by introducing a web-based tool designed to perform and evaluate these exercises. Unlike traditional methods, IXP automates the analysis of student interaction data, improving evaluation, and offering insights into student learning.

3.2 Information technology tools

The use of IT tools in these courses is of utmost importance as it enhances student engagement, provides a better learning experience, and bridges the gap created by the absence of face-to-face education. Student engagement is crucial in online learning, and IT tools facilitate active participation and collaboration (Švábenský et al., 2023). Features such as discussion forums, chat rooms, virtual labs, and serious games allow students to connect with peers and instructors, fostering meaningful discussions and knowledge sharing. For example, gamification and serious games have emerged as powerful tools for teaching online students cybersecurity. Gamification has been used in school education for a long time and has been shown to be effective (Reddy et al., 2021). By integrating game elements and mechanics into the learning process, gamification makes cybersecurity education more engaging and interactive. It leverages the natural inclination of students to play games and fosters active participation, motivation, and knowledge retention. However, serious games simulate real-world cybersecurity scenarios and challenges, allowing students to apply their knowledge and skills in a practical context. These games provide students with a safe environment to explore cybersecurity threats, vulnerabilities, and defense strategies. They promote problem-solving, critical thinking, and teamwork, offering immediate feedback and opportunities for skill development. In general, gamification and serious games improve the effectiveness and enjoyment of cybersecurity education for online students, preparing them to face the ever-evolving challenges of the digital world.

Virtual laboratories play a crucial role in online cybersecurity education by providing students with hands-on experience in a safe and controlled environment (Dopplick, 2015). They offer a simulated platform where students can explore and experiment with various security concepts, tools, and techniques without the risk of causing real-world harm. The work in Ledford et al. (2016) discussed the challenges of integrating cybersecurity into the undergraduate computer science curriculum and proposed a solution through the *CyberPaths* project. The work addressed the lack of sanitized labs and specialized faculty. It focused on a denial of service learning lab that received positive student feedback, indicating its effectiveness in cybersecurity education.

The work in Rahouti and Xiong (2019) discussed the challenges that instructors and students face in providing real-world cybersecurity labs in the computer science and engineering curriculum, particularly in online education programmes. The authors focused on their teaching contributions to the development of cybersecurity labs, the learning of applied cryptography through experimental modules, and the creation of a customized virtual machine. They outlined their methodology for designing the experimental modules and provided details about their pre-built Linux-based portable virtual machine. The aim is to meet the needs of students with varying academic and industrial backgrounds by offering diverse learning and experimental modules. Universities face many challenges in providing hands-on cybersecurity training due, for example, to increasing student enrolment and the technical nature of the development of hands-on cybersecurity skills (Ksiezopolski et al., 2021). To overcome these challenges, Rahouti et al. (2021) proposed using virtual lab experiments on cloud platforms such as Amazon AWS and GENI. They describe the design and implementation of learning modules using Software-Defined Networks (SDN) on GENI for computer networking and security education. The article emphasized the consideration of different difficulty levels to accommodate students with varying backgrounds, and the effectiveness of the learning modules is demonstrated through student assessment. Under the same umbrella is the work of Ksiezopolski et al. (2021) that introduced the concepts and architecture of interactive and accessible cybersecurity laboratories that provide practical learning experiences.

Escape rooms have emerged as an innovative and engaging approach to teaching cybersecurity online. Escape rooms are interactive and scenario-based serious games that aim to enhance knowledge and skills in a fun and engaging way. These games incorporate elements of the learning experience, allowing learners to practice cybersecurity skills in a collaborative virtual environment. By aligning serious gaming elements with educational objectives, game designers and educators can create effective platforms for learners to develop and apply their cybersecurity skills in a gamified setting. For example, Williams and El-Gayar (2022) highlighted the advantages of using a virtual platform for a cybersecurity escape room, including easier facilitation, cost-effectiveness, and the ability to design and adapt the game for various educational outcomes. The concept map provides a framework for game designers, outlining the relationship between gamification, escape room components, and learning skills. The virtual escape room prototype demonstrates its potential in teaching social engineering, password security, and binary concepts, promoting learner understanding and interest in cybersecurity. Taladriz (2021) has incorporated the concept of escape rooms in their work. The work of Malone et al. (2023) has also used a version of an escape room but called it a gamified virtual lab that improved the overall student performance.

The work in Kebande (2024) explored the use of Virtual Laboratories (V Labs) in cybersecurity distance courses, focussing on their impact on active learning (AL) and student engagement. A survey was conducted in Blekinge Tekniska Högskola, Sweden, involving learners and educators experienced with V Labs in their courses. The response rates were 29% for the learners and 73% for the educators, the survey results indicating a positive perception

of V Labs in enhancing AL in cybersecurity education. The findings highlight that V Labs are considered engaging, interactive, and effective in fostering a better understanding of cybersecurity concepts, emphasizing their role in improving AL and problem-solving skills in remote education settings.

Several recent pieces fall under the use of technological platforms that support the teaching of online cybersecurity courses. The following briefly summarizes them:

The work in Moran et al. (2024) introduced tabletop exercises as an effective teaching method and presents the INJECT Exercise Platform (IXP), a web-based tool designed to conduct and evaluate these exercises. Unlike traditional methods, IXP offers automated analysis of student interaction data, enhancing evaluation, and providing insights into student learning. The work shared teaching experience and data from a cybersecurity course utilizing IXP over 3 years, highlighting its benefits for computing education.

The work in Nelson and Shoshitaishvili (2024) introduced DOJO, a cutting-edge open-source learning platform tailored for hands-on cybersecurity education, drawing inspiration from the Capture The Flag (CTF) community's innovative approach. DOJO offers a fully featured learning environment accessible from any browser, empowering students to engage in coding, shell interaction, and network exploration.

The work in OConnor et al. (2024) addressed the critical need to integrate vulnerability research into cybersecurity curricula to address the shortage of workers in the field. Leveraging lightweight, container-based virtualisation, the paper presents an undergraduate course design focussing on vulnerability research. Through hands-on methodology, students are challenged to develop complex binary exploits throughout lectures, labs, and exams.

The work in Rao and Elias-Medina (2024) addressed the cybersecurity workforce shortage by proposing the development of cybersecurity education courseware tailored for Internet of Things (IoT) applications. The work emphasized the importance of hands-on labs in enhancing students' knowledge and skills in securing cyber-physical systems, contributing to bridging the cybersecurity skills gap.

3.3 Gamification

Using gamification in cybersecurity teaching increases the level of participation of the student (Scripcariu and Mătăsaru, 2022). Gamification does not need significant effort since it could be as simple as using badges to improve student motivation (Taladriz, 2021) or utilizing some free gamified platforms such as Kahoot as (Matovu et al., 2022) investigated. Gamification is also a good means of assessment. Although the specific details of the gamification implemented by Karagiannis et al. (2020a,b) are not explicitly mentioned, the work discussed the classification of gamification and game-based learning tools and approaches related to information security and privacy. It explored various methods and tools that can be used to engage students, employees, and trainees in security and privacy programmes for education and awareness. The comparative study by Chicone and Ferebee (2020) explored gamification in cybersecurity education, specifically focussing on the Facebook Capture the Flag (CTF) platform and CTFd. The study replicated a previous investigation and examined the assessment capabilities of both platforms. The findings reveal that while Facebook's CTF has limited assessment features, CTFd[5] offers valuable formative assessment tools that benefit both students and faculty in identifying areas for future learning and improvement. The work in Karagiannis et al. (2020a,b) presented a comparative evaluation of four popular open-source CTF platforms for their suitability for learning purposes. Through a comparative study and one-on-one interviews, the advantages and disadvantages of each platform were identified, providing information for organizers to choose the most appropriate platform. The study also discussed additional features that could improve the platforms. In the context of the Ionian University in Greece, CTFd was found to be the most suitable platform for setting up a hands-on lab and was deemed effective in terms of teaching presence for learning purposes. The work in Malone et al. (2023) used the Riposte platform, a gamified online learning platform for computer science and cybersecurity education. The platform incorporates key features that help facilitate learning. The platform aims to make the learning experience more engaging and motivating for students by applying gamification elements, such as turning exercises into a game. The use of hands-on exercises and gamification elements in a distance learning environment enables the teaching of various cybersecurity concepts effectively. The gamification implemented by Sookhanaphibarn and Choensawat (2020) involved creating five games to increase cybersecurity awareness among children and youth. The games covered various aspects of cybersecurity, such as protecting laptops against cybercrime, complying with computer laws while using social media, understanding viruses and malware, and smart usage of IT and Internet settings. The user evaluation was conducted with undergraduate students, and the results indicated that the games were easy to play and effectively increased knowledge and usefulness.

The work in Giboney et al. (2021) presented Cybermatics PCS, an educational simulation that offers students a realistic cybersecurity experience. It combines elements of educational simulations, case studies, and alternative reality games. The study involving 111 students demonstrates its effectiveness in improving the understanding of penetration testing, boosting programming confidence, and generating interest in cybersecurity careers. The findings emphasize the value of experiential instruction and provide insights for designing authentic learning experiences. The authors hope that Cybermatics PCS will inspire more innovative educational approaches to address the growing demand for cybersecurity professionals. The work in Malone et al. (2021) introduced an online gamified learning platform for the learning of computer science and cybersecurity. The platform offers exercises in a custom game in which students can apply their skills in various areas, such as password security, web security, and reverse engineering. The work highlighted the unique features of the platform, including its distributed infrastructure, game engine, integrated development environment, automated feedback system, and support for individualization.

5 https://github.com/CTFd/CTFd (accessed September 6, 2024).

The use of gamification in recent years continues in cybersecurity online education. For example, the work in Williams et al. (2024) delved into the utilization of gamification and game-based learning to enhance cybersecurity education, particularly for students with non-cyber backgrounds. By designing Capture The Flag (CTF) competitions as cybersecurity frameworks/games, the study demonstrates their effectiveness in engaging students across various disciplines and educational levels. The gamified approach not only increases interest in cybersecurity but also fosters skills such as collaboration, critical thinking, and problem-solving. Moreover, the paper suggests that gamified learning can be adapted to other academic modules and interdisciplinary subjects, promoting cultural inclusion and broadening students' perspectives. The work in Criollo-C et al. (2024) investigated the effectiveness of a game-like mobile application, CiberSecApp, in teaching basic cybersecurity to users, to mitigate risks associated with online activities. Unlike previous studies that focus solely on game design, this research also evaluates user experience using the IBM Computer Usability Satisfaction Questionnaires (CSUQ) and the NASA Task Load Index (TLX). The results suggested that gamification can effectively support cybersecurity education by fostering user motivation and minimizing cognitive stress, highlighting the potential of mobile apps as innovative educational tools for improving cybersecurity awareness and practices.

The adoption of emerging technologies, particularly virtual/Augmented/Extended/Mixed Reality (VR/AR/XR/MR), is advocated to improve cybersecurity education, training, and awareness (Wagner and Alharthi, 2023). Although virtual meeting platforms such as Zoom and Google Classroom are considered sufficient for some aspects of remote teaching, there is a need for platforms that could replicate the hands-on interaction of a physical classroom while addressing distractions and engagement issues as studied by Troja et al. (2023). They explored the potential of using the Metaverse, a virtual reality space, for cybersecurity learning and teaching. Regarding platforms, Topham et al. (2016) argued that cloud-based virtualisation is an effective platform for cybersecurity teaching in online education. This approach uses cloud platforms to create virtual environments in which students can practice cybersecurity concepts. It offers scalability, flexibility, and cost-effectiveness by eliminating the need for physical hardware. Instructors can easily set up complex scenarios and assess students' skills in a safe environment. The hands-on training opportunities and collaboration that cloud-based virtualisation has facilitated prepare students to tackle real-world cybersecurity challenges. In fact, Rahouti and Xiong (2019) addressed the challenges that instructors and students face in providing real-world cybersecurity laboratories for training. They developed a range of cybersecurity labs, including applied cryptography learning modules and a customized virtual machine. The methodology for designing the experimental modules and the details of the pre-built Linux-based portable virtual machine are presented. The work in Knorr (2020) addressed the challenges in teaching cryptography to IT security students and proposed an approach using test-driven software development techniques. The practical experience (i.e., using an online client/server system) gained from courses with approximately 30 students is discussed, highlighting the benefits of automated tests and immediate feedback for learning. The proposed setup helps students focus on improving their software and offers a means to assess their understanding through weighted test cases, even in an exam setting. The work in Moldovan and Gherguleseu (2020) offered an overview and classification of the cybersecurity platforms available in the market. The paper also presents a case study in which personalized group-based assessments were incorporated into a network security and penetration testing module, demonstrating how such platforms can enhance practical cybersecurity skills and transferable workplace skills. The student survey results indicate that the personalized assessment approach received significantly higher ratings than traditional non-personalized assessments.

4 Results

Table 1 represents an organised listing of themes identified in the SLR, along with the papers that fall under each theme. Each row corresponds to a specific theme, with the associated papers cited, offering a clear depiction of how the literature is distributed across various thematic areas.

4.1 How are online cybersecurity courses designed in universities?

To address the question of how cybersecurity courses are designed online, we conducted a systematic literature survey. This survey identified a common theme of "course design" that encompasses various concepts and practices. These include the following:

1. Active Learning Practices: Many online cybersecurity courses incorporate active learning strategies to engage students and enhance their learning experience. Our research shows that approximately 11% of the articles surveyed in this study show an element of active learning practices. These practices may involve interactive exercises, group discussions, case studies, simulations, and hands-on activities that encourage active participation and application of knowledge.
2. Innovative Ways for Building Projects: Online cybersecurity courses often emphasize project-based learning to provide students with practical skills and real-world experience. These courses may incorporate innovative approaches for designing and implementing projects, such as collaborative project work, industry partnerships, and cutting-edge tools and technologies. Approximately 24% of the papers surveyed in this study fall into this category (that is, Innovative Ways for Building Projects).
3. Innovative Assessment Methods: Effective assessments are crucial in online cybersecurity courses to assess students' understanding and mastery of the subject matter. These courses may employ innovative assessment techniques, including practical assessments, scenario-based evaluations, ethical hacking challenges, and online platforms for automated assessment and feedback. Approximately 15% of the articles surveyed in this study fall into this category (i.e., Innovative Assessment Methods).
4. Student Feedback for Course Improvement: Many online cybersecurity courses incorporate mechanisms for continuous

improvement based on student feedback. Common feedback tools, such as surveys, discussion forums, and course evaluations, are implemented to gather student feedback on course content, delivery, and overall learning experience. This feedback helps to refine and improve the design of the course iteratively. Approximately 22% of the articles surveyed in this study discuss the use of student feedback for course improvement, indicating that it is a recognized, though not predominant, focus within online cybersecurity education.

4.2 What IT tools are used to teach online cybersecurity courses in universities?

We identified two prominent themes in the literature: gamification and the use of virtual laboratories.

1. Gamification: Gamification has become a dominant tool in online cybersecurity courses. Our research shows that approximately 27% of the articles surveyed in this study show an element of gamification. Gamification involves incorporating game elements and mechanics into learning to enhance engagement, motivation, and knowledge retention. Gamification techniques such as badges, points, and progress tracking create an interactive and immersive learning environment. Through gamification, students are encouraged to participate, compete, and apply their cybersecurity knowledge and skills in various scenarios.
2. Virtual Labs: Using virtual labs is another critical IT tool in online cybersecurity courses. Our research shows that approximately 26% of the articles surveyed in this study proposed, used, or discussed virtual labs and their importance for cybersecurity online teaching. Virtual labs provide students with a simulated environment to practice and apply their cybersecurity skills in a controlled setting. These labs typically offer a range of realistic scenarios and hands-on activities that mirror real-world cybersecurity challenges. Students can experiment with different techniques, tools, and methodologies, gaining practical experience in network security, penetration testing, incident response, and cryptography. Virtual labs enable students to develop critical thinking, problem-solving, and technical skills necessary for cybersecurity professionals.

4.3 General finding: challenges in online learning

This study reveals several challenges in the realm of online learning, accounting for approximately 20% of the articles surveyed. A notable challenge, as highlighted by Carabantes et al. (2021), was the increased number of student enrolments, which posed difficulties at the beginning of the shift to online education. Anxiety among students, as mentioned by Ahmed et al. (2021), and issues related to course structure and assessment, as described by Crick et al. (2020), were also significant concerns.

In the context of cybersecurity courses, Bai et al. (2020) studied the adaptations required for effective online delivery. They emphasized the importance of meeting the diverse needs of students, including those without access to technology, to ensure a comfortable learning environment. Although replicating internships and network labs online presents challenges, alternative approaches such as temporary jobs related to skills and staggered networking sessions have been explored.

The transition from traditional to online courses, especially during sudden disruptions such as the COVID-19 pandemic, highlighted the need to reconsider conventional teaching methods. As Ryane (2022) pointed out, the students faced significant disruptions in their social lives, some experiencing personal losses. Institutions that spontaneously switched to online delivery faced challenges in measuring class participation. Gamification, as proposed by Taladriz (2021), and the use of Metaverse, as suggested by Troja et al. (2023), are potential solutions to improve engagement.

Hands-on laboratory exercises and access to laboratories for student assignments became difficult during the transition to online learning. As noted in Troja et al. (2021), the provision of laptops for students, despite the various hardware configurations, made troubleshooting and configuration a burden for faculty members. Privacy concerns also hindered group work in technical labs due to the limitations of remote keyboard control features. Instructors faced challenges in overseeing and reviewing individual student work, which affected instructional capacity.

In general, while the COVID-19 pandemic underscored these challenges, our analysis of the study findings suggests a broader need for adaptive strategies in online learning to address various obstacles and improve educational results.

5 Limitation, conclusion, and future work

Despite offering valuable insights, this review has several limitations. First, the study is limited by the scope of available literature, which may exclude emerging practices and tools not yet widely documented. In addition, the reliance on the PRISMA framework, while systematic, inherently depends on publication bias within the field, possibly overlooking unconventional or unpublished approaches to cybersecurity education. Another limitation is the lack of empirical validation of the reported practices; while the literature suggests effective methods, the actual impact on learning outcomes, especially in long-term skill retention and real-world application, remains under-studied. Finally, given the global nature of online education, the review does not extensively address regional or cultural variations in educational practices that may influence the effectiveness of teaching strategies in diverse contexts. Future studies could aim to address these gaps by conducting comparative analyses across different cultural settings and directly assessing the efficacy of instructional techniques.

This paper presents a systematic review of the literature conducted to investigate the current state of the art in the teaching of cybersecurity online by universities. Adherent to the PRISMA approach, a comprehensive analysis of scholarly articles and research papers was performed to identify the prevalent themes and address the research questions that guided this study.

TABLE 1 SLR themes-articles mapping.

Themes	Concepts	Papers
Course design	Active learning practices	Troja et al., 2023; Chandrasekaran and KV, 2023; Affia et al., 2022; Srivatanakul and Annansingh, 2022; Taladriz, 2021; Chung, 2017; Waddell, 2024; Mamatnabiyev et al., 2024
	Innovative projects & Hands-on	Ahmed et al., 2020a,b; Phuong, 2022; Gonzalez et al., 2022; Olagunju, 2019; Carthy et al., 2018; Hölbl and Welzer, 2017; Rajab, 2018; Chandrasekaran and KV, 2023; Andriessen et al., 2022; Chung, 2017; Affia et al., 2022; Fernández-Caramés and Fraga-Lamas, 2020; Yankson et al., 2024; OConnor et al., 2024; Arai et al., 2024; Rao and Elias-Medina, 2024
	Course assessment	Ahmed et al., 2020a,b; Crick et al., 2020; Moldovan and Ghergulescu, 2020; Churi and Rao, 2021; Boubeta-Puig et al., 2022; Scripcariu and Mătăsaru, 2022; Ahmad et al., 2023; Malone et al., 2023; Švábenský et al., 2024; Nelson and Shoshitaishvili, 2024; Kim et al., 2024
	Student feedback	Raj and Savacool, 2010; Hölbl and Welzer, 2017; Bai et al., 2020; Knorr, 2020; Moldovan and Ghergulescu, 2020; Giboney et al., 2021; Boubeta-Puig et al., 2022; Srivatanakul and Annansingh, 2022; Affia et al., 2022; Tchoubar et al., 2022; Ahmad et al., 2023; Chandrasekaran and KV, 2023
IT tools	Gamification	Karagiannis et al., 2020a,b; Malone et al., 2021; Sookhanaphibarn and Choensawat, 2020; Taladriz, 2021; Giboney et al., 2021; Boubeta-Puig et al., 2022; Williams and El-Gayar, 2022; Matovu et al., 2022; Scripcariu and Mătăsaru, 2022; Troja et al., 2023; Williams et al., 2024; Mamatnabiyev et al., 2024; Rajendran and Sundarraj, 2024; Arai et al., 2024; Criollo-C et al., 2024
	Platforms and other tools	Ahmad et al., 2023; Carabantes et al., 2021; Troja et al., 2021; Fernández-Caramés and Fraga-Lamas, 2020; Rahouti and Xiong, 2019; Samonte et al., 2023; Švábenský et al., 2023; Kebande, 2024; Švábenský et al., 2024; Nelson and Shoshitaishvili, 2024; OConnor et al., 2024; Rao and Elias-Medina, 2024
Contingencies	COVID-19 impact	Bai et al., 2020; Fernández-Caramés and Fraga-Lamas, 2020; Crick et al., 2020; Taladriz, 2021; Troja et al., 2023; Carabantes et al., 2021; Jovanović et al., 2022; Gonzalez et al., 2022; Ryane, 2022; Whitman and Mattord, 2023; Ahmed et al., 2020a,b

The review revealed several noteworthy findings regarding the design of online cybersecurity courses. Learner-centered approaches were commonly employed, characterized by active learning practices and practical applications of cybersecurity concepts. Collaborative learning, case studies, and simulations were identified as effective instructional methods that encouraged student engagement and critical thinking. Regarding assessment techniques, universities emphasize the evaluation of practical skills and knowledge acquisition in online cybersecurity courses. Project-based assessments, practical exercises, and online quizzes were prevalent to gauge student proficiency. Furthermore, the review highlighted the prominent role of IT tools in cybersecurity education online. Virtual laboratories, gamification, and simulation environments were frequently used to provide students with hands-on experiences, enhance motivation, and facilitate active learning.

By conducting this systematic review of the literature, a comprehensive overview of current online cybersecurity education practices in universities has been provided. This information can be valuable for educators, curriculum developers, and policy makers in designing and implementing effective online cybersecurity programmes. It is essential to acknowledge that cybersecurity education online continues to evolve, with new approaches and technologies emerging. Future research endeavors should explore the effectiveness of different instructional methods, integrate emerging technologies, and evaluate learner outcomes in online cybersecurity courses.

In summary, this systematic review of the literature contributes to our understanding of the pedagogical approaches employed by universities to teach cybersecurity online. Through the synthesis and analysis of existing literature, current themes have been identified, offering insights into effective teaching practices and paving the way for future research and development in online cybersecurity education.

The following highlights the contribution of this paper:

1. This study is the first known systematic literature survey that investigates the state of teaching cybersecurity courses online by universities.
2. This SLR identifies innovation techniques in the design of online cybersecurity courses.
   (a) Learner-centered approaches with active learning practices and practical applications of cybersecurity concepts.
   (b) Effective instructional methods: collaborative learning, case studies, and simulations.
3. IT tools play a prominent role in teaching online cybersecurity courses. This includes:
   (a) Utilization of virtual labs and simulation environments
   (b) The use of gamification
4. The disruptive impact on the teaching of cybersecurity courses online is limited. However, increased enrolment and the large adoption of online and distance learning models have highlighted the need for adaptive strategies to address various challenges.

While this review synthesizes key findings in online cybersecurity education, certain areas remain under-explored. Future research could investigate the long-term effectiveness of gamification strategies in cybersecurity courses. For instance, studies might examine whether gamification impacts students' retention of cybersecurity skills over time, particularly when transitioning from virtual labs to real-world applications. In addition, the role of cross-cultural differences in online education deserves further exploration. Since online education platforms serve diverse, global audiences, understanding how instructional strategies (e.g., collaborative projects and simulations) resonate

across different cultural contexts could inform more inclusive and effective teaching approaches. Such research could provide a foundation for policy adjustments that support culturally sensitive and universally applicable online cybersecurity education practices.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

AA: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing. CW: Conceptualization, Methodology, Resources, Writing – original draft, Writing – review & editing. SA: Data curation, Investigation, Methodology, Project administration, Resources, Visualization, Writing – review & editing. TG: Investigation, Resources, Validation, Writing – review & editing.

Funding

The author(s) declare financial support was received for the research, authorship, and/or publication of this article. The article processing charges are fully covered by Gulf University for Science and Technology.

Acknowledgments

Declaration of Generative AI and AI-assisted technologies in the writing Process. The authors used ChatGPT 4o, Gramarly, and Writefull8 to improve readability and language. After using this tool/service, the author(s) reviewed and edited the content as needed and assume full responsibility for the publication's content.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Affia, A.-A. O., Nolte, A., and Matulevičius, R. (2022). "Integrating hackathons into an online cybersecurity course," in *2022 IEEE/ACM 44th International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET)*, 134–145. doi: 10.1109/ICSE-SEET55299.2022.9794183

Ahmad, R., Hassan, A., Hsiung, L. H., and Othman, M. F. (2023). "Peer online training (pot) as learning activity in computer security audit and risks management teaching module," in *Knowledge Management in Organisations: 17th International Conference, KMO 2023, Bangkok, Thailand, July 24–27, 2023, Proceedings* (Springer), 222–229. doi: 10.1007/978-3-031-34045-1_19

Ahmed, A., Lundqvist, K., Ferreira, J., and Watterson, C. (2022). "Reflections on agile software development: a conversion master case study," in *2022 IEEE Frontiers in Education Conference (FIE)*, 1–8. doi: 10.1109/FIE56618.2022.9962397

Ahmed, A., Lundqvist, K., Watterson, C., and Baghaei, N. (2020a). "Teaching cybersecurity for distance learners: a reflective study," in *2020 IEEE Frontiers in Education Conference (FIE)*, 1–7. doi: 10.1109/FIE44824.2020.9274062

Ahmed, A., Watterson, C., Baghaei, N., and Lundqvist, K. (2020b). "Distance learning practices: A reflective study," in *Proceedings of the 28th International Conference on Computers in Education. Asia-Pacific Society for Computers in Education*, 664–669.

Ahmed, A., Watterson, C., Lundqvist, K., and Ferreira, J. (2021). "Online student supervision: a reflective study on lessons and challenges," in *2021 IEEE Frontiers in Education Conference (FIE)*, 1–7. doi: 10.1109/FIE49875.2021.9637211

Andriessen, J., Furnell, S., Langner, G., Luciano, C., Quirchmayr, G., Scarano, V., et al. (2022). "Coltrane-towards a methodology and platform supported educational basis for cybersecurity education," in *Human Aspects of Information Security and Assurance*, eds. N. Clarke, and S. Furnell (Cham: Springer International Publishing), 66–76. doi: 10.1007/978-3-031-12172-2_6

Arai, M., Tejima, K., Yamada, Y., Miura, T., Yamashita, K., Kado, C., et al. (2024). Ren-a.i.: a video game for ai security education leveraging episodic memory. *IEEE Access* 12, 47359–47372. doi: 10.1109/ACCESS.2024.3377699

Bai, Y., Gao, C., and Goda, B. (2020). "Lessons learned from teaching cybersecurity courses during covid-19," in *Proceedings of the 21st Annual Conference on Information Technology Education, SIGITE '20* (New York, NY, USA: Association for Computing Machinery), 308–313. doi: 10.1145/3368308.3415394

Boubeta-Puig, J., Valle-Gómez, K., and Estero-Botaro, A. (2022). "Developing gamified activities for improving online teaching-learning processes of the security in computer systems and risk analysis and management subjects," in *EDULEARN22 Proceedings, 14th International Conference on Education and New Learning Technologies* (Palma, Spain: IATED), 9733–9741. doi: 10.21125/edulearn.2022.2346

Carabantes, D. S., Peña, F. C., and Huidobro, C. B. (2021). "Effects of the covid-19 pandemic on e-learning student's dropout levels during cybersecurity programs: a case study," in *2021 XI International Conference on Virtual Campus (JICV)*, 1–4. doi: 10.1109/JICV53222.2021.9600381

Carthy, L., Øvensen, E., Little, R., Sutherland, I., and Read, H. (2018). "Committing the perfect crime: a teaching perspective," in *Proceedings of the European Conference on Information Warfare and Security, ECCWS*, 87–95.

Chandrasekaran, J., and KV, U. (2023). An effective instructional design to enhance learning outcomes of information security course in online mode. *J. Eng. Educ. Transform.* 36:319. doi: 10.16920/jeet/2023/v36is2/23047

Chicone, R. G., and Ferebee, S. (2020). A comparison study of two cybersecurity learning systems: Facebook's open-source capture the flag and CTFD. *Issues Inf. Syst.* 21, 202–212. doi: 10.48009/1_iis_2020_202-212

Chung, W. (2017). "Developing curricular modules for cybersecurity informatics: an active learning approach," in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 164–166. doi: 10.1109/ISI.2017.8004899

Churi, P., and Rao, N. (2021). Teaching cyber security course in the classrooms of NMIMS University. *Int. J. Mod. Educ. Comput. Sci.* 13, 1–15. doi: 10.5815/ijmecs.2021.04.01

Crick, T., Davenport, J. H., Hanna, P., Irons, A., and Prickett, T. (2020). "Overcoming the challenges of teaching cybersecurity in UK computer science

degree programmes," in *2020 IEEE Frontiers in Education Conference (FIE)*, 1–9. doi: 10.1109/FIE44824.2020.9274033

Criollo-C, S., Guerrero-Arias, A., Buenaño-Fernández, D., and Luján-Mora, S. (2024). Usability and workload evaluation of a cybersecurity educational game application: a case study. *IEEE Access* 12, 12771–12784. doi: 10.1109/ACCESS.2024.3352589

Dopplick, R. (2015). Experiential cybersecurity learning. *ACM Inroads* 6:84. doi: 10.1145/2743024

Fernández-Caramés, T. M., and Fraga-Lamas, P. (2020). Use case based blended teaching of iiot cybersecurity in the industry 4.0 era. *Appl. Sci.* 10:5607. doi: 10.3390/app10165607

Giboney, J. S., McDonald, J. K., Balzotti, J., Hansen, D. L., Winters, D. M., and Bonsignore, E. (2021). Increasing cybersecurity career interest through playable case studies. *TechTrends* 65, 496–510. doi: 10.1007/s11528-021-00585-w

Gonzalez, V., Perez, O., and Romero, R. (2022). "Collaboration program to disseminate cybersecurity in the ece curriculum," in *2022 IEEE Frontiers in Education Conference (FIE)*, 1–4. doi: 10.1109/FIE56618.2022.9962613

Hölbl, M., and Welzer, T. (2017). "Experience with teaching cybersecurity," in *2017 27th EAEEIE Annual Conference (EAEEIE)*, 1–4. doi: 10.1109/EAEEIE.2017.8768496

Jovanović, V., Kuzlu, M., Popescu, O., Katsioloudis, P., Vahala, L., Wu, M., et al. (2022). Digital educational modules development for the career and technical cybersecurity pathways during the covid-19 pandemic. *Technol. Interface Int. J.* 22, 22–34.

Karagiannis, S., Maragkos-Belmpas, E., and Magkos, E. (2020a). "An analysis and evaluation of open source capture the flag platforms as cybersecurity e-learning tools," in *Information Security Education. Information Security in Action*, eds. L. Drevin, S. Von Solms, and M. Theocharidou (Cham: Springer International Publishing), 61–77. doi: 10.1007/978-3-030-59291-2_5

Karagiannis, S., Papaioannou, T., Magkos, E., and Tsohou, A. (2020b). "Game-based information security/privacy education and awareness: theory and practice," in *Information Systems*, eds. M. Themistocleous, M. Papadaki, and M. M. Kamal (Cham: Springer International Publishing), 509–525. doi: 10.1007/978-3-030-63396-7_34

Kebande, V. R. (2024). The impact of virtual laboratories on active learning and engagement in cybersecurity distance education. *arXiv preprint arXiv:2404.04952*.

Kim, Y. R., Yang, J., Lee, Y., and Earwood, B. (2024). Assessing cybersecurity problem-solving skills and creativity of engineering students through model-eliciting activities using an analytic rubric. *IEEE Access* 12, 5743–5759. doi: 10.1109/ACCESS.2023.3348554

Knorr, K. (2020). "Learning and grading cryptology via automated test driven software development," in *Information Security Education. Information Security in Action*, eds. L. Drevin, S. Von Solms, and M. Theocharidou (Cham: Springer International Publishing), 3–17. doi: 10.1007/978-3-030-59291-2_1

Ksiezopolski, B., Rusinek, D., Miskiewicz, M., and Wroblewska, A. (2021). "Hands-on cybersecurity labs in online learning," in *EdMedia+ Innovate Learning* (Association for the Advancement of Computing in Education (AACE)), 941–949.

Ledford, H., Mountrouidou, X., and Li, X. (2016). Denial of service lab for experiential cybersecurity learning in primarily undergraduate institutions. *J. Comput. Sci. Coll.* 32, 158–164.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., et al. (2009). The prisma statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. *Ann. Intern. Med.* 151, W-65. doi: 10.7326/0003-4819-151-4-200908180-00136

Malone, M., Wang, Y., and Monrose, F. (2021). "An online gamified learning platform for teaching cybersecurity and more," in *Proceedings of the 22nd Annual Conference on Information Technology Education, SIGITE '21* (New York, NY, USA: Association for Computing Machinery), 29–34. doi: 10.1145/3450329.3476859

Malone, M., Wang, Y., and Monrose, F. (2023). "Securely autograding cybersecurity exercises using web accessible Jupyter notebooks," in *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1, SIGCSE 2023* (New York, NY, USA: Association for Computing Machinery), 165–171. doi: 10.1145/3545945.3569862

Mamatnabiyev, Z., Chronis, C., Varlamis, I., Himeur, Y., and Zhaparov, M. (2024). A holistic approach to use educational robots for supporting computer science courses. *Computers* 13:102. doi: 10.3390/computers13040102

Matovu, R., Nwokeji, J. C., Holmes, T., and Rahman, T. (2022). "Teaching and learning cybersecurity awareness with gamification in smaller universities and colleges," in *2022 IEEE Frontiers in Education Conference (FIE)*, 1–9. doi: 10.1109/FIE56618.2022.9962519

Moldovan, A.-N., and Ghergulescu, I. (2020). "Leveraging virtual labs for personalised group-based assessment in a postgraduate network security and penetration testing module," in *2020 15th International Workshop on Semantic and Social Media Adaptation and Personalization (SMA)*, 1–6. doi: 10.1109/SMAP49528.2020.9248457

Moran, A., Powers, F., Campbell, L., and Rodriguez, M. (2024). The pisces approach to cyber education. *J. Colloq. Inf. Syst. Secur. Educ.* 11:5. doi: 10.53735/cisse.v11i1.190

Nelson, C., and Shoshitaishvili, Y. (2024). "Dojo: applied cybersecurity education in the browser," in *Proceedings of the 55th ACM Technical Symposium on Computer Science Education*, 930–936. doi: 10.1145/3626252.3630836

OConnor, T., Schmith, A., Stricklan, C., Carvalho, M., and Sudhakaran, S. (2024). "PWN lessons made easy with docker: toward an undergraduate vulnerability research cybersecurity class," in *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1, SIGCSE 2024* (New York, NY, USA: Association for Computing Machinery), 986–992. doi: 10.1145/3626252.3630911

Olagunju, A. O. (2019). "Mysecuritylab: a tool for teaching and learning quantitative assessments of security risks," in *Proceedings of the 20th Annual SIG Conference on Information Technology Education, SIGITE '19* (New York, NY, USA: Association for Computing Machinery). doi: 10.1145/3349266.3351349

Phuong, C. (2022). *Teaching cybersecurity: a project-based learning and guided inquiry collaborative learning approach*. Masters Theses and Doctoral Dissertations.

Rahouti, M., and Xiong, K. (2019). "A customized educational booster for online students in cybersecurity education," in *International Conference on Computer Supported Education*, 535–541. doi: 10.5220/0007767205350541

Rahouti, M., Xiong, K., and Lin, J. (2021). Leveraging a cloud-based testbed and software-defined networking for cybersecurity and networking education. *Eng. Rep.* 3:e12395. doi: 10.1002/eng2.12395

Raj, R. K., and Savacool, R. (2010). "Experiences with teaching secure data management," in *2010 IEEE Frontiers in Education Conference (FIE)* (IEEE), S3F-1. doi: 10.1109/FIE.2010.5673383

Rajab, K. D. (2018). The effectiveness and potential of e-learning in war zones: an empirical comparison of face-to-face and online education in Saudi Arabia. *IEEE Access* 6, 6783–6794. doi: 10.1109/ACCESS.2018.2800164

Rajendran, D. P. D., and Sundarraj, R. P. (2024). Designing game-based learning artefacts for cybersecurity processes using action design research: nascent design theory implications. *Bus. Inf. Syst. Eng.* 2024, 1–20. doi: 10.1007/s12599-024-00852-z

Rao, A. R., and Elias-Medina, A. (2024). Designing an internet of things laboratory to improve student understanding of secure IoT systems. *Internet Things Cyber-Phys. Syst.* 4, 154–166. doi: 10.1016/j.iotcps.2023.10.002

Reddy, L., Baghaei, N., Reinders, H., Ahmed, A., and Sardareh, S. A. (2021). Persuasion via gamification: supporting positive behaviour for learning (pb4l) school-wide pedagogy. *Res. Inf. Teach.* 2, 20–25. doi: 10.18296/set.0200

Ryane, I. (2022). "Impact of covid-19 on higher education: case study of a Moroccan Engineering School," in *Proceedings of the 8th International Conference on Advanced Intelligent Systems and Informatics 2022* (Springer), 683–691. doi: 10.1007/978-3-031-20601-6_56

Salam, R. B., Miller, V., and Franqueira, V. N. L. (2023). A systematic literature review on cyber security education for children. *IEEE Trans. Educ.* 66, 274–286. doi: 10.1109/TE.2022.3231019

Samonte, M. J. C., Banganay, K. N. U., Fernandez, K. E., and Jamena, J. N. D. (2023). Cylearn: An assistive web-based e-learning system for cybersecurity skills course. *Int. J. Inf. Educ. Technol.* 13:1889. doi: 10.18178/ijiet.2023.13.6.1889

Scripcariu, L., and Mătăsaru, P.-D. (2022). "Improving online teaching by short-time activities," in *2022 International Conference and Exposition on Electrical And Power Engineering (EPE)*, 043–046. doi: 10.1109/EPE56121.2022.9959856

Sookhanaphibarn, K., and Choensawat, W. (2020). "Educational games for cybersecurity awareness," in *2020 IEEE 9th Global Conference on Consumer Electronics (GCCE)*, 424–428. doi: 10.1109/GCCE50665.2020.9291723

Srivatanakul, T., and Annansingh, F. (2022). Incorporating active learning activities to the design and development of an undergraduate software and web security course. *J. Comput. Educ.* 9, 25–50. doi: 10.1007/s40692-021-00194-9

Švábenský, V., Vykopal, J., and Čeleda, P. (2020). "What are cybersecurity education papers about? A systematic literature review of Sigcse and Iticse conferences," in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education, SIGCSE '20* (New York, NY, USA: Association for Computing Machinery), 2–8. doi: 10.1145/3328778.3366816

Švábenský, V., Vykopal, J., Čeleda, P., and Dovjak, J. (2023). Automated feedback for participants of hands-on cybersecurity training. *Educ. Inf. Technol.* 29, 11555–11584. doi: 10.1007/s10639-023-12265-8

Švábenský, V., Vykopal, J., Čeleda, P., Tkáčik, K., and Popovič, D. (2022). Student assessment in cybersecurity training automated by pattern mining and clustering. *Educ. Inf. Technol.* 27, 9231–9262. doi: 10.1007/s10639-022-10954-4

Švábenský, V., Vykopal, J., Horák, M., Hofbauer, M., and Čeleda, P. (2024). From paper to platform: Evolution of a novel learning environment for tabletop exercises. *arXiv preprint arXiv:2404.10988*.

Švábenský, V., Weiss, R., Cook, J., Vykopal, J., Čeleda, P., Mache, J., et al. (2022). "Evaluating two approaches to assessing student progress in cybersecurity exercises," in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education*, 787–793. doi: 10.1145/3478431.3499414

Taladriz, C. C. (2021). "Flipped mastery and gamification to teach computer networks in a cybersecurity engineering degree during COVID-19," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, 1624–1629. doi: 10.1109/EDUCON46332.2021.9453885

Tchoubar, T., and Rajagopalan, S. R. (2022). "Teaching cybersecurity masters: student coding assessment and engagement with online content," in *Conference Proceedings. The Future of Education 2022*, 1–5.

Topham, L., Kifayat, K., Younis, Y. A., Shi, Q., and Askwith, B. (2016). Cyber security teaching and learning laboratories: a survey. *Inf. Secur.* 35:51. doi: 10.11610/isij.3503

Troja, E., DeBello, J. E., and Roman, N. (2021). "Teaching efficient computer science and cybersecurity courses amidst the COVID-19 pandemic," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, 510–520. doi: 10.1109/EDUCON46332.2021.9454150

Troja, E., DeBello, J. E., and Truong, L. M. (2023). "Teaching effective and gamified cybersecurity using the metaverse: challenges and opportunities," in *2023 IEEE World Engineering Education Conference (EDUNINE)*, 1–6. doi: 10.1109/EDUNINE57531.2023.10102900

Waddell, M. (2024). Human factors in cybersecurity: designing an effective cybersecurity education program for healthcare staff. *Healthcare Manag. Forum* 37, 13–16. doi: 10.1177/08404704231196137

Wagner, P., and Alharthi, D. (2023). Leveraging vr/ar/mr/xr technologies to improve cybersecurity education, training, and operations. *J. Cybersecur. Educ. Res. Pract.* 2024:7. doi: 10.32727/8.2023.32

Whitman, M., and Mattord, H. (2023). Meeting the challenges of large online graduate cybersecurity classes in the age of covid. *J. Colloquium Inf. Syst. Secur. Educ.* 10:6. doi: 10.53735/cisse.v10i1.165

Williams, L., Anthi, E., Cherdantseva, Y., and Javed, A. (2024). Leveraging gamification and game-based learning in cybersecurity education: engaging and inspiring non-cyber students. *J. Colloquium Inf. Syst. Secur. Educ.* 11:186. doi: 10.53735/cisse.v11i1.186

Williams, T., and El-Gayar, O. (2022). "Design of a virtual cybersecurity escape room," in *National Cyber Summit (NCS) Research Track 2021*, eds. K.-K. R. Choo, T. Morris, G. Peterson, and E. Imsand (Cham: Springer International Publishing), 60–73. doi: 10.1007/978-3-030-84614-5_6

Wright, G., Volodarsky, S., Hecht, S., and Saxe, L. (2023). Student satisfaction and the future of online learning in higher education: lessons from a natural experiment. *Online Learn.* 27, 335–355. doi: 10.24059/olj.v27i1.3224

Yankson, B., Berkoh, E., Hussein, M., and Dadson, Y. (2024). "The role of industry-academia partnerships can play in cybersecurity: exploring collaborative approaches to address cybercrime," in *19th International Conference on Cyber Warfare and Security*, 26–33. doi: 10.34190/iccws.19.1.2169