INNOVATIVE APPROACHES IN CYBERSECURITY EDUCATION: A BIBLIOMETRIC STUDY OF PEDAGOGICAL PRACTICES AND TRENDS

Nor Erlissa Abd Aziz[1], Muhamad Khairulnizam Zaini[2]*, Subha Ismail[3], Siti Zaleha Abd Goni[2], Qamarul Nazrin Harun[2]

[1]*Faculty of Information Science, Universiti Teknologi MARA (UiTM), Kelantan, MALAYSIA*
[2]*Facultyof Information Science, Universiti Teknologi MARA (UiTM), Shah Alam, MALAYSIA*
[3]*Tun Abdul Razak Library (PTAR), Universiti Teknologi MARA (UiTM), Shah Alam, MALAYSIA*
erlissa@uitm.edu.my, *nizam0374@uitm.edu.my, subha_ismail@uitm.edu.my, sitizaleha.ag@gmail.com
qamarulnazrin@uitm.edu.my

Received Date: 16/04/2025 *Accepted Date: 15/05/2025* *Published Date:30/10/2025*

Abstract

With the rapid digitalization of today's world and the consequent rise of cybersecurity threats, there has been an increase in educational initiatives that are committed to teaching essential skills for tackling evolving threats. Traditional lecture-based style and fixed content courses for cybersecurity are no longer sufficient as students need real-time, dynamic, and practical skills to deal with new and ever-changing cyber threats. For that reason, several researchers have begun to explore innovative pedagogical strategies in cybersecurity education. This study carries out a comprehensive bibliometric analysis of global research on innovative teaching methods in cybersecurity education and identifies the key trends, influential publications, and emerging pedagogical practices. A dataset of relevant publications in the areas from the past 15 years from Scopus database was analyzed using relevant bibliometric tools like Biblliometrix and VOS viewer. It sheds light on the evolution of the research focus, top authors, journals, and collaboration networks, and mappings of the main teaching methods like gamification, simulations, virtual labs, and flipped classrooms. It also shows the trends in journal word co-occurrence. Additionally, this study highlights the distribution of research and reveals understudied areas of the field. Findings help deepen understanding of the nature of pedagogical innovations that are transforming cybersecurity education and provide useful guidance for educators, curriculum developers, and policymakers. This study closes with a research agenda to address gaps and increase the integration of innovative teaching methods in cybersecurity curricula.

Keywords: *Cybersecurity Education; Bibliometric Analysis; Gamification in Cybersecurity; Pedagogical Trends in Cybersecurity Training*

1.0 Introduction

Cybersecurity has become an integral part of modern-day life for any organization or individual. As the advancement in technology continues, the sophistication of threats affecting data privacy, infrastructure, and the general well-being of the digital society has increased, making cybersecurity even more important. To prepare for these challenges, there have been significant advancements in cybersecurity education to keep pace with this growing importance [1]. While the development and implementation of training programs aimed at educating policymakers, educational institutions are also recognizing the importance of technical expertise needed to combat cyber threats and have made efforts to equip learners with critical thinking and problem-solving skills related to cybersecurity in real-world scenarios [2]. Nevertheless, in an era of rapidly evolving cyber threats, it is also apparent in the academic world where educational strategies have been employed for teaching the cybersecurity to keep pace with the trends. Such education is crucial, especially for educating the digital society in managing cybersecurity risks, ensuring national security, and achieving cyber self-efficacy [3].

e-ISSN 2821-3394

The current trend in the development of cybersecurity education is a clear transition from traditional methods of teaching to more contemporary approaches. Previously, conventional teaching methods such as lectures and fixed curricula have been the trademark of cybersecurity training and have played crucial roles in developing talents for cybersecurity. However, traditional teaching methods of cybersecurity education today seems to not able to equip students with the skills that are required due to the constantly changing context of cyber threats. Often, these methods have been criticized as outdated because they hardly be able to cope up with the ever-changing nature of the cybersecurity threats. As debated, these approaches do not provide many opportunities to engage in any practical learning processes and problem-solving skills to implement cybersecurity in real world experience [4], [5], [6].

To cope with these challenges, the education professionals and the scholars have resorted to different teaching approaches like game-based learning, simulations, peer instruction, virtual laboratories, flipped classrooms and collaborative learning environments. According to recent research, these methods intend to handle the surge in the need for cybersecurity abilities, boost learner participation and learning results [7], [8], [9], [10]. Also, there are many other studies have integrated these approaches into cybersecurity education, demonstrating their effectiveness and its desirable benefits. Such change indicates the progressive improvement in cybersecurity education as well as its adaptation to the emerging threats and risks within the organization.

However, the literature on the development of these approaches, while still ongoing, does not quite tell us how effective these approaches are, how they have been adopted, and how these approaches are in alignment with the recent global objectives of cybersecurity education. Hence, there is a need for consolidating the current body of the literature to find out the common themes, patterns and the potential of existing imbalance in the growth of the field around cybersecurity education.

The goal of this study is to conduct a bibliometric analysis for discovering patterns found in the existing body of knowledge in cybersecurity education. In this, the identified publication trends, influential works, and collaboration networks can be used to identify the major patterns and trends during the development of this field. In addition, the bibliometric analysis offers a valuable opportunity to uncover unexplored regions of research, neglected topics, or uneven implementation of innovative pedagogical strategies [11]. Besides that, this approach not only identifies new trends and future approaches but also provides guidance on developing curricula and policies by referencing evidence-based insights. The focus of this study is to investigate and examine this field's most important research subjects and themes and how this can aid in moving forward the research fields. This study seeks to analyze performance outcomes of the publications, recognize main thematic areas, look into emerging trends and research gaps which can help insights into the design of innovative teaching methodology. We address the following questions to achieve this objective.

- **RQ1. Publication Performance:** What have been the performance results of the publications in the field of cybersecurity education? How has the achievement of these results affected the growth of the field?
- **RQ2. Key Themes and Trends**: What patterns and topics emerge from the cybersecurity education literature?
- **RQ3. Future Research Directions**: What are the trends, gaps, or opportunities that can guide further research and priorities in the area of cybersecurity education?

e-ISSN 2821-3394

2.0 Literature Review

This section presents some of the concepts of this study: an introduction to cybersecurity education, pedagogy and emerging teaching approaches in cybersecurity education, and the use of bibliometrics in educational research. This section lays down the background to a focused analysis of the state of cybersecurity education as a discipline.

2.1 Overview of Cybersecurity Education

Cybersecurity education is a complex field that covers the areas of knowledge and skills that are needed for acquiring, processing, and distributing knowledge and skills toward protecting digital systems and data from cyber threats. As a critical part of modern education systems, it seeks to prepare individuals with the capacity to navigate and counter the risks of the digital landscape through systematic trainings, programs, and approaches [12], [13], [14], [15].

All over the world, cybersecurity education has become more and more important as a way to help people defend themselves against the challenges of the digital age. Cybersecurity should be made part of the education curriculum in order to help students build security awareness and knowledge that will enable them to address cyber threats. Besides that, the area of cybersecurity education has grown tremendously over the years, triggered by a huge demand for specialists due to the global issues where the world alone was estimated to be lacking 2.27 million cybersecurity specialists up to 2021 according to [16]. This scenario has suggested that cybersecurity education has now expanded and become more complex and interdisciplinary, indicating the need for outcomes-based education to be addressed.

In a broader perspective, cybersecurity education is not only important in the formation of a new generation of professionals but also to create awareness among other citizens. A study by [17] exhibits that most adults have poor cybersecurity literacy and awareness, which makes them prone to cyber risks. Also, according to the study, the public still lacks adequate knowledge on cybersecurity, showing that the significance of this education should have been introduced at an early age. In turn, as educational institutions must modify curricula in response to these problems, early prevention at schools and higher rates of adult education are very much needed to develop a more informed population in terms of cybersecurity.

Meanwhile, it is also apparent that educators started to adopt the modern ways of teaching, for example through gamification, simulations, virtual labs, flipped classes, collaborative learning environments as an innovative strategy for increasing student engagement, knowledge retention, and hands-on skills [18], [19], [20]. From the research perspectives, such a transition embodies the increasing requirement for pedagogical practices that are dynamic and robust to educate students on the intricacies of the cybersecurity domain.

2.2 Impact of pedagogical innovations of Cybersecurity education on student engagement and skill development

The efforts made in developing cybersecurity education have been enhanced by adopting methods that engage students in practical and innovative ways. The innovations of these are meant to make the learning process more interesting, realistic and applicable, all with the aim of more successfully retaining the attention of students in cybersecurity classes. Gamification adoption is one of the milestones in cybersecurity education. Gamification refers to adding game elements into non-game content which include competition, rewards, and progress tracking in order to motivate interest in the content. Research suggests that students' learning and performance as well

e-ISSN 2821-3394

as their practical and theoretical skills in the field of cybersecurity are positively affected through the use of gamification [21], [22].

The use of cyber ranges and simulated training environments for experience-based learning is yet another significant pedagogical innovation in teaching and learning in cybersecurity [23], [24], [25], [26]. These platforms allow students to proactively defend against cyber-attacks, carry out penetration testing, and respond to incidents in a realistic but controlled and safe environment. These simulations enhance critical thinking, decision making, and problem-solving skills of the learners through exposure to real life security challenges. In addition, such opportunities for experiential learning ensure that students gain the necessary technical skills in this field, which fill the gap between theory and practice.

2.3 Role of Bibliometric Studies in Cybersecurity education Research

Bibliometric studies play an important role in education including cybersecurity teaching and research because they help analyze academic literature, identify future areas of knowledge development, and formulate current research interests [27]. A researcher can strategically apply comprehensive citation analysis, co-authorship network examination, and keyword clustering in order to assist in assessing the evolution and impact of cybersecurity education, identify significant studies, and detect new topics. Such assessment techniques enable educational institutions and policymakers to detect underdeveloped fields along with the specific areas where additional research is needed. Apart from that, the bibliometric studies enable researchers to monitor the implementation of cybersecurity frameworks and pedagogical methods and technological developments which affect cybersecurity curriculum delivery throughout various educational institutions [28].

Besides uncovering research trends, this study believes that bibliometrics can contribute to evidence-based cybersecurity education decision-making by emphasizing the most cited works, leading authors, and the collaborations between academia and industry. It allows researchers to identify authoritative sources that shape the development of curricula, the need for particular skills and competencies, and thus the development of educational frameworks for cybersecurity training and programs.

3.0 Research Methodology

A systematic literature search through Scopus database is optimized to enabled the performance of a bibliometric analysis related to cybersecurity education and teaching methodologies. The specified research query aimed to collect studies which explored cybersecurity education methods alongside instructional methods. The research approach and search query were designed as follows:

3.1 PRISMA Approach for Bibliometric Analysis

This study uses the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to implement a systematic, transparent bibliometric analysis of cybersecurity education research. The process comprised four phases, identification, screening, eligibility, and inclusion. A structured search query for cybersecurity education and teaching approaches in Scopus online database was deployed and 217 publications retrieved initially. Duplicate records were removed and non-relevant document types in the screening phase, after which title and abstract review was performed to confirm the records were aligned with study's objectives. The study then proceeded with the eligibility phase, where initial articles were full text

e-ISSN 2821-3394

analyzed for inclusion into the dataset. Then, the library of 197 publications was analyzed with *Bibliometri*x [29] and *VOS viewer* [30] for publication trend, citation networks and a thematic evolution. This study employed PRISMA to ensure that such a rigorous, reproducible, and transparent process was applied for the selection of the studies, resulting in more reliable findings in cybersecurity education research.

3.2 Search Query on Scopus database

> TITLE-ABS-KEY (("cybersecurity education" OR "information security education" OR "teaching cybersecurity" OR "cybersecurity training" OR "security awareness education") AND ("teaching methods" OR "pedagogy" OR "instructional strategies" OR "educational practices" OR "curriculum development" OR "active learning" OR "innovative teaching" OR "experiential learning" OR "gamification"))AND PUBYEAR > 2009 AND PUBYEAR < 2025 AND NOT AUTHLASTNAME("") AND (LIMIT-TO (SUBJAREA,"COMP") OR LIMIT-TO (SUBJAREA,"BUSI") OR LIMIT-TO (SUBJAREA,"SOCI") OR LIMIT-TO (SUBJAREA,"ENGI") OR LIMIT-TO (SUBJAREA,"MATH") OR LIMIT-TO (SUBJAREA,"DECI")) AND (EXCLUDE (PREFNAMEAUID,"Undefined"))

3.3 Search Query Components

3.2.1 Focus on Cybersecurity Education and Teaching Methods.

Terms such as "cybersecurity education," "information security education," "teaching cybersecurity," "cybersecurity training," and others were used to search studies focusing on cybersecurity education and pedagogical techniques. Also present were instructional methodologies with keywords "teaching methods, pedagogy, curriculum development, and gamification."

3.2.2 Timeframe Restriction

To ensure the inclusion of relevant and recent literature, only publications from 2010 to 2024 are included: (PUBYEAR > 2009 AND PUBYEAR < 2025). This was helpful for analysis of contemporary trends and innovations in cybersecurity education.

3.2.3 Exclusion of Missing Author Names

Publications with missing author details were excluded via the condition NOT AUTHLASTNAME(") and that all retrieved documents will have an author properly indexed.

3.2.4 Subject Area Filtering

The search was limited to studies on the following subject areas in order to maintain relevance.

- Computer Science **(COMP)** – The primary domain of cybersecurity education.
- Business, Management, and Accounting **(BUSI)** – Covers cybersecurity awareness in corporate environments.
- Social Sciences **(SOCI)** – Encompasses studies on cybersecurity education and awareness.
- Engineering **(ENGI)** – Includes cybersecurity applications in engineering disciplines.

e-ISSN 2821-3394

- Mathematics **(MATH)** – Addresses algorithmic and security-related mathematical models.
- Decision Sciences **(DECI)** – Focuses on decision-making in cybersecurity training and education.

To increase the accuracy and integrity of the dataset, the condition EXCLUDE (PREFNAMEAUID, "Undefined") was applied that omits the articles that have undefined or missing author identifiers.

4.0 Analysis, Results and Discussion of the Bibliometric Analysis

The dataset covers a research span from 2010 to 2024, exhibiting a strong annual growth rate of 23.17%, which shows an upward trend in the field of cybersecurity education. The 196 documents, spanning from 119 outlets of publication, encompass a wide variety of scholarly contributions. Each of the documents has been cited on average 6.158 times, which has a moderate impact within the academic community. The high contemporary focus of the dataset is emphasized by the average document age of 3.54 years, indicating that current events and trends have had great importance to the dataset. Additionally, the dataset includes 1,058 Keywords Plus and 504 author keywords, suggesting great thematic diversity and evolution of terminology in cybersecurity education research.

It also points to strong collaborative efforts, as 598 authors were involved in the work, and there was an average of 3.58 co-authors per document. International collaboration, however, is still low (10.2%), suggesting a lot of room for growth in global partnerships, while single-authored documents constitute 23 publications. The dataset is dominated by conference papers, with 141 documents, reflecting the central role of conferences in pushing forward research in this field. The dataset also includes 34 peer-reviewed journal articles, 16 book chapters, 3 books, and only 2 review papers, which points out that systematic reviews or meta-analysis are potential areas for research. Overall, this dataset is strong in establishing an initial base of bibliometric analysis aiming to identify trends, gaps in the research area, and potential directions for future development in the area of cybersecurity education. **Table 1** below illustrates the main information of bibliometric analysis on the subject.

TABLE 1
Main Information of the Bibliometric analysis on the subject

Description	**Results**
MAIN INFORMATION ABOUT DATA	
Timespan	2010:2024
Sources (Journals, Books, etc)	121
Documents	198
Annual Growth Rate %	31.45
Document Average Age	4.20
Average citations per doc	6.167
DOCUMENT CONTENTS	
Keywords Plus (ID)	1062
Author's Keywords (DE)	512
AUTHORS	
Authors	613

e-ISSN 2821-3394

Authors of single-authored documents	23
AUTHORS COLLABORATION	
Single-authored docs	24
Co-Authors per Doc	3.64
International co-authorships %	11.62
DOCUMENT TYPES	
Article	33
Book	3
Book chapter	15
Conference paper	143
Review	3

4.1 The Key Trends on Evolution of Cybersecurity education research

The evolution of cybersecurity education research focus from traditional teaching methods to contemporary and innovative methods is illustrated in **Figure 1** below. From 2010 to 2013, the annual production of scientific papers was stagnant, implying that the modern pedagogical techniques of teaching cybersecurity education were not widely explored or applied. This time, probability that the traditional lecture-based teaching still filling the landscape of education. The lack of significant growth implies a lack of urgency and a lack of awareness regarding the need for pedagogical advancement of cybersecurity.

Beginning in 2014, there is a slow increase in research output until 2017, indicating the onset of a shift in researching how cybersecurity education practices can be enhanced. This peak in 2016 shows that there is an emerging interest in exploring new educational ways to tackle the quickly changing requirements of the field. Nevertheless, the drop in 2017 and 2018 may indicate difficulties in adopting or carrying out contemporary methods, like gamification, simulations, and hands-on training, because of many institutions persist to emphasized on conventional methods. **The Table 2** below, indicates the trends of productions for the past 15 years.

TABLE 2

Annual Scientific Production (Year vs Publications)

Year	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
No.	1	1	0	4	7	7	6	6	4	17	19	25	24	31	46

The biggest difference happens from 2019 onwards (with 17 publications in 2019 to 46 publications in 2024), in which scientific production increases rapidly and consistently, demonstrates an immense change in modernizing cybersecurity education. During this time, virtual labs, collaborative learning, and flipped classrooms start to take off, where contemporary teaching methods have geared towards addressing the dynamic and practical nature of the field. From 2021 to 2024, annual production continues to increase to its highest level yet and demonstrates that the need for new ideas in providing student engagement, skill development, and practical learning is being seen more and more as valuable. **The Figure 1** below illustrates the annual scientific productions of studies related from 2010 to 2024.

e-ISSN 2821-3394

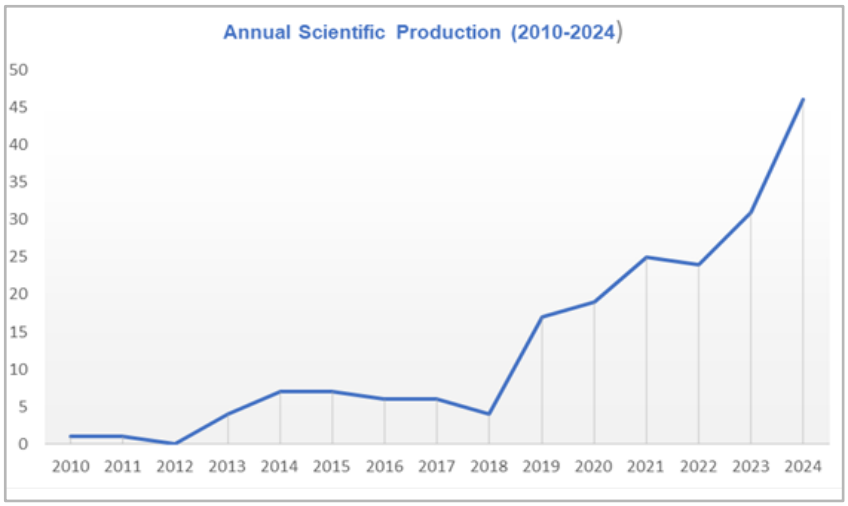

Figure 1. The Annual Scientific Productions (2010 - 2024)

4.2 Citation Performance Trends

The bibliometric analysis of cybersecurity education publications from 2010 to 2024 reveals notable trends in citation performance and publication volume. Mean Citations per Article (MeanTCperArt) shows a rather high fluctuation through the years, and reaches its highest peaks in 2014 (35.86) and 2018 (30.75), which means that articles published in these years had a great impact. Like the Mean Citations per Year (MeanTCperYear), 2018 (3.84) and 2014 (2.99) are the highest citation rates per year. Nevertheless, there is a considerable drop in mean TC per article for more recent publications, specifically from 2022 to 2024 when MeanTCperArt reduces to 6.29 in 2022, 2.29 in 2023, and 0.26 in 2024. This is to be expected, since newer publications have not yet had enough time to accumulate citations. **Table 3** below summarizes the data.

TABLE 3
Annual Scientific Production (Year vs Publications)

Year	MeanTCperArt	N	MeanTCperYear	CitableYears
2010	0.00	1	0.00	16
2011	0.00	1	0.00	15
2013	5.00	4	0.38	13
2014	35.86	7	2.99	12
2015	11.71	7	1.06	11
2016	10.00	6	1.00	10
2017	9.33	6	1.04	9
2018	30.75	4	3.84	8
2019	7.29	17	1.04	7
2020	5.79	19	0.96	6
2021	6.48	25	1.30	5
2022	6.29	24	1.57	4
2023	2.29	31	0.76	3
2024	0.26	46	0.13	2

e-ISSN 2821-3394

According to **Figure 2** below, the number of publications has increased steadily over time, especially after 2019 when there was a significant increase in 2023 (31 articles) and 2024 (46 articles). This indicates that there seems to be an increasing interest in researching cybersecurity education. However, the Citable Years metric, which represents the number of years an article has been published that a citation could be made, does further any newer publications. In conjunction with an increasing publication volume and declining citation averages in recent years, these results suggest that while there is growth in research on cybersecurity education, newer publications may take longer to receive citations and recognition. These circumstances speak to the necessity of monitoring citations longitudinally in order to determine the effects research has had in this area over time.

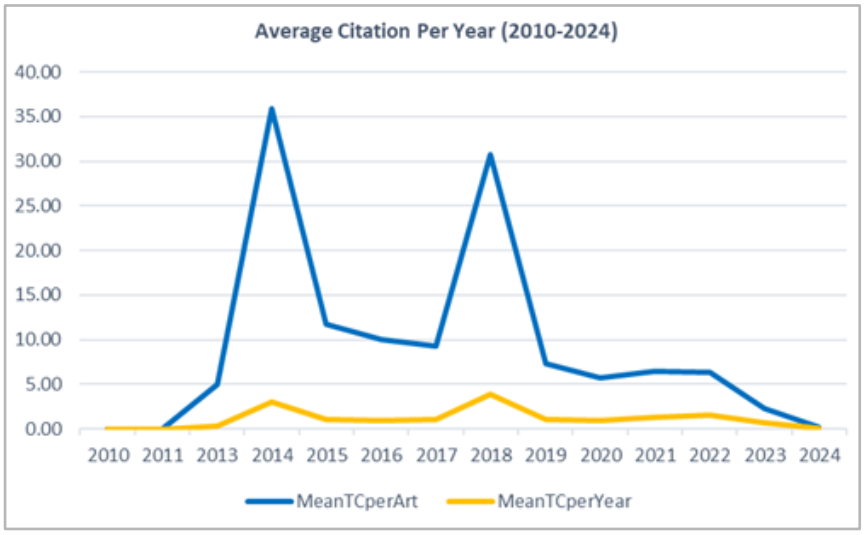

Figure 2. Average citation Per Year (MeanTCperArt vs MeanTCperYear) 2010-2025

Overall, these findings show that while there has been an increase in the number of published articles in the last few years, the average citation per article is relatively low, indicating the field of cybersecurity education research is growing but has yet to reach its potential in terms of impact.

4.3 The Most Relevant Sources

4.3.1 Top Sources related to Cybersecurity Education Research

Table 4 shows the top 15 sources which have published the most articles related to cybersecurity education research. The most prominent source is the *Proceedings: Frontiers in Education Conference (FIE)* with 13 articles, then *ACM International Conference Proceeding Series* with 9 articles. Besides, several other major venues including *Annual Conference on Innovation and Technology in Computer Science Education (ITICSE), IEEE Global Engineering Education Conference (EDUCON*) and *Lecture Notes in Computer Science* each had 6 articles which indicated their significance for the dissemination of research in this field.

TABLE 4
Top 15 sources related to the subjects

e-ISSN 2821-3394

No.	Sources	Articles
1	Proceedings: Frontiers in Education Conference, FIE	13
2	ACM International Conference Proceeding Series	9
3	Annual Conference on Innovation and Technology in Computer Science Education, ITICSE	6
4	IEEE Global Engineering Education Conference, EDUCON	6
5	Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	6
6	Advances In Intelligent Systems and Computing	5
7	ASEE Annual Conference and Exposition, Conference Proceedings	5
8	CEUR Workshop Proceedings	4
9	Communications In Computer and Information Science	4
10	Education And Information Technologies	4
11	Springer Proceedings in Complexity	4
12	Information (Switzerland)	4
13	Innovations In Cybersecurity Education	3
14	Journal Of Information Systems Education	3
15	Lecture Notes in Networks and Systems	3

Advances in Intelligent Systems and Computing, ASEE Annual Conference and Exposition, and *CEUR Workshop Proceedings* also facilitate amounting with 4 to 5 articles published per journal or conference proceedings. Sources such as *Education and Information Technologies, Communications in Computer* and *Information Science and Springer Proceedings in Complexity* provide further literature, attesting to the interdisciplinary interest in cybersecurity education.

Among the sources that are relevant are Innovations in *Cybersecurity Education*, *Journal of Information Systems Education,* and *Lecture Notes in Networks and Systems*, which each publish 3 articles. These sources highlight the increasing attention to cybersecurity education that extends to computer science, engineering, as well as education research. This analysis shows the wide variety of publication venues used by the researchers to advance knowledge in the area of Cybersecurity Education.

4.3.2 Top Most Relevant Authors

The analysis of the most relevant authors in cybersecurity education research reveals the inherent concentration of contributions from a small segment of authors who dominate the field, where *Aunshul Rege* leads with 10 publications and a fractionalized count of 3.87. Other notable contributors on this domain include *Rachel Bleiman* (7 articles, 2.20 fractionalized) and *Katorah Williams* (5 articles, 1.50 fractionalized) indicating high level of collaborative research on this domain. *H. Liu, T.J. O'Connor, E. Stavrou*, and *C. Zhong* have 4 publications each, while *Brilingaitė, Crick, Irons,* and *Mäses* have 3 publications each with single fractionalized scores each. The wide distribution of fractionalized contributions can be seen as a research landscape of high collaboration where individual contributions depend on their co-authorship roles. **The Table 5** below provides the information on the most relevant authors in the field.

e-ISSN 2821-3394

TABLE 5
Top 15 most relevant authors

No.	Authors	Articles	Articles Fractionalized
1	Rege, Aunshul	10	3.87
2	Bleiman, Rachel	7	2.20
3	Williams, Katorah	5	1.50
4	Liu, H.	4	1.20
5	Oconnor, T.J.	4	1.83
6	Stavrou, E.	4	1.50
7	Zhong, C.	4	1.17
8	Brilingaitė, A.	3	0.62
9	Crick, T.	3	0.95
10	Irons, A.	3	0.95
11	Mäses, S.	3	0.87
12	Ribaudo, M.	3	1.03
13	Vykopal, J.	3	0.92
14	Xu, J.	3	0.57
15	Yuan, X.	3	0.57

The tabulated data is also subjected to a critical analysis for both strengths and challenges in cybersecurity education research. As for advantages, we could see that the number of scholars who dominate the field does indicate that the field is still led by a few people, which may potentially hinder the diversification of concepts and perspectives on this area. In another view, data have shown that the presence of many low fractionalized scores for many authors implies a high level of collaboration, but also indicates that only few authors who do consistently lead the studies for the past 15 years. In this context, lack of sustained, long-term engagement of many contributors could create a concern whether the field can sustain researchers over time and in the future.

4.3.3 Top Most Relevant Author's Affiliations

The examination of the most relevant author affiliations in cybersecurity education research suggests that a few institutions make most of the contributions. *Temple University* leads with 10 publications, significantly outpacing all other institutions and showcasing an unmatched dedication to researching cybersecurity education. Other universities such as *Indiana University Kokomo*, *Masaryk University*, *Norwegian University of Science and Technology*, and *Vilnius University* each contributed 4 publications, which is above average in the field, and showcases active participation. The remaining, which included *Edith Cowan University, Florida Institute of Technology,* and *Swansea University*, contributed 3 publications each, which demonstrates a steady, moderate, and commitment towards research in cybersecurity education. **Table 6** below entails the information.

e-ISSN 2821-3394

TABLE 6
Top 15 most relevant Author's Affiliations

No.	Affiliation	Articles
1	Temple University	10
2	Indiana University Kokomo	4
3	Masaryk University	4
4	Norwegian University of Science and Technology	4
5	Vilnius University	4
6	Edith Cowan University	3
7	Faculty of Technical Science	3
8	Florida Institute of Technology	3
9	Norfolk State University	3
10	Open University of Cyprus	3
11	Riga Technical University	3
12	Swansea University	3
13	University of Central Lancashire Cyprus	3
14	University of Genoa	3
15	University of Tampa	3

This data indicates that while research in cybersecurity education is spatially dispersed, it is still concentrated in certain academic institutions only. The dominance of *Temple University* suggests either an institutional specialization or active research in cybersecurity teaching practices. Still, the low publication counts across most other institutions suggest that there is lacking attention towards cybersecurity education research which can impede the development of this field.

4.3.4 Top Most Relevant Corresponding Author's Countries

The examination of the most prolific author's countries for the cybersecurity education research has shown that *the United States* is the most notable country by far, having contributed 37 articles at 18.9%. From the data, it is obvious that other nations are significantly behind. This indicates the prominence and dominance of researchers in this area are from the *US*. Next, comes *Italy* with 6 publications 3.1% and then *Greece, Cyprus, Estonia, India, Japan, Latvia, Norway, and Portugal* each estimated at 2-4 contributed articles. Importantly, the SCP metric shows that most publications are produced by institutions of a single country and there are a few international co-authorships as well. However, *Estonia* and *Latvia* have different numbers, they have a higher percentage of MCP at 50 percent and 100 percent respectively. This means that researchers from these countries have a greater degree of international collaboration than other countries on these specific subjects. The **Table 7** below indicates the numbers.

TABLE 7
Top 10 Corresponding Author's Countries

e-ISSN 2821-3394

No.	Country	Articles	Articles %	SCP	MCP	MCP %
1	USA	37	18.9	35	2	5.4
2	Italy	6	3.1	5	1	16.7
3	Greece	4	2	4	0	0
4	Cyprus	2	1	2	0	0
5	Estonia	2	1	1	1	50
6	India	2	1	2	0	0
7	Japan	2	1	2	0	0
8	Latvia	2	1	0	2	100
9	Norway	2	1	2	0	0
10	Portugal	2	1	2	0	0

The data above shows that cybersecurity education research seems to be focused heavily on the United States while other regions are contributing little. In addition, most countries not having high MCP percentages means that international cooperation is almost nonexistent, which greatly limits the knowledge exchange and standard setting for adaptable cybersecurity education materials. The U.S. continues to dominate due to its substantial investment into and strong infrastructure for cybersecurity, however, the poor coverage of Asian, African, and South American countries indicates that there is a need to be more inclusive and form international collaborations to make the research more comprehensive and effective in solving the problems pertaining to cybersecurity education globally. Increasing international cooperation as well as cross-institutional collaboration will help diversify and improve the effectiveness of cybersecurity education research internationally.

4.3.5 Top Most Global Cited Documents

The most influential works of the field are revealed at the analysis of the most cited documents in cybersecurity education. The most cited paper is Konak *et al.* [30], published in *Computers & Education*, which has 137 citations. This paper discusses the implementation of *Kolb's Experiential Learning Cycle* and how it can aid in student's learning in virtual computer labs. This suggests that this paper, as well as much of the academic literature in experiential learning, is well regarded, as well as highlighting the necessity of such approaches in cybersecurity education. The second most cited study, Jin *et al*. [31], has 89 citations and focuses on game-based cybersecurity training for high schoolers. His study has the highest citation rate of 12.71 per year. Several other notable studies include Mirkovic & Peterson [31], Chothia & Novakovic [32] that describe capture-the-flag (CTF) exercises and their effectiveness as CTF exercises in pedagogy for cybersecurity education. There is also Crick *et al.* [33], [34] work on the cybersecurity education and its accreditation in the UK which adds more evidence towards the interest in regulated cybersecurity programs. The **Table 8** below summarizes the findings.

TABLE 8
Top 10 Most Global Cited Documents

e-ISSN 2821-3394

No.	Paper	Document Title	Total Citations	TC per Year	Normalized TC
1	Konak A, 2014, COMPUT EDUC	Using Kolb's Experiential Learning Cycle to improve student learning in virtual computer laboratories	137	12.45	4.07
2	Jin G, 2018, SIGCSE - PROC ACM TECH SYMP COMPUT SCI EDUC	Game-based Cybersecurity Training for High School Students	89	12.71	3.02
3	Mirkovic J, 2014, USENIX SUMMIT GAMING, GAMES, GAMIFICATION SECUR EDUC, 3GSE	Class capture-the-flag exercises	53	4.82	1.58
4	Chothia T, 2015, USENIX SUMMIT GAMING, GAMES, GAMIFICATION SECUR EDUC, 3GSE	An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education	46	4.60	3.96
5	Olano M, 2014, USENIX SUMMIT GAMING, GAMES, GAMIFICATION SECUR EDUC, 3GSE	SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education	35	3.18	1.04
6	Crick T, 2019, PROC FRONT EDUC CONF FIE	A UK Case Study on Cybersecurity Education and Accreditation	33	5.50	5.08
7	Deng Y, 2022, J ARTIF INTELL TECHNOL	Problem-Based Cybersecurity Lab with Knowledge Graph as Guidance	31	10.33	5.47
8	Van Steen T, 2021, CYBERPSYCHOL BEHAV SOC NETWORKING	Successful Gamification of Cybersecurity Training	27	6.75	4.89
9	Henshel DS, 2016, PROC IEEE MIL COMMUN CONF MILCOM	Predicting proficiency in cyber defense team exercises	26	2.89	2.46
10	Crick T, 2020, PROC FRONT EDUC CONF FIE	Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes	24	4.80	4.19

According to the data, the most cited works imply that interactive and gamifications, also experiential learning methods are the most predominant approach used in current cybersecurity education. Notably, the high citation counts of most recent work such as [5] and [35] reveal a rising interest in AI driven problem-based labs and simulations as well as gamified cybersecurity training.

From the data, lack of research from non-Western institutions and authors in top cited documents reveals that studies which are influential in cybersecurity education are still limited to certain regions. To address the issue of global cybersecurity challenges, this indicates that more research contributions should be diversified and more cross-regional collaboration needed to develop cybersecurity education strategies.

e-ISSN 2821-3394

4.4 The Trending Topics in Cybersecurity Education (2010-2024)

4.4.1 Topics by Author's Keywords

The examination of the author keyword in cybersecurity education subjects within the studied timeframe demonstrates the change in research interests over the years as indicated in the **Table 9** below. The analysis of available literature for the years 2011 to 2016 shows that a major part of the research was centered on *"Information Security Education"* (2011), *"Information Security"* (2014), and *"Curriculum Development"* (2015) which suggest that these periods focused more on the building blocks of teaching concepts in cybersecurity. The later years come with the incorporation of *"Experiential Learning"* (2018) and *"Pedagogy"* (2015) which point to a shift towards the adoption of innovative teaching styles. The general concept of *"Education"* was heavily discussed from 2021 to 2023, signifying further discussions around methods of teaching cybersecurity. Other than that, the recent data shifts towards more focus on *"Serious Games"* (2021), *"Cybersecurity Education"* (2020), *"Gamification"* (2020), and "Active Learning" (2022), where their Q3 and median values suggest a growing and stable prominence in the area.

TABLE 9
Trending Topics by Author's Keywords (2010-2024)

Term	Frequency	Year (Q1)	Year (Median)	Year (Q3)
Information Security Education	8	2011	2013	2016
Information Security	9	2014	2017	2020
Experiential Learning	11	2018	2019	2022
Curriculum Development	13	2015	2020	2021
Pedagogy	7	2015	2020	2021
Computer Science Education	6	2019	2020	2021
Education	14	2016	2021	2023
Serious Games	5	2021	2021	2024
Cybersecurity Education	52	2020	2022	2023
Gamification	44	2020	2022	2023
Active Learning	7	2022	2023	2024

These trends imply that the nature of cybersecurity education research has moved from broad and traditional to more interactive and student-centered approaches in teaching and learning. After 2020, *gamification* and *serious games* have demonstrated rising popularity, reinforcing the trend towards technology enhanced education, towards engagement driven learning approaches. The acknowledgement of *"Active Learning"* as a prominent field (2022-2024) suggests that there is a recent wave towards more practical and hands-on practices, thus, keeping a focus on practical skills when designing a cybersecurity education and training program is so much relevant. Other than that, the absence of keywords related to AI driven education, personalized learning and adaptive curricula for cybersecurity indicates possibly gaps in the research landscape and worth a further exploration.

e-ISSN 2821-3394

4.4.2 Co-occurrence networks based on Author's Keywords

The visualization in **Figure 3** below, represents a co-occurrence network of keywords related to cybersecurity education, generated using bibliometric analysis tool; VOSviewer. The nodes in the network correspond to keywords used in research articles, while the links represent their co-occurrence relationships. The size of each node indicates the frequency of the keyword's usage, and the thickness of the links reflects the strength of co-occurrence between terms. Different colors represent clusters, which group keywords based on thematic similarity or shared research focus areas.

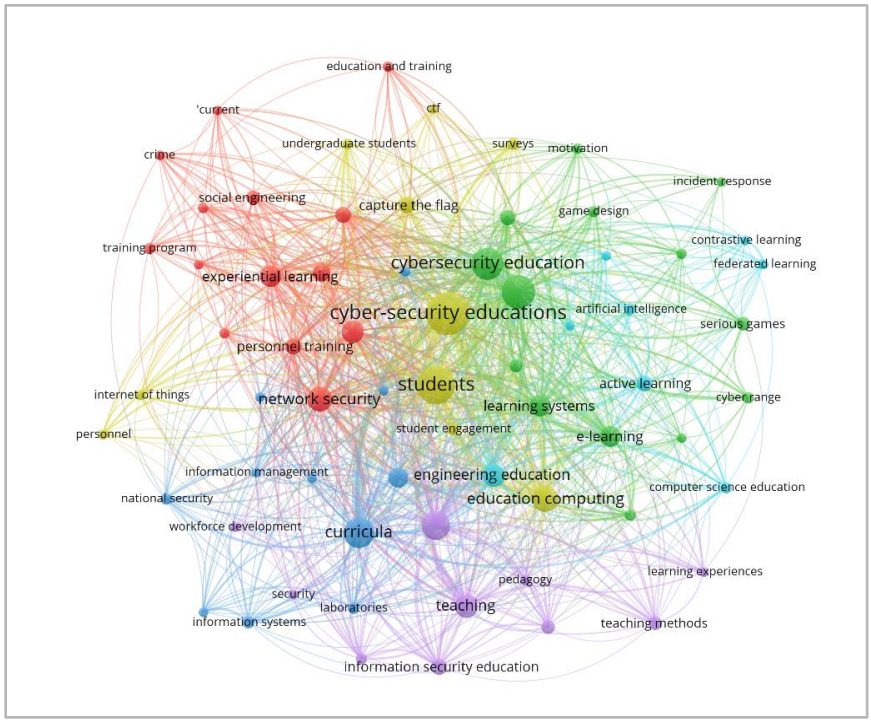

Figure 3. Co-occurrence networks by Keywords and Keywords Plus

The analysis of co-occurrence networks indicates one of the key dominant aspects of cybersecurity education research which is the most frequent concentration node *"cybersecurity education* or *cyber-security educations*." This indicates that those terms are the central or most cited in the literature and is suggestive of a lot of work done in this area. Cluster analysis and sub-network visualization shows that the network is divided into various clusters each pertaining to a specific area of interest in cybersecurity education.

Based on the clusters of research focus as illustrated by **Figure 3**, the *"experiential learning", "network security", "capture the flag (CTF)",* and *"social engineering"* are some of the keywords attributed to the red cluster. This shows the focus on the constructions of learning through practical approaches. The latter emphasizes the application of gamified approaches and simulation exercises as methods of developing cybersecurity competencies. *"Active learning", "e-learning", "serious games"*, and *"cyber range"* are some of the terms in the green cluster. They suggest the use of the newest technologies in instruction for active and productive learning. On the other hand, the blue cluster concentrates on curriculum and instructional design, which is suggested by the words

e-ISSN 2821-3394

"curricula", "pedagogy", "teaching", and *"information security education".* In this case, the focus is might related on how to create and organize effective education programs for cybersecurity. Finally, the yellow cluster centers around *"students", "engineering education",* and *"education computing"* showcasing a more learner-centric approach to Cybersecurity Education in Engineering and Computing disciplines.

Other than that, the network also shows *"federated learning," "artificial intelligence," "contrastive learning,"* and *"game design"* as emerging keywords, suggesting an increasingly sophisticated use of technology in teaching cybersecurity. The way these concepts are related indicates high interdependence among them, which confirms the multidisciplinary character of educational research in cybersecurity. As *"active learning"* and *"serious games"* are associated with *"student engagement"* and *"teaching methods,"* they demonstrate the relevance of engaging and holistic approaches to learning and instruction. This cloud illustrates the change in cyber security education practices from relying on lectures to employing high technology resources.

The variety of themes also indicates gaps that need to be studied, like the implementation of tools powered by AI with federated learning systems, which offer great potential for further examination. Overall, the network emphasizes the necessity of collaboration and creativity in curriculum construction to solve issues related to teaching and improve the quality of cybersecurity education.

5.0 Discussion and Conclusions

The significance of this study lies in the quantitative and visualized mapping of research trends rather than in hypothesis testing or experimental results. The bibliometric outputs presented in this study such as publication trends, keyword co-occurrence, authorship networks, and thematic evolution serve as the core findings that reveal how research in cybersecurity education has evolved over time. These outputs are significant because they expose:

- The growth trajectory and global research attention toward cybersecurity education;
- The influential authors, institutions, and collaboration networks driving this field; and
- The emerging thematic clusters and conceptual directions shaping future research priorities.

Collectively, these insights provide a data-driven understanding of the knowledge structure within cybersecurity education an essential contribution for scholars, policymakers, and educators aiming to strengthen digital resilience and workforce readiness in the cybersecurity domain.The analysis has captured important aspects of the development of cybersecurity education research noting important gaps, trends, and possibilities for future research. The results indicate a shift from conventional instruction to more active and technology-centered approaches like gamified learning, simulations, flipped classroom models, and virtual laboratories. Though educational innovations have been prepared, many essential gaps and priorities for research still exist.

5.1 Emerging Trends in Cybersecurity education

There has been an upward trend in the research output in cybersecurity education over the last decade especially after 2019 when annual publications increased from 17 in 2019 to 46 in 2024.

e-ISSN 2821-3394

This shows emerging business and academic interest in improving the educational systems so as to cope with the changing cybersecurity challenges. The following are key emerging themes:

- *Experiential learning and gamification:* There is increased attention on student centered learning through the use of cyber ranges, CTF exercises and serious games as engagement and skill development tools.
- *Shifts from passive to active learning:* The terms *"cybersecurity education"* (52), *"gamification"* (44), and *"active learning" (7)* are demonstrative of focus on active teaching methods.
- *Collaboration networks and institutional impact:* Despite the growing research output, most of the publications (18.9%) still come from the US. This shows a concentration of the western institutions in cybersecurity education research.

5.2 Gaps and Challenges in Cybersecurity Education Research

However, although great progress has been made, the analysis shows existing gaps in research:

- *Low cross-country co-authoring works:* Only about 11.62 percent of the studies involve cross country collaboration.
- *Uneven distribution of research efforts:* The total number of publications is 37, led by the U.S. but the contributions from other countries (8 to 13 per country) are significantly lower.
- *Lack of AI-driven, adaptive learning methodologies:* Gamification, and experiential learning are the current fads while research on AI based personalized learning with associated techniques like federated learning, adaptive cybersecurity training is largely unanswered by research.
- *Lack of systematic reviews and meta-analyses:* There are only 3 review papers in the dataset, which provide opportunity to integrate and build evidence based best practices in cybersecurity education.

5.3 Future Research Directions

In order to tackle these gaps and optimize the effectiveness of cybersecurity education research, this study has suggestions for further studies as follows:

- *Researching more effective work schemes through the use of AI:* The use of artificial intelligence, machine learning, and federated learning within the processes of cybersecurity training could better facilitate personalized education, threat modeling, and adaptive skill set building.
- *Fostering international collaborations:* These types of partnerships will encourage diversification and development of security research perspectives at a global stage which will support the development of the internationally relevant cybersecurity curriculum.
- *Longitudinal assessment of impact:* There should be longitudinal studies with focus on problem-based learning, gamification and simulations to assess their efficiency on real life cybersecurity skill acquisition in the future.

e-ISSN 2821-3394

- *Designing the cybersecurity curriculum for new challenges and threats:* Aligning education with the dynamic nature of cyber threats, industry requirements, and international governance policies is a challenging task and needs further investigation.
- *Future studies to explore how national security and information warfare narratives influence curriculum design, policy formation, and talent development within cybersecurity education*: As cybersecurity becomes increasingly intertwined with national interests and geopolitical stability, educational institutions play a pivotal role in preparing a workforce capable of addressing complex security challenges. Integrating themes of national security and information warfare into academic curricula could help bridge the gap between theoretical knowledge and practical defense applications. Moreover, understanding how these narratives shape policy directions may guide universities and training institutions in aligning their programs with national cybersecurity strategies. This alignment would not only enhance the relevance of cybersecurity education but also foster the development of a skilled and adaptive talent pipeline capable of contributing to both civilian and defense-oriented digital resilience initiatives.

5.4 Implications for Policy and Practice

Other than that, these outcomes have considerable implications for practitioners, curriculum developers, and policymakers as follows:

- To ensure that students are able to apply cybersecurity skills in real life, curriculum designers should include the use of practical, participatory instructional methods.
- International research initiatives within regions of higher learning should be developed to mitigate the gaps in cybersecurity training.
- Advanced cybernetic educators are to be focused on artificial intelligence-based cybersecurity education to ensure adequate adaptive skills of cybernetic specialists in the future.

5.5 Conclusion

This bibliometric study illustrates the continuous progression which requires that instruction in cybersecurity must become more multifaceted and technologically centric than it currently is. At the same time, there are still challenges that need to be met, such as lack of international collaboration, insufficient coverage of AI-assisted education, and a lack of systematic research literature on the discipline. Meeting these obstacles will rely on interdisciplinary research, political will, and novel solutions to pedagogy and will help construct the future of education in the field of cybersecurity. In that context, interdisciplinary approaches will be essential in the next research on the intersection of cybersecurity education and new technologies. Focusing on foreign relations and carrying out the evaluation of the effectiveness of innovative teaching techniques over time will strengthen the impact of teaching cybersecurity. By using the results from bibliometric analyses, educators and decision-makers will be able to address the needs of learners in combating cyberattacks by creating the relevant learning programs.

e-ISSN 2821-3394

Acknowledgements:

The authors would like to acknowledge the Faculty of Information Science, Universiti Teknologi MARA (UiTM), for the support provided throughout this research.

References:

[1] M. M. Khan, "Cybersecurity awareness," *Indian Sci. J. Res. Eng. Manage.*, vol. 8, no. 10, pp. 1–14, 2024, doi: 10.55041/ijsrem36233.

[2] S. M. Hussain, S. R. K. Tummalapalli, and A. S. N. Chakravarthy, "Cyber security education: Enhancing cyber security capabilities, navigating trends and challenges in a dynamic landscape," in *Advances in Cyber Security and Digital Forensics*, pp. 9–33, 2024.

[3] P. Perälä and M. Lehto, "Educating cybersecurity experts: Analysis of cybersecurity education in Finnish universities," in *Proc. Eur. Conf. Cyber Warfare and Security*, vol. 23, no. 1, 2024.

[4] D. Aoyama, K. Yonemura, and A. Shiraki, "Effective methods in cybersecurity education for beginners," in *Proc. 12th Int. Conf. Information and Education Technology (ICIET)*, Mar. 2024, pp. 372–375.

[5] Y. Deng, Z. Zeng, K. Jha, and D. Huang, "Problem-based cybersecurity lab with knowledge graph as guidance," *J. Artif. Intell. Technol.*, vol. 2, pp. 55–61, 2022, doi: 10.37965/jait.2022.0066.

[6] C. D. Coleman and E. Reeder, "Three reasons for improving cybersecurity instruction and practice in schools," in *Proc. Society for Information Technology & Teacher Education Int. Conf.*, Washington, DC, USA, Mar. 2018, pp. 1020–1025.

[7] C. Phuong, N. Saied, and L. Yang, "A hands-on education framework for cybersecurity," in *Proc. IEEE Frontiers in Education Conf. (FIE)*, 2023, pp. 1–5, doi: 10.1109/FIE58773.2023.10343268.

[8] J. Collins and V. Ford, "Teaching by practice: Shaping secure coding mentalities through cybersecurity CTFs," *J. Cybersecurity Education, Research & Practice*, 2023, doi: 10.32727/8.2023.8.

[9] Z. Kaplan, N. Zhang, and S. V. Cole, "A capture the flag (CTF) platform and exercises for an intro to computer security class," in *Proc. 27th ACM Conf. Innovation and Technology in Computer Science Education*, vol. 2, pp. 597–598, Jul. 2022.

[10] I. Ahmed and V. Roussev, "Peer instruction teaching methodology for cybersecurity education," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 88–91, 2018.

[11] K. H. Abdullah, M. H. Roslan, N. S. Ishak, M. Ilias, and R. Dani, "Unearthing hidden research opportunities through bibliometric analysis: A review," *Asian Journal of Research in Education and Social Sciences*, vol. 5, no. 1, pp. 251–262, 2023.

[12] N. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," *Int. J. Inf. Educ. Technol.*, vol. 10, no. 5, pp. 378–382, 2020, doi: 10.18178/IJIET.2020.10.5.1393.

[13] L. Tsado, "Cybersecurity education: The need for a top-driven, multidisciplinary, school-wide approach," *J. Cybersecurity Education, Research and Practice*, vol. 2019, no. 1, Art. no. 4, 2019.

[14] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National initiative for cybersecurity education (NICE) cybersecurity workforce framework," *NIST Special Publication*, vol. 800, p. 181, 2017.

[15] E. Sobiesk, J. Blair, G. Conti, M. Lanham, and H. Taylor, "Cyber education: A multi-level, multi-discipline approach," in *Proc. 16th Annu. Conf. Information Technology Education*, Sep. 2015, pp. 43–47.

[16] A. Vaish, R. Kumar, S. Bobek, and S. Sternad, "Development of cyber security platform for experiential learning," *J. Cybersecurity Education, Research and Practice*, vol. 2024, no. 1, 2024.

[17] F. Breitinger, J. Ricci, and I. Baggili, "Survey results on adults and cybersecurity education," *Educ. Inf. Technol.*, 2018, doi: 10.1007/s10639-018-9765-8.

[18] S. Grover, B. Broll, and D. Babb, "Cybersecurity education in the age of AI: Integrating AI learning into cybersecurity high school curricula," in *Proc. 54th ACM Tech. Symp. Computer Science Education*, vol. 1, pp. 980–986, Mar. 2023.

[19] J. Hajny *et al.*, "Framework, tools and good practices for cybersecurity curricula," *IEEE Access*, vol. 9, pp. 94723–94747, 2021, doi: 10.1109/ACCESS.2021.3093952.

[20] J. LeClair, S. Abraham, and L. Shih, "An interdisciplinary approach to educating an effective cyber security workforce," in *Proc. InfoSecCD'13: Information Security Curriculum Development Conf.*, Oct. 2013, pp. 71–78.

[21] L. Williams, E. Anthi, Y. Cherdantseva, and A. Javed, "Leveraging gamification and game-based learning in cybersecurity education: Engaging and inspiring non-cyber students," *J. Colloquium Inf. Syst. Secur. Educ.*, vol. 11, no. 1, p. 8, 2024, doi: 10.53735/cisse.v11i1.186.

[22] T. Wu, K. Y. Tien, W. C. Hsu, and F. H. Wen, "Assessing the effects of gamification on enhancing information security awareness knowledge," *Appl. Sci.*, vol. 11, p. 9266, 2021, doi: 10.3390/app11199266.

[23] A. Ahmed, C. Watterson, S. Alhashmi, and T. Gaber, "How universities teach cybersecurity courses online: A systematic literature review," *Frontiers in Computer Science*, vol. 6, 1499490, 2024, doi: 10.3389/fcomp.2024.1499490.

[24] C. Beauchamp and H. M. Matusovich, "A mixed-method study exploring cyber ranges and educator motivation," *J. Cybersecurity Education, Research and Practice*, vol. 2023, no. 2, Art. no. 7, 2023, doi: 10.32727/8.2023.21.

[25] M. N. Katsantonis, A. Manikas, I. Mavridis, and D. Gritzalis, "Cyber range design framework for cyber security education and training," *Int. J. Inf. Secur.*, vol. 22, no. 4, pp. 1005–1027, 2023.

e-ISSN 2821-3394

[26] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, and M. A. Ferrag, "Cyber ranges and testbeds for education, training, and research," *Appl. Sci.*, vol. 11, no. 4, p. 1809, 2021, doi: 10.3390/app11041809.

[27] T. Sarı and A. Aypay, "A bibliometric study of issues in educational policy," *Educ. Sci.*, vol. 14, no. 6, p. 568, 2024, doi: 10.3390/educsci14060568.

[28] L. Sautunnida, R. Ridayani, K. Khairani, E. Kurniasari, A. Utami, and I. Fajri, "Digital legal education and cybersecurity awareness: A bibliometric study on student behavior," *MUKADIMAH: J. Pendidikan, Sejarah, dan Ilmu-ilmu Sosial*, vol. 8, pp. 473–486, 2024, doi: 10.30743/mkd.v8i2.9726.

[29] M. Aria and C. Cuccurullo, "Bibliometrix: An R-tool for comprehensive science mapping analysis," *J. Informetrics*, vol. 11, no. 4, pp. 959–975, 2017.

[30] N. J. Van Eck and L. Waltman, *VOSviewer Manual*. Leiden Univ., 2019. [Online]. Available: https://www.vosviewer.com/documentation/Manual_VOSviewer_1.6.13.pdf

[31] A. Konak, T. K. Clark, and M. Nasereddin, "Using Kolb's experiential learning cycle to improve student learning in virtual computer laboratories," *Comput. Educ.*, vol. 72, pp. 11–22, 2014, doi: 10.1016/j.compedu.2013.10.013.

[32] G. Jin, M. Tu, T. H. Kim, J. Heffron, and J. White, "Game-based cybersecurity training for high school students," in *Proc. 49th ACM Tech. Symp. Computer Science Education*, 2018, pp. 68–73.

[33] J. Mirkovic and P. A. Peterson, "Class capture-the-flag exercises," in *Proc. USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, 2014.

[34] T. Chothia and C. Novakovic, "An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education," in *Proc. USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*, Washington, DC, USA, 2015.

[35] T. Crick, J. H. Davenport, P. Hanna, A. Irons, and T. Prickett, "Overcoming the challenges of teaching cybersecurity in UK computer science degree programmes," in *Proc. IEEE Frontiers in Education Conf. (FIE)*, Uppsala, Sweden, 2020, pp. 1–9, doi: 10.1109/FIE44824.2020.9274033.

[36] T. Crick, J. H. Davenport, A. Irons, and T. Prickett, "A UK case study on cybersecurity education and accreditation," in *Proc. IEEE Frontiers in Education Conf. (FIE)*, Covington, KY, USA, 2019, pp. 1–9, doi: 10.1109/FIE43999.2019.9028407.

[37] T. Van Steen and J. Deeleman, "Successful gamification of cybersecurity training," Cyberpsychol. Behav. Soc. Netw., vol. 24, 2021, doi: 10.1089/cyber.2020.0526.

e-ISSN 2821-3394
