Empowering Bright Internet and Bright Artificial Intelligence (AI)

(Short Title: Bright Internet and Bright AI)

Journal Name: Decision Support Systems

Background

The rapid evolution of technology with the established interconnectedness of our global society has led us to an unprecedented era of opportunities. Concurrently, the negative aspects of information and communication technologies (ICT) are also on the rise. More recently, as Artificial Intelligence (AI) systems are becoming prevalent in our daily lives and organizations' processes, the topic of AI is a subject of intense debate, encompassing both its potential benefits and negative consequences it might inflict upon individuals, organizations, society, and governance. Accordingly, two prominent issues that require intensive research are the intersection between cybersecurity and AI. CIOs in the United States regard cybersecurity and privacy as the most essential organizational issue in the last ten consecutive years. In this respect, previous studies have shed light on the dual nature of AI, demonstrating its capacity to yield positive outcomes alongside detrimental impacts within organizational contexts (Mikalef et al., 2022). However, there is no promising vision of mitigating the cybersecurity community as vaccines can preventively overcome an impending AI-driven pandemic.

AI has become popular since AlphaGo won the human champion in 2016. The recent advancements in generative AI (GAI), such as OpenAI's ChatGPT and Google's Bard, have sparked the promise of revolutionizing many management processes. It appears that Large Language Models and GAI have demonstrated their potential and give high expectations of a revolutionary change in human intellectual jobs in many aspects and various domains. For example, it will provide positive value for human society regarding automating tasks that humans cannot perform well and economically. However, it will also give the adverse threats of deep fake and changing the robot-manipulated weapons of crimes and wars.

Given this context, this special issue pays attention to the Principles of Bright Internet, which aims to preventively mitigate the threat sources from the origins (Lee, 2015; Lee et al., 2020). For instance, AI and intelligent models can be used to build spam filtering models for inbound and outbound spam mail. This can be regarded as AI-enabled Bright Internet. Similarly, we can look at AI with the Principle of Bright Internet: Origin Responsibility, Deliverer Responsibility, Identifiable Anonymity, Privacy Protection, and Global Collaboration to prevent such risks (Lee 2015; Lee et al. 2018; Lee et al. 2020). Note that let us call this perspective of research Bright AI, but the themes of Bright AI do not intend to limit these principles and perspectives, although it can be a useful framework. From a comprehensive view, it can cover relevant high-level principles, such as fairness, transparency, accountability, social responsibility, and privacy, to ensure the responsible development and execution of AI systems (De Cremer 2020; Mikalef et al., 2022).

Objectives of the Special Issue

This special issue calls the various research perspectives and topics of Bright Internet and Bright AI that can maximize the benefit of AI controlling the risks that AI may cause as ethics of AI and humans. The Bright Origin can be studied from the perspective of individual, organizational, and national origins.

Recall the Bright Internet was proposed as an approach to preventive cybersecurity that can mitigate the threat sources from the origins. It was announced in 2015 as a grand vision of the Association of Information Systems (Lee 2015). Since then, the first Bright Internet Global Symposium has been held every December 2017 in Seoul as a workshop at the International Conference of Information Systems. It was held annually in Seoul, San Francisco, Munich, Austin, and Hyderabad. The history of the symposium is posted at www.brightintenet.org. The Bright Internet Regional Symposium was also held annually. Since 1998, the symposium has been held in cooperation with the International Conference on Electronic Commerce (htttp://www.icec.net). The theme of the forthcoming ICEC2024 in Seoul is "Empowering Bright Internet and Bright AI" as a continuing endeavor. This Special Issue will be organized in cooperation with the symposium of ICEC2024 that will be held on May 29, 2024, in Seoul, South Korea. Authors of high-quality symposium papers will be invited to submit their complete versions for fast-track review in the special issue.

In this special issue, we are interested in novel and thought-provoking contributions about Bright Internet and Bright AI across all levels and domains. We welcome a wide spectrum of research on related issues without any constraints in terms of theory, method, or context. Potential topics of interest for this special issue include the following areas in general but not limited to:

- AI and its impact on Bright Internet in general
- AI and ethical implications for Bright Internet
- AI governance for Bright Internet
- Fostering collaboration with AI for Bright Internet
- AI security challenges faced by individuals, organizations, communities, and/or countries and strategies to address them
- Privacy and data breaches relevant to the usage of AI systems for Bright Internet
- Novel preventive security mechanisms using AI for deterring cyber threat
- Transparency and explainability in AI systems for Bright Internet
- Bias and fairness considerations in AI systems for Bright Internet
- Trust and accountability mechanisms for AI systems for Bright Internet
- Building a trustful society based on the trustful email-based ID
- Organizational Bright Origin as Social Responsibility
- Effect of outbound spam mail management
- Balancing privacy with cybersecurity and self-defense right
- Framework of Origin Responsibility of AI
- Balancing the Identifiability and Anonymity of AI
- Applications of Bright Internet in e-Commerce Platform
- Applications of Bright Internet in Social Networks
- Regulation and market-driven models of Bright Internet deployment
- Stakeholders of Bright Internet and Business Models
- Generative AI: Framework of intellectual property right and ownership
- Addressing discrimination and the dark side of AI
- Social and ethical governance of virtual digital human for Bright Internet

- Digital responsibility of AI systems for Bright Internet
- Ethical AI in Bright Internet Ecosystem
- AI and digital inclusion

Special Issue Guest Editors

Daegon Cho (daegon.cho@kaist.ac.kr): Coordinating guest editor
College of Business, KAIST, Korea
Shan Liu (shanliu@xjtu.edu.cn)
Xi'an Jiaotong University, China
Dan J. Kim (dan.kim@unt.edu)
University of North Texas, USA

Special Issue Guest Advisory Editor

Jae Kyu Lee (jklee@kaist.ac.kr)
Xi'an Jiaotong University, China and College of Business, KAIST, Korea

Submission Timeline

Submission start date: January 1, 2024.
Submission deadline: July 31, 2024.
Target publication date: April 2025.

Submission Guidelines

All the submissions should follow the general author guidelines of *Decision Support Systems* available at https://www.elsevier.com/journals/decision-support-systems/0167-9236/guide-for-authors.
Kindly submit your paper to the Special Issue category (SI: Empowering Bright Internet and Bright AI) through the online submission system (https://www.editorialmanager.com/decsup/default2.aspx) of *Decision Support Systems*. Each paper submitted in the SI would undergo a minimum of 2-3 rounds of double-blind peer review. Each manuscript would have 2-3 reviewers who would attempt to provide constructive feedback.

To be invited for a fast-track ICEC 2024 symposium paper, submit a complete version of the paper to ICEC 2024 submission systems first. Selected manuscripts will be invited to submit via the submission system of *Decision Support Systems*. For information regarding the paper submission procedure for ICEC2024, please visit http://ICEC.net.

References

Benjamin, V., Valacich, J. S., & Chen, H. (2019). DICE-E: A framework for conducting Darknet identification, collection, evaluation with ethics. *MIS Quarterly*, *43*(1), 1–22.

Bera, D., Ogbanufe, O., & Kim, D. L. (2023). Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and intentions. *Decision Support Systems*, *171*, 113977.

Bose, I., & Leung, A. C. M. (2019). Adoption of identity theft countermeasures and its short- And long-term impact on firm value. *MIS Quarterly*, *43*(1), 313–327.

Chau, M., Li, T. M. H., Wong, P. W. C., Xu, J. J., Yip, P. S. F., & Chen, H. (2020). Finding people with emotional distress in online social media: A design combining machine learning and rule-BASED classification. *MIS Quarterly*, *44*(2), 933–956.

Danaher, B., Hersh, J., Smith, M. D., & Telang, R. (2020). The effect of piracy website blocking on consumer behavior. *MIS Quarterly*, *44*(2), 631–659.

Dennis, A. R., Moravec, P. L., & Kim, A. (2023). Search & Verify: Misinformation and source evaluations in Internet search results. *Decision Support Systems*, *171*, 113976.

De Cremer, D. (2020). What does building a fair AI really entail. *Harvard Business Review*.

Ju, J., Cho, D., Lee, J. K., & Ahn, J. H. (2021). Can It Clean Up Your Inbox? Evidence from South Korean Anti-spam Legislation. *Production and Operations Management*, *30*(8), 2636–2652.

Lee, J. K. (2015). Guest editorial: Research framework for AIS grand vision of the bright ICT initiative. *MIS quarterly*, *39*(2), iii-xii.

Lee, J. K. (2016). Reflections on ICT-enabled bright society research. *Information Systems Research*, *27*(1), 1–5.

Lee, J. K., Chang, Y., Kwon, H. Y., & Kim, B. (2020). Reconciliation of Privacy with Preventive Cybersecurity: The Bright Internet Approach. *Information Systems Frontiers*, *22*(1), 45–57.

Lee, J. K., Cho, D., & Lim, G. G. (2018). Design and validation of the bright internet. *Journal of the Association for Information Systems*, *19*(2), 63–85.

Lee, J. K., Park, J., Gregor, S., & Yoon, V. (2021). Axiomatic theories and improving the relevance of information systems research. *Information Systems Research*, *32*(1), 147–171.

Mikalef, P., Conboy, K., Lundström, J. E., & Popovič, A. (2022). Thinking responsibly about responsible AI and 'the dark side' of AI. *European Journal of Information Systems*, 31(3), 257-268.

Samtani, S., Chai, Y., & Chen, H. (2022). Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-Based Deep Structured Semantic Model. *MIS Quarterly*, *46*(2), 911–946.

Shin, Y. Y., Lee, J. K., & Kim, M. (2018). Preventing state-led cyberattacks using the bright internet and internet peace principles. *Journal of the Association for Information Systems*, *19*(3), 152–181.

Wei, X., Zhang, Z., Zhang, M., Chen, W., & Zeng, D. D. (2022). Combining Crowd and Machine Intelligence to Detect False News on Social Media. *MIS Quarterly*, *46*(2), 977–1008.

Xu, J., Chen, D., Chau, M., Li, L., & Zheng, H. (2022). Peer-to-Peer Loan Fraud Detection: Constructing Features from Transaction Data. *MIS Quarterly*, *45*(3), 1777–1792.