

REFERENCES

- [1] C. S. Shieh, T. T. Nguyen, and M. F. Horng, "Detection of Unknown DDoS Attack Using Convolutional Neural Networks Featuring Geometrical Metric," *Mathematics*, vol. 11, no. 9, May 2023, doi: 10.3390/math11092145.
- [2] R. Nishant, M. Kennedy, and J. Corbett, "Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda," *Int J Inf Manage*, vol. 53, Aug. 2020, doi: 10.1016/j.ijinfomgt.2020.102104.
- [3] D. Ghelani and T. Kian Hua, "Conceptual Framework of Web 3.0 and Impact on Marketing, Artificial Intelligence, and Blockchain," *International Journal of Information and Communication Sciences*, vol. 7, no. 1, p. 10, 2022, doi: 10.11648/j.ijics.20220701.12.
- [4] B. Pertiwi Sudirman and P. Kencana Sari, "Differences in Information Security Behavior of Smartphone Users in Indonesia Using Pearson's Chi-square and Post Hoc Test," *Int J Adv Sci Eng Inf Technol*, vol. 13, no. 2, 2023, doi: <https://doi.org/10.18517/ijaseit.13.2.17975>.
- [5] P. K. Sari, P. W. Handayani, A. N. Hidayanto, S. Yazid, and R. F. Aji, "Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors," Dec. 01, 2022, *MDPI*. doi: 10.3390/healthcare10122531.
- [6] D. Gates and I. Hennessey, "AI in Paediatrics," in *AI in Clinical Medicine*, Wiley, 2023, pp. 210–218. doi: 10.1002/9781119790686.ch21.
- [7] M. Abdelkhalek, G. Ravikumar, and M. Govindarasu, "ML-based Anomaly Detection System for DER Communication in Smart Grid," in *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, IEEE, Apr. 2022, pp. 1–5. doi: 10.1109/ISGT50606.2022.9817481.
- [8] T. Alashoor, H. Aldawood, B. Alsulayyim, S. Almutairi, and E. R. Alotaibi, "An Online Randomized Field Experiment on the Importance of Privacy Education, Training, and Awareness (PETA)," in *2023 3rd International Conference on Computing and Information Technology (ICCIT)*, IEEE, Sep. 2023, pp. 106–110. doi: 10.1109/ICCIT58132.2023.10273938.
- [9] C. Candiwan, M. Azmi, and A. Alamsyah, "Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era," *International Journal of Safety and Security Engineering*, vol. 12, no. 2, pp. 229–237, Apr. 2022, doi: 10.18280/ijssse.120212.
- [10] S. Jawhar, J. Miller, and Z. Bitar, "AI-Driven Customized Cyber Security Training and Awareness," in *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2024, pp. 1–5. doi: 10.1109/ICAIC60265.2024.10433829.
- [11] M. F. Ansari, P. K. Sharma, and B. Dash, "Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training," *International Journal of Smart Sensor and Adhoc Network*, pp. 61–72, Mar. 2022, doi: 10.47893/IJSSAN.2022.1221.
- [12] A. Schreiber and I. Schreiber, "Bridging knowledge gap: the contribution of employees' awareness of AI cyber risks comprehensive program to reducing emerging

- AI digital threats,” *Information & Computer Security*, Apr. 2024, doi: 10.1108/ICS-10-2023-0199.
- [13] A. López González, M. Moreno, A. C. Moreno Román, Y. Hadfeg Fernández, and N. Cepero Pérez, “Ethics in Artificial Intelligence: an Approach to Cybersecurity,” *Inteligencia Artificial*, vol. 27, no. 73, pp. 38–54, Jan. 2024, doi: 10.4114/intartif.vol27iss73pp38-54.
 - [14] S. Alateyyat and M. Soltan, “Utilizing Artificial Intelligence in Higher Education: A Systematic Review,” in *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSYS)*, IEEE, Jan. 2024, pp. 371–374. doi: 10.1109/ICETSYS61505.2024.10459629.
 - [15] M. Afzaal, X. Shanshan, D. Yan, and M. Younas, “Mapping Artificial Intelligence Integration in Education: A Decade of Innovation and Impact (2013–2023)—A Bibliometric Analysis,” *IEEE Access*, vol. 12, pp. 113275–113299, 2024, doi: 10.1109/ACCESS.2024.3443313.
 - [16] S. Russel and P. Norvig, “Artificial Intelligence A Modern Approach Third Edition.”
 - [17] K. Goebel and S. Rane, “AI in Industrial IoT Cybersecurity [Industrial and Governmental Activities],” *IEEE Comput Intell Mag*, vol. 19, no. 1, pp. 14–15, Feb. 2024, doi: 10.1109/MCI.2023.3332547.
 - [18] W. Shieh, “Editorial Cybersecurity in Modern Life,” *IEEE Trans Reliab*, vol. 72, no. 4, pp. 1294–1294, Dec. 2023, doi: 10.1109/TR.2023.3329329.
 - [19] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, “Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review,” *Comput Ind*, vol. 137, p. 103614, May 2022, doi: 10.1016/j.compind.2022.103614.
 - [20] K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, and T. Tran, “Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity,” *Computer (Long Beach Calif)*, vol. 52, no. 12, pp. 45–52, Dec. 2019, doi: 10.1109/MC.2019.2942584.
 - [21] M. Homaei, Ó. Mogollón-Gutiérrez, J. C. Sancho, M. Ávila, and A. Caro, “A review of digital twins and their application in cybersecurity based on artificial intelligence,” *Artif Intell Rev*, vol. 57, no. 8, Aug. 2024, doi: 10.1007/s10462-024-10805-3.
 - [22] M. Akhtar and T. Feng, “An overview of the applications of Artificial Intelligence in Cybersecurity,” *EAI Endorsed Transactions on Creative Technologies*, vol. 8, no. 29, p. 172218, Dec. 2021, doi: 10.4108/eai.23-11-2021.172218.
 - [23] S. Grover, B. Broll, and D. Babb, “Cybersecurity Education in the Age of AI: Integrating AI Learning into Cybersecurity High School Curricula,” in *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1*, New York, NY, USA: ACM, Mar. 2023, pp. 980–986. doi: 10.1145/3545945.3569750.
 - [24] F. Farahmand, “Integrating Cybersecurity and Artificial Intelligence Research in Engineering and Computer Science Education,” *IEEE Secur Priv*, vol. 19, no. 6, pp. 104–110, Nov. 2021, doi: 10.1109/MSEC.2021.3103460.
 - [25] S. Jawhar, J. Miller, and Z. Bitar, “AI-Driven Customized Cyber Security Training and Awareness,” in *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2024, pp. 1–5. doi: 10.1109/ICAIC60265.2024.10433829.

- [26] A. Zacharis, V. Katos, and C. Patsakis, "Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle," *Int J Inf Secur*, vol. 23, no. 4, pp. 2691–2710, Aug. 2024, doi: 10.1007/s10207-024-00860-w.
- [27] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.
- [28] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: a lifecycle model," *Information Technology & People*, vol. 36, no. 8, pp. 94–125, Dec. 2023, doi: 10.1108/ITP-07-2022-0515.
- [29] O. Sarker, A. Jayatilaka, S. Haggag, C. Liu, and M. A. Babar, "A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness," *Journal of Systems and Software*, vol. 208, p. 111899, Feb. 2024, doi: 10.1016/j.jss.2023.111899.
- [30] C. Candiwan and L. M. Rianda, "Transactions at Your Fingertips: Influential Factors in Information Security Behavior for Mobile Banking Users," *International Journal of Safety and Security Engineering*, vol. 14, no. 3, pp. 795–806, Jun. 2024, doi: 10.18280/ijss.140312.
- [31] B. R. Chasanah and C. Candiwan, "Analysis of College Students' Cybersecurity Awareness In Indonesia," *SISFORMA*, vol. 7, no. 2, pp. 49–57, Nov. 2020, doi: 10.24167/sisforma.v7i2.2706.
- [32] S. Hu, C. Hsu, and Z. Zhou, "Security Education, Training, and Awareness Programs: Literature Review," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 752–764, Jul. 2022, doi: 10.1080/08874417.2021.1913671.
- [33] L. Kraus, V. Švábenský, M. Horák, V. Matyás, J. Vykopal, and P. Celeda, "Want to Raise Cybersecurity Awareness? Start with Future IT Professionals.," in *Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. I*, New York, NY, USA: ACM, Jun. 2023, pp. 236–242. doi: 10.1145/3587102.3588862.
- [34] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132132–132143, 2022, doi: 10.1109/ACCESS.2022.3230286.
- [35] X. Li and L. Lei, "A bibliometric analysis of topic modelling studies (2000–2017)," *J Inf Sci*, vol. 47, no. 2, pp. 161–175, Apr. 2021, doi: 10.1177/0165551519877049.
- [36] A. Sulich, T. Zema, and L. Kulhanek, "Towards a Secure Future: A Bibliometric Analysis of the Relations Between Cybersecurity and Sustainable Development," *Procedia Comput Sci*, vol. 225, pp. 1448–1457, 2023, doi: 10.1016/j.procs.2023.10.133.
- [37] O. S. Albahri and A. H. Alamoodi, "Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database," *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 158–169, Dec. 2023, doi: 10.58496/MJCS/2023/018.

- [38] S. Patel *et al.*, “Review and Analysis of Massively Registered Clinical Trials of COVID-19 using the Text Mining Approach,” *Rev Recent Clin Trials*, vol. 16, no. 3, pp. 242–257, Jul. 2021, doi: 10.2174/1574887115666201202110919.
- [39] A. Kirby, “Exploratory Bibliometrics: Using VOSviewer as a Preliminary Research Tool,” *Publications*, vol. 11, no. 1, p. 10, Feb. 2023, doi: 10.3390/publications11010010.