Penerbit Akademia Baru

Journal of Advanced Research Design

Journal homepage:
https://akademiabaru.com/submit/index.php/ard
ISSN: 2289-7984


# Fortifying Information System and Cybersecurity in Engineering Education: A Thematic Review

Irma Syarlina Che Ilias[1,*], Jawahir Che Mustapha[2], Liyana Adilla Burhanuddin[3,4], Mohammed A. Al-Sharafi[5]

[1] Computer Engineering Technology Section, Malaysian Institute of Information Technology, Universiti Kuala Lumpur, 1016, Jalan Sultan Ismail, 50250, Kuala Lumpur, Malaysia
[2] Informatics and Analytics Section, Malaysian Institute of Information Technology, Universiti Kuala Lumpur, 1016, Jalan Sultan Ismail, 50250, Kuala Lumpur, Malaysia
[3] Department of Engineering, King's College London, Strand, WC2R 2LS London, United Kingdom
[4] Department of Electronic Systems Engineering (ESE), Malaysia–Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia
[5] IRC for Finance and Digital Economy, KFUPM Business School, King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia

**ARTICLE INFO**

***Article history:***
Received 1 March 2024
Received in revised form 12 October 2024
Accepted 5 November 2024
Available online 30 November 2024

***Keywords:***
Information system; cybersecurity; engineering education; thematic review

**ABSTRACT**

In today's digital landscape, the seamless integration of robust information systems and cybersecurity into engineering education is critical for preparing future engineers to tackle complex cyber threats. However, current engineering curricula often lack sufficient focus on these critical domains, creating a gap that must be addressed to keep pace with the rapid evolution of cyber threats. This paper aims to address this gap by recommending strategies to enhance cybersecurity and information system integration in engineering programs, emphasizing adapting to emerging technologies. A systematic literature review conducted using Scopus and Mendeley databases identified 98 publications from 2013 to 2022, of which 67 were deemed relevant after filtering for duplicates and irrelevance. Thematic analysis was used to categorize the literature into five main themes, offering insights into key challenges and opportunities for integrating cybersecurity into engineering education. The study finds that adaptation to the evolving cybersecurity landscape and promoting interdisciplinary collaboration are pivotal to advancing curricula. This study concludes that adapting curricula to the evolving cybersecurity landscape is essential for equipping graduates with the skills needed to protect tomorrow's digital infrastructure. Further research is recommended to assess these integrations' long-term impact on graduates and explore how emerging technologies will continue to reshape educational paradigms.

## 1. Introduction

In the rapidly evolving digital era, the seamless integration of robust information systems and cybersecurity into engineering education is a compelling necessity. The escalating frequency and

* *Corresponding author.*
*E-mail address: irmasyarlina@unikl.edu.my*

https://doi.org/10.37934/ard.122.1.8599

complexity of cyberattacks pose a substantial threat to our globally interconnected society, placing a significant responsibility on engineering institutions [1,2]. These institutions bear the crucial task of preparing the next generation of engineers, equipping them to navigate the complex realm of information systems while adeptly guarding against ever-evolving cyber threats. Achieving this transformative goal requires a departure from conventional, isolated educational methodologies in favor of interdisciplinary approaches fostering cyber awareness and providing immersive, industry-integrated learning experiences [3,4]. Within this dynamic and ever-evolving educational milieu, engineering students must acquire proficiency in core technical domains and cultivate the competencies required to fortify the digital bedrock of our contemporary world. Through a comprehensive, forward-thinking approach to engineering education, students are empowered to excel as digital custodians, ensuring the enduring resilience of the digital future.

The compelling necessity to reinforce the integration of Information Systems and Cybersecurity in Engineering Education is underscored by the wealth of research published between 2013 and 2022. This decade has witnessed remarkable advancements in information systems and cybersecurity, making it a pivotal period for exploring best practices, addressing challenges, and capitalizing on opportunities in the field [5]. A review of these research publications provides a systematic framework for understanding the intricacies of incorporating information systems and cybersecurity into engineering curricula. This structured approach serves as a valuable tool for organizing and synthesizing the abundance of insights contained within these publications, facilitating the extraction of essential lessons and evidence-based strategies to enhance engineering education. By harnessing this wealth of knowledge, the accumulated wisdom from the past decade is thoughtfully applied to meet engineering students' present and future needs within our increasingly interconnected world.

Recognizing the evolving landscape, this study identifies crucial gaps in the integration of emerging technologies, such as artificial intelligence and the Internet of Things, into engineering education. While much progress has been made in information systems and cybersecurity, there remains a lack of comprehensive exploration of these technologies' implications within curricula. Moreover, interdisciplinary collaboration and the ability to adapt to constantly evolving cyber threats have not been fully addressed. By exploring these under-examined areas, this study aims to provide valuable insights into how engineering education can evolve to meet the demands of the digital age. The significance of this study lies in its potential to inform educational institutions on how best to enhance their curricula to produce future-ready engineers who are well-equipped to safeguard the digital realm. The objective of this study is to systematically review the integration of information systems and cybersecurity into engineering education over the past decade, identifying key challenges and proposing strategies to fortify curricula for future advancements.

## 2. Methodology

The methodology used in this research is thematic review process. Table 1 summarizes the outcomes derived from an extensive literature search conducted using the Scopus and Mendeley databases. The primary aim of this search was to support the initiation of a systematic review focused on scientific articles found in previous studies [6-9]. Therefore, this systematic review aims to enhance the comprehension of the current academic knowledge pertaining to the intersection of information systems and cybersecurity within engineering education. This systematic review's initial phase yielded a total of 98 publications, drawn from both the Mendeley and Scopus databases. It is noteworthy that the process commenced with a substantial volume of potential articles, comprising 17 from Mendeley and 81 from Scopus. These preliminary findings underscore the foundational stage of the systematic review, wherein a comprehensive selection of relevant scholarly articles is gathered and examined.

To ensure the inclusivity and relevance of the articles, specific selection criteria were meticulously applied during the search. These criteria encompassed articles published within the time frame of 2013 to 2022 and articles that incorporated keywords such as “cybersecurity,” “information system,” or “engineering education.” The application of these criteria refined the search results to form a final pool of 98 publications, which will be subjected to detailed analysis and assessment in subsequent phases of the systematic review. In essence, the compilation of these 98 publications signifies a pivotal milestone in the systematic review process, marking the initial step towards the comprehensive exploration and synthesis of existing academic knowledge in the field of information systems and cybersecurity as they relate to engineering education.

**Table 1**
Search strings from Scopus and Mendeley

| Database | Search string | Results |
|---|---|---|
| Mendeley | “Cybersecurity' AND “Information System” AND “Engineering Education” | 17 |
| Scopus | “Cybersecurity” AND “Information System” AND “Engineering Education” | 81 |

To enhance the quality and relevance of the review, a rigorous process was implemented. Initially, duplicate entries were removed to ensure the analysis was grounded in a unique and distinct set of articles. Subsequently, a meticulous examination of the abstracts of the identified articles was conducted. The primary objective here was to exclude articles that did not closely align with the specific aims and focus of the study. This diligent approach culminated in a streamlined collection of 67 papers, which now form the foundational basis of this review, as indicated in Figure 1. In the context of this research, the term “thematic review” was adopted, and Atlas.Ti was integrated as a supportive tool. This choice is inspired by a model introduced by Zairul [6], seamlessly harmonizing with the chosen approach. Thematic analysis has been prioritized as the central methodology for conducting this comprehensive literature review [7].

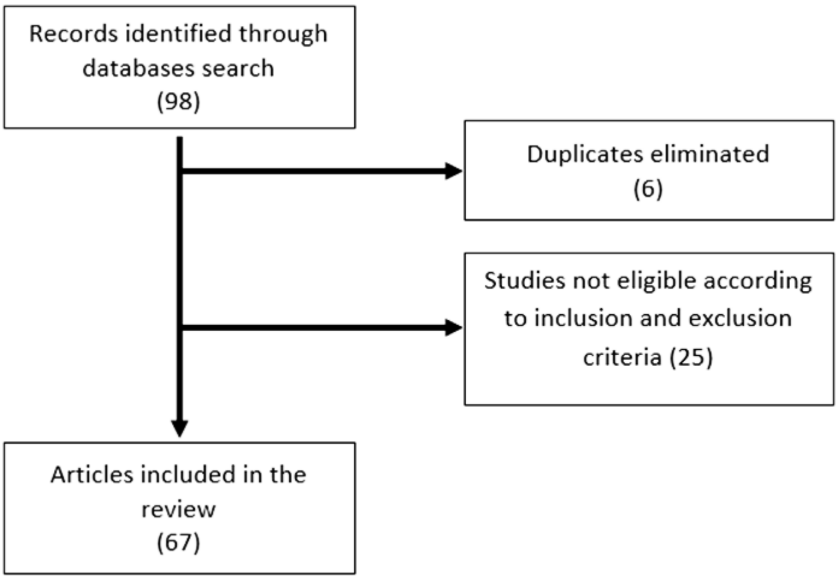


**Fig. 1.** The process flow of article selection within the thematic review

As defined by Braun *et al.,* [10] in their influential work from 2012, thematic analysis is distinguished by its systematic approach to identifying recurring patterns and constructing meaningful themes. This method has proven to be instrumental in the in-depth exploration of the subject matter, enabling the derivation and categorization of significant themes and patterns within the expansive domain of information systems and cybersecurity within the sphere of engineering education on a global scale. This research endeavour goes beyond a comprehensive review; it encompasses the analysis and interpretation of the findings that have been gathered. These findings serve as the foundation for well-informed and constructive recommendations, guiding future research efforts in this critical area of study. The ultimate objective is to contribute to advancing engineering education by illuminating vital insights and potential areas for further exploration and innovation.

In the subsequent phase of the research, all 67 sets of metadata were methodically imported into the data analysis software, Atlas.Ti, and designated as primary documents. This systematic approach facilitated the structured and organized management of the extensive dataset. Initially obtained from Mendeley, the metadata contained valuable information about the selected articles, forming the foundational basis for subsequent analyses. Leveraging the capabilities of Atlas.Ti, a sequence of code groupings was automatically initiated, visually represented in Figure 2 to illustrate the software's organizational framework. The implementation of Atlas.Ti's classification system played a crucial role in optimizing the systematic approach to data analysis. Through the utilization of this system, the sorting process was significantly streamlined, fostering a structured and organized framework for data analysis. This, in turn, enabled the efficient arrangement and categorization of the extensive dataset, making it more manageable for subsequent analyses.

During the initial coding round, a total of 14 primary codes were generated, serving as the fundamental building blocks for the analysis. These codes encapsulated key themes and concepts extracted from the dataset. To further refine organization and effectively address the core research questions, these primary codes were thoughtfully arranged into thematic clusters. This systematic categorization process was a strategic endeavor aimed at deriving meaning from the data and revealing significant patterns and insights within the extensive dataset. Ultimately, this meticulous categorization and organization process culminated in the identification of five main categories, carefully designed to comprehensively address and resolve the core research inquiries. This methodical approach ensured a comprehensive response to the research questions, rendering the insights derived from the dataset well-structured and meaningful for the subsequent in-depth analysis.

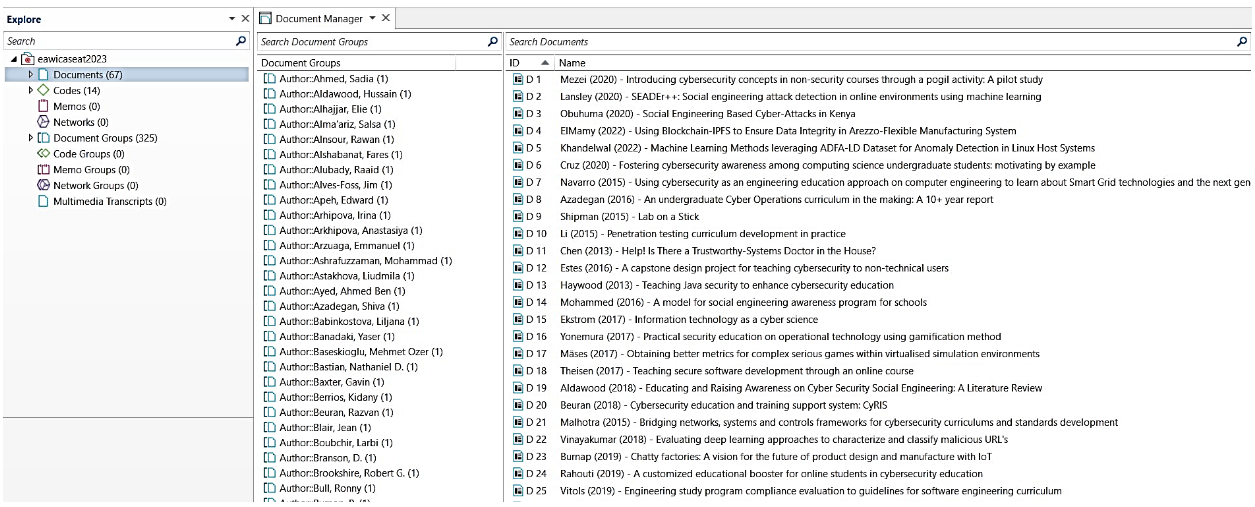


**Fig. 2.** The code group established from Mendeley metadata

## 3. Results

### *3.1 Research Publication*

The limitations encountered in the process of database queries, particularly the constraints imposed by key search phrases such as "cybersecurity" and "information system," led to a critical observation. This observation revealed that the published articles within the domain of engineering education exhibited significant disparities in terms of subject matter, emerging trends, and structural characteristics. A thorough analysis revealed that these research themes were distinctly addressed in 67 articles. Delving further into the data presented in Table 2, it provides valuable insights into the frequency and distribution of articles in the field of information systems, cybersecurity, and engineering education. The publication landscape exhibits notable variations across the years, reflecting the dynamic nature of research in this intersection. Notably, the year 2020 emerges as a prolific period with a surge in publications, featuring diverse conferences such as the European Conference on Cyber Warfare and Security, IST-Africa Conference, and Proceedings of the 21st Annual Conference on Information Technology Education (SIGITE'20). This surge underscores a heightened interest and engagement in information systems and cybersecurity within engineering education during that particular year.

Examining the data further, it is evident that specific conferences, such as the American Society for Engineering Education Annual Conference and IEEE EDUCON, consistently contribute to the body of literature in subsequent years, indicating their significance in shaping discussions around fortifying information systems and cybersecurity in engineering education. The diversity of conferences and journals across the years highlights the multifaceted exploration. However, the analysis also reveals a relative scarcity of publications during the year 2014, with only one recorded article. This anomaly prompts further investigation into the factors contributing to this low output, potentially uncovering shifts in research emphasis or external factors influencing publication trends during that specific year. The nuanced examination of each year's publication output enhances our understanding of the evolving landscape, providing valuable context to the research

**Table 2**
Publication of articles reviewed per year

| Year | Publication |
|---|---|
| 2013 | IEEE security & privacy; Proceedings of IEEE Southeastcon |
| 2014 | IEEE frontiers in education conference (FIE) proceedings |
| 2015 | Journal of Information Technology Education: Innovations in Practice; NY Cyber Security & Engineering Technology Association Conference; Proceedings of the 16th Annual Conference on Information Technology Education (SIGITE'15) |
| 2016 | 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA); IEEE Conference on Intelligence and Security Informatics (ISI); Proceedings of the 17th Annual Conference on Information Technology Education (SIGITE'16) |
| 2017 | European Conference on Games Based Learning; Proceedings of the 18th Annual Conference on Information Technology Education; Proceedings of the International Workshop on Secure Software Engineering in DevOps and Agile Development (SecSE2017) |
| 2018 | 13th International Conference on Malicious and Unwanted Software (MALWARE); 7Th IEEE international conference on control system, computing and engineering (ICCSCE); IEEE international conference on teaching, assessment, and learning for engineering (TALE); IEICE TRANSACTIONS on Information and Systems; Information Technology & People; Journal of Intelligent & Fuzzy Systems |
| 2019 | American Society for Engineering Education, Proceedings of ASEE Annual Conference; CEUR Workshop Proceedings; Engineering for rural development; IEEE International Conference on Big Data (Big Data); IEEE technology & engineering management conference (TEMSCON); IET Conference Publications; Journal of Applied Research in Higher Education; Procedia Computer Science; Proceedings of the 11th International |

**Table 2**
Publication of articles reviewed per year

| Year | Publication |
|---|---|
| | Conference on Computer Supported Education (CSEDU 2019); Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE'19) |
| 2020 | 20th European Conference on Cyber Warfare and Security, American Society for Engineering Education; Proceedings of ASEE Annual Conference (3); IEEE 61th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON); IEEE Access, Intermountain Engineering, Technology and Computing (IETC); International Journal on Interactive Design and Manufacturing; IST-Africa Conference (IST-Africa); Journal of Information and Telecommunication; Latvian Journal of Physics and Technical Sciences; Proceedings of the 2020 Conference for Industry and Education Collaboration (CIEC 2020); Proceedings of the 21st Annual Conference on Information Technology Education (SIGITE'20); Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE'20); Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) |
| 2021 | 1st Babylon International Conference on Information Technology and Science 2021 (BICITS 2021); 2nd Quantum Software Engineering and Technology Workshop co-located with IEEE International Conference on Quantum Computing and Engineering (QCE21); 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA); American Society for Engineering Education; Proceedings of ASEE Annual Conference (3); Emerging Trends in Industry 4.0 (ETI 4.0); IEEE Access, IEEE Global Engineering Education Conference (EDUCON); Information; International Conference Automatics and Informatics (ICAI); World Engineering Education Forum/Global Engineering Deans Council (WEEF/GEDC); Proceedings of the International Workshop on Advanced in Information Security Management and Applications (AISMA 2021) |
| 2022 | 2nd International Conference on Intelligent Technologies (CONIT); American Society for Engineering Education, Proceedings of ASEE Annual Conference; European Simulation and Modelling Conference (ESM 2022); IEEE 8th Information Technology International Seminar (ITIS); IEEE Global Engineering Education Conference (EDUCON); INGENIARE-Revista Chilena de Ingeniería; Journal of Advanced Computer Science and Applications (IJACSA); Journal of Manufacturing Systems, Ninth International Conference on Software Defined Systems (SDS) |

### *3.2 Research Theme*

In the subsequent phase of this study, the chosen articles underwent an exhaustive and iterative review process. This process was characterized by meticulous comparisons that aimed to unveil both shared attributes and discrepancies within the content of these articles. The primary objective of this rigorous approach was to ensure a high degree of cohesion and uniformity in shaping the identified themes, specifically focusing on the dynamic relationship between information systems and cybersecurity within the domain of engineering education. The outcomes of this rigorous thematic review are thoughtfully documented in Table 3, which serves as a comprehensive repository systematically categorizing the reviewed publications into their respective thematic clusters. From this comprehensive examination, five predominant themes have emerged, each representing a pivotal dimension in the landscape of information systems and cybersecurity in engineering education. These themes encompass curriculum integration, cyber awareness, resource management, security education, and technology adaptation. The subsequent sections of this study will delve into these themes, offering profound discussions and meticulous analyses of each one. These discussions illuminate the nuanced aspects, challenges, and opportunities underlying these critical themes. They provide a comprehensive and insightful exploration of the intricate interplay between information systems and cybersecurity within the context of engineering education.

**Table 3**
The tabulation of author's discussion on issues according to theme

| Themes | Authors |
|---|---|
| Curriculum integration | [1,3,11-22] |
| Cyber awareness | [2,4,20,23-29] |
| Resource management | [4,11,12,15,18,22,27,30-32] |
| Security education | [15,18,33-36] |
| Technology adaptation | [3, 12-14,16,18-21,24-28,30, 34,36-39,41-67 |

### *3.2.1 Curriculum integration*

In engineering education, the integration of information systems and cybersecurity into the curriculum poses a complex challenge. The primary objective is to tailor engineering curricula to seamlessly incorporate these critical components while maintaining a balance between core engineering subjects and the necessary knowledge and skills related [1,3,68]. Kannan *et al.,* [1] emphasize the gap in foundational computing courses for cybersecurity, Khader *et al.,* [3] propose a comprehensive framework for awareness across disciplines, and Loo *et al.,* [68] focuses on integrating cybersecurity into STEM, particularly Cyber-Physical Systems security, revealing diverse approaches to curriculum integration in engineering education. An opportunity arises in promoting interdisciplinary synergy among engineering, computer science, and cybersecurity domains [15-17,22]. Estes *et al.,* [15] focuses on developing cybersecurity skills in non-computing students through a Vulnerable Web Server. Ekstrom *et al.,* [16] explore integrating cybersecurity into established computing disciplines and the Information Technology perspective. Rahouti *et al.,* [17] addresses challenges in providing real-world cybersecurity labs for online students. Cletus *et al.,* [22] emphasize Social Engineering Awareness, proposing a behavioral change model for effective training programs, showcasing diverse approaches to curriculum integration in engineering education.

Collaboration and knowledge exchange across these fields enrich the educational experience, preparing students for effective problem-solving in complex, real-world scenarios [18,19]. Vitol *et al.,* [18] focus on evaluating and comparing software engineering study programs' compliance with ACM/IEEE guidelines. In contrast, Zinkus *et al.,* [19] emphasize active learning through a social networking simulation to enhance students' understanding of computer science, cybersecurity, and privacy. Fostering partnerships with industry stakeholders provides practical exposure [69]. Internships, hands-on projects, and industry-driven curriculum elements bridge the gap between theory and practice, equipping engineering graduates to excel in information systems and cybersecurity roles [11,21]. Garces *et al.,* [11] focus on adapting engineering education to Industry 4.0 and BIM, emphasizing experiential learning, teaching methodologies, and CDIO. In contrast Luh *et al.,* [21] propose PenQuest, a digital game based on cyber-attack and defense, aligning with MITRE ATT&CK and NIST SP 800-53, for security education. The integration of information systems and cybersecurity into engineering education is essential for preparing students.

### *3.2.2 Cyber awareness*

Cultivating cyber awareness in engineering education reveals multifaceted dynamics. One key aspect center on effecting behavioral change and fostering active student engagement [25,27,68]. Loo *et.al.,* [68] emphasizes cybersecurity education in the context of Cyber-Physical Systems (CPS), addressing the lack of security awareness in STEM graduates. Aldawood *et al.,* [25] focuses on innovative information security education programs to enhance user awareness and reduce cyber incidents. Campbell *et al.,* [27] investigates cybersecurity issues related to social engineering in organizations, proposing solutions such as education, policies, and continuous training to counteract human deception. While instilling cyber awareness is paramount, the challenge lies in motivating students to adopt security-conscious behaviors [4]. This challenge presents an opportunity for innovative and relatable educational strategies that inspire students to take personal responsibility for cybersecurity [21,23]. Luh *et al.,* [21] introduced PenQuest, a digital attack and defense game, to enhance security education by simulating cyber-attacks and defense scenarios. In contrast, Obuhuma *et al.,* [23] focuses on Social Engineering's prevalence, exploring user understanding and countermeasures, emphasizing the need for awareness and education.

Moreover, the ever-changing landscape of cyber threats necessitates ongoing curriculum updates, presenting the challenge of keeping educational content current and pertinent [22,24]. Cletus *et al.,* [22] focuses on improving Social Engineering Awareness, Training, and Education (SEATE) programs, proposing a behavioral change model. In contrast, Mohammed *et al.,* [24] emphasizes designing awareness programs targeting human vulnerabilities in schools, with a model demonstrating behavior change. In this challenge, the opportunity arises to embrace agile curriculum development approaches, allowing swift adaptation to emerging cybersecurity issues and ensuring that students remain well-prepared for the evolving threat landscape [3,28]. Khader *et al.,* [3] focuses on proposing a conceptual Cybersecurity Awareness Framework for academia to improve graduates' cybersecurity awareness systematically. In contrast, Baseskioglu *et al.,* [28] emphasizes the increasing importance of informing end-users about internet technology and security weaknesses, advocating for education to reduce cyberattacks. Additionally, cybersecurity education extends beyond technical aspects, encompassing ethical, legal, and societal dimensions [29]. Balancing this nuanced landscape poses challenges but also offers the prospect of providing comprehensive cybersecurity education that integrates ethical considerations, legal frameworks, and societal implications, producing well-rounded and cyber-aware engineers.

### *3.2.3 Resource management*

In the realm of engineering education, resource management assumes a pivotal role, particularly when intertwined with information systems and cybersecurity. A nuanced aspect involves the allocation and prioritization of budgets [13,27,70]. Azadegan *et al.,* [13] focuses on the development and evolution of an undergraduate cyber operations program, addressing challenges and lessons learned over 14 years. Campbell *et al.,* [27] investigates social engineering issues and proposes solutions, emphasizing education, policies, and processes. Maxwell *et al.,* [70] explores feature engineering in machine learning for cybersecurity, analyzing data types and ranges for intrusion detection. The key difference lies in their specific focuses: program development, social engineering defense, and machine learning for cybersecurity features. Institutions grapple with the challenge of efficiently distributing limited resources to cater to traditional educational needs while fortifying cybersecurity infrastructure [17,71]. Rahouti *et al.,* [17] focuses on addressing resource challenges in providing real-world cyber labs for online cybersecurity education. Kilber *et al.,* [71] explore the quantum computing threat landscape, emphasizing defensive measures and recommending proactive reduction of the cyberattack surface. The key difference lies in their specific focuses: online cyber labs development and quantum computing threat mitigation. This challenge presents an opportunity to craft strategic resource allocation models that strike an effective balance between these crucial aspects [20,72]. Dawson *et al.,* [20] emphasizes hands-on, dynamic labs for secure software engineering education, while Theisen *et al.,* [72] focuses on MOOCs to retrain professionals, stressing engagement and effective online course strategies.

Moreover, the ever-evolving nature of cybersecurity necessitates access to cutting-edge technologies and tools for education, posing a challenge in ensuring that students remain up-to-date [12,38,39]. Sneps-sneppe *et al.,* [12] focuses on the lag in telecommunications education and the impact of cybersecurity on training. Shipman *et al.,* [38] introduces Lab on a Stick (LoaS) for portable, customizable cybersecurity labs. Vinayakumar *et al.,* [39] evaluates deep learning models for automatic feature extraction in malicious URL detection, outperforming handcrafted features. Collaborations with cybersecurity industry leaders offer the opportunity to provide students with hands-on experience using industry-standard technologies [14,30,31]. Li *et al.,* [14] focuses on developing a penetration testing curriculum to address the shortage of skilled cybersecurity professionals. Hempenius *et al.,* [30] reviews practices to minimize VM resource requirements, enhancing virtual lab performance. Yoon *et al.,* [31] emphasizes team collaboration skills, using Transactive Memory Systems Theory for a Team Knowledge Sharing Assignment in cybersecurity education.

Finally, the development of cybersecurity talent takes center stage, with challenges encompassing the preparation of students for the workforce with practical skills [32,37]. Fuertes *et al.,* [32] focuses on developing an educational environment for Industry 4.0, emphasizing hands-on tasks and practical understanding. Hernandez *et al.,* [37] reviews the state-of-the-art of Industry 4.0, analyzing human talent, qualifications, university courses, and future trends related to IR4.0 education. Opportunities arise in the establishment of collaborative programs with industry partners, offering internships and real-world projects that bridge the gap between academia and industry, resulting in graduates who are well-prepared for the [4,73]. Cruz *et al.,* [4] focuses on a hands-on approach to introductory cybersecurity education, engaging students through vulnerability analysis of IoT devices. Striuk, *et al.,* [73] analyzes the historical evolution of software engineering training, emphasizing the fundamental core and learning outcomes for software engineers. These intricate factors emphasize the significance of well-balanced resource management in cultivating cybersecurity-aware engineers ready for successful careers.

### *3.2.4 Security education*

Security education within engineering education is instrumental in fortifying information systems and cybersecurity. The development of a comprehensive curriculum involves creating coursework that spans the spectrum of security topics, from fundamental principles to advanced practices [41]. Challenges include crafting an inclusive curriculum, while opportunities emerge in adopting a modular approach that enables students to progress through varying levels of expertise [17]. Bridging the gap between theory and application represents another facet, with challenges surrounding the provision of practical, hands-on experiences in simulated or real-world cybersecurity scenarios [20]. Here, opportunities manifest in the establishment of dedicated labs, simulations, and projects that empower students to apply their theoretical knowledge in practical contexts [33]. Furthermore, collaboration with industry experts and professionals plays a pivotal role, ensuring that security education remains abreast of rapidly changing industry trends [40]. Challenges include curriculum alignment, while opportunities surface in partnering with industry leaders to provide guest lectures, industry projects, and internships, thereby affording students valuable insights into the real-world dynamics of cybersecurity [17]. These detailed reflections highlight the diverse aspects of security education in engineering programs, underscoring the necessity for a comprehensive, practical, and industry-integrated approach to cybersecurity knowledge and competencies.

#### *3.2.5 Technology adaptation*

In the field of engineering, the theme of technology adaptation assumes paramount significance as it grapples with the fast-paced technological advancements that define the digital age. An essential aspect revolves around the challenge of staying abreast of this ever-evolving landscape, where tools and technologies swiftly become obsolete [13,15,25,27,39,45-47,53,58,65]. Authors offer diverse insights on technology adaptation in cybersecurity education. From curriculum evolution and social engineering defenses to machine learning for URL detection and gaming in OT security, they address challenges with varied perspectives, highlighting the dynamic nature of staying current in this rapidly evolving landscape. Ensuring that students receive training on the latest cybersecurity solutions presents a challenge, emphasizing the need for adaptable and future-ready curricula that focus on principles and versatile skills rather than specific tools as per discuss in previous study [3,14,24, 37,38,41,46,53,66,68,73]. Authors contribute diverse perspectives on technology adaptation in cybersecurity education. Topics range from a comprehensive Cybersecurity Awareness Framework, CPS security education, and penetration testing curriculum to addressing human vulnerabilities in social engineering. Others explore mobile-oriented training environments, industry 4.0 talent requirements, and the implementation of cyber ranges for hands-on practice. Each author emphasizes unique aspects, including the incorporation of security into STEM education, holistic CPS modeling, and the creation of portable cybersecurity labs. Despite common themes of skills development and awareness, the authors showcase varied approaches and foci within the dynamic landscape of cybersecurity education.

Furthermore, adapting to emerging technologies such as artificial intelligence and the Internet of Things brings forth curriculum integration challenges [19,21,35,36,49,56,59-61,66,67]. Authors offer diverse perspectives on technology adaptation in engineering education. Topics cover adjusting engineering education for Industry 4.0 and Building Information Modeling (BIM), exploring social engineering in cybersecurity, utilizing AI for cybersecurity, integrating games-based construction learning for programming education, securing flexible manufacturing systems with blockchain, and evaluating anomaly detection in operating systems. Some focus on incorporating cybersecurity principles into Engineering Technology Education and bridging the knowledge gap between engineers and IT/Cybersecurity professionals. Others emphasize the role of data science in STEM education and interdisciplinary research projects. Each author uniquely addresses technology adaptation challenges in the dynamic landscape of engineering and cybersecurity education.

However, opportunities arise in harnessing these technologies to fortify cybersecurity practices and apply them practically within disciplines [28,35,36,43,48,49,60,61,71]. Authors also offer diverse perspectives on technology adaptation in engineering education and cybersecurity. Baseskioglu *et al.,* [28] emphasizes the need for end-user awareness in the context of online security and cyberbullying. Kilber *et al.,* [71] focuses on the quantum threat and defensive measures for quantum computing systems. Elmamy, *et al.,* [35] proposes using blockchain for securing intelligent manufacturing systems in the Fourth Industrial Revolution. Khandelwal *et al.,* [36] explores anomaly detection in operating systems with a focus on machine learning. Yasinsac *et al.,* [43] discusses the state of trustworthy systems and the need for PhD programs in the field. Burnap [48] presents the "Chatty Factories" project, exploring IoT-enabled data-driven systems in design and manufacturing. Chan *et al.,* [49] explores AI applications in cybersecurity. Alnsour *et al.,* [60] advocates for incorporating cybersecurity principles into engineering and IT education. Banadaki *et al.,* [61] focuses on data science education and its applications in STEM projects, including cybersecurity. Each author contributes a unique perspective on the intersection of technology, cybersecurity, and engineering education.

Encouraging cybersecurity research and innovation within engineering education stands as a vital aspect, with resource limitations and fostering a culture of research as challenges [26,30,42,52,62]. Astakhova *et al.,* [26] focuses on machine learning for cost-effective internal testing against social engineering, Hempenius *et al.,* [30] in minimize VM resource needs, Navarro *et al.,* [42] integrates Smart Grid cybersecurity into engineering education Yousuf *et al.,* [52] targets underrepresented minorities with a new cybersecurity degree, and Quweider *et al.,* [62] addresses the graduate shortage through a holistic bachelor's program. Each author contributes uniquely to technology adaptation in information systems and cybersecurity education. In response, opportunities unfold through the provision of research avenues, access to cutting-edge labs, and faculty mentorship, empowering students to contribute to groundbreaking research and innovative solutions in the sphere of information systems and cybersecurity [16,18,20,50,55].

Ekstrom *et al.,* [16] explores the integration of cybersecurity into established computing disciplines, emphasizing Information Technology's perspective Vitols *et al.,* [18] evaluates the compliance of a software engineering program with ACM/IEEE guidelines. Dawson *et al.,* [20] focuses on experiential learning and secure software engineering labs in response to the growing demand for cybersecurity professionals. Crichigno [50] addresses the cybersecurity workforce gap through curricular material based on virtual laboratories and industry alliances. Dawson [55] discusses the online teaching of cybersecurity during a pandemic, emphasizing partnerships to meet national security needs, including collaborations with the military and industry. Each author uniquely contributes to technology adaptation in information systems and cybersecurity education. These subtle factors emphasize the constantly evolving nature of integrating technology into engineering education and stress the essential requirement for progressive approaches that empower students with the necessary knowledge and skills in the ever-shifting realm of information systems and cybersecurity.

## 4. Conclusions

This comprehensive literature review and thematic analysis of information systems and cybersecurity integration within engineering education reveal a multifaceted landscape. The study responds to the research objective by identifying key challenges in integrating cybersecurity into engineering curricula, including motivating cyber awareness, managing resources, developing comprehensive security education, and keeping up with evolving technology. The analysis also uncovers significant opportunities through interdisciplinary collaboration, innovative pedagogical methods, and partnerships with industry, all of which enhance students' preparedness to address modern cybersecurity challenges. Moreover, the findings underscore the need for future research to assess the impact of these integrations on graduates' readiness and explore the role of emerging technologies in reshaping educational paradigms. Collaboration between key stakeholders—industry players, intelligence providers, regulators, academics, and end-users—emerges as a crucial factor in improving cybersecurity education and awareness. This collaborative approach can help simultaneously address the dual agenda of enhancing education and cybersecurity practices. Therefore, future studies should examine these collaborative efforts in greater detail, ensuring that all stakeholders proactively share knowledge and expertise.

**Acknowledgement**
The author expresses gratitude to Universiti Kuala Lumpur (UniKL) for their gracious provision of financial assistance.

## References

[1] Kannan, Uma, and Rajedran Swamidurai. "Integrating cybersecurity concepts across undergraduate computer science and information systems curriculum." In *2021 ASEE Annual Conference*. 2021.
[2] Khader, Mohammed, Marcel Karam, and Hanna Fares. "Cybersecurity awareness framework for academia." *Information* 12, no. 10 (2021): 417. https://doi.org/10.3390/info12100417
[3] Cruz, Tiago, and Paulo Simões. "Fostering cybersecurity awareness among computing science undergraduate students: Motivating by example." In *20th European Conference on Cyber Warfare and Security*, p. 72. 2020.
[4] Khattak, Muhammad Adil, Muhammad Khairy Harmaini Shaharuddin, Muhammad Saiful Islam Haris, Muhammad Zuhaili Mohammad Aminuddin, Nik Mohamad Amirul Nik Azhar, and Nik Muhammad Hakimi Nik Ahmad. "Review of cyber security applications in nuclear power plants." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 7, no. 1 (2017): 43-54.
[5] Zairul, Mohd. "A thematic review on student-centred learning in the studio education." *Journal of Critical Reviews* 7, no. 2 (2020): 504-511. https://doi.org/10.31838/jcr.07.02.95
[6] Kanafiah, Siti Farah Haryatie Mohd, Abdul Rahman Mohd Kasim, Syazwani Zokri, and Nur Syamilah Arifin. "A thematic review on mathematical model for convective boundary layer flow." *Journal of Advanced Research in Fluid Mechanics and Thermal Sciences* 86, no. 2 (2021): 107-125. https://doi.org/10.37934/arfmts.86.2.107125
[7] Braun, Virginia, and Victoria Clarke. *Thematic analysis*. American Psychological Association, 2012.
[8] Kuzlu, Murat, and Otilia Popescu. "Upgrading of a data communication and computer networks course in engineering technology program." *ASEE Virtual Annual Conference Content Access* (2020):1-15. https://doi.org/10.18260/1-2--35436
[9] Loo, Sin Ming, and Liljana Babinkostova. "Cyber-physical systems security introductory course for STEM students." *ASEE Annual Conference and Exposition, Conference Proceedings* (2020): 29171-1-29171-9. https://dx.doi.org/10.18260/1-2--34366
[10] Garcés, Gonzalo, and Camilo Peña. "Adaptar la educación en ingeniería al BIM ya la Industria 4.0: Una visión desde la teoría experiencial de Kolb en el laboratorio." *Ingeniare. Revista Chilena De Ingeniería* 30, no. 3 (2022): 497-512. https://doi.org/10.4067/S0718-33052022000300497
[11] Sneps-Sneppe, M., D. Namiot, and R. Pauliks. "Information System Cyber Threats and Telecommunications Engineering Courses." *Latvian Journal of Physics and Technical Sciences* 57, no. 1-2 (2020): 52-61. https://doi.org/10.2478/lpts-2020-0007
[12] Azadegan, Shiva, and Michael O'Leary. "An undergraduate cyber operations curriculum in the making: A 10+ year report." In *2016 IEEE Conference on Intelligence and Security Informatics* (ISI), p. 251-254. IEEE, 2016. https://doi.org/10.1109/ISI.2016.7745484
[13] Li, Chengcheng. "Penetration testing curriculum development in practice." *Journal of Information Technology Education. Innovations in Practice* 14 (2015): 85. https://doi.org/10.28945/2189
[14] Estes, Tanya, James Finocchiaro, Jean Blair, Johnathan Robison, Justin Dalme, Michael Emana, Luke Jenkins, and Edward Sobiesk. "A capstone design project for teaching cybersecurity to non-technical users." In *Proceedings of the 17th Annual Conference on Information Technology Education*, p. 142-147. 2016. https://doi.org/10.1145/2978192.2978216
[15] Ekstrom, Joseph J., Barry M. Lunt, Allen Parrish, Rajendra K. Raj, and Edward Sobiesk. "Information technology as a cyber science." In *Proceedings of the 18th Annual Conference on Information Technology Education*, p. 33-37. 2017. https://doi.org/10.1145/3125659.3125697
[16] Rahouti, Mohamed, and Kaiqi Xiong. "A customized educational booster for online students in cybersecurity education." In *CSEDU (2)*, p. 535-541. 2019. https://doi.org/10.5220/0007767205350541
[17] Vitols, Gatis, Irina Arhipova, and Liga Paura. "Engineering study program compliance evaluation to guidelines for software engineering curriculum." *Engineering for rural development. Latvia University of Life Sciences and Technologies, Jelgava* 18 (2019): 1910-1914. https://doi.org/10.22616/ERDev2019.18.N328
[18] Zinkus, Maximilian, Oliver Curry, Marina Moore, Zachary Peterson, and Zoë J. Wood. "Fakesbook: A social networking platform for teaching security and privacy concepts to secondary school students." In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, p. 892-898. 2019. https://doi.org/10.1145/3287324.3287486
[19] Dawson, Maurice, Pedro Taveras, and Danielle Taylor. "Applying software assurance and cybersecurity NICE job tasks through secure software engineering labs." *Procedia Computer Science* 164 (2019): 301-312. https://doi.org/10.1016/j.procs.2019.12.187
[20] Luh, Robert, Sebastian Eresheim, Stefanie Größbacher, Thomas Petelin, Florian Mayr, Paul Tavolato, and Sebastian Schrittwieser. "PenQuest reloaded: A digital cyber defense game for technical education." In *2022 IEEE Global*

*Engineering Education Conference (EDUCON)*, p. 906-914. IEEE, 2022. https://doi.org/10.1109/EDUCON52537.2022.9766700
[21] Cletus, Azaabi, Benjamin Weyory, and Alex Opoku. "Improving social engineering awareness, training and education (SEATE) using a behavioral change model." *International Journal of Advanced Computer Science and Applications* 13, no. 5 (2022). https://doi.org/10.14569/IJACSA.2022.0130572
[22] Obuhuma, James, and Shingai ZIVUKU. "Social engineering based cyber-attacks in kenya." In *2020 IST-Africa Conference (IST-Africa)*, p. 1-9. IEEE, 2020. http://dx.doi.org/10.4067/S0718-33052022000300497
[23] Mohammed, Saba, and Edward Apeh. "A model for social engineering awareness program for schools." In *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*, p. 392-397. IEEE, 2016. https://doi.org/10.1109/SKIMA.2016.7916253
[24] Aldawood, Hussain, and Geoffrey Skinner. "Educating and raising awareness on cyber security social engineering: A literature review." In *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)*, p. 62-68. IEEE, 2018. https://doi.org/10.1109/TALE.2018.8615162
[25] Astakhova, Liudmila, and Ivan Medvedev. "Scanning the resilience of an organization employees to social engineering attacks using machine learning technologies." In *2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, p. 606-610. IEEE, 2020. https://doi.org/10.1109/USBEREIT48449.2020.9117746
[26] Campbell, Curtis C. "Solutions for counteracting human deception in social engineering attacks." *Information Technology & People* 32, no. 5 (2019): 1130-1152. https://doi.org/10.1108/ITP-12-2017-0422
[27] Başeskioğlu, Mehmet Özer, and Abdülkadir Tepecik. "Cybersecurity, computer networks phishing, malware, ransomware, and social engineering anti-piracy reviews." In *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, p. 1-5. IEEE, 2021. https://doi.org/10.1109/HORA52670.2021.9461272
[28] Alma'ariz, Salsa, Raden Budiarto Hadiprakoso, and Nurul Qomariasih. "Soceng warriors: Game-based learning to increase security awareness against social engineering attacks." In *2022 IEEE 8th Information Technology International Seminar (ITIS)*, p. 124-129. IEEE, 2022. https://doi.org/10.1109/ITIS57155.2022.10009041
[29] Striuk, Andrii M., and Serhiy O. Semerikov. "The dawn of software engineering education." In *Computer Science & Software Engineering. Proceedings of the 2nd Student Workshop (CS&SE@ SW 2019), Kryvyi Rih, Ukraine, November 29, 2019*, no. 2546, p. 35-57. CEUR Workshop Proceedings, 2019.
[30] Maxwell, Paul, Elie Alhajjar, and Nathaniel D. Bastian. "Intelligent feature engineering for cybersecurity." In *2019 IEEE International Conference on Big Data (Big Data)*, p. 5005-5011. IEEE, 2019. https://doi.org/10.1109/BigData47090.2019.9006122
[31] Hempenius, Nicholas, Te-Shun Chou, and Lee Toderick. "Challenges of virtual machine performance in information and computer technology virtual lab environments." In *Proceedings of the 2020 Conference for Industry and Education Collaboration* (2020).
[32] Yoon, Kay, and Sang-Yoon Chang. "Teaching team collaboration in cybersecurity: A case study from the transactive memory systems perspective." In *2021 IEEE Global Engineering Education Conference (EDUCON)*, p. 841-845. IEEE, 2021. https://doi.org/10.1109/EDUCON46332.2021.9453894
[33] Fuertes, Juan José, Miguel Ángel Prada, José Ramón Rodríguez-Ossorio, Raúl González-Herbón, Daniel Pérez, and Manuel Domínguez. "Environment for education on industry 4.0." *IEEE Access* 9 (2021): 144395-144405. https://doi.org/10.1109/ACCESS.2021.3120517
[34] Hernandez-de-Menendez, Marcela, Carlos A. Escobar Díaz, and Ruben Morales-Menendez. "Engineering education for smart 4.0 technology: A review." *International Journal on Interactive Design and Manufacturing (IJIDeM)* 14 (2020): 789-803. https://doi.org/10.1007/s12008-020-00672-x
[35] Kilber, Natalie, Daniel Kaestle, and Stefan Wagner. "Cybersecurity for quantum computing." *arXiv preprint arXiv:2110.14701* (2021). https://doi.org/10.48550/arXiv.2110.14701
[36] Shipman, Peter, and Ronny Bull. "Lab on a stick." In *Proceedings of the 16th Annual Conference on Information Technology Education*, p. 33-38. 2015. https://doi.org/10.1145/2808006.2808034
[37] Theisen, Christopher, Ted Zhu, Kevin M. Oliver, and Laurie A. Williams. "Teaching secure software development through an online course." In *SecSE@ ESORICS*, p. 19-33. 2017.
[38] Vinayakumar, R., K. P. Soman, and Prabaharan Poornachandran. "Evaluating deep learning approaches to characterize and classify malicious URL's." *Journal of Intelligent & Fuzzy Systems* 34, no. 3 (2018): 1333-1343. https://doi.org/10.3233/JIFS-169429
[39] Mezei, Razvan A., Mario Guimaraes, and Xuguang Chen. "Introducing Cybersecurity Concepts in Non-Security Courses through a POGIL Activity: A Pilot Study." In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, p. 1290-1290. 2020. https://doi.org/10.1145/3328778.3372575

[40] Beuran, Razvan, Cuong Pham, Dat Tang, Ken-ichi Chinen, Yasuo Tan, and Yoichi Shinoda. "Cybersecurity education and training support system: CyRIS." *IEICE TRANSACTIONS on Information and Systems* 101, no. 3 (2018): 740-749. https://doi.org/10.1587/transinf.2017EDP7207
[41] Von Solms, Sune, and Lynn A. Futcher. "Adaption of a secure software development methodology for secure engineering design." *IEEE Access* 8 (2020): 125630-125637. https://doi.org/10.1109/ACCESS.2020.3007355
[42] Kim, Tae-Hoon, Ge Jin, Michael Tu, and Tianyang Guan. "Credential Harvesting using Raspberry Pi." In *2020 ASEE Virtual Annual Conference Content Access*. 2020.
[43] ElMamy, Sidi Boubacar, Hassen Gharbi, Hichem Mrabet, and Abderrazak Jemai. "Using blockchain-IPFS to ensure data integrity in Arezzo-flexible manufacturing system." *European Simulation and Modelling Conference.* 2022.
[44] Khandelwal, Pulkit, Praveen Likhar, and Ravi Shankar Yadav. "Machine learning methods leveraging ADFA-LD dataset for anomaly detection in linux host systems." In *2022 2nd International Conference on Intelligent Technologies (CONIT)*, p. 1-8. IEEE, 2022. https://doi.org/10.1109/CONIT55038.2022.9848305
[45] Navarro, Daniel, Jean C. Méndez, Kidany Berríos, Eduardo Ortiz-Rivera, and Emmanuel Arzuaga. "Using cybersecurity as an engineering education approach on computer engineering to learn about Smart Grid technologies and the next generation of electric power systems." In *2014 IEEE frontiers in education conference (FIE) proceedings*, p. 1-8. IEEE, 2014. https://doi.org/10.1109/FIE.2014.7044336
[46] Yasinsac, Alec, and Cynthia Irvine. "Help! is there a trustworthy-systems doctor in the house?" *IEEE Security & Privacy* 11, no. 1 (2013): 73-77. https://doi.org/10.1109/MSP.2013.10
[47] Haywood, Adley, Huiming Yu, and Xiaohong Yuan. "Teaching Java security to enhance cybersecurity education." In *2013 Proceedings of IEEE Southeastcon*, p. 1-6. IEEE, 2013. https://doi.org/10.1109/SECON.2013.6567447
[48] Yonemura, Keiichi, Kuniaki Yajima, Ryotaro Komura, Jun Sato, and Yoshihiro Takeichi. "Practical security education on operational technology using gamification method." In *2017 7Th IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, p. 284-288. IEEE, 2017. https://doi.org/10.1109/ICCSCE.2017.8284420
[49] Mäses, Sten, Bil Hallaq, and Olaf Maennel. "Obtaining better metrics for complex serious games within virtualised simulation environments." In *European Conference on Games Based Learning*, p. 428-434. *Academic Conferences International Limited*, p. 428-434. 2017.
[50] Malhotra, Yogesh. "Bridging networks, systems and controls frameworks for cybersecurity curriculums and standards development." *Journal of Operational Risk* 13, no. 1 (2018). https://doi.org/10.21314/JOP.2018.201
[51] Burnap, Pete, David Branson, Dave Murray-Rust, John Preston, Dan Richards, Dan Burnett, Nicola Edwards, Rhiannon Firth, Katerina Gorkovenko, Mojtaba Khanesar, Mike Lakoju, Tom Smith, and James Thorpe. "Chatty factories: A vision for the future of product design and manufacture with IoT." In *Conference on Living in the Internet of Things,* p. 4-6. 2019. https://doi.org/10.1049/cp.2019.0129
[52] Chan, Leong, Ian Morgan, Hayden Simon, Fares Alshabanat, Devin Ober, James Gentry, David Min, and Renzhi Cao. "Survey of AI in cybersecurity for information technology management." In *2019 IEEE technology & engineering management conference (TEMSCON)*, p. 1-8. IEEE, 2019. https://doi.org/10.1109/TEMSCON.2019.8813605
[53] Crichigno, Jorge, Sadia Ahmed, John H. Gerdes, and Robert G. Brookshire. "Building a cybersecurity pipeline through experiential virtual labs and workforce alliances." In *2019 ASEE Annual Conference & Exposition*. 2019.
[54] Arkhipova, Anastasiya. "Multisociometrical readiness characteristics in information security management." In *Proceedings of the International Workshop on Advanced in Information Security Management and Applications (AISMA 2021)*, p. 25-34. 2021.
[55] Yousuf, Asad, A. G. De La Cruz, and Frederick T. Sheldon. "Computer science technology-cyber security option." In *ASEE Virtual Annual Conference Content Access*. 2021. http://dx.doi.org/10.18260/1-2--36830
[56] Pickering, Cynthia Kay, Caroline VanIngen-Dunn, and Maria A. Reyes. "Work-focused experiential learning to increase STEM student retention and graduation at two-year Hispanic-serving institutions." In *ASEE Annual Conference*. 2021.
[57] Thamer, Noor, and Raaid Alubady. "A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research." In *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, p. 210-216. IEEE, 2021. https://doi.org/10.1109/BICITS51482.2021.9509877
[58] Dawson, Maurice, Andreas Vassilakos, and Ahmed ben Ayed. "Strengthening university computing programs to meet national security needs." In *2021 World Engineering Education Forum/Global Engineering Deans Council (WEEF/GEDC)*, p. 542-544. IEEE, 2021. https://doi.org/10.1109/WEEF/GEDC53299.2021.9657325
[59] Hainey, Thomas, Gavin Baxter, and Amanda Ford. "An evaluation of the introduction of games-based construction learning in upper primary education using a developed game codification scheme for scratch." *Journal of Applied Research in Higher Education* 12, no. 3 (2020): 377-402. https://doi.org/10.1108/JARHE-02-2018-0031

[60] Trifonov, Roumen, Ognian Nakov, Slavcho Manolov, Georgy Tsochev, and Galya Pavlova. "" Cyber-security of industrial computer systems"-Differentiaton as a separate discipline." In *2021 International Conference Automatics and Informatics (ICAI)*, p. 414-419. IEEE, 2021. https://doi.org/10.1109/ICAI52893.2021.9639645

[61] Rambabu, S., N. Thirupathi Rao, M. Ramakotaiah, J. Simhadri Raju, and J. Venumurali. "Security vulnerabilities affecting on addititve manufacturing systems in the era of Industry 4.0: an extensive review." *2021 Emerging Trends in Industry 4.0 (ETI 4.0)* (2021): 1-5. https://doi.org/10.1109/ETI4.051663.2021.9619291

[62] Kunicina, Nadezhda, Anatolijs Zabasta, Ojars Krumins, Andrejs Romanovs, and Antons Patlins. "Cybersecurity curricula recommendations development for technical background and engineering skills in international dimension." In *2020 IEEE 61th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON)*, p. 1-6. IEEE, 2020. https://doi.org/10.1109/RTUCON51174.2020.9316573

[63] Alnsour, Rawan, and Basil Hamdan. "Incorporating SCADA Cybersecurity in Undergraduate Engineering Technology & Information Technology Education." In *2020 Intermountain Engineering, Technology and Computing (IETC)*, p. 1-4. IEEE, 2020. https://doi.org/10.1109/IETC47856.2020.9249163

[64] Banadaki, Yaser. "Enabling data science education in stem disciplines through supervised undergraduate research experiences." In *Proceedings ASEE Annual Conference*. 2022.

[65] Quweider, Mahmoud K., Fitratullah Khan, Liyu Zhang, and Hangsheng Lei. "Crafting a degree, empowering students, securing a nation: The creation of a modern cyber security degree for the 21st century." In *2022 ASEE Annual Conference & Exposition*. 2022.

[66] Mounnan, Oussama, Otman Manad, Larbi Boubchir, Abdelkrim El Mouatasim, and Boubaker Daachi. "Deep learning-based speech recognition system using blockchain for biometric access control." In *2022 Ninth International Conference on Software Defined Systems (SDS)*, p. 1-2. IEEE, 2022. https://doi.org/10.1109/SDS57574.2022.10062921

[67] Rahman, Md Habibor, and Mohammed Shafae. "Physics-based detection of cyber-attacks in manufacturing systems: A machining case study." *Journal of Manufacturing Systems* 64 (2022): 676-683. https://doi.org/10.1016/j.jmsy.2022.04.012

[68] Nelson, James, and Brent Donham. "Institutional review panel for cybersecurity research and education." In *2022 ASEE Annual Conference & Exposition*. 2022.

[69] Jillepalli, Ananth A., Daniel Conte de Leon, Brian K. Johnson, Yacine Chakhchoukh, Ibukun A. Oyewumi, Mohammad Ashrafuzzaman, Frederick T. Sheldon, Jim Alves-Foss, and Michael A. Haney. "METICS: A holistic cyber physical system model for ieee 14-bus power system security." In *2018 13th International Conference on Malicious and Unwanted Software (MALWARE)*, p. 95-102. IEEE, 2018. https://doi.org/10.1109/MALWARE.2018.8659367

[70] Lansley, Merton, Francois Mouton, Stelios Kapetanakis, and Nikolaos Polatidis. "SEADer++: social engineering attack detection in online environments using machine learning." *Journal of Information and Telecommunication* 4, no. 3 (2020): 346-362. https://doi.org/10.1080/24751839.2020.1747001

[71] Chi, Cai, Melor Md Yunus, Karmila Rafiqah M. Rafiq, Hamidah Hameed, and Ediyanto Ediyanto. "A Systematic Review on Multidisciplinary Technological Approaches in Higher Education." *International Journal of Advanced Research in Future Ready Learning and Education* 36, no. 1 (2024): 1-10. https://doi.org/10.37934/frle.36.1.110

[72] Mijan, Rohana, Noor Aziah Abdullah, and Norsiah Abdul Hamid. 2024. "The preliminary result of technology digital branding practices in Malaysian Cyberspace". *Journal of Advanced Research in Computing and Applications* 30, no. 11 (2023):12-18. https://doi.org/10.37934/arca.30.1.1218

[73] Padeli, Wahidah, Wan Azani Mustafa, Faizuniah Pangil, Kadzrina Abd Kadir, and Vidyarini Dwita. "Knowledge management and the Fourth Industrial Revolution (4IR): A recent systematic review." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 51, no. 2 (2025): 18-33. https://doi.org/10.37934/araset.51.2.1833