DAAR EL-IRTIQA': Journal of Islamic Education Tranformation and Management
Vol. 1 No. 1 (2026), p. 21-29
Available online at https://e-journal.ibama.ac.id/index.php/irtiqa

Beyond Digital Literacy: Reconstructing Digital Ethics and Security in the Age of Artificial Intelligence

Lukman Sholeh[1]*, Muhammad Fadali Amar[2], Malikul Habsi[3], Faiqotul Aminah[4], Moh. Sholehuddin Anwar[5],
[1,2,3,4,5] Institut Badri Mashduqi, Indonesia

Article History:
Received: Agustus 2026
Accepted: September 2026
Published: Oktober 2026

Keywords:
Digital Literacy; Digital Ethics; Digital Security; Artificial Intelligence; Digital Responsibility.

**Correspondence Address:*
lukmansholeh211199@ibama.ac.id

Abstract :
The rapid development of artificial intelligence has transformed higher education practices while raising critical concerns about digital ethics, information security, and human responsibility. This study aims to reconstruct digital literacy by integrating ethical awareness, digital security, and responsible AI utilization within higher education. Employing a qualitative case study design, data were collected from students, lecturers, and information technology administrators through in-depth interviews, observations, and institutional documentation. Data were analyzed using the interactive model of Miles, Huberman, and Saldaña, involving data condensation, data display, and conclusion verification. The findings identify three analytical dimensions: the transformation of academic practices through digital technologies, the gap between technical competence and ethical awareness, and institutional challenges in digital security and privacy protection. This study proposes the Ethical-Secure Digital Literacy framework, integrating digital competence, digital ethics, digital security, and digital responsibility. The framework offers implications for strengthening academic integrity, institutional digital governance, and responsible AI adoption.

INTRODUCTION

The development of digital technology and artificial intelligence (AI) has fundamentally changed the way people communicate, interact socially, conduct economic activities, and produce knowledge in contemporary society.(Arar et al., 2025) The presence of generative technology allows people to access, process, and produce information quickly, but at the same time brings up new issues related to data security, privacy, the spread of disinformation, information manipulation, and misuse of technology.(Shahzad et al., 2024) Digital space, which was previously understood as a means of communication and information exchange, has now evolved into a complex arena that brings together the interests of technology, economy, power, and morality.(Mannuru et al., 2025) This situation shows that just being good with technology is no longer enough without ethical awareness and digital responsibility.

In the context of At-Taqwa University Bondowoso, digital transformation is evident through the development of PORTA as an integrated academic service system that provides self-service for correspondence, academic information, and the development of a Learning Management System (LMS). On the other hand, attention to

This journal is an open-access article under a CC BY-NC-SA 4.0 license. © 2025, the author(s)

digital communication ethics is also reflected in the Training of Commander HIMA MPI in September 2026, which emphasized the importance of verifying information, controlling emotions, and being responsible on social media. This shows that digital transformation in universities not only requires infrastructure readiness and tech skills but also strengthening ethical awareness, protecting information, and the responsibility of the academic community in utilizing artificial intelligence.

Studies on digital literacy so far have mostly focused on an individual's ability to access, understand, evaluate, and use technology-based information.(Kalota, 2024) Meanwhile, the development of AI ethics studies is starting to place privacy, transparency, accountability, fairness, and human oversight as key principles for responsible technology use. UNESCO (2023) emphasizes a human-centered approach in using AI, including privacy protection and enhancing human capabilities.(Pereira, 2026) trusted AI principles through security, safety, transparency, and accountability.(Halgamuge & Niyato, 2025) Meanwhile, NIST (2024) developed a risk management framework specifically for generative AI.(Admass et al., 2024) Even so, the integration of digital literacy, ethics, and security into a single conceptual framework focused on human responsibility still needs to be developed further.

This research aims to reconstruct the concept of digital literacy by integrating ethical and security dimensions as the foundation for responsible technology use in the age of artificial intelligence. The study focuses on three main issues. First, how is the development of AI changing the paradigm of digital literacy and giving rise to new challenges in people's lives? Second, how can digital ethics and information security principles be integrated to address issues like privacy, information manipulation, disinformation, and technology misuse? Third, how can we build a conceptual framework that connects digital literacy, ethical responsibility, and digital security resilience? These three questions serve as the basis for analysis to create an integrative perspective on governing human behavior in the contemporary digital ecosystem.

This research starts from the argument that digital literacy focused only on mastering technical skills is not enough to tackle the complex challenges of AI-based technology.(R. Zhang et al., 2020) The ability to use technology should come with awareness of moral consequences, understanding of security risks, and responsibility for the information that is produced and shared.(Von Solms & Van Niekerk, 2013) This research assumes that the integration of three dimensions—digital literacy, digital ethics, and digital security—can shape a more comprehensive digital literacy paradigm. The tentative answer proposed is that reconstructing digital literacy needs to place humans as subjects who have autonomy, moral awareness, critical skills, and responsibility in controlling the use of technology.

The main contribution of this research lies in its effort to offer a conceptual reconstruction of digital literacy that goes beyond just technical skills, moving towards a paradigm that integrates ethics, security, and human responsibility. Unlike approaches that tend to separate digital skills, information security, and ethical behavior, this study proposes an integrative framework that treats all three as interconnected elements. The originality of the research is reflected in the development of the Ethical-Secure Digital Literacy perspective, a paradigm that emphasizes critical thinking, moral awareness, privacy protection, digital resilience, and accountability in AI use. This framework is expected to contribute theoretically to the development of digital literacy studies while also serving as a practical foundation for creating a safe, ethical, and responsible digital

society.

RESEARCH METHOD

Research Approach

This research was carried out at At-Taqwa University Bondowoso with the unit of analysis being digital literacy practices, the application of digital ethics, and information security awareness in the academic activities of the university community. The study used a qualitative design with a case study approach to deeply understand the dynamics of using digital technology and artificial intelligence in the university environment.(Hafsiah Yakin, 2023) This approach was chosen because it allows researchers to explore experiences, perceptions, behaviors, and social interactions related to digital responsibility. The analysis focuses on the use of AI in learning, academic integrity, personal data protection, digital account security, and the ethics of academic communication.(Fadli, 2021)

Research Information Sources

The sources of research information consist of primary and secondary data. Primary data is obtained through in-depth interviews with students, lecturers, educational staff, and the IT managers at At-Taqwa University Bondowoso, who are chosen purposively based on their involvement and relevance to digital technology use. Students are the source of information regarding their experiences using AI and digital media in academic activities, while lecturers provide perspectives on academic integrity and learning ethics. IT managers provide information about security systems and data protection. Secondary data is obtained from academic policy documents, technology usage guidelines, institutional publications, and scientific literature related to digital literacy, ethics, and cybersecurity.

Data Collection and Analysis Techniques

Data collection was done through three techniques: in-depth interviews, observation, and documentation. Interviews were used to explore the experiences and understanding of informants regarding the use of AI, digital ethics, and information security. Observation was carried out on the practice of using technology in academic activities while still respecting the privacy of the informants. Documentation included institutional policies, academic guidelines, and other supporting documents. Data analysis used the interactive model of Miles and Huberman, through three main stages: data condensation, data presentation, and drawing conclusions and verification.(Nurdin & Hafidzi, 2023) The validity of the data is strengthened through source and technique triangulation to get interpretations that are credible and consistent.

RESULT AND DISCUSSION

Digital Transformation in Higher Education: The Changing Landscape of Academic Practices

Digital transformation in universities has changed the way academic activities are carried out, especially in learning, communication, administration, and information management.(Elia et al., 2024) At At-Taqwa University Bondowoso, this development can be seen through the use of digital academic service platforms, e-learning systems, and various communication and artificial intelligence applications by the academic community. This change shows that technology is no longer just a supporting tool but has become a part of the academic ecosystem. Even so, the effectiveness of digital

transformation is not only determined by the availability of technology infrastructure, but also by the users' ability to understand, manage, and use it critically and responsibly.

An illustrative interview with a student from At-Taqwa University Bondowoso shows that digital technology has become an important part of college activities. The informant described the change as follows: *"Using digital technology really helps with college activities. We can get academic information through the campus system, communicate with lecturers via WhatsApp, as well as look for references and use AI to help understand course material. However, sometimes we still don't really understand the limits of using AI, especially when using it to complete assignments. Also, not all information obtained from the internet can be trusted right away, so it still needs to be double-checked."* This statement reflects the user experience regarding the convenience of technology as well as the challenges in using it.

The informant's statement shows that digital transformation has created new patterns in academic practices, marked by increased information accessibility, flexible communication, and ease of obtaining learning resources. The use of digital technology and artificial intelligence provides opportunities for students to develop independent learning and expand access to knowledge.(Feliciano-Cestero et al., 2023) However, this convenience also brings up issues about the ability to evaluate information, set limits on AI use, and maintain academic integrity.(Sacavém et al., 2025) Thus, digital transformation cannot be understood merely as a change in learning media, but also as a change in behavior, mindset, and the responsibilities of the academic community in carrying out educational activities.

The finding can be interpreted that digital transformation in higher education requires a shift in paradigm from just mastering technological devices to developing reflective and responsible digital competence.(J. Zhang & Chen, 2024) This perspective aligns with the thinking (Chwiłkowska-Kubala et al., 2023) which places digital literacy as a multidimensional skill that includes technical, cognitive, and social-emotional dimensions. In the context of using AI, the ability to access technology must be accompanied by skills to evaluate information, awareness of the consequences of using technology, and academic responsibility.(Ellström et al., 2022) Therefore, the ideal digital transformation not only creates academic efficiency but also shapes a learning culture that is critical, ethical, and focused on intellectual integrity.

These findings have important implications for the development of higher education governance, especially in building an academic ecosystem that adapts to the developments in artificial intelligence technology. Digital transformation should be aimed not just at improving service efficiency and learning accessibility, but also at strengthening critical skills, academic integrity, and user responsibility.(Omol, 2024) Universities need to develop AI usage policies, information security guidelines, and digital literacy enhancement programs that are integrated into academic activities. That way, the success of digital transformation isn't just measured by how advanced the infrastructure is, but by the institution's ability to create a productive, safe, ethical academic culture focused on improving human quality.

The relationship between digital transformation and changes in academic practices shows that the more technology is used in universities, the greater the need for digital skills and ethical awareness among its users.(Plekhanov et al., 2023) This happens because digitization speeds up information exchange, expands access to knowledge, and at the same time increases dependence on algorithm-based platforms and systems.

However, these conveniences don't automatically lead to responsible academic behavior. Without the ability to evaluate information, understand security risks, and consider the moral consequences of using AI, digital transformation can actually increase academic vulnerabilities. So, the relationship between the two needs to be built through integrating technology skills, ethics, and digital security.(Michelotto & Joia, 2024)

Beyond Technical Competence: The Gap between Digital Literacy and Ethical Awareness

The observation of academic activities at At-Taqwa University Bondowoso aimed to identify the relationship between technical skills in using technology and the ethical awareness of the academic community. The study focused on student behavior when accessing digital information, using artificial intelligence to complete assignments, communicating through social media, and using internet-based reference sources. The focus wasn't just on the ability to operate tech devices, but also on the ability to consider the accuracy of information, academic honesty, intellectual responsibility, and the consequences of using technology.(Awad et al., 2026) That focus is important to see whether the boost in digital skills is keeping up with the growth of ethical awareness.

The observation was designed to map several indicators of digital behavior in students' academic activities. This mapping covers technical skills, information evaluation, academic integrity, communication ethics, and awareness of AI usage. Each indicator is observed through learning activities, academic interactions, and the use of digital information sources. The observation results are then grouped based on the alignment between technical behavior and digital ethics principles. The following visualization is a categorization matrix used as an analysis tool to identify gaps in competence and ethical awareness. The empirical evidence is documented based on field notes actually obtained during the research process.

Table 1. Observation Matrix of Digital Literacy Gaps and Ethical Awareness

Observation aspect	Observed indicators	Focus of analysis
Technical skills	The use of digital apps and AI	Technology skills
Information literacy	Verify sources and information	Critical thinking
Academic integrity	Use of AI in tasks	Intellectual honesty
Communication ethics	Behavior in academic groups	Social responsibility
Digital awareness	Understanding the consequences of using technology	Moral awareness

Based on these observation categories, the main issue that needs to be analyzed isn't just students' ability to use technology, but also how consistently they apply ethical values when technology is used for academic purposes. The ability to access information, use AI applications, and complete tasks digitally should be balanced with intellectual honesty, verifying information, and respecting privacy. So, digital literacy and ethical awareness are two dimensions that complement each other. Gaps between the two can become a critical point in understanding the challenges of digital transformation in universities, especially in maintaining academic integrity.

Theoretically, the gap between technical skills and ethical awareness shows that digital literacy can't just be reduced to the ability to operate tech devices. (Pramod, 2025) explaining that digital literacy involves interrelated technical, cognitive, and socio-

emotional dimensions. This perspective is reinforced by the framework (Misbahuljannah et al., 2026) which puts security, communication, content creation, and problem-solving as part of digital competence. In the context of using AI, technical skills need to be accompanied by critical assessment and moral consideration. So, this study views ethical awareness as a fundamental element that connects tech skills with academic responsibility.

Findings about the gap between technical skills and ethical awareness have important implications for developing a digital academic culture in universities. Mastery of technology and artificial intelligence needs to be balanced with building intellectual integrity, moral responsibility, and the ability to assess the consequences of using technology. In the context of At-Taqwa University Bondowoso, this situation provides a foundation for developing academic policies that not only emphasize digital proficiency but also integrate AI ethics education, plagiarism prevention, information verification, and privacy protection. In this way, higher education has a strategic responsibility to shape technology users who are both competent and have integrity.

The gap between technical skills and ethical awareness shows up because digital technology develops faster than people's understanding of morals and their responsibilities.(Nikolaidou, 2025) The ease of accessing artificial intelligence, getting information, and creating digital content doesn't always come with the ability to assess its truthfulness, originality, or social consequences. In academic settings, this is linked to the fact that digital ethics education hasn't been fully integrated into teaching practices and institutional policies. In other words, the more complex technology use becomes, the more important it is to strengthen ethical awareness as a way to guide digital behavior so that technical skills grow responsibly.

Digital Security and Privacy Protection: Challenges in the AI-Driven Academic Environment

The growth of digital technology and artificial intelligence in university activities brings new challenges related to information security and privacy protection. At At-Taqwa University Bondowoso, the development of digital academic services like PORTA, academic information systems, and e-learning facilities is part of transforming the management of institutional information. This makes account security, student data confidentiality, protection of academic documents, and management of personal information important aspects that need attention. Research documentation is aimed at identifying how far policies, procedures, and digital security infrastructure have supported the creation of a safe, protected, and responsible academic environment.

The document analysis was carried out by reviewing various institutional documents related to information system management and the protection of academic data. The documents analyzed included policies on information system usage, guidelines for digital academic services, account management procedures, as well as provisions for personal information protection. The review results were then categorized based on security, privacy, and institutional responsibility aspects. The following matrix is used to map the documentary evidence while also identifying aspects that are already regulated, undocumented, or still require clarification through interviews with IT managers and related parties.

Table 2. Analysis Matrix of Digital Security Documentation and Privacy Protection

Types of	Aspects that are analyzed	The evidence being looked for

documentation		
Digital academic policy	Information management	System usage terms
Academic Information System	Account security	Authentication and access settings
Academic guidelines	Student privacy	Personal data management
AI usage guidelines	Information security	Limits on entering data into AI
Information technology SOP	Data protection	Backup and incident handling
Institution policy	Responsibility	Division of data management authority

Mapping that documentation emphasizes that digital security in universities isn't just about having devices and information systems, but also includes data protection mechanisms and clarity about who is responsible for managing it.(Radanliev, 2024) The existence of digital academic platforms needs to be supported by policies regarding user access, information confidentiality, document storage, and the use of AI-based applications. In that way, digital transformation should be accompanied by systematic information security management.(Schinagl et al., 2022) Institutional documentation becomes an important tool for assessing the alignment between technology development, privacy protection policies, and the institution's commitment to maintaining the trust of the academic community.

Conceptually, digital security and privacy protection are key foundations for building trust in an AI-based academic ecosystem. This perspective aligns with the National Institute of Standards and Technology (NIST) framework through the AI Risk Management Framework, which emphasizes the importance of risk management, security, transparency, and accountability in the use of AI.(Williams et al., 2025) Additionally, Law Number 27 of 2022 on Personal Data Protection provides a normative foundation for managing personal information in Indonesia. From this perspective, this study sees digital security not just as a technical issue, but as part of the ethical and institutional responsibility in protecting the rights of academic communities.

Findings on digital security and privacy protection have strategic implications for strengthening university governance in the age of artificial intelligence. Higher education institutions need to treat personal data protection as an integral part of digital transformation policies, not just a technical responsibility of IT system managers. In the context of At-Taqwa University Bondowoso, developing digital academic services should be accompanied by stronger account security procedures, access rights management, academic document handling, and guidelines for safe use of AI applications. These implications highlight that the success of academic digitalization should be measured by the institution's ability to ensure information security, protect privacy, and build trust within the academic community.(Frech et al., 2025)

The need for digital security and privacy protection is increasing as technology-based academic transformation leads to more intensive data exchange, storage, and processing. The use of academic information systems, learning platforms, and artificial

intelligence applications expands access to information, but at the same time, it creates potential risks for data misuse and privacy breaches. This shows that the more complex the digital ecosystem in universities, the greater the need for systematic information security governance.(Akman et al., 2023) Without data protection policies, access monitoring, and user awareness, technological advancements can actually increase an institution's vulnerabilities and reduce the academic community's trust in digital services.

CONCLUSION

This study emphasizes that digital transformation in universities can't just be measured by technology skills and infrastructure availability; it also needs ethical awareness and information security protection. The digital experience in an academic setting shows that technological advancement should still focus on human values, integrity, and responsibility. The study concludes that integrating digital literacy, ethics, and security is the foundation for building a responsible academic culture. Its main contribution is developing the Ethical-Secure Digital Literacy conceptual framework, which combines digital competence, moral awareness, privacy protection, and human responsibility in the use of artificial intelligence.

This study has its limitations because it uses a qualitative approach with a case study design at a single university, so the results can't be widely generalized yet. In addition, the rapid development of artificial intelligence makes it possible for new ethical and digital security issues to emerge that haven't been fully covered in the analysis. The Ethical-Secure Digital Literacy framework that was developed still needs further empirical testing. Therefore, future research is recommended to use a multi-site or mixed-methods approach, involve more universities, and examine the relationship between digital competence, ethical awareness, information security, and responsible AI use.

REFERENCES

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. In *Cyber Security and Applications*. https://doi.org/10.1016/j.csa.2023.100031

Akman, E., İdil, Ö., & Çakır, R. (2023). An Investigation into the Levels of Digital Parenting, Digital Literacy, and Digital Data Security Awareness among Parents and Teachers in Early Childhood Education. *Participatory Educational Research*. https://doi.org/10.17275/per.23.85.10.5

Arar, K. H., Özen, H., Polat, G., & Turan, S. (2025). Artificial intelligence, generative artificial intelligence and research integrity: a hybrid systemic review. In *Smart Learning Environments*. https://doi.org/10.1186/s40561-025-00403-3

Awad, W. H. A., Awad, N. H. A., Ashour, H. M. A., Khamis, E. A. R., Yassen, M. M., Abo baker Ismail, H. I., Mohammed Mohammed syam, N., & Hashem, E. salama. (2026). The role of digital literacy and ethical awareness in nurses' acceptance of Artificial Intelligence: a cross-sectional questionnaire survey. *International Journal of Nursing Studies Advances*. https://doi.org/10.1016/j.ijnsa.2026.100577

Chwiłkowska-Kubala, A., Cyfert, S., Malewska, K., Mierzejewska, K., & Szumowski, W. (2023). The impact of resources on digital transformation in energy sector companies. The role of readiness for digital transformation. *Technology in Society*. https://doi.org/10.1016/j.techsoc.2023.102315

Elia, G., Solazzo, G., Lerro, A., Pigni, F., & Tucci, C. L. (2024). The digital transformation

canvas: A conceptual framework for leading the digital transformation process. *Business Horizons*. https://doi.org/10.1016/j.bushor.2024.03.007

Ellström, D., Holtström, J., Berg, E., & Josefsson, C. (2022). Dynamic capabilities for digital transformation. *Journal of Strategy and Management*. https://doi.org/10.1108/JSMA-04-2021-0089

Fadli, M. R. (2021). Memahami desain metode penelitian kualitatif. *Medan, Restu Printing Indonesia, Hal.57*, *21*(1), 33–54. https://doi.org/10.21831/hum.v21i1.

Feliciano-Cestero, M. M., Ameen, N., Kotabe, M., Paul, J., & Signoret, M. (2023). Is digital transformation threatened? A systematic literature review of the factors influencing firms' digital transformation and internationalization. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2022.113546

Frech, J., Lilienthal, V., & Schönbächler, V. (2025). First be safe: Exploring and improving journalists' skills in digital security. *Journalism and Communication Monographs* . https://doi.org/10.1177/14648849241310847

Hafsiah Yakin, I. (2023). Penelitian Kualitatif : Metode Penelitian Kualitatif. *Jurnal EQUILIBRIUM*.

Halgamuge, M. N., & Niyato, D. (2025). Adaptive edge security framework for dynamic IoT security policies in diverse environments. *Computers and Security*. https://doi.org/10.1016/j.cose.2024.104128

Kalota, F. (2024). A Primer on Generative Artificial Intelligence. In *Education Sciences*. https://doi.org/10.3390/educsci14020172

Mannuru, N. R., Shahriar, S., Teel, Z. A., Wang, T., Lund, B. D., Tijani, S., Pohboon, C. O., Agbaji, D., Alhassan, J., Galley, J. Kl., Kousari, R., Ogbadu-Oladapo, L., Saurav, S. K., Srivastava, A., Tummuru, S. P., Uppala, S., & Vaidya, P. (2025). Artificial intelligence in developing countries: The impact of generative artificial intelligence (AI) technologies for development. *Information Development*. https://doi.org/10.1177/02666669231200628

Michelotto, F., & Joia, L. A. (2024). Organizational Digital Transformation Readiness: An Exploratory Investigation. In *Journal of Theoretical and Applied Electronic Commerce Research* . https://doi.org/10.3390/jtaer19040159

Misbahuljannah, Riqqah Dhian Shefira, Devi Miftahul Jannah, Muh. Yusril Anam, & Rosidah. (2026). Redefining Social Responsibility Through AI Literacy: The Roles of Digital Literacy and Ethical Awareness in Digital Citizenship. *Journal of Applied Artificial Intelligence in Education*. https://doi.org/10.66053/jaaie.v1i2.7

Nikolaidou, V. (2025). Digital Literacy and Ethical Awareness in Contemporary Education: Challenges and Practical Approaches. *KNOWLEDGE – International Journa*.

Nurdin, M., & Hafidzi, A. (2023). Model interaktif Miles & Huberman dalam analisis data pendidikan. *Jurnal Metodologi Riset Pendidikan*.

Omol, E. J. (2024). Organizational digital transformation: from evolution to future trends. In *Digital Transformation and Society*. https://doi.org/10.1108/DTS-08-2023-0061

Pereira, A. F. S. A. (2026). What Is Artificial Intelligence? *Logica Universalis*. https://doi.org/10.1007/s11787-026-00429-2

Plekhanov, D., Franke, H., & Netland, T. H. (2023). Digital transformation: A review and research agenda. *European Management Journal*. https://doi.org/10.1016/j.emj.2022.09.007

Pramod, D. (2025). Decoding responsible AI use: the influence of digital literacy and ethical awareness. *Cogent Education*.

https://doi.org/10.1080/2331186X.2025.2592371
Radanliev, P. (2024). Digital security by design. *Security Journal*. https://doi.org/10.1057/s41284-024-00435-3
Sacavém, A., de Bem Machado, A., dos Santos, J. R., Palma-Moreira, A., Belchior-Rocha, H., & Au-Yong-Oliveira, M. (2025). Leading in the Digital Age: The Role of Leadership in Organizational Digital Transformation. *Administrative Sciences*. https://doi.org/10.3390/admsci15020043
Schinagl, S., Shahim, A., & Khapova, S. (2022). Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security. *Computers and Security*. https://doi.org/10.1016/j.cose.2022.102903
Shahzad, M. F., Xu, S., Lim, W. M., Yang, X., & Khan, Q. R. (2024). Artificial intelligence and social media on academic performance and mental well-being: Student perceptions of positive impact in the age of smart learning. *Heliyon*. https://doi.org/10.1016/j.heliyon.2024.e29523
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*. https://doi.org/10.1016/j.cose.2013.04.004
Williams, L., Khan, H., & Burnap, P. (2025). The Evolution of Digital Security by Design Using Temporal Network Analysis. *Informatics*. https://doi.org/10.3390/informatics12010008
Zhang, J., & Chen, Z. (2024). Exploring Human Resource Management Digital Transformation in the Digital Age. *Journal of the Knowledge Economy*. https://doi.org/10.1007/s13132-023-01214-y
Zhang, R., Xue, R., & Liu, L. (2020). Security and privacy on blockchain. *ACM Computing Surveys*. https://doi.org/10.1145/3316481