International Conference
NEW PERSPECTIVES in SCIENCE EDUCATION

Introducing the Principles of Cybersecurity, Artificial Intelligence, and IoT Applications into the STEM Curriculum to Enhance Students' Hands-on Learning, Conducting Real-World Case Studies and Project-Based Assessments is truly a Novel and Sensational Approach

Olakunle Abayomi Ajala[1], Daniel Alabi Soladoye[2]

Indiana Wesleyan University, United States[1]
Obafemi Awolowo University, Ile-Ife, Nigeria[2]

Abstract

The evolving technology has reshaped industry settings making Cybersecurity, AI, and IoT align with industries' demands. Industries possess security threats making security education more essential, and IoT has revolutionized industries in which STEM student needs these skills to be future-ready. Integrating cybersecurity, AI, Internet of Things (IoT) into STEM education is crucial for preparing future leaders and professionals. This framework is to introduce cybersecurity principles, Artificial intelligence, and IoT applications into the STEM curriculum to enhance student hands-on learning, real-world case studies, and project-based assessments, also this framework not only aims to equip students with the necessary competencies to navigate and secure interconnected digital environment but in addition, prepares student with the necessary skill set they need to navigate through real life digital landscape. Furthermore, the framework helps students develop a firsthand mindset in the security field and also highlights the opportunities possessed by artificial intelligence, smart technologies, and other evolving technologies. These studies discussed the best practices STEM students need, challenges they might face, and implementation strategies. The research also emphasized the need for interdisciplinary collaboration among educators (Teachers and Lectures), industry experts, and policymakers. The proposed model aligns with the evolving Technology relating to Cybersecurity, AI, and IoT and expected demands in the global digital landscape, to ensure that STEM graduates are well-equipped with the necessary skills and prepare for future careers and challenges in the cybersecurity landscape, Artificial intelligence (AI), IoT, and emerging technologies.

Keywords: *STEM Education, Cybersecurity, Artificial intelligence (AI), Internet of Things (IoT), Digital Literacy, Future-Ready Workforce.*

1. Introduction

1.1 Science, Technology, Engineering, and Mathematics (STEM) Education

STEM curricula typically emphasize engineering ideas, mathematics, and the natural sciences, with a rising emphasis on technology and creativity. STEM education is defined as an interdisciplinary approach to student learning that studies science, technology, engineering, and mathematics at school, at work, and worldwide to acquire STEM literacy abilities that can help students compete in the new knowledge-based economic age [1]. Competence in STEM fields is becoming increasingly important as the industry 4.0 revolution and the growth of IoT, artificial intelligence, and cybersecurity accelerate. The rise of the industrial 4.0 era has forced all fields to compete to catch up. This influences the STEM learning technique in educational settings [2]. STEM growth is undoubtedly felt by primary school pupils, and it is required for success in college, career, and STEM professional domains [3]. The STEM approach allows prospective teachers, particularly elementary school teachers, to understand the concepts and principles of science, technology, engineering, and mathematics that are used in an integrated manner to develop processes, products, and systems that can be used in everyday life [4].
Students and other stakeholders such as scientists, engineers, and policymakers, believe STEM education to be an instructional, creative, and inspiring way since it increases creativity and drives to learn and can help with job decisions [5]. STEM can help students improve their critical thinking skills [6],

gain experience, boost their enthusiasm and motivation, develop an understanding of the engineering design process, and integrate science, technology, engineering, and mathematics to solve real-world problems [7]. However, there is still a dearth of integration of cybersecurity, Artificial intelligence (AI) and the Internet of Things (IoT) into STEM curricula at many educational institutions. This discrepancy may be attributed to several factors, including the rapid advancement of technology, the ignorance of educators, and the absence of a standardized framework for integrating several fields.

1.2 Cybersecurity, AI and IoT

As technology advances at an unprecedented rate STEM students need to have a solid foundation in cyber science education to effectively contribute to the digital world. Cyber science education is the process of educating and learning about cybersecurity, digital literacy, and other relevant skills. Topics covered in this discipline include data privacy, online safety, digital ethics, coding, network security, and digital forensics. The major purpose of cyber science education is to provide students with the information and skills they need to improve their critical thinking, problem-solving, and collaboration abilities (Spencer, 2024). Cybersecurity is the process, action, ability, or condition that ensures information and communications systems and the data they contain are safe from harm, illegal use alteration, or exploitation [8].

Understanding cybersecurity concepts and practices is critical across sectors in today's digital age. According to a recent study, computing areas will account for the majority of STEM-related occupations and around two-thirds of all new STEM positions between 2019 and 2029 [9], [10]. Graduates who have both technology and cybersecurity expertise have a competitive advantage in the labour market because they are well-equipped to meet the problems provided by cyber threats and breaches [11].

Similarly, the Internet of Things (IoT) concept is rapidly gaining traction in powering many aspects of life. The Internet of Things connects many devices to build a network that communicates data and information and can be operated remotely over the Internet. This network allows users to manage real-time data and automate complicated procedures. Initially, the IoT was envisioned as a network of real-world objects (or things) with limited storage and processing capacity that prioritized dependability, performance, security, and privacy. However, IoT has emerged as a prominent disruptive technology, allowing ubiquitous and pervasive computing scenarios [12]. IoT devices are constantly expanding and are predicted to reach 1.6 trillion US dollars in size by 2025 [13]. There is growing interest in employing IoT technology in agriculture, the food processing sector, environmental monitoring, security surveillance, robots and drones, education, and other important areas [14], [15].

The rapid growth of IoT applications has increased the demand for experienced professionals with strong IoT hands-on skills. However, undergraduate students in STEM education still lack experience in how to use IoT technologies to develop such innovative applications. This is in part because the current computing curricula do not adequately cover the fundamental concepts of IoT [16].

Educational models need to change from traditional, content-focused learning to strategies that promote interdisciplinary knowledge, critical thinking, and lifelong learning to prepare the next generation for the future-ready workforce. Conventional educational approaches, which have mostly emphasized discipline-specific knowledge and content-based learning, are becoming less and less adequate to meet the demands of the quickly changing labour market. Many old occupations are becoming obsolete as regular work across sectors is automated, while new employment that did not exist ten years ago is developing [17]. The speed at which technology is developing, especially in the areas of artificial intelligence and robotics, is changing the nature of cognitive work in addition to displacing manual labour. Artificial intelligence (AI) is a fast-expanding discipline with applications in a variety of areas, including STEM education, big data analytics, materials informatics, and machine learning [18], [19], [20].

Rapid technological breakthroughs, growing global interconnectedness, and the creation of intricate social, economic, and environmental concerns are all contributing factors to the world's current extraordinary rate of change. Because of this change, educational systems urgently need to adapt as companies, society, and daily life are being reshaped. In addition to navigating a world impacted by automation, robots, artificial intelligence (AI), and the Internet of Things (IoT), the workforce of the future will be required to address global concerns including resource shortages, inequality, and climate change. In this regard, education must foster the flexibility, inventiveness, and resilience required to prosper in a constantly shifting environment in addition to imparting information [21].

Essentially, despite the contributions that these emerging technologies (cybersecurity, AI and the IoT) can offer several sectors, including the educational sector, there is a notable lack of effective frameworks that include them (cybersecurity, AI and the IoT) into STEM curriculum. To address both technical and soft skills, this study intends to explore how educational institutions may create and execute a thorough framework that successfully incorporates cybersecurity, AI and IoT ideas into STEM education.

2. Methodology

The study uses a review analysis to assess previous studies and materials on STEM, cybersecurity, AI, the IoT, and education. Some of the consulted databases included ScienceDirect, JSTOR, Google Scholar, Springer, and IEEE.

3. Findings

3.1 Integration of Cybersecurity, AI and Iot Into STEM Education

The integration of cyber science education into specific STEM fields, such as computer science, engineering, and mathematics, has been the subject of previous research. For instance, a study talked about a beginning course on cyber-physical systems security for Boise State University STEM students [22]. These studies concentrate on how to successfully integrate cyber ideas and abilities into STEM courses that are already in place. According to these studies findings, integrating cyber science instruction into STEM curricula encourages interdisciplinary cooperation, develops students' critical thinking and problem-solving abilities, and gets them ready for jobs in the digital age [23]. Additionally, a study emphasized how cyber science education may help close the gender gap in STEM [24].

Several studies stress the use of AI and big data in education. Use of adaptive e-learning systems driven by AI and big data in higher education institutions to support instructors and students in the teaching process while also providing insights on the educational implications of these technologies in higher education [25]. Another set of authors explains the creation of a novel teaching paradigm based on AI technology, which includes artificial intelligence hardware and software such as big data and cloud computing. The approach encompasses pre-class, in-class, and post-class instruction, offering insights into how AI may be integrated into the teaching process [26].

Furthermore, several studies emphasize the necessity of investigating the application of learning analytics, computational analytical tools, and artificial intelligence in higher education. A study emphasizes the importance of learning analytics in tracking student progress, assessing university data, and devising evaluations [27]. Starcic investigates the role of human learning and learning analytics in the age of artificial intelligence, stressing the significance of comprehending human learning processes and utilizing learning analytics to improve educational results [28].

However, to educate students for the employment of the future, educators are realizing how important it is to include AI principles in their curricula [18], [19], [20]. Interactive, hands-on methods that encourage learning by doing are one way to teach AI.

Furthermore, IoT technologies have the potential to monitor students' physical fitness data, increase supply chain traceability, and improve logistics management in educational settings [29], [30]. IoT is an effective educational tool for learning programming, addressing educational challenges, and providing critical applications for both students and instructors [31]. IoT can assist overcome educational hurdles such as geography and economic inequities, creating new potential for educational access and diversity [32].

The integration of IoT in education has the potential to provide more individualized and dynamic learning experiences, as well as new channels for instructional delivery [33], [34]. Furthermore, IoT offers a great chance to adapt educational possibilities for people with impairments, promoting inclusive learning settings [35]. Numerous nations have launched programs to use technology for educational improvement. Singapore, for example, implemented the Intelligent Nation Masterplan in 2006, with a strong emphasis on technology-enabled education [36]. South Korea began the Smart Education Project, which intended to restructure the educational system and enhance pedagogical techniques [37].

Furthermore, it has been demonstrated that incorporating IoT technology into the educational process enhances learning quality and unleashes the creative potential of both teachers and students [38]. The

intriguing possibility of connecting and instructing students in smart campus environments is presented by the integration of the Internet of Things in education.

3.2 Role of AI, Iot and Cybersecurity in the Digital Transformation

STEM and computer science education have a complex and advantageous relationship. Triplett [39] emphasized the value of STEM fields as the foundation of our technologically advanced civilization. The development of the information, abilities, and mentality necessary for resolving complex issues and promoting technological innovation depends heavily on STEM education [40]. Innovation, teamwork, problem-solving, interdisciplinary learning, and the practical application of STEM ideas may all be stimulated by including cyber science education in the STEM curriculum [41]. Students who study cyber science also acquire important knowledge on the moral, legal, and societal implications of technology use [41], [42]. The integration of cybersecurity principles into STEM curricula allows educators to design authentic learning experiences that effectively reflect the changing demands of the digital landscape, and it also acts as a catalyst for increasing diversity and promoting inclusion in these fields. By introducing cybersecurity concepts at an early age, educational institutions can encourage interest and engagement among underrepresented groups, which in turn helps to develop a more diverse STEM workforce [43].
Beyond cybersecurity, AI has a function in education. It enables individualized learning experiences, enabling teachers to modify their lessons according to the needs of each unique student. AI improves overall learning results by allowing instructors to concentrate on more intricate educational exchanges by automating repetitive chores [39]. Additionally, based on student achievement, AI may dynamically modify task complexity, fostering an adaptable learning environment that accommodates a variety of learners [44].
The utilization of Internet of Things (IoT) devices in the educational process offers several distinct advantages [45]. These advantages can be categorized as follows:
Training purposes: IoT devices are useful resources for studying certain courses, especially in the STEM (science, technology, engineering, and mathematics) disciplines.
Control function: Internet of Things devices serve as self-control tools that let people keep an eye on their actions. This encourages self-control skills to be formed and offers a way to get outside help when needed.
Ergonomic function: By helping with activities like time management, planning, and improving the effectiveness of instructional procedures, IoT devices help people to be more productive.

3.3 Challenges

Despite the positive impacts of cybersecurity, AI and the IoT, in several sectors and curricula, there are still issues in integrating and expanding cyber science instruction, AI and the IoT in STEM fields [46]. The absence of standardized evaluation techniques to accurately gauge students' cybersecurity, AI and IoT, expertise is a major obstacle. The effectiveness of cyber science education programs, AI and IoT depends on the development of credible and trustworthy evaluation instruments that are in line with the intended learning objectives. The lack of certified educators with pedagogical experience in STEM education and a thorough knowledge of cybersecurity concepts, AI and the IoT is another difficulty. To overcome this obstacle, professional development initiatives that provide educators with specific training and assistance in cyber science teaching, AI and the IoT within STEM fields are essential [47].
Another urgent issue is guaranteeing fair access to infrastructure, technology, and resources. It is crucial to create plans that close the digital gap and give underprivileged areas access to high-quality resources for cyber science education, AI and IoT. Collaboration between academic institutions, legislators, and business partners is crucial to addressing these issues. This kind of cooperation is essential for creating all-encompassing plans that support the smooth integration of cybersecurity, AI and the IoT into STEM at different educational levels [48].

3.4 Multi-Level Framework of Technology Acceptance and Use (MFTAU)

MFTAU (Multi-Level Framework of Technology Acceptance and Use) is a framework to consider while integrating cybersecurity, AI and IoT into the educational curriculum. Venkatesh created the MFTAU

model. This model combines the findings of theoretical analysis and presents them in the form of a multilevel framework. The MFTAU framework examines technology acceptance and usage at two levels of analysis: higher-level contextual factors (HC) and individual-level contextual factors (IC). These two stages presumably influence an individual's willingness to adopt and use technology [49]. Individual-level Contextual Factors (IC) account for the moderating effects of age, gender, and experience in UTAUT [50]. Higher-level Contextual Factors (HC) comprise the physical surroundings of the particular user, which acts as the immediate context for the adoption and usage of technology. Students' engagement and use of cybersecurity, artificial intelligence, and the Internet of Things (IoT) can be improved by incorporating these cutting-edge technologies into STEM courses through the Multi-Level Framework of Technology Acceptance and Use (MFTAU). By taking into account several levels of impact, including organizational, environmental, and human aspects, the MFTAU framework aids in understanding how instructors and students embrace and use technology in a learning environment.

3.5 Approaches for Integrating Cybersecurity, AI and the Iot into STEM Curricula Cross-Disciplinary Approaches

Beyond the boundaries of conventional computer science programs, incorporating cybersecurity, AI topics, and the IoT into other areas provides a holistic educational approach. Teachers may provide a more comprehensive learning experience that emphasizes the significance of cybersecurity, AI and IoT in daily life by incorporating cybersecurity principles into topics like language arts, arithmetic, and social studies. Students might investigate the moral ramifications of internet privacy and the effects of cyber laws on society, for instance, in social studies class. Cryptographic algorithms and their use in protecting digital communications can be covered in math classes [51]. This technique also helps students to see the actual uses of cybersecurity knowledge, AI and IoT in many circumstances, promoting a more in-depth and nuanced understanding of the subject. It also promotes collaborative learning and critical thinking, as students examine how cybersecurity, AI and IoT challenges influence numerous elements of life and professional domains [52].

PROJECT-BASED LEARNING AND REAL-WORLD APPLICATIONS: Through actual situations and hands-on projects, project-based learning (PBL) provides an efficient way to introduce students to cybersecurity, AI and IoT principles. This method improves students' problem-solving abilities and comprehension of cybersecurity, AI and IoT methods by enabling them to apply theoretical knowledge to actual issues. Students might, for example, work on projects that model the development of safe software, examine a fictitious network's weaknesses, or create defences against cyberattacks [53].

COLLABORATION WITH INDUSTRY EXPERTS: Cybersecurity, AI and IoT education may be greatly improved by utilizing collaborations with cybersecurity, AI and IoT companies and experts. Industry professionals give students current information and real-world viewpoints by sharing their insightful opinions on the newest methods, instruments, and trends in the area. Professionals in cybersecurity, AI and IoT may provide schools with guest lectures, workshops, and mentoring programs that enhance the learning environment and give students access to networking possibilities [54].

CURRICULUM DESIGN AND DEVELOPMENT: Some crucial actions must be taken when creating an effective STEM curriculum, which integrates cybersecurity, AI and IoT, to guarantee that it both academic requirements and student demands. Teachers must first establish precise learning goals and outcomes in the areas of cybersecurity, AI and IoT. For instance, this involves identifying the fundamental ideas and abilities that students ought to learn, such as comprehending cyber threats, putting security measures in place, and identifying moral dilemmas about digital privacy [55].

INFRASTRUCTURE AND RESOURCES: Build technologically advanced learning spaces with sensors, IoT devices, and cybersecurity resources. With the use of this infrastructure, students may participate in actual simulations and experiments that reinforce theoretical ideas [56]. As an adjunct to classroom training, give students access to online resources such as tutorials, simulations, and collaborative platforms so they may independently research IoT and cybersecurity topics [57].

STAKEHOLDER ENGAGEMENT: Working with stakeholders such as parents, industry experts, policymakers and educational officials to promote and advocate for the integration of cybersecurity, AI and the IoT, into STEM curricula. Collaboration with these stakeholders can give useful insights and resources for ensuring program quality and relevance [58].

4. Conclusion

Integrating cybersecurity, AI, and IoT into STEM courses is a forward-thinking technique that boosts student engagement with hands-on learning and real-world applications. As educational institutions adopt this unique method, students are better equipped to handle an increasingly complicated technology context. This comprehensive educational model supports intellectual progress while also preparing future professionals for the obstacles they will confront in their jobs.

REFERENCES

[1] Reeve, E. M. “Implementing science, technology, mathematics and engineering (STEM) education in Thailand and ASEAN (Bangkok: Institute for the Promotion of Teaching Science and Technology)”, 2013.
[2] Wicaksono AG. Penyelenggaraan pembelajaran IPA berbasis pendekatan STEM dalam menyongsong era revolusi industri 4.0. LENSA (Lentera Sains): Jurnal Pendidikan IPA. 2020 May 25;10(1):54-62.
[3] Tran, Y. “Computer Programming Effects in Elementary: Perceptions and Career Aspirations in STEM. Technology, Knowledge and Learning”, 2018, 23(2), 273–299. DOI:10.1007/s10758-018-9358-z
[4] Kelana, J.B., Wardani, D.S., Firdaus, A.R., Altaftazani, D.H., Rahayu, G.D.S. “The effect of STEM approach on the mathematics literacy ability of elementary school teacher education student”, Journal of Physics: Conference Series, 2020.
[5] Ugras, M. “The Effect of STEM Activities on STEM Attitudes, Scientific Creativity and Motivation Beliefs of the Students and Their Views on STEM Education”, International Online Journal of Educational Sciences,2018, 10(5), 165-182
[6] Elfrida Yanty Siregar, Y., Rachmadtullah, R., Pohan, N., Rasmitadila, & Zulela, M. “The impacts of science, technology, engineering, and mathematics (STEM) on critical thinking in elementary school”, Journal of Physics: Conference Series, 2019, 1175, 012156. doi:10.1088/1742-6596/1175/1/012156
[7] Daugherty, M.K., Carter, V., Swagerty, L. “Elementary STEM Education: The Future for Technology and Engineering Education?”, Journal of STEM Teacher Education, 2014, 49(1), 45-55.
[8] National Initiative for Cybersecurity Careers and Studies, “NICE Cybersecurity Workforce Framework | National Initiative for Cybersecurity Careers and Studies,” National Institute of Standards and Technology, 2019. [Online]. Available: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework. [Accessed: 20-Mar-2019].
[9] Burrell, D. N., Dattola, A., Dawson, M. E., & Nobles, C. “A practical exploration of cybersecurity faculty development with microteaching”, In Information Resources Management Association (Ed.), Research anthology on advancements in cybersecurity education (pp. 477–490). IGI Global, 2022, https://doi.org/10.4018/978-1-6684-3554-0.ch023
[10] Zilberman, A., & Ice, L. “Why computer occupations are behind strong STEM employment growth in the 2019-29 decade. U.S. Bureau of Labor Statistics”, 2021 https://www.bls.gov/opub/btn/volume-10/why-computer-occupations-are-behind- strong-stem-employment-growth-hm
[11] Cheng, E. C. K., & Wang, T. “Institutional strategies for cybersecurity in higher education institutions. Information”, 2022, 13(4), 192. https://doi.org/10.3390/info13040192
[12] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, ‘‘A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of nano things (IoNT),’’ in Proc. Internet Technol. Appl. (ITA), Sep. 2015, pp. 219–224.
[13] Vailshery, S. “Forecast End-User Spending on IoT Solutions Worldwide From 2017 to 2025 [Online]”, 2021, Available: https://www.statista.com/statistics/976313/global-iot-market-size/
[14] Da Xu, L., He, W. and Li, S. “Internet of things in industries: A survey”, IEEE Transactions on Industrial Informatics, 2014, 10(4), pp.2233-2243.
[15] Li, S., Da Xu, L. and Zhao, S. ”5G Internet of Things: A survey. Journal of Industrial Information Integration”, 2018, 10, pp.1-9.
[16] Ahmed, A.A.; Bellam, K.; Yang, Y.; Preuss, M. “Integrating IoT Technologies into the CS Curriculum at PVAMU: A Case Study”, Educ. Sci. 2022, 12, 840. https://doi.org/ 10.3390/educsci12110840
[17] Schwab, K. “The fourth industrial revolution”, Crown Business, 2016
[18] Li, D.X.; Mendez, E.A. “Artificial Intelligence in STEM Education: Interactive Hands-on Environment using Open Source Electronic Platforms”, Rev. Tecnol. En Marcha 2023, 36, 45–52.

[19] Mannodi-Kanakkithodi, A.; McDannald, A.; Sun, S.; Desai, S.; Brown, K.A.; Kusne, A.G. “A framework for materials informatics education through workshops”, MRS Bull. 2023, 48, 560–569.
[20] Sahu, C.; Ayotte, B.; Banavar, M.K. “Integrating machine learning concepts into undergraduate classes”, In Proceedings of the 2021 IEEE Frontiers in Education Conference (FIE), Lincoln, NE, USA, 13–16 October 2021; pp. 1–5.
[21] Spencer A. “Cyber Science Education within STEM”, Cybersecurity and Innovative Technology Journal. 2024 Dec 31;2(2):67-78.
[22] Loo, S. M. & Babinkostova, L. "Cyber-Physical Systems Security Introductory Course for STEM Students". ASEE Annual Conference and Exposition, Conference Proceedings, 2020-June, 29171-1 - 29171-9. https://dx.doi.org/10.18260/1-2--34366
[23] Wenner, J. A., Frary, M., & Simmonds, P. J. “Supporting STEM graduate students in strengthening their professional identity through an authentic interdisciplinary partnership”, Studies in Graduate and Postdoctoral Education, 2024, 15(1), 96–116. https://doi.org/10.1108/SGPE-02-2023-0017
[24] Maqsood, S., & Chiasson, S. “Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens”, ACM Transactions on Privacy and Security, 2021, 24(4), 1–37. https://doi.org/10.1145/3469821
[25] Khan, M.A., Khojah, M., Vivek “Artificial intelligence and big data: The advent of new pedagogy in the adaptive e-learning system in the higher educational institutions of Saudi Arabia”, Educ. Res. Int., 2022, 1263555.
[26] Liu, Y.; Chen, L.; Yao, Z.” The application of artificial intelligence assistant to deep learning in teachers’ teaching and students’ learning processes” Front. Psychol, 2022, 13, 9175.
[27] Montuori, L.; Alcazar-Ortega, M.; Vargas-Salgado, C.; Alfonso-Solar, D. “Learning Analytics as Data-driven Decision Making in Higher Education: A Case Study”, In Proceedings of the INNODOCT 2022. International Conference on Innovation, Documentation and Education, Valencia, Spain, 2–7 November 2022; pp. 83–89.
[28] Static, A.I. “Human learning and learning analytics in the age of artificial intelligence” Br. J. Educ. Technol. 2019, 50, 2974–2976.
[29] Sang, Y.; Wang, L. “Physical Fitness Data Monitoring of College Students Based on the Internet of Things and Blockchain”, Front. Public Health, 2022, 10, 940951.
[30] Yujie, H.; Qiuxia, H. Innovative Mode of Logistics Management of “Internet of Things + Blockchain”-Integrated E-Commerce Platform. Comput. Intell. Neurosci. 2022, 7766228.
[31] Hassan Al-Taai, S.H.; Abbas Kanber, N.H.; Mohammed al Dulaimi, W.A. “The Importance of Using the Internet of Things in Education”, Int. J. Emerg. Technol. Learn. (Ijet) 2023, 18, 19–39.
[32] Shahin, Y. “Technological acceptance of the Internet of Things (IoT) In Egyptian schools”, International Journal of Instructional Technology and Educational Studies, 2020, 1(1), pp.6-10.
[33] Bakla, A. “A Critical Overview of Internet of Things in Education”, Mehmet Akif Ersoy Üniversitesi Eğitim Fakültesi Dergisi, 2019, (49), pp.302–327.
[34] Morais, C., Pedrosa, D., Fontes, M.M., Cravino, J. and Morgado, L. “Detailing an e-Learning course on software engineering and architecture using BPMN”, In First International Computer Programming Education Conference (ICPEC 2020) (pp. 17-1). Schloss Dagstuhl–Leibniz-Zentrum für Informatik.
[35] Mcrae, L., Ellis, K. and Kent, M. “Internet of Things (IoT): Education and Technology. The relationship between education and technology for students with disabilities”, 2018, Curtin University. Available from: https://www.ncsehe.edu.au/wp-content/uploads/2018/02/ IoTEducation_Formatted_Accessible.pdf.
[36] Hua, M.T.A. “Promises and Threats: iN2015 Masterplan to Pervasive Computing in Singapore. Science, Technology and Society”, 2012, 17(1), pp.37–56. Available from: https: //doi.org/10.1177/097172181101700103.
[37] Zhu, Z.T., Yu, M.H. and Riezebos, P. “A research framework of smart education. Smart Learning Environments”, 2016, 3(1), p.4. Available from: https://doi.org/10.1186/ s40561-016-0026-2.
[38] Pervez, S., ur Rehman, S. and Alandjani, G. “Role of Internet of Things (IoT) in Higher Education. Proceedings of ADVED 2018 - 4th International Conference on Advances in Education and Social Sciences”, 2018, October, pp.1–9.
[39] Triplett, W.J. “Artificial intelligence in STEM education”, Cybersecurity and Innovative Technology Journal, 2023, 1(1), pp.23-29.

[40] Hu, C.C. “Exploring the impact of CPS-based robot-assisted teaching in STEM education: Enhancing knowledge, skills, and attitudes”, International Journal of Human-Computer Interaction, 2023, 1–21. https://doi.org/10.1080/10447318.2023.2262278\
[41] Osadchyi, V. V., Valko, N. V., & Kushnir, N. O. “Design of the educational environment for stem-oriented learning”, Information Technologies and Learning Tools, 2020, 75(1), 316–330. https://doi.org/10.33407/itlt.v75i1.3213
[42] Balon, T., & Baggili, I. A. “Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education”, Education and Information Technologies, 2023, 28(9), 11759–11791.https://doi.org/10.1007/s10639-022-11451-4
[43] Ivy, J., Kelley, R., Cook, K., & Thomas, K. “Incorporating cyber principles into middle and high school curriculum”, International Journal of Computer Science Education in Schools, 2020, 4(2), 3–23. https://doi.org/10.21585/ijcses.v4i2.101
[44] Simmons, R. T, & Park, J. S. “Innovating Cybersecurity Education Through AI-augmented Teaching”, In European Conference on Cyber Warfare and Security, 2024.
[45] Shapovalov, Y.B., Bilyk, Z.I., Usenko, S.A., Shapovalov, V.B., Postova, K.H., Zhadan, S.O. and Antonenko, P.D. “Harnessing personal smart tools for enhanced STEM education: exploring IoT integration”, Educational Technology Quarterly, 2023, (2), pp.210-232.
[46] Mazhar, T., Talpur, D. B., Hanif, S., Ullah, I., Adhikari, D., & Anwar, M. S. “Analysis of cybersecurity issues and solutions in education. In A. A. A. El-Latif, Y. Maleh, M. A. El-Affendi, & S. Ahmad (Eds.)”, Cybersecurity management in education technologies (pp. 64–85). CRC Press, 2023. https://doi.org/10.1201/9781003369042-5
[47] Triplett, W. J. “Addressing cybersecurity challenges in education”, International Journal of STEM Education for Sustainability, 2023a, 3(1), 47–67. https://doi.org/10.53889/ijses.v3i1.132
[48] Hossain, K. A. “Practices and challenges of modern leadership in the era of technological advancement”, Scientific Research Journal, 2023, XI(XI), 10–70. https://doi.org/10.31364/SCIRJ/v11.i11.2023.P1123972
[49] Venkatesh, Viswanath, James Y.L. T., & Xin, X. “Unified theory of acceptance and use of technology: A synthesis and the road ahead”, Journal of the Association for Information Systems, 2016, 17 (5), 328-376.
[50] Isaias, P., Reis, F., Coutinho, C. and Lencastre, J.A. “Empathic technologies for distance/mobile learning: An empirical research based on the unified theory of acceptance and use of technology (UTAUT)”, Interactive Technology and Smart Education, 2017, 14(2), 159- 180. https://doi.org/10.1108/ITSE-02-2017-0014
[51] Sullivan, A., & Palmer, B. “Incorporating cybersecurity concepts across disciplines”, Journal of Educational Technology & Innovation, 2021, 9(3), 44-60.
[52] Peters, R., & Kluge, M. “Cross-disciplinary approaches to cybersecurity education”, Technology & Society Journal, 2022, 20(1), 58-71.
[53] Thomas, J. W. “Project-based learning for cybersecurity education”, In Advances in Cybersecurity Education (pp. 97-110). Springer, 2022.
[54] Barker, M., & Green, T. “Enhancing cybersecurity education through industry collaboration”, Journal of Cybersecurity Education, 2021, 12(4), 33-47.
[55] National Institute of Standards and Technology (NIST). National Initiative for Cybersecurity Education (NICE) framework, 2022. Retrieved from https://csrc.nist.gov/projects/nice-framework
[56] He, J., Lo, D.C.T., Xie, Y. & Lartigue, J. ”Integrating Internet of Things (IoT) into STEM undergraduate education: A case study of a modern technology infused Courseware for embedded system course”, IEEE Frontiers in Education Conference (FIE) (pp. 1-9), IEEE, 2016.
[57] Chen, R., Zheng, Y., Xu, X., Zhao, H., Ren, J. & Tan, H.Z., 2020. “STEM teaching for the Internet of Things maker course: A teaching model based on the iterative loop”, Sustainability, 2020, 12(14), p.5758.
[58] Adams, R., & Green, T. “Overcoming resistance to curriculum changes in education”, Journal of Educational Policy, 2021, 14(2), 67-82.