



Mapping Trends, Gaps and Future Directions in Cybersecurity Literacy E-Module Development Using Problem-Based Learning for Adolescents: A Bibliometric Analysis

Anggi Prasetya¹, Rayendra^{2*}, Zelhendri Zen³, Rahmi Pratiwi⁴, Tengku Hamid Darmawan⁵

¹⁻⁴Department of Educational Technology, Universitas Negeri Padang, Indonesia

⁵Literature Programme, School of Humanities, Universiti Sains Malaysia, Malaysia

*Correspondence to: rayendra@fip.unp.ac.id

Abstract: Growing exposure of adolescents to the digital environment has heightened the need to develop effective cybersecurity literacy education. Nevertheless, current instructional approaches are still largely grounded in theoretical methods and provide little practical experience, especially when it comes to embedding Problem-Based Learning (PBL) in digital learning materials such as e-modules. To address this, the current study aims to map research directions, identify gaps, and examine how PBL-focused cybersecurity literacy e-modules have evolved through bibliometric analysis. The data were collected from the Scopus database covering the years 2015 to 2025 and were analyzed using VOSviewer and Bibliometrix, with PRISMA-based screening. The analysis shows a clear increase in publications after 2019, primarily focusing on technical cybersecurity, cybersecurity education, and digital learning technologies. However, the use of project-based learning in cybersecurity literacy and e-module design remains limited and fragmented, indicating a conceptual gap between pedagogical approaches and cybersecurity content. Therefore, the study indicates that integrating problem-based learning into structured electronic modules may strengthen adolescents' critical thinking and problem-solving skills, providing a coherent framework and evidence-based guidance for further educational improvement.

Keywords: bibliometric research; cybersecurity Education; cybersecurity literacy; e-module; problem-based learning (PBL)

Recommended citation: Prasetya, A., Rayendra., Zen, Z., Pratiwi, R. & Darmawan, T. H. (2026). Mapping Trends, Gaps and Future Directions in Cybersecurity Literacy E-Module Development Using Problem-Based Learning for Adolescents: A Bibliometric Analysis. *Journal of Innovation in Educational and Cultural Research*, 7(4), 800-811.

INTRODUCTION

Adolescents are a highly active group of internet users, yet vulnerable to various online risks such as fraud, account hacking, online sexual exploitation, cyberbullying, and misuse of personal data. A review of internet safety education programs for adolescents shows that the forms of online harm targeted by these programs are diverse, including cyberbullying, sexting, online sexual exploitation, fraud, and hacking. Therefore, cybersecurity literacy education needs to be designed with appropriate, evidence-based messages to be relevant to real-life risk dynamics (Finkelhor et al., 2021; Sun et al., 2026). Systematic reviews indicate an increasing emphasis on cybersecurity awareness in youth due to heightened online security risks from widespread internet access (Quayyum et al., 2021; Rodríguez-Correa et al., 2025). Despite its high urgency, cybersecurity education in schools often remains one-way, informational, such as lectures or counseling, and lacks practical experience, even though cybersecurity competency is closely linked to the ability to apply safe procedures in real-world situations. Some studies of students between the ages of 12 and 18, based on surveys, show that although students have some knowledge of safe internet practices, this is not aligned with or reflected in their day-to-day internet practices and behaviors. Therefore, the surveys advocated incorporating formal safe internet practices into the school curriculum and indicated the need to develop and increase teachers' skills so they can promote safe internet practices and behaviors among students (Lazarov et al., 2025; Panjani & Mudgal, 2025). Time should not be a concern for educators limiting their activities, as continuing advancements necessitate that educators remain aligned with and responsive to prevailing situations and educational contexts (Prasetya, 2023).

In the area of digital education, systematic literature reviews (SLRs) do more than show what research has been done. They also highlight the challenges that come with online modifications of standard teaching materials. The development of educational designs that include lower levels of interactivity generally leads to lower levels of learner engagement. Thus, a less interactive design necessitates a more learner-centered design that aims to create and enhance experiential learning. Such a design creates and encourages learners to engage more actively in the learning process (Ahmed et al., 2024; Tan et al., 2025). Because case-oriented learning places students in complex, genuine problem situations, it is considered vital for developing students' cybersecurity literacy. This type of learning allows students to develop and reinforce critical skills such as reasoning, teamwork, and self-directed learning to address and overcome the challenges presented by the ever-changing nature of cyber threats. This problem-based learning approach further promotes the development of

critical analytical skills, strengthens cognitive flexibility, and encourages active, meaningful student engagement by delivering contextualized, hands-on learning experiences. In cybersecurity education, instructional models and teaching frameworks that emphasize hands-on practice and learner engagement through interactive learning settings are more effective than traditional approaches at developing practical, job-relevant skills. Specifically, this advantage is supported by evidence reported in studies (Khalil & Abuzir, 2024; Sockalingam et al., 2025). Recent findings indicate that the effectiveness of PBL is shaped by problem design, the chosen implementation approach, and the learning setting, and it frequently improves critical thinking and application abilities relative to traditional methods. It has been shown that PBL design must be conducted through systematic, context-sensitive planning to accommodate variability in student characteristics, problem complexity, and learning quality (Hafizah et al., 2024; Sisrayanti et al., 2024). Variations in student characteristics, problem complexity, and learning quality will continually yield differences in outcomes; thus, PBL design must be undertaken through careful and systematic planning related to the specific context (Lu & Singh, 2024).

Within the growing body of literature on cybersecurity education, current research suggests that much of the work focuses on general or higher-education contexts. Meanwhile, the systematic, structural integration of cybersecurity education into primary and secondary school levels remains insufficiently treated and only lightly examined in global reviews. Integrating cybersecurity into formal education is frequently fragmented and fails to clearly define the competencies required to support students' development from primary through secondary levels. As a result, there is an urgent need for a more structured and sustainable curriculum framework (Panagopoulos et al., 2023; Taha & Dahabiyeh, 2021). Furthermore, when analyzing the current state of cybersecurity education, including the available research on larger-scale curriculum development, focus on effective teaching strategies, such as interactive or scenario-based learning, workshops, and project-based strategies, constitutes only a small part of what is available. A majority of the literature focuses on the use of these strategies in the context of out-of-school activities, and very few of these strategies have been developed as comprehensive digital resources. One example is the e-modules that present context-based, real-world scenarios and the steps that can be followed to solve them (Arishia et al., 2024). Considering academic evaluations, current scholarship shows that while digital modules and app-based cybersecurity education frameworks have been studied, creating consistent and valid assessment frameworks that include competency indicators based on a Problem-Based Learning (PBL) model remains highly underdeveloped. Accordingly, the majority of studies in cybersecurity education have focused on measuring students' understanding of basic digital security vocabulary and constructs. Even so, these studies do not assess students' ability to think critically and solve problems, nor their ability to use risk mitigation techniques in the context of the real world.

More recent research has shown that assessment in cybersecurity education continues to focus on evaluating awareness and understanding, while elements of performance, including assessment of decision-making within real-world scenarios, have yet to be incorporated into learning evaluation frameworks (Salahdine & Kaabouch, 2019; Baioni et al., 2024). Furthermore, a methodological meta-analysis found that most selected studies focus on solitary techniques, including gamification and mobile app development, and fail to meaningfully discuss pedagogical techniques that incorporate problem-based learning and the construction of cybersecurity literacy e-modules. This has resulted in a profound gap in the application of active learning and the scaffolding of digital resources, which has the potential to restrict the outcome of investigations to formal learning design in secondary education (Mukherjee et al., 2024). The literature shows that cybersecurity literacy e-module designs that consistently integrate Problem-Based Learning (PBL) approaches for adolescents remain limited and poorly structured. Most studies focus more on improving conceptual knowledge than on measuring problem-solving skills and implementing security strategies in authentic situations. Furthermore, there is no integrated pedagogical framework that connects PBL principles with academically replicable digital module designs. Therefore, a comprehensive synthesis of cross-disciplinary studies is crucial for formulating pragmatic, evidence-based recommendations for advancing formal learning initiatives targeting adolescents. Given the identified research gaps, this investigation aims to conduct a systematic and methodologically rigorous literature review to provide a comprehensive assessment of the current and future landscape of cybersecurity education (Sulich et al., 2023; Sulich & Sołoducho-Pelc, 2025).

METHODS

This research uses a bibliometric analysis approach, employing quantitative methods to evaluate and map the development of the scientific literature based on publication databases, citations, keywords, and collaborative relationships between authors and countries (Donthu et al., 2021). Bibliometric analysis enables the identification of research growth patterns, the intellectual structure of a field, and thematic trends in the evolving state of affairs over time in an objective, data-based manner (Aria & Cuccurullo, 2017; Ali et al., 2025). This approach was chosen because it provides relevant data output that provides a comprehensive picture of the dynamics of research on cybersecurity literacy, problem-oriented learning, and the development of electronic modules in the context of youth education.

Bibliographic data were extracted from internationally recognized scientific databases, Scopus and/or Web of Science. These two resources are the most familiar and most referenced in bibliometric studies to ensure quality control of bibliometrics and citations, as well as coverage of international journals (Mongeon & Paul-Hus, 2016; Shaikh & Güngör, 2025). The search method was formulated using various combinations of keywords and Boolean logic, such as: "cybersecurity literacy" OR "cybersecurity education" AND "problem-based learning" OR "PBL" AND "e-module" OR "digital module" AND "adolescents" OR "high school". To help monitor the growth of the research, a time frame for the publications of 2015–2025 was established. All search results are exported in a bibliographic format (CSV or BibTeX) that includes authors, titles, year of publication, source, abstract and keywords, and citation count. The dataset is then processed to remove duplicates, harmonize authors, and fix metadata inconsistencies. Data cleansing is the most important step in bibliometric analysis primarily because it establishes the foundation to yield accurate results in network mapping and scientific visualization (Zupic & Čater, 2015; Alhuay-Quispe et al., 2022). The document identification and screening process was conducted continuously to ensure alignment of the documents with the research. This step entails initial document identification in the database, removal of duplicates, title and abstract screening, and making the final inclusion decision based on relevance to the research. The process used to select the data is illustrated in Figure 1.

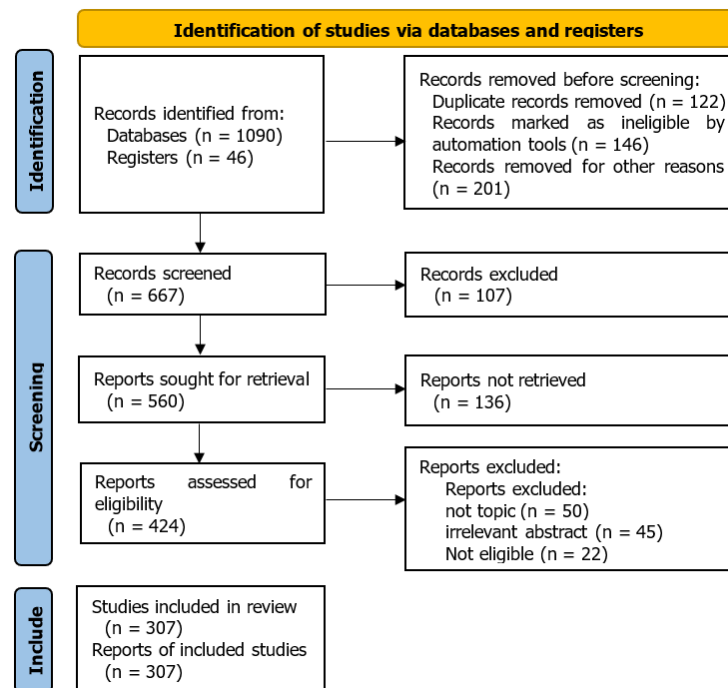


Figure 1. PRISMA on Artificial Intelligence in Education Publication

In relevant studies, selection of manuscripts alternates with the public relations and integrated scanning model (PRISMA) to meet PRISMA standards for flexibility and methodological rigor. During the identification process, approximately 1,136 records were created, including 1,090 primary articles with 46 additional records from secondary databases. A preliminary sifting and cleansing process identified and eliminated 469 records (41.29%). Duplicate records ($n = 122$) were reviewed and excluded by automated systems ($n = 146$) and by the reviewers ($n = 201$). In total, 667 records (58.71% of total records) moved to the next step of title and abstract filtering. To apply a selection method that is precise, rigorous, and meaningful, a large number of irrelevant and overlapping publications present a primary challenge to contemporary systematic reviews of the literature (Kolaski et al., 2023).

During the screening process, 107 records, or 16.04% of the screened articles, were categorized as irrelevant, resulting in 560 reports (49.29% of the original total) requiring full-text retrieval. Subsequently, full-text reports were not retrieved for 136 reports (24.29% of those requested). Thus, 424 articles (37.32% of the original total) were reviewed for eligibility. Based on the reviews, 117 articles (27.59% of the reviewed articles) were removed. Of the 117 articles removed, 50 ($n = 50$) had mismatched themes, 45 ($n = 45$) had irrelevant abstracts, and 22 ($n = 22$) did not meet eligibility criteria. Based on the review process, 307 articles, constituting 72.41% of the articles reviewed for eligibility and 27.03% of the total articles, were incorporated in the final analysis. The multistage filtering process underscores the importance of methodological screening in bibliometric research conducted in rapidly growing fields with a high degree of fragmentation (Ma & Ismail, 2025).

The final stage included 307 studies selected for the systematic review following the specified criteria. This methodology helped eliminate bias by refining the screening design and selection process used to include studies in the systematic review. After completing the selection process, VOSviewer was used to analyze the

data and demonstrate co-authorship networks, co-citations, and keyword occurrences to elucidate thematic clusters and identify intellectual linkages among the selected studies (Van Eck & Waltman, 2010; Hassan & Duarte, 2024). Additionally, the Bibliometrix software package, an R package, is employed for advanced descriptive analysis, such as annual publication trends, the most productive journals, and the most influential authors and institutions (Aria & Cuccurullo, 2017). This study design is based on principles of transparency, replicability, and methodological rigor. These principles are illustrated in Figure 2.

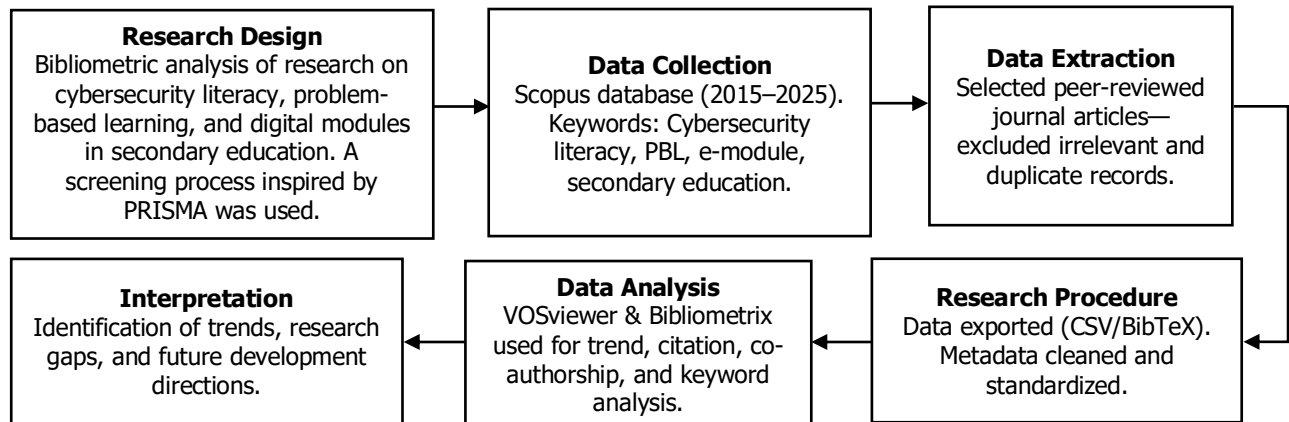


Figure 2. Research Flowchart

The research workflow begins with study design and bibliometric analysis, alongside data collection from the Scopus database covering the years 2015 to 2025. This is followed by article screening based on the PRISMA methodology. The subsequent workflow steps include the extraction and refinement of metadata, data normalization, and analysis through the Bibliometrix package to reveal citations and collaborations and the research area's conceptual framework. This figure substantiates the claim that the methodological framework for bibliometric research was systematically and holistically applied at each step to maintain the integrity of the research corpus, minimize research bias, and enhance the methodological rigor of bibliometric research (Donthu et al., 2021).

RESULT AND DISCUSSION

Research on educational cybersecurity literacy has revealed a pronounced, sustained pattern in recent years, particularly in embedding digital security content into school curricula and building students' competencies. A recent study highlighted the need to develop a more structured and integrated cybersecurity education framework at the secondary level, both to equip students to address increasingly complex digital risks and to build competency readiness in a technology-driven economy (B. J. Blažič & Blažič, 2024). In addition, research examining how cybersecurity awareness practices and barriers are defined within educational institutions has highlighted the need for a more structured and flexible pedagogical approach that can respond to continually evolving digital threats (Arishia et al., 2024).

The bibliometric findings presented in this study are supported by empirical research demonstrating that embedding cybersecurity curricula in educational systems is not only relevant but also essential, given the limitations of available resources, the need for age-appropriate instructional materials, and the lack of pedagogical support in secondary educational institutions (Childers et al., 2025). Moreover, even in the curriculum setting, European research indicates that cybersecurity subjects are often kept separate from the formal structure of the school curriculum, despite the substantial risks. This situation calls for a more holistic and context-sensitive approach to learning (A. J. Blažič & Blažič, 2024). In addition to assessing thematic frameworks and considering conceptual linkages, it is also necessary to ascertain the geographical distribution of academic contributions to cybersecurity literacy in educational contexts. This author country mapping exercise will enable the location of knowledge production and the emerging patterns of global research collaboration concerning the advancement of the area of study to be identified.

The leading three countries are the United States, the United Kingdom, and Italy, and the United States has the greatest advantage, as seen in single-country publications (SCPs) and multi-country publications (MCPs), which show the United States taking the largest role in funding research in this area. The presence of European and some Asian nations in the top ranks supports the statement that research in educational settings and cybersecurity is a global research priority (A. J. Blažič & Blažič, 2024). The large number of MCPs also indicates active international research collaborative networks (Samodra et al., 2026). These results clearly demonstrate that progress in cybersecurity literacy within education is still primarily shaped by developed countries (Aksnes et al., 2019; Humied, 2023). Limited contributions from developing nations present the chance to enhance regional research driven by collaboration. Analysis of the authors' distribution map reveals leading researchers

who have contributed significantly to the body of work on empirical studies of educational context-related cybersecurity literacy. These researchers are credited with empirical studies based on their Scopus research citations and their publication records in the cited work (Oktarina et al., 2025; Kumar, 2025; Rodríguez-Correa et al., 2025). This identification is essential for understanding the key figures who have driven the conceptual and methodological development of this discipline (Bahamar, 2024; Tran, 2026). The following table captures ten leading researchers of cybersecurity literacy from a bibliometric perspective by way of the h-index, g-index, and m-index; total citations; and publications. This inclusion enhances research evaluation metrics by providing a value-added perspective on researchers' publication records in terms of quality and quantity, and by highlighting contextual research excellence and leading researchers in educational context-related cybersecurity literacy. Table 1 shows the key researchers in the field of educational cybersecurity literacy.

Table 1. Top Ten in the Cybersecurity Space

Author	h-index	g-index	M-index	TC	NP
Vykopal J	10	16	1.429	355	16
Čeleda P	10	14	1.429	341	14
Švabenský V	10	15	1.429	348	15
Beuran R	7	9	0.636	266	9
Deng Y	7	9	0.778	205	9
Ahmed I	5	8	0.455	92	8
Crick T	5	5	0.625	98	5
Herman GL	5	9	0.556	93	9
Huang D	5	5	0.556	123	5
Kaza S	5	8	0.455	70	13

Below, Table 2 shows the top 10 countries making the most significant impact in the field. This is assessed primarily using the h-index, g-index, total citations (TC), and number of publications (NP). The key researchers in this field are J. Vykopal, P. Čeleda, and V. Švabenský, who have the highest number of citations, indicating research productivity and impact. R. Beuran and Y. Deng also have research productivity in the field of educational cybersecurity literacy, and their work has been cited a considerable amount. There is a notable difference in the value of the m-index, indicating rapid growth in overall research in this field and correlating with overall growth in research on cybersecurity literacy. In addition to the analysis of the spatial distribution, this also includes an analysis.

Table 2. Top Contributing Countries in Cybersecurity

Countries	Articles	Articles %
USA	165	15.1
United Kingdom	27	2,5
Italy	24	2,2
India	16	1.5
Czech Republic	15	1,4
China	13	1,2
Germany	13	1,2
Malaysia	13	1,2
United Arab Emirates	11	1,0
Indonesia	10	0,9

Table 2 shows the countries with the most research on cybersecurity and education literacy. The United States published 165 papers (15.1%) and holds the most considerable dominance for the most impactful work on the world stage for research on cybersecurity education, followed by the United Kingdom (27 papers; 2.5%) and Italy (24 papers; 2.2%), as participants in this research activity from Europe. India (1.5%) and the Czech Republic (1.4%) have also published papers, and exemplify the diversification of this research. In general, it can be said that the developed countries primarily do this research. In contrast, the increasing participation of developed countries indicates the beginning of a process of international participation by developing countries in research production, as stated in a Scopus-based bibliometric study (Abdollah et al., 2025).

Countries in Asia, specifically China (1.2%), Malaysia (1.2%), and the United Arab Emirates (1.0%), showed positive participation rates. Meanwhile, Indonesia (0.9%) represents the participation rate typical of developing countries. Overall, the results show that research output is generally concentrated in developed countries, especially the United States and Western Europe, and that research from Asia is relatively more important. This reflects the developed countries having the infrastructure for research and the global sentiment of having cybersecurity literacy as a priority area of concern in education. These results agree with findings that

the United States has the highest contribution to cybersecurity research and that the concentration of research output is mainly in developed countries (Loan et al., 2021). Figure 3 provides a general overview of the dataset and complements the country-level productivity analysis. The overview creates a general bibliometric profile for the years 2015-2025 for cybersecurity literacy research in education. It captures the timing of publications, the total number of sources, the total number of documents, the annual growth rate, authors, collaboration levels, the number of keywords, the average number of citations, and the average number of bibliographic references. Together, these indicators help provide a structural evolution, collaboration pattern, and the scientific impact of the field over the last decade. The indicators suggest that the field is experiencing major structural shifts, with rapid growth in publications, strengthened collaboration networks, and a diversification of research themes across related fields, as reflected in a Scopus-based bibliometric analysis. The analysis shows a sustained increase and identifies the dominant international collaboration networks in cybersecurity research and education (Islam et al., 2026).



Figure 3. Publication Results Based on Bibliometric Analysis

Figure 3 shows that 1,090 documents were detected and processed from 452 source documents. The data reveal that the domain of cybersecurity literacy research, particularly within the context of education, learning technologies, and computer science, is evidenced by an interdisciplinary approach. The annual growth rate suggests an increase of 30.96% in research output over the past 10 years and indicates an increased focus and growing interest in implementing formal education addressing cybersecurity. This trend is an outcome of the global digital transformation and the increasing exposure and vulnerability of students to security risks in data (European Union Agency for Cybersecurity, 2023). This trajectory indicates that cybersecurity literacy is being increasingly understood not only as a technical issue but also as an essential capability within the educational framework of the 21st century. From the perspective of scientific collaboration, the participation of 2,703 contributors, along with a mean contribution of 3.53 per manuscript, underscores the importance of cooperative research efforts.

This pattern mirrors worldwide trends in education and technology research, in which cross-disciplinary collaboration is a key driver for producing pedagogical innovation (Schleicher, 2020). The international collaboration rate of 17.43% suggests that this topic is now on the international stage. However, there are considerable opportunities for creating cross-border collaborations. The authors selected 2,162 distinct keywords. This diversity reflects the different theories and methods in research on cybersecurity literacy, from research on teaching and learning to research on the development and enhancement of digital competencies. The presence of 7,500 references indicates that the research has comprehensive coverage of former studies. The average age of documents at 3.65 years illustrates that the research area is responsive to the emerging challenges of the fast-changing world of technology. Furthermore, the average citation of 5,906 per document suggests that the research field has a considerable level of impact and is growing.

These overall descriptive statistics indicate that the focus on cybersecurity literacy in education has strategically gained momentum, especially in the last few years. Because of this, it has become an area with high potential for future research. This is especially true for applying different teaching techniques, such as Problem-Based Learning, to design relevant Practical e-learning modules for youth. This sustained pattern of growth of research interest in the field indicates that, concurrently, cybersecurity literacy has gone from being an abstract idea to being a priority for the majority of researchers in the field of education. The overall positive trend of research interest in the field, particularly since 2019, with the first research period of 2015-2017, indicates that productivity in this area was very low. This trend suggests that the first research phase involved exploring the incorporation of literacy in cybersecurity education frameworks.

The analytical findings from Biblioshiny show a more consistent rise from 2018 to 2021, highlighting growing scholarly attention to the importance of digital security in technology-mediated education. This pattern is consistent with the results reported by Kraiwanit et al. (2025), who determined that the growing complexity of digital threats drives the rise in cybersecurity awareness within education. The largest surge occurred from 2023 to 2025, during which the research output trajectory increased markedly, culminating in a peak at the close of the observation period. This acceleration is likely explained by the growing need to enhance cybersecurity skills among the younger population, especially in educational settings that are becoming increasingly digitalized (Chiner et al., 2025). The rapidly expanding digital transformation has also prompted

researchers to investigate more proactive, context-driven learning strategies to develop cyber risk awareness and mitigation capabilities (Zaqueu & Mawela, 2023). However, an increase in the volume of publications does not necessarily demonstrate the level of pedagogical integration. Several studies point out that in the formal education systems, cybersecurity education focuses on the attainment of declarative knowledge, rather than developing skills for problem-solving within real-world contexts (Betuš et al., 2026). This shows that there remains a critical need for a more structured approach to teaching and problem-solving, such as Problem-Based Learning, despite the increasing body of literature. The balance of scientific rigor and impact is illustrated in the distribution of mean annual citations shown in Figure 4.

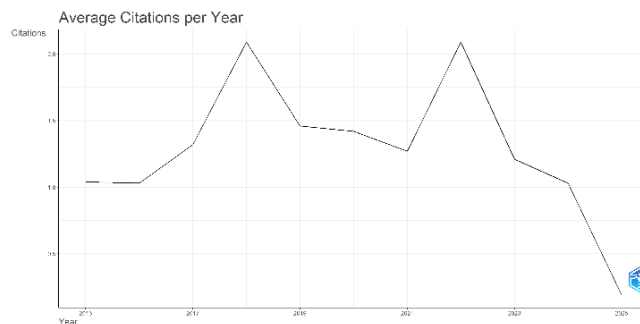


Figure 4. Trend in Average Annual Citations

Figure 4 indicates that the average number of citations per article varied throughout the defined observation period. The highest citation counts occurred at certain intervals, whereas a decline occurred in more recent years. This effect can be explained by the aggregated nature of citations, which requires time to unfold; thus, relatively recent papers have not yet had sufficient time to reach their full citation impact (Thuan et al., 2026). Moreover, beyond the documents' temporal dimension, this inconsistency may also suggest that not every publication contributes meaningful conceptual or methodological progress relevant to the development of cybersecurity education (Donthu et al., 2021). The quantitative trajectory and dynamics of this scholarly influence can be further clarified by examining the development of research themes.

This study of the development of research topics provides a fuller explanation of how thematic emphasis is changing within the body of literature on cybersecurity literacy and education. In the initial period (2015–2017), subjects including information science, computer networks, and big data were particularly salient, indicating the growing integration of information technology and data analytics within the educational framework at that time (Shaikh & Güngör, 2025). Over time, especially between 2018 and 2020, themes such as computer science education and data security became more prominent, suggesting a change in discussion from technical matters toward educational and curricular domains. More meaningful changes occurred after 2021, as terms such as cybersecurity education, cybersecurity, students, and educational computing appeared more frequently and for longer periods. This reflects a shift in the research framework from a basic focus on technical considerations to the full integration of cybersecurity into structured educational contexts (Ali et al., 2025). This pattern is consistent with research suggesting that, in educational settings, cybersecurity studies increasingly view learners as active participants in digital learning rather than passive entities requiring protection (Ulven & Wangen, 2021).

The current discourse on AI and its relation to teaching methods indicates a convergence in the thoughtful application of advanced technologies and educational frameworks in the technology education research context, in accordance with the demands for flexible and personalized learning in the digital age (Almasri, 2024). However, themes that incorporate both Problem-Based Learning and related digital module designs, along with elements of Cyber Security Literacy, have not yet surfaced as a prominent cluster. This suggests a significant gap in the related body of knowledge and the potential for further research. An analysis of the available conceptual framework in this area is undertaken through cluster mapping of document integration, which illustrates how references connect through documents to construct thematic categories; the graphical representation of the clusters is included in Figure 5.

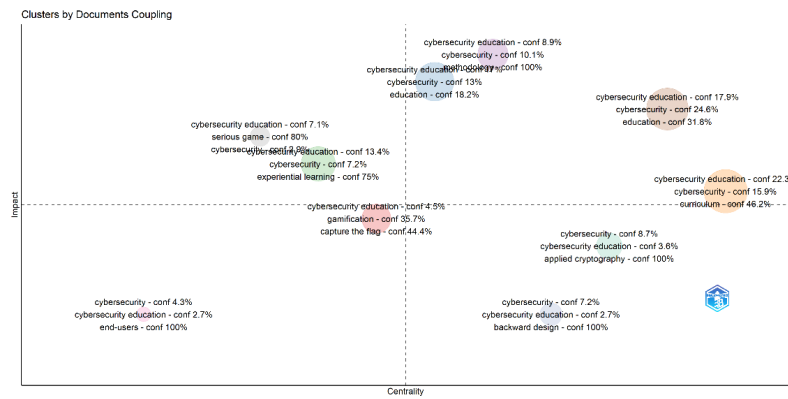


Figure 5. Research Clusters Based on Bibliographic Coupling Analysis

Figure 5 shows cluster distribution over two main dimensions: centrality, which indicates how connected topics are, and impact, which reflects the strength of influence or contribution to the field. Upper-right clusters are high centrality and high impact, represented by clusters of cybersecurity, cybersecurity education, and education. This indicates that cybersecurity education is a main focus of current research (Liu et al., 2025). Lower-right clusters, such as curriculum, applied cryptography, and backward design, show high centrality but lower impact. This indicates that curriculum and instructional design are becoming more prominent yet are still not fully incorporated into the mainstream discourse. They still lack the conceptual integration in the discourse of cybersecurity literacy (Ahmed et al., 2024).

They are, like serious games, experiential learning, and gamification, substantial alternative contributions to pedagogy, yet remain peripheral to mainstream scholarship. Game-based learning and gamification have been used within cybersecurity education to improve students' engagement, motivation, and understanding of conceptual security within the context of practical application, although the focus is often limited to higher education and particular technical skills (Bostrom et al., 2024; Pramod, 2024). Paradoxically, within these groups, although there is a high emphasis on innovative learning approaches, the intentional convergence of cybersecurity literacy, problem-based learning, and e-module development has not yet appeared as a dominant group with high centrality and high impact. This reveals a state of conceptual fragmentation in relation to the discipline of cybersecurity, whereby the integration of content, curriculum, and the design of active learning strategies is still in the early stages. This provides an opportunity for more integrative research to be conducted within this area. Overall, using document coupling to create cluster mappings revealed both central and peripheral themes and illustrated that within the literature, the integration of the technical and pedagogical aspects is less than optimal. This finding illustrates the importance of designing a learning model that aligns the three elements and incorporates a Problem-Based Learning approach in the development of a contextual cybersecurity literacy e-module for adolescents. The mapping of the co-occurrence of keywords was used to perform an in-depth analysis of the existing conceptual framework of cybersecurity and the related literature. This type of mapping shows the semantic connections between topics in the existing scientific literature. Figure 6 shows the map of this network.

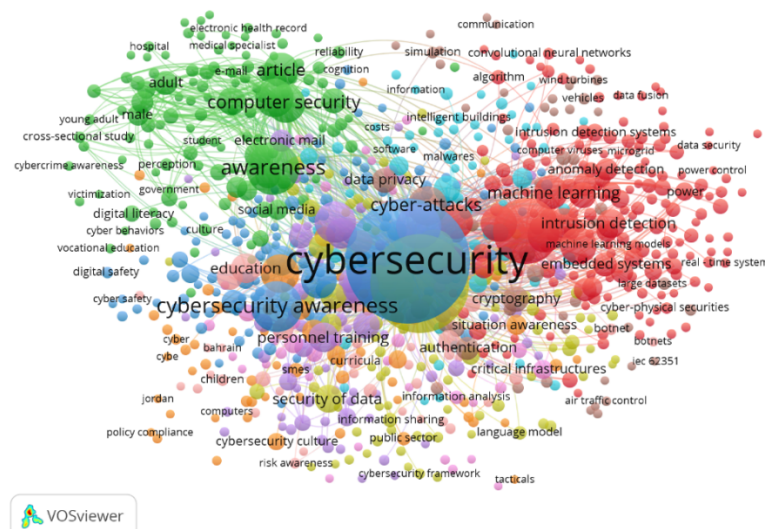


Figure 6. Visualization of the research keyword co-occurrence network

As illustrated in Figure 6, multiple interconnected clusters emerge, capturing the thematic structure of research regarding educational cybersecurity literacy. In the center of the network, the node 'cybersecurity' reflects the most captured and interconnected research and denotes its presence across multiple research domains. The red cluster includes subjects related to machines and systems, such as machine learning and intrusion and anomaly detection, as well as systems and embedded systems. This reflects the overwhelming representation of automated threat and modern security systems in the literature (Domalewska et al., 2025). This cluster suggests that the predominant focus of academic research is still on technological and systems-level solutions to the challenges of cybersecurity, particularly in the context of threat identification and mitigation (Larena-Luengo et al., 2025). In contrast, the green cluster focuses on the user and the behavioral side of things, with phrases including awareness, computer security, and digital literacy, and includes students and adults, showing increased emphasis on the human side and the role of cybersecurity awareness within the classroom. The blue cluster presents the interstitial issues dichotomized by cyberattacks, data privacy, and information that connect the technical and the conceptual (Gutierrez & Silva, 2025). Education-related terms such as education, training, and awareness of cybersecurity appear in several different clusters instead of a unified and distinct group. This shows that elements of education have been incorporated but have not yet been systematically integrated into the domain (Alt & Ibolya, 2021; Livingstone et al., 2017).

Connections between boundaries of pedagogical themes and highly technical areas remain relatively sparse, despite the overall interconnectivity of the network. Techniques of active learning, such as Problem-Based Learning, do not seem to appear as central or strongly interconnected nodes in the network. This finding aligns with the results of previous bibliometric studies indicating that the design of curricula and pedagogy, instructional strategies, and technical research in cybersecurity generally develop in parallel, as opposed to a coordinated or integrated approach (Bada & Nurse, 2019; Truong et al., 2021), even though novel methods such as game-based learning and collaborative learning are being examined increasingly.

This pattern suggests that multiple pathways exist for the continued refinement of academic discourse. These pathways include: 1) the technical dimensions of cybersecurity; 2) the digital and cybersecurity awareness of users; and 3) the conceptual and data-related aspects of privacy and cyberattacks. While there is overlap in the network of these thematic areas, there are limitations on the degree to which they can be merged into a single pedagogical framework. Therefore, within the context of adolescent cybersecurity, advances in technology and pedagogical techniques continue to be viewed as separate domains (Peraza-Balderrama et al., 2024; Chiner et al., 2025; Caverio et al., 2025). Nonetheless, earlier research has shown that active learning methods, including Problem-Based Learning, effectively improve critical thinking, analytical reasoning, and problem-solving abilities in real-world learning settings (Arianto et al., 2025), suggesting substantial prospects for future integrative research.

CONCLUSION

This study seeks to clarify research trends, theoretical frameworks, and intellectual progressions in cybersecurity literacy within educational settings by conducting a bibliometric analysis of publications indexed in Scopus. The findings indicate a marked rise in scholarly attention worldwide over the past decade, with this growth especially concentrated in fields connected to technical cybersecurity, cybersecurity education, and digital educational technologies. Nevertheless, the assessment identified clear conceptual limitations, particularly the insufficient integration of cybersecurity literacy with pedagogical approaches that effectively support adolescents' learning pathways. Prior studies emphasize the significance of technical skills and awareness. However, the use of systematic instructional designs, particularly Problem-Based Learning (PBL) operationalized through e-modules, remains underexplored. Accordingly, this study provides significant insights into advancing cybersecurity literacy by differentiating between the technical and pedagogical domains and considering the deployment of problem-based learning (PBL) e-modules as a method of enhancing the pragmatic dimension of cybersecurity. This study also describes a foundational structure for the development of future studies in this area. It also offers pragmatic guidance for instructors and educational planners on designing and developing appropriate, flexible cybersecurity literacy modules that are most relevant to the needs of the contemporary digital environment.

REFERENCES

- Abdollah, B., Mohd Zaki, N. I., & Mustapa, S. (2025). Cybersecurity Awareness and Digital Education: A Global Bibliometric Analysis. *International Journal of Modern Education*, 7(28), 859.
- Ahmed, A., Watterson, C., Alhashmi, S., & Gaber, T. (2024). How Universities Teach Cybersecurity Courses Online: A Systematic Literature Review. *Frontiers in Computer Science*, 6, 1499490.
- Aksnes, D. W., Langfeldt, L., & Wouters, P. (2019). Citations, Citation Indicators, and Research Quality: An

- Overview of Basic Concepts and Theories. *Sage Open*, 9(1), 2158244019829575.
- Alhuay-Quispe, J., Estrada-Cuzcano, A., & Bautista-Ynofuente, L. (2022). Analysis and Data Visualization in Bibliometric Studies. *JLIS.it*, 13(2), 58–73.
- Ali, A. S., Zaaba, Z. F., Singh, M. M., Anuar, N. B., & Shariff, M. R. B. M. (2025). Advancing Cybersecurity in ASEAN: Current Trends, Emerging Challenges, and Opportunities for Enhanced Resilience. *International Journal of Information Security*, 24(5), 200.
- Almasri, F. (2024). Exploring the Impact of Artificial Intelligence in Teaching and Learning of Science: A Systematic Review of Empirical Research. *Research in Science Education*, 54(5), 977–997.
- Alt, M.-A., & Ibolya, V. (2021). Identifying Relevant Segments of Potential Banking Chatbot Users Based on Technology Adoption Behavior. *Market-Tržište*, 33(2), 165–183.
- Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-Tool for Comprehensive Science Mapping Analysis. *Journal of Informetrics*, 11(4), 959–975.
- Arianto, F., Sumarno, A., Setyaedhi, H. S., Shofiana, F. R., & Hanif, M. (2026). Deep Digital Learning (DDL) Model Effect on Higher Education Critical Thinking and Problem-Solving Skills: A Quasi-Experimental Study. *Jurnal Eduscience*, 13(1), 39–50.
- Arishia, A. A., Kamarudinb, N. H., Bakarc, K. A. A., Shukurd, Z. B., & Hasan, M. K. (2024). Cybersecurity Awareness in Schools: A Systematic Review of Practices, Challenges, and Target Audiences. *International Journal of Advanced Computer Science and Applications*, 15(12).
- Bada, M., & Nurse, J. R. C. (2019). Developing Cybersecurity Education and Awareness Programmes for Small and Medium-Sized Enterprises (SMEs). *Information & Computer Security*, 27(3), 393–410.
- Bahlamar, A. R. U. (2024). Digital Media Literacy in Scholarly Discourse: A Bibliometric Analysis of Scopus-Indexed Publications. *Khizanah al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, 12(2), 253–266.
- Baioni E Silva, G., Longati, A. A., Sargo, C. R., Furlan, F. F., Capaz, R. S., Lora, E. E. S., & Milessi, T. S. (2024). Life Cycle Analysis of Succinic Acid Production in the Brazilian Biorefinery Context. *Sustainability*, 16(3), 1234.
- Betuš, M., Betušová, I., Wittenberger, G., Konček, M., & Hnilica, M. (2026). Building Safe and Sustainable Universities: An Integrated Governance Framework for Physical, Cyber, and Psychosocial Security. *Sustainability*, 18(5), 2581.
- Blažič, A. J., & Blažič, B. J. (2024). Toward Effective Learning of Cybersecurity: New Curriculum Agenda and Learning Methods. *Journal of Cybersecurity*, 10(1), tyae018.
- Blažic, B. J., & Blažic, A. J. (2024). *Towards Modern Teaching and Effective Learning of Cybersecurity*. International Society for Technology, Education, and Science.
- Bostrom, S., Karlberg, M., Schell, C., & Klang, N. (2024). Evaluation of the Collaborative and Proactive Solutions Model in an Alternative Educational Setting. *Education Sciences*, 14(3), 245.
- Cavero, A. O. B., Salazar, G. D. A., Lazo, V. D. H., Huaroto, J. J. B., & Castañeda, G. Z. (2025). Emerging Technologies: A Systematic Literature Review to Strengthen Cybersecurity. *LACCEI*, 1(12).
- Childers, G., Pinheiro, W. A., Daramola, O., Linsky, C. L., Payne, B., Byers, J., & Baker, D. (2025). Exploring K-12 Teachers' Definitions and Perspectives of Cybersecurity. *Journal of Cybersecurity Education, Research and Practice*, 2025(1).
- Chiner, E., Gómez-Puerta, M., Mengual-Andrés, S., & Merma-Molina, G. (2025). Teacher and School Mediation for Online Risk Prevention and Management: Fostering Sustainable Education in the Digital Age. *Sustainability*, 17(8), 3711.
- Domalewska, D., Gasztold, A., & Arcos, R. (2025). Mapping the Role of Social Sciences in Cybersecurity Research. *Studia Politologiczne*, 77, 244–264.
- Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to Conduct a Bibliometric Analysis: An Overview and Guidelines. *Journal of Business Research*, 133, 285–296.
- European Union Agency for Cybersecurity. (2023). *Cybersecurity Education Initiatives in the EU Member States: December 2022*. Publications Office.
- Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2021). Youth Internet Safety Education: Aligning Programs With the Evidence Base. *Trauma, Violence, & Abuse*, 22(5), 1233–1247.

- Gutierrez, G. T., & Silva, C. A. Z. (2025). Technological Cybersecurity Strategies for the Digital Protection of Adolescents: A Systematic Review. *LACCEI*, 2(13).
- Hafizah, M., Solin, S., Purba, C. T., Sihotang, M. M., Rahmad, R., & Wirda, M. A. (2024). Meta-Analysis: The Impact of Problem-Based Learning (PBL) Models on Students' Critical Thinking Skills. *Journal of Digital Learning and Education*, 4(3), 1–13.
- Hassan, W., & Duarte, A. E. (2024). Bibliometric Analysis: A Few Suggestions. *Current Problems in Cardiology*, 49(8), 102640.
- Humied, I. A. H. (2023). Key Determinants and Strategies for Cybersecurity Education in Yemen. *Journal of Digital Educational Technology*, 3(2), ep2304.
- Islam, R., Yildirim, G., Rahman, A., & Kamal, M. S. (2026). Artificial Intelligence in Cybersecurity and Education: A Bibliometric Review of Emerging Trends and Research Frontiers. *Sustainable Futures*, 11, 101807.
- Khalil, D. R. A., & Abuzir, Y. (2024). Cybersecurity in the Internet of Things: The Detection of the Types of Upcoming Digital Information by Using Classification Techniques. *Journal of Soft Computing and Artificial Intelligence*, 5(2), 41–62.
- Kolaski, K., Logan, L. R., & Ioannidis, J. P. A. (2023). Guidance to Best Tools and Practices for Systematic Reviews. *Systematic Reviews*, 12(1), 96.
- Kraiwanit, T., Limna, P., Sonsuphap, R., & Chutipat, V. (2025). Predictors of Digital Fraud: Evidence From Thailand. *Journal of Risk and Financial Management*, 18(12), 671.
- Kumar, J. A. (2025). The Global Landscape of Research on AI Literacy: A Bibliometric Analysis of Trends, Collaborations, and Emerging Themes. *2025 IEEE Frontiers in Education Conference (FIE)*, 1–10.
- Larena-Luengo, A., Herraiz, J. J. M., Ferrer-Oliva, M., & Medina-Merodio, J.-A. (2025). Mapping the Literature on the Factors That Influence Cybersecurity: A Bibliographic Coupling Analysis. *Cogent Business & Management*, 12(1), 2531265.
- Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., ... Fujdiak, R. (2025). Lessons Learned From Using Cyber Range to Teach Cybersecurity at Different Levels of Education. *Technology, Knowledge and Learning*, 1–36.
- Liu, N., Long, S., & Martin, F. (2025). Systematic Review of Elementary Cybersecurity Education: Curriculum, Pedagogy, and Barriers. *Journal of Cybersecurity Education, Research and Practice*, 2025(1).
- Livingstone, S., Ólafsson, K., Helsper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A., & Folkvord, F. (2017). Maximizing Opportunities and Minimizing Risks for Children Online: The Role of Digital Skills in Emerging Strategies of Parental Mediation. *Journal of Communication*, 67(1), 82–105.
- Loan, F. A., Bisma, B., & Nahida, N. (2021). Global Research Productivity in Cybersecurity: A Scientometric Study. *Global Knowledge, Memory and Communication*, 71(4–5), 342–354.
- Lu, Y., & Singh, C. K. S. (2024). The Effectiveness of the PBL Teaching Model on the Achievement and Critical Thinking Skills Development of Chinese Undergraduate Students: A Systematic Review. *Journal of Higher Education Theory and Practice*, 24(3).
- Ma, H., & Ismail, L. (2025). Bibliometric Analysis and Systematic Review of Digital Competence in Education. *Humanities and Social Sciences Communications*, 12(1), 185.
- Mongeon, P., & Paul-Hus, A. (2016). The Journal Coverage of Web of Science and Scopus: A Comparative Analysis. *Scientometrics*, 106(1), 213–228.
- Mukherjee, M., Le, N. T., Chow, Y.-W., & Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information*, 15(2), 117.
- Oktarina, A. D., Hamdi, S., Wijaya, A., Zafrullah, Z., & Rashid, S. (2025). Research Trends on the Implementation of Digital Literacy in Education: A Bibliometric Analysis of the Scopus Database. *Indonesian Journal on Learning and Advanced Education (IJOLAE)*, 481–502.
- Panagopoulos, N., Karamanis, K., & Anastasiou, S. (2023). Exploring the Impact of Different Leadership Styles on Job Satisfaction Among Primary School Teachers in the Achaia Region, Greece. *Education Sciences*, 14(1), 45.
- Panjani, H., & Mudgal, A. (2025). A Study of Cyber Safety Awareness Among Students and Educational

- Initiatives. *Indian Journal of Educational Technology*, 7(2), 246–256.
- Peraza-Balderrama, J. N., Valdés-Cuervo, Á. A., Parra-Pérez, L. G., & Urías-Murrieta, M. (2024). Multidimensional Scale to Assess Digital Security in Adolescents. *Revista Electrónica de Investigación Educativa*, 26, 1–19.
- Pramod, D. (2024). Gamification in Cybersecurity Education: A State of the Art Review and Research Agenda. *Journal of Applied Research in Higher Education*, 17(4), 1162–1180.
- Prasetia, A. (2023). Peran Orang Tua Siswa dalam Menghindari Fenomena Loss Learning to Loss Generation pada Masa Pandemi COVID-19. *Journal of Educational Learning and Innovation (ELI)*, 3(1), 107–117.
- Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity Awareness for Children: A Systematic Literature Review. *International Journal of Child-Computer Interaction*, 30, 100343.
- Rodríguez-Correa, P. A., Valencia-Arias, A., Rojas, E. M., León, A. O., Rubio, R. H. M., Coronado, M. H. V., & García, J. A. J. (2025). Information Security Education: A Thematic Trend Analysis. *F1000Research*, 14, 5.
- Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11(4), 89.
- Samodra, I., Rahmawati, F., & Prayitno, B. A. (2026). A Decade of Advancing Creative Thinking Skills in Science Education: Trends and Research Frontiers From a Bibliometric Analysis (2015–2025). *Discover Education*, 5(1), 116.
- Schleicher, A. (2020). *Education at a Glance 2020: On Education*. OECD Publishing.
- Shaikh, G., & Güngör, S. K. (2025). Artificial Intelligence in Education: Insights From a Bibliometric Study (2010–2025) Based on Scopus and Web of Science. *International Journal of Modern Education Studies*, 9(2).
- Sisrayanti, Maksum, H., Waskito, & Sabrina, E. (2024). The Effect of the Problem-Based Learning Model on 21st Century Student Skills: A Meta-Analysis. *The Indonesian Journal of Computer Science*, 13(2).
- Sockalingam, N., Lo, K., Teo, J., Wei, C. C., Jiet, D. C. J., Herremans, D., ... Leong, P. K. (2025). Towards the Future of Education: Cyber-Physical Learning. *Discover Education*, 4(1), 82.
- Sulich, A., & Sołoducho-Pelc, L. (2025). Cybersecurity and Sustainable Development–Bibliometric Study. *Procedia Computer Science*, 270, 5625–5633.
- Sulich, A., Zema, T., & Kulhanek, L. (2023). Towards a Secure Future: A Bibliometric Analysis of the Relations Between Cybersecurity and Sustainable Development. *Procedia Computer Science*, 225, 1448–1457.
- Sun, J., Ghazali, A. H. A., & Abdul, R. S. N. (2025). Risky Online Self-Disclosure in Adolescents: A Meta-Analytic Review of Predictors and Outcomes. *Frontiers in Psychology*, 16, 1734301.
- Taha, N., & Dahabiyeh, L. (2021). College Students Information Security Awareness: A Comparison Between Smartphones and Computers. *Education and Information Technologies*, 26(2), 1721–1736.
- Tan, T., Abdullah, R. S., & Mas'ud, Z. (2025). Cybersecurity Education Using Gamification: Systematic Literature Review. *International Journal of Academic Research in Business and Social Sciences*, 1(10).
- Thuan, N. D., Chau, L. M. T., & Nhi, N. T. (2026). Trends and Applications of ICT in Physics Education: A Bibliometric Analysis Using the Scopus Database From 2000 to 2025. *Multidisciplinary Reviews*, 9(8), 2026383.
- Tran, N. (2026). *Mapping Scholarly Publishing on School Leaders' Digital Competence: A Bibliometric Analysis of Scopus Data, 2006–2025*. Mendeley Data.
- Truong, N., Sun, K., Wang, S., Guitton, F., & Guo, Y. (2021). Privacy Preservation in Federated Learning: An Insightful Survey From the GDPR Perspective. *Computers & Security*, 110, 102402.
- Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, 13(2), 39.
- Van Eck, N. J., & Waltman, L. (2010). Software Survey: VOSviewer, a Computer Program for Bibliometric Mapping. *Scientometrics*, 84(2), 523–538.
- Zaqueu, P., & Mawela, T. (2023). Factors Contributing to Cybersecurity Awareness, Education and Training. *Procedia Computer Science*, 58–69.
- Zupic, I., & Čater, T. (2015). Bibliometric Methods in Management and Organization. *Organizational Research Methods*, 18(3), 429–472.