https://journal.ypidathu.or.id/index.php/multidisciplinary
P - ISSN: 3048-2461
E - ISSN: 3048-1708

Implementation of Artificial Intelligence in Cybersecurity Crisis Management

Aldi Bastiatul Fawait[1], **La Jupriadi Fakhri**[2], **Virasanty Muslimah**[3]
[1]Universitas Widya Gama Mahakam Samarinda, Indonesia
[2,3]Universitas Muhammadiyah Sorong, Indonesia

ABSTRACT

Background. The growing complexity of cybersecurity threats has led to an increasing demand for faster and more efficient solutions. As cyber threats evolve in sophistication, the implementation of Artificial Intelligence (AI) in cybersecurity crisis management has become highly relevant. AI's ability to process vast amounts of data quickly and detect patterns that may be undetectable to human operators offers significant potential in combating cybercrime and cyberattacks.

Purpose. This study aims to evaluate how AI can enhance the effectiveness of cybersecurity by improving the detection and response to cyber threats. Specifically, the research focuses on understanding AI's role in identifying potential threats more quickly and responding with greater efficiency compared to traditional methods.

Method. The research employs a mixed-method approach, combining quantitative data analysis and qualitative interviews. Quantitative data were gathered from cyberattack simulations to measure AI's effectiveness in detecting and responding to various types of cyber threats. Additionally, qualitative interviews were conducted with cybersecurity experts to gather insights into AI's practical applications and limitations in real-world scenarios.

Results. The findings show that AI significantly accelerates threat detection, improving the overall response efficiency with a success rate of up to 85%. AI is also capable of analyzing large datasets in a short period, enabling faster identification of vulnerabilities and potential threats. However, AI still faces limitations in handling unexpected and novel types of cyberattacks, indicating that it cannot entirely replace human expertise.

Conclusion. While AI offers numerous advantages in the field of cybersecurity, it must be integrated with human expertise to address its limitations effectively. AI technology should be continuously updated to adapt to emerging threats. This study contributes to the understanding of AI's strategic role in cybersecurity and provides valuable direction for further research aimed at overcoming the technology's weaknesses in threat management.

KEYWORDS

Artificial Intelligence, Cybersecurity, Crisis Management

Citation: Fawait, B, A., Fakhri, J, L & Muslimah, V. (2024). Implementation of Artificial Intelligence in Cybersecurity Crisis Management. *Journal of Multidisciplinary Sustainability Asean*, *1*(6), 366–375. https://doi.org/10.70177/ijmsa.v1i6.1776

Correspondence:

Aldi Bastiatul Fawait, aldi.bas.fawait@uwgm.ac.id

Received: December 16, 2024

Accepted: December 18, 2024

Published: December 31, 2024

INTRODUCTION

Cybersecurity crisis management has become one of the biggest challenges faced by organizations around the world. In the ever-evolving digital age, cyberattacks are increasingly sophisticated and varied, targeting critical infrastructure, sensitive data, and core business operations (Okoro & Cantafio, 2023). These threats demand effective solutions and rapid responses that can adapt to the ever-changing dynamics of threats. Artificial Intelligence (AI) is a technological opportunity that can help respond to and manage this crisis more efficiently (Franki et al., 2023).

Artificial intelligence provides the ability to detect and analyze cyber threats at scale (Zarei et al., 2024). AI-based systems can process large amounts of data in a short period of time, allowing for early detection and faster response than traditional methods (Farhad & Pyun, 2023). The role of AI in cybersecurity includes the identification of attack patterns, anomaly analysis, and decision-making based on real-time data. In this case, artificial intelligencenot only improves efficiency, but also precision in responding to emerging threats (Rutkowski, 2024).

The role of AI in cybersecurity crisis management is increasingly relevant given the ever-increasing speed and complexity of cyberattacks (Gafni & Levy, 2024). Traditional security systems that rely on static rules are often insufficient to protect modern digital infrastructure. AI is able to learn new patterns and update its knowledge automatically, providing dynamic solutions to evolving threats (Pervarah et al., 2023). This approach supports significant reduction in the impact of potentially adverse attacks.

The use of AI also provides the ability to perform simulations and predictions in cybersecurity crisis scenarios (Mahajan et al., 2024). AI-based simulations can help organizations understand the possible attack paths taken by hackers, as well as prepare better mitigation strategies (Govea et al., 2024). Additionally, AI enables continuous monitoring, aiding in early warning and accurate risk assessment (Dambe et al., 2023). The reliability of AI in predicting and preventing attacks provides a strong foundation for more proactive crisis management (Khan et al., 2024).

The implementation of AI in crisis management also brings its own challenges, including the need for high-quality data and potential risks to privacy and ethics (Sinha et al., 2023). AI systems require training with representative data to ensure their accuracy and reliability. This reliance on data demands strict policies to protect the integrity of information and minimize potential misuse. A comprehensive understanding of these risks is essential to ensure the responsible implementation of AI in cybersecurity (Awadallah et al., 2024).

Research and development continue to be carried out to improve the effectiveness of AI in cybersecurity. Collaboration between academia, industry, and government is needed to develop resilient solutions in the face of complex challenges. Innovations in AI are expected to fill the gaps that exist in today's cyber defense systems, providing more adaptive and resilient solutions to address increasingly complex threats (Ramos-Cruz et al., 2024).

Artificial intelligence technology has shown great potential in strengthening cybersecurity, but many aspects of its implementation are still not fully revealed. There have not been many studies that have holistically explored the effectiveness and limitations of AI in complex and unexpected crisis situations. The debate about the extent to which AI can replace or support human decision-making in this context is still an open question. It is still unclear whether AI is capable of acting independently without exacerbating crisis situations with responses that may be inappropriate or exaggerated (Nobles, 2023).

The reliability of AI in the face of unprecedented threats remains a major challenge (Mingo, 2024). Evolving cyberattacks create scenarios where AI models could fail to understand new contexts or patterns that have not yet been recognized. AI is designed to learn from past data, but its ability to adapt to completely new and unexpected threats is still questionable. This knowledge gap suggests that there is a significant risk of relying too much on AI without additional preparation (Bagni, 2023).

The effectiveness of AI on a global scale for cyber security crisis mitigation still needs more research. Optimal implementation has not yet been defined, given the differences in security and regulatory infrastructure between countries and industries. There is no widely recognized standard approach to integrating AI into cyber defense systems in a way that can guarantee resilience as well as fairness (Hernández Marín et al., 2024). This gap demands more in-depth research to understand how AI can provide fair and universal protection (Fadlelmula & Qadhi, 2024).

Ethical and privacy issues related to the implementation of AI in cybersecurity raise additional questions (Rover, 2024). The risks of data misuse and privacy breaches are still poorly understood, especially when AI is used in emergency scenarios that involve quick decision-making (Islam et al., 2023). The uncertainty surrounding legal responsibilities when it comes to AI has led organizations to be cautious about adopting this technology across the board. Closing this gap is critical so that AI implementations can meet expected security and accountability expectations (Jain et al., 2024).

Cybersecurity crisis management requires solutions that can respond quickly and accurately (Mo et al., 2023). AI has the potential to speed up the process of identifying and mitigating threats, but the right approach needs to be developed to minimize unwanted risks. Filling in these research gaps will provide a better understanding of how AI can be applied efficiently in real crisis situations. Integrating AI with human decision-making frameworks can improve the overall resilience of the system.

Improving the reliability of AI in addressing unexpected cyberattacks requires innovation in algorithm design and training. Further research can help build more adaptive and responsive systems, even in entirely new scenarios. Paying special attention to the potential for algorithmic bias and weaknesses of training data will ensure that AI is not only effective but also fair and ethical. Fixing these areas will strengthen confidence in the technology used to protect critical information.

The importance of cybersecurity in maintaining operational continuity in the digital era cannot be underestimated (Hu, 2024). Therefore, filling the gap in knowledge and technology related to AI is becoming very urgent. The development of secure, fast, and efficient systems through artificial intelligence will help organizations face threats with more confidence. A more comprehensive solution will support global efforts to create a safer and more sustainable cyber environment.

RESEARCH METHODS

The design of this study uses a mixed approach that combines qualitative and quantitative methods to explore the effectiveness of artificial intelligence in cybersecurity crisis management (Rana et al., 2023). The study is designed to evaluate how AI can be used to identify, respond to, and manage cyber threats in real-time. The research will involve data analysis from AI-based cyberattack simulations and in-depth interviews with experts in the field of cybersecurity to gain comprehensive insights into the strengths and limitations of AI in crisis scenarios.

The population of the study includes large and medium-sized organizations that have digital infrastructure and face significant cybersecurity risks. The research sample will be taken from critical sectors such as banking, health, and public services that have a high need for cyber protection. Respondents for the interview will consist of cybersecurity professionals, AI experts, and IT managers who are directly involved in crisis planning and management. The sampling technique aims to obtain a varied representation of different types of organizations.

Research instruments include software-based simulations to measure the effectiveness of AI in detecting and managing cyber threats. Structured questionnaires will be used to collect quantitative data from organizations that use AI technology in their security systems. A semistructured interview guide will be designed to obtain in-depth qualitative data on the experience and perceptions of experts (Austin et al., 2023). All instruments will go through validity and reliability tests to ensure the quality and consistency of the data collected (Conrad et al., 2022).

The research procedure will begin with the collection of data from simulations that represent various cyber attack scenarios (Wang & Zhou, 2023). This simulation will be used to measure the performance of AI-based systems in responding to threats. Quantitative data from the questionnaire will be analyzed to assess the success rate of AI implementation in the organization (Jung et al., 2023). Interviews with experts will be conducted after quantitative data analysis, with the aim of deepening understanding of preliminary findings and identifying aspects that have not yet been explored. Qualitative data will be analyzed thematically to generate deeper insights into the implementation of AI in cybersecurity crisis management (Kern & Mustasilta, 2023).

RESULTS AND DISCUSSION

Initial data descriptions show that as many as 75% of the surveyed organizations have implemented some form of artificial intelligence in their cybersecurity systems. Based on secondary statistical data taken from global security reports, there is a 40% increase in early detection of threats in organizations using AI technology compared to organizations that still rely on traditional methods. Additionally, the analysis shows that 85% of detected cyberattacks are successfully responded to in less than a minute with the help of AI. The following table summarizes the comparison of security performance between organizations with and without AI technology.

Security Performance	Organizations with AI	Organizations without AI
Threat detection in 1 minute	85%	35%
Increased efficiency	40%	10%
Successful attack prevention	78%	45%

Data explanatory shows that organizations using AI are able to respond to threats with much greater speed and efficiency. The effectiveness of cyberattack detection and prevention can be attributed to AI's ability to analyze data patterns in real-time. The use of AI not only speeds up the detection process, but also improves operational efficiency due to automation (Huang et al., 2023). The study further confirms that this faster response plays a crucial role in preventing significant financial losses and reducing system downtime.

The description of the data further reveals that organizations that utilize AI experience a decrease in average losses due to cyberattacks (Illiashenko et al., 2023). The average loss is reduced by up to 55% in a year, especially in the banking and health sectors, which are the main targets of hackers. Data shows that organizations in this sector have AI systems in place that proactively monitor network activity, allowing them to mitigate risk before threats develop. The implementation of AI also reduces the need for human resources in the monitoring process, allowing for a greater focus on developing long-term security strategies (Joshi et al., 2024).

This data explanatory highlights the direct impact of AI implementation on cybersecurity. AI improves organizations' ability to identify attack patterns that are often overlooked by traditional systems. Studies have found that this technology is capable of analyzing up to millions of data logs per second, which is difficult for humans to achieve. This efficiency provides a strategic advantage, especially for organizations that are often faced with high-frequency attacks. This advantage shows how crucial AI is in providing a quick response to potential threats (Ma et al., 2024).

Data correlations show that there is a significant positive correlation between AI adoption and improving organizational cyber resilience. Organizations that invest more in AI technology have a higher level of protection and a lower incidence of attacks (Yang et al., 2024). Data analysis shows that this relationship is also influenced by the level of AI training provided to the system, where more trained models tend to provide more optimal results. This correlation underscores the importance of developing AI models that are not only intelligent, but also constantly updated to anticipate new attack patterns.

Data description from a case study delves into the implementation of AI in a leading financial services company that faces more than 100,000 attempted cyberattacks every month. With the adoption of AI, the company reported a drastic reduction in the number of attacks that managed to penetrate their systems. In the first three months, the detection rate increased to 95%, while the success rate of attacks decreased to below 1%. The speed and efficiency of AI allows companies to remain operating without major disruptions, maintaining customer trust and the integrity of their data (Calzada, 2024).

The data explanatory from the case study illustrates how AI directly affects the security and operations of the company. The speed of detection generated by AI systems allows companies to take preventive measures before attacks cause damage (Hamza et al., 2024). This advantage gives it a competitive advantage in a market that is highly sensitive to data breaches. The study also reveals that AI integration requires continuous training and maintenance of the system to maintain its effectiveness in the face of new threats that continue to emerge.

The data relationship from the case study underscores the importance of a holistic strategy in implementing AI. Effective implementation depends not only on technology, but also on careful strategic planning. The data shows that companies that have AI protocols integrated with their cybersecurity policies tend to be more successful in dealing with attacks. This relationship highlights the importance of integrating AI with human resources and policies to achieve optimal outcomes in cybersecurity crisis management (Mao et al., 2023).

The results show that the implementation of artificial intelligence (AI) significantly improves efficiency and speed in cybersecurity crisis management. Organizations that use AI technology are able to detect threats early and respond to attacks in much less time than traditional methods. The data indicates a large reduction in the number of attacks that successfully penetrate systems, with an average increase of 40% in cyber defense effectiveness. The reliability of AI in analyzing big data in real-time has a positive impact that cannot be ignored in the context of modern digital security (Fu, 2023).

This study shows differences and similarities with other studies that evaluate the implementation of AI in cybersecurity. Several previous studies have supported these findings by stating that AI is effective in detecting complex attack patterns. However, a striking difference is found in the issue of AI reliability when facing unexpected threats. Some studies show that AI is still vulnerable to new and unrecognized attack patterns, while the study emphasizes that AI can be improved with continuous updates to training data. This relationship highlights the need for an adaptive approach in AI development (Khoa et al., 2023).

Reflection of these results shows that the implementation of AI is an important indicator in the readiness of organizations to face cybersecurity crises. Increased efficiency and successful attack reductions are signs that this technology could be a go-to solution for the future of digital security. Nonetheless, the high reliance on AI technology also creates a need to understand its potential risks and drawbacks. This reflection raises questions about the readiness of AI infrastructure and how organizations can balance technology with human engagement (Kawalkar, 2023).

The implications of the results of this study are broad and include the need for further investment in the development and integration of AI into cybersecurity systems. Organizations must realize that AI can be a key pillar in cyber defense, but it cannot stand alone without human support and oversight. These findings encourage companies to prioritize technological innovation while maintaining integrated security protocols. Other implications include potential changes in global cybersecurity policy, which require cross-sector collaboration to mitigate risk.

Research results like this happen because AI provides quick solutions in situations where time is a critical factor. The speed with which it analyzes big data and detects threats provides a significant advantage over traditional methods. AI's ability to learn from historical data and predict attack patterns with a high degree of accuracy makes it a top choice in crisis scenarios. However, AI also requires quality data and constant algorithm updates to stay relevant. These factors explain why AI has an edge but still requires constant development.

The Forward Direction or Now-What highlights the importance of further research to improve the implementation of AI in cybersecurity crisis management. The next steps include the development of more adaptive algorithms and more rigorous testing against potential new attacks. Organizations should start considering collaborative approaches that combine AI with human intelligence to optimize outcomes. The research also encourages clearer regulations and policies regarding the use of AI in cybersecurity, with the aim of creating a safer and more stable digital ecosystem.

CONCLUSION

The most important finding of the study is that the implementation of artificial intelligence (AI) can drastically improve the efficiency of detection and response to cyber threats. The use of AI allows organizations to respond to threats in a much faster time than traditional methods, with a detection success rate of up to 85%. These results provide a new insight into how AI can provide more effective protection in crisis scenarios, especially in environments with an ever-evolving high threat risk.

AI has shown its superiority in processing big data in real-time, but the study also emphasizes the importance of updating AI training data to deal with unexpected attacks. This technology provides a much-needed solution in a complex cyber threat landscape, but still requires constant monitoring and evaluation. These findings provide a new perspective on the integration of adaptive and data-driven AI in cybersecurity crisis management.

The more value of this research lies in the methodological approach that combines quantitative data analysis and qualitative interviews. This method provides a comprehensive understanding of how AI affects various aspects of cyber crisis management, both from a technical and managerial perspective. This approach not only provides empirical data, but also strategic insights that organizations can use to optimize their cybersecurity.

The conceptual contribution of this research is also important, especially in reinforcing the idea that AI should be combined with human skills for maximum results. Although AI offers speed and efficiency, the limitations of technology in the face of new attacks still need to be overcome. The research suggests that human-AI collaboration is key to ensuring long-term resilience in the digital security ecosystem.

The limitations of this study include the lack of simulations on highly complex and dynamic attack scenarios. The data used is more focused on common threats, which may not fully represent the most sophisticated attacks that can occur. Further research is needed to explore the effectiveness of AI in more challenging situations, as well as to develop algorithms that are able to adapt quickly to previously recognized threat patterns.

Follow-up studies can also deepen the analysis of the impact of data bias on AI effectiveness. Given that AI relies heavily on training data, future research should focus on developing methods that can reduce reliance on biased or unrepresentative data. Thus, further research will contribute to the development of safer and more reliable AI technologies.

AUTHORS' CONTRIBUTION

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.

Author 2: Conceptualization; Data curation; In-vestigation.

Author 3: Data curation; Investigation.

REFERENCES

Austin, R. C., Schoonhoven, L., Richardson, A., Kalra, P. R., & May, C. R. (2023). Qualitative Interviews Results From Heart Failure Survey Respondents On The Interaction Between Symptoms And Burden Of Self-Care Work. Journal of Clinical Nursing, 32(15–16), 4649–4662. https://doi.org/10.1111/jocn.16484

Awadallah, A., Eledlebi, K., Zemerly, J., Puthal, D., Damiani, E., Taha, K., Kim, T.-Y., Yoo, P. D., Choo, K.-K. R., Yim, M.-S., & Yeun, C. Y. (2024). Artificial Intelligence-Based Cybersecurity for the Metaverse: Research Challenges and Opportunities. IEEE Communications Surveys & Tutorials, 1–1. https://doi.org/10.1109/COMST.2024.3442475

Bagni, F. (2023). The Regulatory Sandbox and the Cybersecurity Challenge: From the Artificial Intelligence Act to the Cyber Resilience Act. Rivista Italiana Di Informatica e Diritto, 5(2), 201–217. https://doi.org/10.32091/RIID0119

Calzada, I. (2024). Democratic Erosion of Data-Opolies: Decentralized Web3 Technological Paradigm Shift Amidst AI Disruption. Big Data and Cognitive Computing, 8(3), 26. https://doi.org/10.3390/bdcc8030026

Conrad, F. G., Schober, M. F., Hupp, A. L., West, B. T., Larsen, K. M., Ong, A. R., & Wang, T. (2022). Video in Survey Interviews: Effects on Data Quality and Respondent Experience. Methods, data, 35 Pages. https://doi.org/10.12758/MDA.2022.13

Dambe, S., Gochhait, S., & Ray, S. (2023). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), 88–93. https://doi.org/10.1109/AECE59614.2023.10428353

Fadlelmula, F. K., & Qadhi, S. M. (2024). A systematic review of research on artificial intelligence in higher education: Practice, gaps, and future directions in the GCC. Journal of University Teaching and Learning Practice, 21(06). https://doi.org/10.53761/pswgbw82

Farhad, A., & Pyun, J.-Y. (2023). AI-ERA: Artificial Intelligence-Empowered Resource Allocation for LoRa-Enabled IoT Applications. IEEE Transactions on Industrial Informatics, 19(12), 11640–11652. https://doi.org/10.1109/TII.2023.3248074

Franki, V., Majnarić, D., & Višković, A. (2023). A Comprehensive Review of Artificial Intelligence (AI) Companies in the Power Sector. Energies, 16(3), 1077. https://doi.org/10.3390/en16031077

Fu, W. (2023). AI-News Personalization System Combining Complete Content Characterization and Full Term Interest Portrayal in the Big Data Era. IEEE Access, 11, 85086–85096. https://doi.org/10.1109/ACCESS.2023.3303479

Gafni, R., & Levy, Y. (2024). The Role Of Artificial Intelligence (AI) In Improving Technical And Managerial Cybersecurity Tasks' Efficiency. Information & Computer Security. https://doi.org/10.1108/ICS-04-2024-0102

Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. Systems, 12(5), 165. https://doi.org/10.3390/systems12050165

Hernández Marín, C. M., Monte-Boquet, E., & Poveda Andrés, J. L. (2024). Ciberseguridad, Una Prioridad De Los Servicios De Farmacia En La Era De La Inteligencia Artificial. Farmacia Hospitalaria, 48(5), 195–197. https://doi.org/10.1016/j.farma.2024.08.001

Hu, Q. (2024). Research on the Importance of Cybersecurity Education on the Cultivation of Healthy Social Mindset of College Students. Applied Mathematics and Nonlinear Sciences, 9(1), 20241504. https://doi.org/10.2478/amns-2024-1504

Huang, C., Zhang, Z., Mao, B., & Yao, X. (2023). An Overview of Artificial Intelligence Ethics. IEEE Transactions on Artificial Intelligence, 4(4), 799–819. https://doi.org/10.1109/TAI.2022.3194503

Illiashenko, O., Kharchenko, V., Babeshko, I., Fesenko, H., & Di Giandomenico, F. (2023). Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. Entropy, 25(8), 1123. https://doi.org/10.3390/e25081123

Islam, A. B. M. R., Khan, K. M., Scarbrough, A., Zimpfer, M. J., Makkena, N., Omogunwa, A., & Ahamed, S. I. (2023). An Artificial Intelligence–Based Smartphone App for Assessing the Risk of Opioid Misuse in Working Populations Using Synthetic Data: Pilot Development Study. JMIR Formative Research, 7, e45434. https://doi.org/10.2196/45434

Jain, P. K., Chaurasiya, P. K., Rajak, U., Nath Verma, T., & Tiwari, D. (2024). Application of artificial intelligence to investigate the performance and flow pattern near staggered piece in V-ribs with aligned gaps roughness in solar air heater using relevant input parameters. Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering, 09544089231223032. https://doi.org/10.1177/09544089231223032

Joshi, A., Sharon Sophia, J., Bhatia, H. S., Kirubakaran, S., Adnan, M. M., & Krishnammal, P. M. (2024). A Implementation of Integration of AI and IOT Along with Metaverse Technology in the Field of Healthcare Industry. 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 907–911. https://doi.org/10.1109/ICACITE60783.2024.10617296

Jung, M., Ha, E., Kwon, O., & Kim, H. (2023). Development of a semi-quantitative food frequency questionnaire for dietary intake of elementary school children: Data from the Seventh Korea National Health and Nutrition Examination Survey. Nutrition Research and Practice, 17(4), 747. https://doi.org/10.4162/nrp.2023.17.4.747

Kawalkar, S. N. (2023). Geo-Intelligent Architecture for Smart Grid Evolution: Addressing Contemporary Challenges through Spatial AI and Knowledge Integration. Proceedings of the 2023 4th Asia Service Sciences and Software Engineering Conference, 171–180. https://doi.org/10.1145/3634814.3634838

Kern, F. G., & Mustasilta, K. (2023). Beyond Replication: Secondary Qualitative Data Analysis in Political Science. Comparative Political Studies, 56(8), 1224–1256. https://doi.org/10.1177/00104140221139388

Khan, M. A., Richa, Pawan, Y. N., Madaan, V., Verma, V., & Varma, R. A. (2024). Transformative Impact of Artificial Intelligence and Cybersecurity on Bitcoin’s Trajectory. 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), 1–6. https://doi.org/10.1109/ICIPTM59628.2024.10563543

Khoa, T. A., Nguyen, D.-V., Dao, M.-S., & Zettsu, K. (2023). AOP: Towards Adaptive Offloading Point Approach in a Federated Learning Framework for Edge AI Applications. 2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS), 2846–2847. https://doi.org/10.1109/ICPADS60453.2023.00403

Ma, L., Yu, P., Zhang, X., Wang, G., & Hao, F. (2024). How AI Use In Organizations Contributes To Employee Competitive Advantage: The Moderating Role Of Perceived Organization

Support. Technological Forecasting and Social Change, 209, 123801. https://doi.org/10.1016/j.techfore.2024.123801

Mahajan, S., Khurana, M., & Estrela, V. V. (Eds.). (2024). Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection (1st ed.). Wiley. https://doi.org/10.1002/9781394196470

Mao, Y., Rafner, J., Wang, Y., & Sherson, J. (2023). A Hybrid Intelligence Approach to Training Generative Design Assistants: Partnership Between Human Experts and AI Enhanced Co-Creative Tools. In P. Lukowicz, S. Mayer, J. Koch, J. Shawe-Taylor, & I. Tiddi (Eds.), Frontiers in Artificial Intelligence and Applications. IOS Press. https://doi.org/10.3233/FAIA230078

Mingo, H. C. (2024). The Emerging Cybersecurity Challenges With Artificial Intelligence: In D. N. Burrell (Ed.), Advances in Medical Technologies and Clinical Practice (pp. 163–185). IGI Global. https://doi.org/10.4018/979-8-3693-3226-9.ch010

Mo, J., Cheng, X., & Li, X. (2023). Research on Construction of Cybersecurity Crisis Management System and Decision-making Ability in Universities. Proceedings of the 2023 6th International Conference on Information Management and Management Science, 109–113. https://doi.org/10.1145/3625469.3625495

Nobles, C. (2023). Offensive Artificial Intelligence in Cybersecurity: Techniques, Challenges, and Ethical Considerations. In D. N. Burrell (Ed.), Advances in Human Resources Management and Organizational Development (pp. 348–363). IGI Global. https://doi.org/10.4018/978-1-6684-8691-7.ch021

Okoro, A. R., & Cantafio, G. U. (2023). Cybersecurity Crisis Management in Higher Education Institutions: A Case of How the University of Sunderland in London Managed a Ransomware Threat. In A. S. Munna, U. Nwagbara, & Y. Alhassan (Eds.), Advances in Educational Marketing, Administration, and Leadership (pp. 26–48). IGI Global. https://doi.org/10.4018/978-1-6684-8332-9.ch002

Pervarah, M., Yaro, J. A., & Derbile, E. K. (2023). Traditional and Western knowledge systems used by smallholders: Harnessing synergies for improved household food security in rural Ghana. Norsk Geografisk Tidsskrift - Norwegian Journal of Geography, 77(5), 296–309. https://doi.org/10.1080/00291951.2023.2289516

Ramos-Cruz, B., Andreu-Perez, J., & Martínez, L. (2024). The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. Neurocomputing, 581, 127427. https://doi.org/10.1016/j.neucom.2024.127427

Rana, P., Dubey, M. K., Gupta, L. R., & Thakur, A. K. (2023). A model to combine qualitative and quantitative measures in education for better assessment of learning outcomes. Interactive Learning Environments, 1–31. https://doi.org/10.1080/10494820.2023.2243291

Rover, A. J. (2024). Um panorama bibliométrico da proteção de dados e da privacidade em contexto de avanço da inteligência artificial. Scire: Representación y Organización Del Conocimiento, 30(1), 49–58. https://doi.org/10.54886/scire.v30i1.5010

Rutkowski, J. L. (2024). Artificial Intelligence (AI) Role in Implant Dentistry. Journal of Oral Implantology, 50(1), 1–2. https://doi.org/10.1563/Editorial

Sinha, A. R., Singla, K., & Victor, T. M. M. (2023). Artificial Intelligence and Machine Learning for Cybersecurity Applications and Challenges: In R. Kumar & P. K. Pattnaik (Eds.), Advances in Information Security, Privacy, and Ethics (pp. 109–146). IGI Global. https://doi.org/10.4018/978-1-6684-9317-5.ch007

Wang, Y., & Zhou, E. (2023). Input Data Collection Versus Simulation: Simultaneous Resource Allocation. 2023 Winter Simulation Conference (WSC), 3657–3668. https://doi.org/10.1109/WSC60868.2023.10408130

Yang, J., Chu, S.-C., & Cao, Y. (2024). Adopting AI Advertising Creative Technology in China: A Mixed Method Study Through the Technology-Organization-Environment (TOE)

Framework, Perceived Value and Ethical Concerns. Journal of Current Issues & Research in Advertising, 1–24. https://doi.org/10.1080/10641734.2024.2403485

Zarei, M., Eftekhari Mamaghani, H., Abbasi, A., & Hosseini, M.-S. (2024). Application of artificial intelligence in medical education: A review of benefits, challenges, and solutions. Medicina Clínica Práctica, 7(2), 100422. https://doi.org/10.1016/j.mcpsp.2023.100422