ComniTech: Journal of Computational Intelligence and Informatics
https://dx.doi.org/000000000
P-ISSN: 3063-315X E-ISSN: 3063-0630

Cyber Security Risks in the Rapid Development of Generative Artificial Intelligence: A Systematic Literature Review

Rebecca La Volla Nyoto*[1], Mariza Devega2, Nyoto[3]

[1]Information Systems, Faculty of Computer Science, Universitas Lancang Kuning, Pekanbaru, Indonesia.
[2]Informatics Engineering, Faculty of Computer Science, Universitas Lancang Kuning, Pekanbaru, Indonesia.
[3]Management, Faculty of Business, Institut Bisnis dan Teknologi Pelita Indonesia

* Rebecca La Volla Nyoto
Email: rebecca@unilak.ac.id

Received 05/12/2024, Revised 29/12/2024, Accepted 29/12/2024, Published 31/12/2024

Abstract

This study aims to identify the cybersecurity risks arising from the use of Generative Artificial Intelligence (GenAI). By employing a systematic literature review (SLR) method and following the PRISMA 2020 guidelines, this research systematically selects and analyzes relevant literature to discover and understand the risks associated with the use of GenAI. From the seventeen studies successfully collected and reviewed, various cybersecurity risks were identified, including phishing attacks, social engineering, ransomware, malware, deepfakes, misinformation, data leakage, misuse of personal data, executable attack code generation, privacy risks, and intellectual property violations. These findings provide crucial insights into the potential threats that may emerge from the irresponsible use of GenAI. The study is designed to offer valuable information for various stakeholders in their risk mitigation efforts and in the development of relevant regulations concerning the ethical use of GenAI. It is hoped that these findings will serve as a solid foundation for developing more effective security strategies and policies to address the challenges posed by this technology, and encourage the implementation of improved protective measures to tackle emerging risks.

Keywords: generative artificial intelligence (GenAI), cybersecurity, systematic literature review

Introduction

In today's rapidly evolving digital era, technology is dynamically advancing with trends that continue to grow over time. The development of information technology trends to date broadly includes blockchain, the Internet of Things (IoT), cloud computing, big data analytics, Virtual Reality (VR), Augmented Reality (AR), and artificial intelligence (AI) (Taherdoost, 2022; Păvăloaia & Necula, 2023). Among these trends, Artificial Intelligence (AI) has become one of the most popular developments utilized in various areas of life today. AI is designed to mimic human intelligence and perform tasks that typically require thinking and decision-making, such as natural language processing, pattern recognition, and decision-making (Saddi et al., 2024).


ComniTech: Journal of Computational Intelligence and Informatics
https://dx.doi.org/000000000
P-ISSN: 3063-315X E-ISSN: 3063-0630

Over time, AI has evolved from a basic concept into more advanced technology. One of the latest developments in the field of AI is Generative Artificial Intelligence (GenAI), which refers to technology capable of creating new content that resembles human work, such as text, images, or sound (Teo et al., 2024). Unlike other AI applications that focus on data analysis or pattern recognition, GenAI actively creates new outputs based on given inputs. Popular examples of GenAI include ChatGPT, which generates text based on prompts, and DALL-E, which creates images based on textual descriptions (Polito & Pupillo, 2024; Su & Yang, 2023).

Advancements in GenAI offer significant benefits across various sectors, including business, education, and healthcare, by providing innovative ways to create content and solutions (Fui-Hoon Nah et al., 2023). However, alongside its potential benefits, GenAI also faces new challenges and risks that must be carefully understood and managed, particularly cybersecurity risks (Fui-Hoon Nah et al., 2023).

Cybersecurity, as defined by Nobles (2023), is a category of information security that focuses on protecting the confidentiality, integrity, and availability (CIA) of digital information assets. This definition encompasses potential threats arising from the compromise of these assets through internet-based channels (Oladipupo Amoo et al., 2024; Nobles, 2023). The mentioned definition of cybersecurity emphasizes the importance of maintaining the CIA, especially since modern cyber threat actors can utilize forms of artificial intelligence like GenAI to enhance the sophistication of cyberattacks (Krishnamurthy, 2023).

This study will focus on the urgent need to explore and understand the potential cybersecurity risks arising from the use of GenAI. The study will conduct an in-depth analysis of cybersecurity risks or threats that may emerge due to the utilization of GenAI by internet users. A systematic literature review (SLR) methodology is employed to support this analysis, with the research question being: "What are the cybersecurity risks associated with the use of generative artificial intelligence technology?" This research question aims to collate all forms of risks into a unified framework to facilitate the formulation of appropriate mitigation strategies and policies in the future.

Materials and Methods

The study employs the Systematic Literature Review (SLR) method to address research questions related to the forms of cybersecurity risks arising from the use of generative artificial intelligence. Broadly speaking, SLR is an interpretive method for answering a research question by examining previous studies relevant to the specified question (Page et al., 2021). The SLR process in this study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 framework. PRISMA 2020, the latest version of PRISMA 2009, is considered one of the best protocols or guidelines for conducting SLR (Dhingra et al., 2024). PRISMA aims to facilitate the systematic review process (Dhingra et al., 2024; Page et al., 2021). Initially, the results of the literature search are compiled into a table, duplicates are removed, and filtering is conducted based on manuscript type, publication year, and venue. The first screening results are then further filtered based on the abstract's relevance to the research question. This second screening stage produces literature that is further refined using additional exclusion criteria and full-text content. After several stages of screening, the selected literature is assessed for quality, credibility, and content validity (Mangaroo-Pillay & Coetzee, 2022).

The PRISMA flow adapted in this study is limited to utilizing screening guidelines to obtain the final PRISMA literature selection result. This approach streamlines the SLR process while maintaining the research direction. After modifications, the process consists of only three stages: the identification stage, the screening stage, and the final selection stage. First, in the identification stage, the platforms for literature sources are determined, and the number of findings is recorded. Findings at this stage are obtained after applying inclusion criteria (Dey et al.,


ComniTech: Journal of Computational Intelligence and Informatics
https://dx.doi.org/000000000
P-ISSN: 3063-315X E-ISSN: 3063-0630

2024). Next, during the screening stage, further selection is conducted using exclusion criteria and abstract reviews. This process produces literature findings ready for full-text content review. Finally, in the final determination stage, the number of literature passing the screening process is finalized.**Source Platforms**

The research sources will be obtained from various reliable and relevant research article platforms and databases. In this study, the sources include IEEE Xplore, Arxiv, ScienceDirect, and Google Scholar. The selection of these sources is based on several considerations, including ease of access offered by each platform and the completeness and quality of available research articles. IEEE Xplore and ScienceDirect are known for their extensive collections of journals and conference proceedings in computer science and related disciplines. Slightly different from these two platforms, Google Scholar offers wide coverage, enabling literature searches across various relevant sources. Additionally, Arxiv is chosen for its reputation in providing access to numerous articles, often encompassing early-stage research and the latest innovations. The decision to use these sources was made considering their ability to provide comprehensive and up-to-date information, supporting an in-depth literature search within the research scope. By utilizing this combination of sources, the study aims to produce a thorough literature review.

Inclusion and Exclusion Criteria

Defining inclusion and exclusion criteria is crucial for selecting literature in SLR using the PRISMA 2020 framework. This process ensures the selection of literature that aligns with the study's objectives or research questions (Albhirat et al., 2024). These criteria are carefully designed so that inclusion and exclusion points help narrow down the literature findings and eliminate irrelevant results.

The Boolean search strategy on the sources will focus on keywords relevant to the research question, such as "cybersecurity," "generative," "artificial intelligence," "genai," and "risk." More specifically, the search terms will be combined to form the following Boolean search query: ((“generative artificial intelligence” OR “genai” OR “GAI”) AND (“cybersecurity” OR “security” OR “cyber”)). Searches will be performed in the context of titles, abstracts, and keywords, adjusted to the search system on the respective source platforms. One critical point in this search is that selected literature must have been published within the last ten years to expand insights into research developments (Wach et al., 2023). Below are the inclusion (I) and exclusion (E) criteria used:

Inclusion Criteria (I):

- **I01:** Literature published within the last ten years, from 2015 to 2024.
- **I02:** Literature has a "published" status and is in the form of a complete manuscript.
- **I03:** Literature is in the form of a publication article.
- **I04:** Literature is accessible.
- **I05:** Literature discusses generative AI and cybersecurity.

Exclusion Criteria (E):

- **E01:** Literature in the form of books or magazines.
- **E02:** Literature not in English.
- **E03:** Literature outside the field of computer science.

ComniTech: Journal of Computational Intelligence and Informatics
https://dx.doi.org/000000000
P-ISSN: 3063-315X E-ISSN: 3063-0630

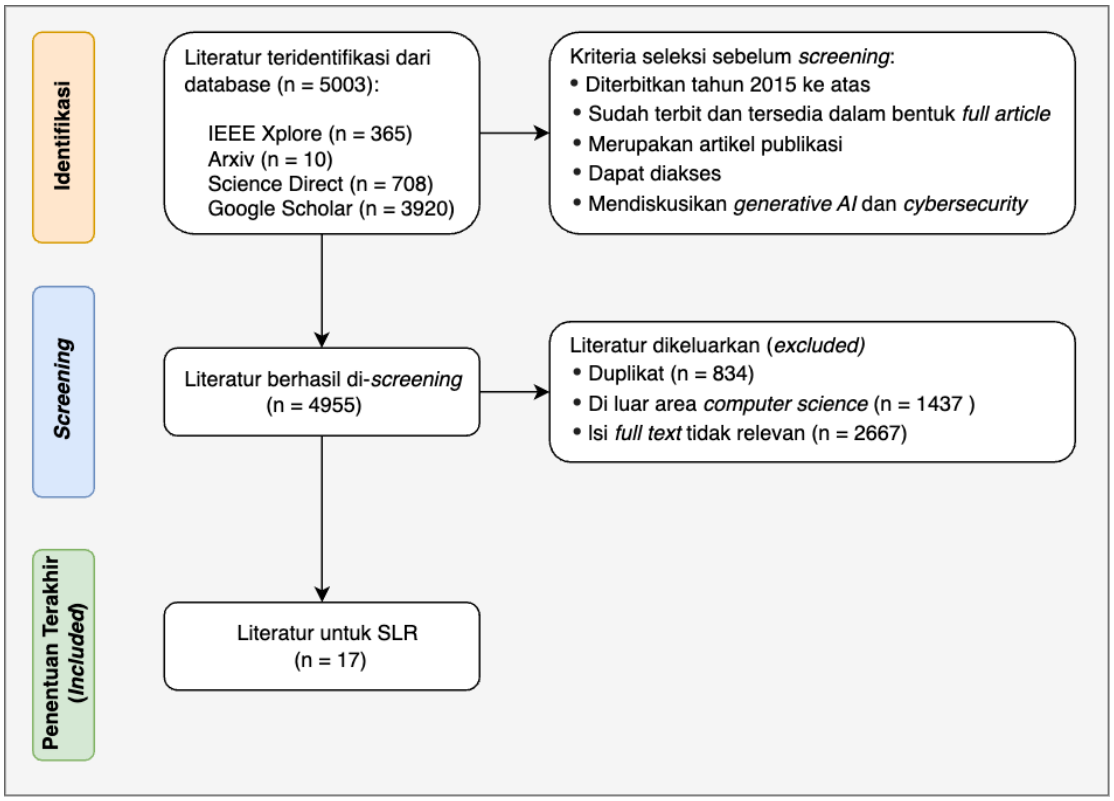

Fig 1. Flow of Research SLR Following PRISMA 2020

Based on the PRISM selection flow in Page et al. (2021), the final result is seventeen literatures that meet the criteria and can be used for SLR. The seventeen literatures come from different sources/databases, and have different publication years. The mapping of the distribution of literature sources and the distribution of publication years are listed in Table 1 and Figure 2, respectively.

Sources	Initial Literature Count	Final Literature Count
IEEE Xplore	365	3
Arxiv	10	5
ScienceDirect	708	3
Google Scholar	3920	6

From the PRISMA screening, five pieces of literature were found to be from 2023, and twelve pieces of literature were from 2024.

ComniTech: Journal of Computational Intelligence and Informatics
https://dx.doi.org/000000000
P-ISSN: 3063-315X E-ISSN: 3063-0630

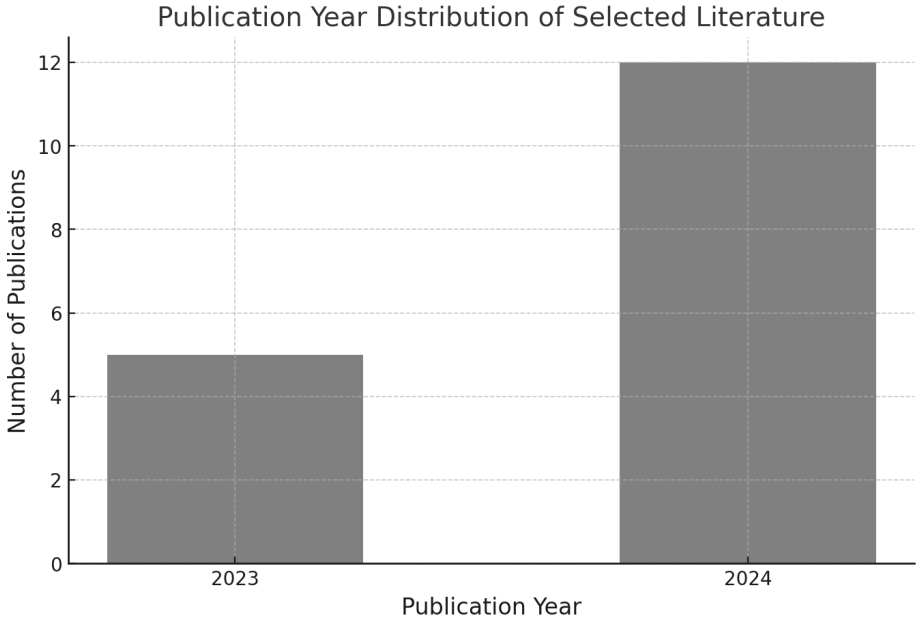

Fig 2. Mapping the Distribution of Literature Publication Year

The literature that was successfully collected for SLR needs was re-analyzed with the help of the Atlas.ti 9 application. The goal is that findings related to cybersecurity risks by GenAI can be easily highlighted in each literature. In addition to making highlighting easier, this application can also assist in identifying patterns of similar risk findings when highlighting text (Mangaroo-Pillay & Coetzee, 2022).

Results and Discussion

Cybersecurity risk findings from seventeen SLR literatures (articles) were successfully identified with the help of the Atlas.ti 9 application. From these findings, it is known that some literatures contain the same risk information. A summary of the SLR literature risk findings is presented in Table 2. The findings are labeled with different colors to facilitate categorization in further discussion.

Table 1. Cybersecurity Risks by Generative Artificial Intelligence (SLR Results)

Source	Cyber Security Risks
Gupta et al. (2023); Metta et al. (2024); Sebastian (2023); Okey et al. (2023); Wang (2024); Dwivedi & Elluri (2024)	Phishing
Gupta et al. (2023); Sebastian (2023); Dwivedi & Elluri (2024); Okey et al. (2023); Metta et al. (2024)	Social engineering
Gupta et al. (2023); Metta et al. (2024); Wang (2024)	Ransomware
Gupta et al. (2023); Mira (2021); Acosta-Urigüen et al. (2024); Mangaroo-Pillay & Coetzee (2022); Oliveira et al. (2024); Polito & Pupillo (2024); Gupta et al. (2023)	Malware

ComniTech: Journal of Computational Intelligence and Informatics
https://dx.doi.org/000000000
P-ISSN: 3063-315X E-ISSN: 3063-0630

Fui-Hoon Nah et al. (2023); Metta et al. (2024); Wang (2024); Metta et al. (2024); Golda et al. (2024); Krishnamurthy (2023)	Deepfakes
Wang (2024); Dwivedi & Elluri (2024); Golda et al. (2024); Metta et al. (2024); Fui-Hoon Nah et al. (2023); Novelli et al. (2024); Wach et al. (2023)	Misinformation dan false information
Sebastian (2023); Golda et al. (2024); Wach et al. (2023); Novelli et al. (2024); Krishnamurthy (2023)	Data leakage
Golda et al. (2024); Wach et al. (2023); Novelli et al. (2024)	Personal data misuse
Fui-Hoon Nah et al. (2023); Novelli et al. (2024); Wu et al. (2023)	Executable attack code generation
Wach et al. (2023); Golda et al. (2024); Sebastian (2023); Novelli et al. (2024)	Privacy risk
Wach et al. (2023); Sebastian (2023)	Intellectual property violation

Phishing and Social Engineering

Phishing and social engineering are forms of manipulation used in cyberattacks to obtain sensitive information or illegally access systems (Kulkarni & Nath, 2024). Phishing typically involves attackers posing as senders of communications or messages that appear legitimate. Phishing is often conducted through email to collect personal data, such as passwords or financial information, by impersonating trusted entities or organizations (Metta et al., 2024). On the other hand, social engineering involves psychological manipulation to deceive individuals into performing certain actions, such as disclosing confidential information or clicking malicious links (Gupta et al., 2023; Kulkarni & Nath, 2024).

Research (Gupta et al., 2023; Metta et al., 2024; Sebastian, 2023; Okey et al., 2023; Wang, 2024; Dwivedi & Elluri, 2024) collectively reveals the dangers and risks of phishing and social engineering as consequences of irresponsible use of Generative AI (GenAI). GenAI can generate customized messages that appear relevant to the victim's conditions and needs (Sebastian, 2023). Even small pieces of information gathered by attackers can be processed into tailored messages that match the victim's profile (Gupta et al., 2023).

Malware, Ransomware, and Executable Attack Code Generation

Malware, ransomware, and executable attack code generation are significant issues in cybersecurity that have become increasingly complex with technological advancements. Malware encompasses various types of malicious software designed to damage, steal, or access data illegally (Mira, 2021). Ransomware, as a type of malware, encrypts data on the victim's system, enabling attackers to demand ransom to restore access to the data (Chinmaya et al., 2023).

ComniTech: Journal of Computational Intelligence and Informatics
https://dx.doi.org/000000000
P-ISSN: 3063-315X E-ISSN: 3063-0630

Research (Mangaroo-Pillay & Coetzee, 2022; Gupta et al., 2023; Dwivedi & Elluri, 2024) highlights that GenAI facilitates the creation of sophisticated executable codes at the user's command. This capability enables the development of more effective ransomware and malware (Wang, 2024). Furthermore, GenAI can be utilized to create SQL injection codes and other execution procedures (Fui-Hoon Nah et al., 2023). With GenAI's ability to instantly generate code, attacks have become more innovative, even by individuals without advanced coding expertise (Okey et al., 2023).

Deepfakes

Deepfakes are technologies that can produce highly realistic media content, such as videos or audio, resembling specific individuals (Romero Moreno, 2024). Cybersecurity risks associated with deepfakes include public fraud and manipulation, where individuals or organizations may become targets (Romero Moreno, 2024). Research (Ranka et al., 2024) details how deepfakes can be used to create fake videos of political figures during elections, conveying statements that were never made. This increases the complexity of challenges in information verification and digital security, amplifying the risk of disinformation and reputational harm to involved individuals or organizations (Kumar, 2024).

The use of GenAI in deepfakes has become a significant threat. Studies (Fui-Hoon Nah et al., 2023; Metta et al., 2024; Romero Moreno, 2024) reveal that GenAI enables the creation of deepfake content without clear legal frameworks (Golda et al., 2024). This violates the concept of individual consent, causing individuals to lose control over how their identity is used (Wang, 2024).

Misinformation and False Information

Misinformation and false information can influence perceptions and decision-making for individuals or organizations. While GenAI is recognized for its sophistication, it is not always reliable as it is prone to producing incorrect answers (Monteith et al., 2024). Research (Dwivedi & Elluri, 2024; Golda et al., 2024) demonstrates how GenAI creates vulnerabilities for the spread of misinformation, partly due to its question-and-answer (QnA) approach that generates responses even if they are inaccurate (Wach et al., 2023). Furthermore, data poisoning and sabotage of GenAI’s training data contribute to the creation of flawed outputs, exacerbating the dissemination of misinformation and false information (Okey et al., 2023).

Data Leakage, Personal Data Misuse, Privacy Risk, and Intellectual Property Violation

In the context of Generative Artificial Intelligence (GenAI), risks related to data leakage, personal data misuse, privacy risks, and intellectual property violations have become major concerns, particularly with regulations like GDPR governing data protection (Golda et al., 2024). GenAI training data often includes copyrighted material or other forms of protected intellectual property (Sebastian, 2023).

Research (Golda et al., 2024; Wach et al., 2023; Okey et al., 2023) identifies these risks as consequences of unregulated GenAI use. For example, personal data is often used to generate content without explicit consent (Golda et al., 2024). Additionally, users' search histories and thought processes during GenAI usage are recorded

as training data, raising privacy concerns (Dwivedi & Elluri, 2024). Studies (Golda et al., 2024; Sebastian, 2023) emphasize the need for transparency and explicit consent regarding the use of personal data, as well as the potential exploitation of private data for creating deepfakes and other illicit content, which are not yet fully addressed by GDPR or similar regulations worldwide (Golda et al., 2024).

Conclusion

This research has identified various cybersecurity risks arising from the use of Generative Artificial Intelligence (GenAI) through a systematic literature review (SLR) approach. From the literature reviewed, it was found that GenAI carries significant risks in several aspects, including phishing attacks, social engineering, ransomware, malware, deepfakes, misinformation, data leakage, misuse of personal data, executable attack code generation, privacy risks, and intellectual property violations. These risks represent potentially serious threats to cybersecurity and data integrity, and emphasize the need for effective mitigation measures. The findings underscore the importance of developing stricter policies and regulations to govern the use of GenAI, to prevent misuse and protect personal data and intellectual property rights. This research also emphasizes the need for collaborative efforts from various parties, including researchers, policy makers, and industry practitioners, to address the challenges faced and ensure that GenAI technology is used ethically and responsibly. Thus, it is hoped that the results of this research can serve as a basis for the development of more effective security strategies and policies and advance safer practices in the use of GenAI.

References

Taherdoost, H. (2022). An Overview of Trends in Information Systems: Emerging Technologies That Transform The Information Technology Industry. *Cloud Computing and Data Science*, 1–16. https://doi.org/10.37256/ccds.4120231653

Păvăloaia, V. D., & Necula, S. C. (2023). Artificial Intelligence as a Disruptive Technology—A Systematic Literature Review. *MDPI*. https://doi.org/10.3390/electronics12051102

Saddi, V. R., Gopal, S. K., Mohammed, A. S., Dhanasekaran, S., & Naruka, M. S. (2024). Examine The Role of Generative AI in Enhancing Threat Intelligence and Cyber Security Measures. In *2024 2nd International Conference on Disruptive Technologies, ICDT 2024* (pp. 537–542). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICDT61202.2024.10489766

Teo, Z. L., Quek, C. W. N., Wong, J. L. Y., & Ting, D. S. W. (2024). Cybersecurity in the generative artificial intelligence era. *Elsevier B.V.* https://doi.org/10.1016/j.apjo.2024.100091

Polito, C., & Pupillo, L. (2024). Artificial Intelligence and Cybersecurity. *Intereconomics, 59*(1), 10–13. https://doi.org/10.2478/ie-2024-0004

Su, J., & Yang, W. (2023). Unlocking the Power of ChatGPT: A Framework for Applying Generative AI in Education. *ECNU Review of Education, 6*(3), 355–366. https://doi.org/10.1177/20965311231168423

Fui-Hoon Nah, F., Zheng, R., Cai, J., Siau, K., & Chen, L. (2023). Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration. *Routledge*. https://doi.org/10.1080/15228053.2023.2233814

Nobles, C. (2023). Offensive artificial intelligence in cybersecurity: Techniques, challenges, and ethical considerations. In *Real-World Solutions for Diversity, Strategic Change, and Organizational Development:*

Perspectives in Healthcare, Education, Business, and Technology (pp. 348–363). IGI Global. https://doi.org/10.4018/978-1-6684-8691-7.ch021

Amoo, O. O., Osasona, F., Atadoga, A., Ayinla, B. S., Farayola, O. A., & Abrahams, T. O. (2024). Cybersecurity Threats in the Age of IoT: A Review of Protective Measures. *International Journal of Science and Research Archive, 11*(1), 1304–1310. https://doi.org/10.30574/ijsra.2024.11.1.0217

Krishnamurthy, O. (2023). Enhancing Cyber Security Enhancement Through Generative AI. *International Journal of Use*, 9. Retrieved from http://www.ijuse.in

Acosta-Urigüen, M., et al. (2024). Conceptualizing the Active Ageing Index (AAI): A Systematic Literature Review of Frameworks and Supporting Digital Tools. In *Proceedings of the 10th International Conference on Information and Communication Technologies for Ageing Well and e-Health* (pp. 276–283). SCITEPRESS. https://doi.org/10.5220/0012722000003699

Dhingra, V., Keswani, S., Sama, R., & Noor Mohamed Qureshi, M. R. (2024). Social Media Influencers: A Systematic Review Using PRISMA. *Cogent OA*. https://doi.org/10.1080/23311975.2024.2368100

Page, M. J., et al. (2021). The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *The BMJ, 372*. https://doi.org/10.1136/bmj.n71

Rizzo, G., Migliore, G., Schifani, G., & Vecchio, R. (2024). Key Factors Influencing Farmers' Adoption of Sustainable Innovations: A Systematic Literature Review and Research Agenda. *Springer Science and Business Media B.V.* https://doi.org/10.1007/s13165-023-00440-7

Dey, R., Kassim, S., Maurya, S., Mahajan, R. A., Kadia, A., & Singh, M. (2024). A Systematic Literature Review on the Islamic Capital Market: Insights Using the PRISMA Approach.

Albhirat, M. M., et al. (2024). The PRISMA Statement in Enviropreneurship Study: A Systematic Literature and A Research Agenda. *Elsevier Ltd.* https://doi.org/10.1016/j.clet.2024.100721

de Oliveira, U. R., Menezes, R. P., & Fernandes, V. A. (2024). A Systematic Literature Review on Corporate Sustainability: Contributions, Barriers, Innovations and Future Possibilities. *Springer Science and Business Media B.V.* https://doi.org/10.1007/s10668-023-02933-7

Mangaroo-Pillay, M., & Coetzee, R. (2022). Lean Frameworks: A Systematic Literature Review (SLR) Investigating Methods and Design Elements. *Journal of Industrial Engineering and Management, 15*(2), 202–214. https://doi.org/10.3926/jiem.3677

. Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3300381

Metta, S., et al. (2024). Generative AI in Cybersecurity.

Sebastian, G. (2023). Do ChatGPT and Other AI Chatbots Pose a Cybersecurity Risk? International Journal of Security and Privacy in Pervasive Computing, 15(1), 1–11. https://doi.org/10.4018/ijsppc.320225

Okey, O. D., Udo, E. U., Rosa, R. L., Rodríguez, D. Z., & Kleinschmidt, J. H. (2023). Investigating ChatGPT and cybersecurity: A perspective on topic modeling and sentiment analysis. Computers & Security, 135. https://doi.org/10.1016/j.cose.2023.103476

Wang, M. (2024). Generative AI: A New Challenge for Cybersecurity. https://doi.org/10.32996/jcsts

Dwivedi, R., & Elluri, L. (2024). Exploring Generative Artificial Intelligence Research: A Bibliometric Analysis Approach. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3450629

Yigit, Y., Buchanan, W. J., Tehrani, M. G., & Maglaras, L. (2024). Review of Generative AI Methods in Cybersecurity. arXiv. Retrieved from http://arxiv.org/abs/2403.08701

Romero Moreno, F. (2024). Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content. International Review of Law, Computers and Technology. https://doi.org/10.1080/13600869.2024.2324540

Takale, D. G., Mahalle, P. N., & Sule, B. (2024). Cyber Security Challenges in Generative AI Technology.

Golda, A., et al. (2024). Privacy and Security Concerns in Generative AI: A Comprehensive Survey. IEEE Access, 12, 48126–48144. https://doi.org/10.1109/ACCESS.2024.3381611

Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity.

Wach, K., et al. (2023). The Dark Side of Generative Artificial Intelligence: A Critical Analysis of Controversies and Risks of ChatGPT. Entrepreneurial Business and Economics Review, 11(2), 7–30. https://doi.org/10.15678/EBER.2023.110201

Ye, X., Yan, Y., Li, J., & Jiang, B. (2024). Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective. Telecommunications Policy. https://doi.org/10.1016/j.telpol.2024.102851

Wu, X., Qiu, Q., Li, J., & Zhao, Y. (2023). Intell-Dragonfly: A Cybersecurity Attack Surface Generation Engine Based On Artificial Intelligence-Generated Content Technology. arXiv. Retrieved from http://arxiv.org/abs/2311.00240

Kulkarni, A. V., & Nath, S. (2024). Human Susceptibility to Social Engineering Attacks: An Innovative Approach to Social Change. In 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI) (pp. 1–6). IEEE. https://doi.org/10.1109/IATMSI60426.2024.10502492

Mira, F. (2021). A Systematic Literature Review on Malware Analysis. In 2021 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS) (pp. 1–5). IEEE. https://doi.org/10.1109/IEMTRONICS52119.2021.9422537

Chinmaya, B. J., Kudtarkar, S. A., & Mohana. (2023). Targeted Ransomware Attacks and Detection to Strengthen Cybersecurity Strategies. In 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 1039–1044). IEEE. https://doi.org/10.1109/ICACRS58579.2023.10404203

Ranka, H., et al. (2024). Examining the Implications of Deepfakes for Election Integrity.

Kumar, S. (2024). Online Defamation in the Digital Age: Issues and Challenges with Particular Reference to Deepfakes and Malicious Bots. International Journal of Law and Policy, 2(8), 32–41. https://doi.org/10.59022/ijlp.200

Monteith, S., Glenn, T., Geddes, J. R., Whybrow, P. C., Achtyes, E., & Bauer, M. (2024). Artificial Intelligence and Increasing Misinformation. The British Journal of Psychiatry, 224(2), 33–35. https://doi.org/10.1192/bjp.2023.136