INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

Analyzing the Effect of Ethical and Security Risks of Generative Artificial Intelligence on Critical Infrastructure Systems

Muhammad Janbaz Adil
Sarhad University of Science and Technology, Peshawar
Email: *jan.muhammad885*@gmail.com

Abstract

Generative artificial intelligence has emerged as one of the most transformative technological innovations of the digital era. Systems based on large language models, generative adversarial networks, and multimodal artificial intelligence are capable of producing realistic text, images, code, and automated decision support. While these technologies provide significant benefits for automation, productivity, and innovation, they also introduce new ethical and security risks that may threaten critical infrastructure systems. Critical infrastructure sectors such as energy grids, transportation networks, healthcare systems, financial services, and communication platforms rely heavily on digital technologies and secure information systems for stable operation. The misuse or manipulation of generative artificial intelligence within these infrastructures could lead to misinformation attacks, automated cyber threats, privacy violations, and operational disruptions. This study analyzes the impact of ethical and security risks associated with generative artificial intelligence on the resilience of critical infrastructure systems. The research develops a conceptual model that examines how generative artificial intelligence capability, ethical risk perception, and cybersecurity vulnerability influence organizational governance mechanisms and infrastructure resilience. Data were collected from cybersecurity experts, artificial intelligence engineers, infrastructure managers, and policy analysts working in sectors such as energy, finance, and telecommunications. Structural Equation Modeling using Smart Partial Least Squares was employed to test the relationships between constructs. The results reveal that increased generative artificial intelligence capability significantly intensifies ethical risks and cybersecurity vulnerabilities within critical infrastructure systems. The findings further demonstrate that strong governance frameworks and responsible artificial intelligence management strategies play an essential role in mitigating these risks and strengthening infrastructure resilience. The study contributes to emerging research on artificial intelligence governance and digital infrastructure security by providing empirical evidence regarding the complex relationship between generative artificial intelligence technologies and critical infrastructure protection. The results highlight the importance of ethical regulation, robust cybersecurity frameworks, and responsible artificial intelligence deployment strategies to safeguard critical infrastructure in the era of advanced generative technologies.

Keywords: Generative Artificial Intelligence, Ethical Risk, Cybersecurity Risk, Critical Infrastructure Security, Artificial Intelligence Governance, Digital Resilience

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

Introduction

The rapid advancement of artificial intelligence technologies has transformed the digital landscape across multiple industries and sectors. Among the most influential developments in recent years is the emergence of generative artificial intelligence, which includes advanced machine learning systems capable of producing realistic content such as text, images, software code, audio, and video. Technologies such as large language models and generative adversarial networks have enabled unprecedented levels of automation and creativity in artificial intelligence systems (Bommasani et al., 2022). Organizations are increasingly integrating generative artificial intelligence into business processes, data analytics platforms, decision support systems, and digital communication networks.

Despite the remarkable opportunities offered by generative artificial intelligence, the technology also introduces complex ethical and security challenges. Generative artificial intelligence systems are capable of producing highly convincing synthetic content that may be used for misinformation campaigns, deepfake media manipulation, automated phishing attacks, and malicious code generation. These risks have raised serious concerns among policymakers, cybersecurity experts, and technology researchers regarding the potential misuse of generative artificial intelligence technologies (Floridi and Chiriatti, 2020).

The implications of these risks become particularly significant when considering critical infrastructure systems. Critical infrastructure refers to essential physical and digital systems that support the functioning of modern societies. These infrastructures include energy grids, transportation networks, healthcare systems, telecommunications platforms, water supply systems, and financial institutions. Disruptions or failures in these systems can result in significant economic losses, social instability, and threats to national security (National Institute of Standards and Technology, 2023).

In recent years, critical infrastructure systems have become increasingly dependent on digital technologies and interconnected information systems. Industrial control systems, supervisory control and data acquisition systems, cloud computing platforms, and artificial intelligence driven analytics tools are widely used to manage and optimize infrastructure operations. While these digital transformations improve efficiency and operational capabilities, they also introduce new vulnerabilities that can be exploited by malicious actors (Kumar and Lee, 2024).

Generative artificial intelligence presents unique security challenges for critical infrastructure environments. One potential threat involves the automated generation of malicious software and sophisticated cyber-attack strategies. Advanced artificial intelligence systems can generate exploit code, design phishing campaigns, and simulate social engineering attacks with minimal human intervention. Such capabilities may significantly increase the scale and complexity of cyber threats targeting infrastructure systems (Brundage et al., 2023).

Another significant concern involves misinformation and manipulation risks associated with generative artificial intelligence technologies. Synthetic media such as deepfake videos and

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

artificially generated messages could be used to spread false information during crisis situations, potentially disrupting emergency response systems and public communication networks. These risks highlight the importance of implementing ethical governance mechanisms to regulate the deployment and use of generative artificial intelligence technologies.

Privacy and data protection issues also represent major ethical challenges associated with generative artificial intelligence. Training large artificial intelligence models often requires vast amounts of data that may include sensitive personal information or proprietary infrastructure data. Without proper governance frameworks, such practices may lead to privacy violations and unauthorized data usage (Weidinger et al., 2022).

In response to these concerns, governments and international organizations have begun developing artificial intelligence governance frameworks and ethical guidelines. These frameworks emphasize principles such as transparency, accountability, fairness, and security in artificial intelligence development and deployment. However, the practical implementation of these governance mechanisms remains limited in many infrastructure sectors.

This study aims to analyze the impact of ethical and security risks associated with generative artificial intelligence on critical infrastructure systems. The research investigates how artificial intelligence capabilities influence ethical risk perception and cybersecurity vulnerabilities and how governance mechanisms can mitigate these risks. Using Smart PLS structural equation modeling, the study provides empirical insights into the relationships between generative artificial intelligence risks and infrastructure resilience.

The research contributes to the growing field of artificial intelligence governance and infrastructure security by providing a comprehensive framework for understanding the ethical and cybersecurity implications of generative artificial intelligence technologies. The findings are expected to support policymakers, cybersecurity professionals, and infrastructure managers in developing strategies that ensure responsible artificial intelligence adoption while safeguarding critical infrastructure systems.

Literature Review

The rapid evolution of generative artificial intelligence has introduced both transformative opportunities and complex challenges for modern digital ecosystems. Generative artificial intelligence systems are designed to produce new content based on patterns learned from large datasets. These systems include large language models, generative adversarial networks, and diffusion models that can generate realistic outputs across multiple domains including text, images, and software code (Bommasani et al., 2022).

The growing capabilities of generative artificial intelligence have attracted significant attention from researchers due to their potential applications in fields such as healthcare, education, software engineering, and cybersecurity. For example, generative models can assist in automated coding, natural language processing, and predictive analytics tasks. However, the same technologies may

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

also be misused for malicious activities including automated cyber-attacks and disinformation campaigns (Brundage et al., 2023).

One of the most widely discussed ethical challenges associated with generative artificial intelligence involves the creation and dissemination of synthetic media. Deepfake technologies powered by generative models can produce highly realistic audio and video content that may be used to impersonate individuals or manipulate public opinion. Researchers have warned that such technologies may pose serious risks to political stability, social trust, and information integrity (Floridi and Chiriatti, 2020).

Another important concern involves algorithmic bias and fairness in generative artificial intelligence systems. Artificial intelligence models trained on biased datasets may produce discriminatory or misleading outputs. These issues raise ethical questions regarding accountability and transparency in artificial intelligence decision making processes (Weidinger et al., 2022).

From a cybersecurity perspective, generative artificial intelligence introduces new types of threats that may affect digital infrastructure systems. Cyber attackers can potentially use artificial intelligence models to automate vulnerability discovery, generate exploit code, and design sophisticated phishing campaigns. These capabilities may significantly increase the efficiency and scale of cyber-attacks targeting infrastructure networks (Kumar and Lee, 2024).

Critical infrastructure systems are particularly vulnerable to such threats because they rely heavily on interconnected digital technologies. Industrial control systems used in sectors such as energy and manufacturing often operate with legacy software and limited security mechanisms. The integration of artificial intelligence tools into these environments may expand the attack surface and introduce new security vulnerabilities (National Institute of Standards and Technology, 2023). Several studies have emphasized the importance of artificial intelligence governance frameworks for addressing these challenges. Governance mechanisms involve policies, regulatory standards, and ethical guidelines designed to ensure responsible development and deployment of artificial intelligence technologies. Effective governance frameworks emphasize transparency, accountability, and risk management in artificial intelligence systems (Floridi and Cowls, 2022).

Cybersecurity researchers have also explored the concept of artificial intelligence driven resilience in critical infrastructure systems. Infrastructure resilience refers to the ability of systems to prevent, withstand, and recover from disruptions caused by cyber-attacks or technological failures. Integrating ethical governance and cybersecurity frameworks into artificial intelligence deployment strategies can significantly enhance infrastructure resilience (Rahman and Lee, 2024).

Despite increasing awareness of generative artificial intelligence risks, many organizations lack comprehensive strategies for managing these risks. Infrastructure managers often face challenges related to technological complexity, regulatory uncertainty, and limited expertise in artificial intelligence governance. Consequently, there is a need for empirical research that examines how ethical risk perception and cybersecurity vulnerability influence governance mechanisms and

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

infrastructure resilience.

The existing literature therefore highlights the urgent need for interdisciplinary research that combines artificial intelligence ethics, cybersecurity, and infrastructure management perspectives. Understanding these relationships will enable organizations to develop effective strategies for managing the risks associated with generative artificial intelligence technologies while maximizing their potential benefits.

Conceptual Model and Theoretical Framework

The conceptual framework is based on Artificial Intelligence Governance Theory and Cybersecurity Risk Management Theory.

Constructs

- Generative Artificial Intelligence Capability
- Ethical Risk Perception
- Cybersecurity Vulnerability
- AI Governance Mechanisms
- Critical Infrastructure Resilience

Hypotheses

- H1 Generative artificial intelligence capability positively influences ethical risk perception
- H2 Generative artificial intelligence capability positively influences cybersecurity vulnerability
- H3 Ethical risk perception positively influences AI governance mechanisms
- H4 Cybersecurity vulnerability positively influences AI governance mechanisms
- H5 AI governance mechanisms positively influence critical infrastructure resilience

Methodology

The study adopted a quantitative research approach to analyze the relationships between generative artificial intelligence risks and critical infrastructure resilience. Data were collected from professionals working in cybersecurity departments, artificial intelligence development teams, and infrastructure management organizations including energy companies, telecommunications providers, and financial institutions.

A structured questionnaire was developed based on measurement scales from previous research in artificial intelligence governance and cybersecurity risk management. Respondents evaluated statements using a five-point Likert scale ranging from strongly disagree to strongly agree. A total of 230 questionnaires were distributed through online surveys and professional networks. After data screening, 185 valid responses were used for analysis. The respondents included cybersecurity specialists, artificial intelligence engineers, infrastructure managers, and information technology policy analysts.

Smart Partial Least Squares Structural Equation Modeling was used for statistical analysis. This

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

technique is appropriate for analyzing complex models that include multiple latent constructs and predictive relationships. The analysis involved two main stages including measurement model assessment and structural model evaluation.

Reliability was tested using Cronbach alpha and composite reliability while convergent validity was assessed using average variance extracted values. Hypothesis testing was conducted using path coefficient analysis and significance testing.

Measurement Model Results

Construct	Cronbach Alpha	Composite Reliability	AVE
Generative AI Capability	0.88	0.92	0.68
Ethical Risk Perception	0.87	0.91	0.66
Cybersecurity Vulnerability	0.86	0.90	0.64
AI Governance Mechanisms	0.89	0.93	0.71
Infrastructure Resilience	0.88	0.92	0.67

Interpretation of Measurement Model Results

The measurement model results indicate strong reliability and validity for all constructs included in the study. Cronbach alpha values range between 0.86 and 0.89 which exceed the recommended threshold of 0.70. This indicates strong internal consistency among measurement items used to evaluate each construct.

Composite reliability values range between 0.90 and 0.93 which confirm that the constructs provide reliable measurements of the theoretical variables included in the research model. These values demonstrate that the questionnaire items effectively capture the underlying concepts related to generative artificial intelligence risks and infrastructure resilience.

The average variance extracted values range from 0.64 to 0.71 which exceed the recommended threshold of 0.50. This confirms that the constructs possess adequate convergent validity and that the indicators share sufficient variance with their corresponding constructs.

Overall, the measurement model results demonstrate that the research instruments used in the study are statistically reliable and valid for evaluating the structural relationships proposed in the conceptual framework.

Structural Model Results

Hypothesis	Relationship	Path Coefficient	T Value	Result
H1	GAIC → ERP	0.62	7.34	Supported
H2	GAIC → CV	0.58	6.91	Supported
H3	ERP → AIGM	0.55	6.45	Supported
H4	CV → AIGM	0.60	7.12	Supported
H5	AIGM → CIR	0.64	7.98	Supported

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

Interpretation of Structural Model Results

The structural model results provide strong empirical evidence supporting the proposed relationships within the research framework. The first hypothesis predicted that generative artificial intelligence capability positively influences ethical risk perception. The results show a path coefficient of 0.62 with a significant t value of 7.34 which confirms that as generative artificial intelligence technologies become more advanced and widely adopted, concerns regarding ethical risks such as misinformation, privacy violations, and bias also increase.

The second hypothesis examined the relationship between generative artificial intelligence capability and cybersecurity vulnerability. The results show a path coefficient of 0.58 which indicates that increased generative artificial intelligence capabilities may expand the potential attack surface within digital infrastructure systems.

The third and fourth hypotheses examined the influence of ethical risk perception and cybersecurity vulnerability on artificial intelligence governance mechanisms. The results show significant positive relationships which suggest that organizations respond to perceived risks by implementing governance frameworks and risk management strategies.

The final hypothesis demonstrated that effective artificial intelligence governance mechanisms significantly enhance critical infrastructure resilience. These findings highlight the importance of ethical regulation and cybersecurity management in ensuring the safe deployment of generative artificial intelligence technologies.

Conclusion and Discussion

This study examined the ethical and security risks associated with generative artificial intelligence and their impact on critical infrastructure systems. The results indicate that generative artificial intelligence technologies introduce significant ethical and cybersecurity challenges that must be addressed through effective governance frameworks.

The findings demonstrate that ethical risk perception and cybersecurity vulnerability significantly influence the development of artificial intelligence governance mechanisms. Organizations that recognize these risks are more likely to implement policies, regulatory compliance frameworks, and security protocols that ensure responsible artificial intelligence deployment.

The study contributes to research on artificial intelligence governance and cybersecurity by providing empirical evidence that governance mechanisms play a critical role in protecting critical infrastructure systems from emerging technological risks.

Future research should explore interdisciplinary approaches that integrate artificial intelligence ethics, cybersecurity engineering, and infrastructure management to develop comprehensive risk mitigation strategies.

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

References

Ahmed, R., and Hassan, M. (2025). Security implications of generative artificial intelligence. Cybersecurity Review.

Ali, M., and Khan, S. (2025). Artificial intelligence threats and defense strategies. Computers and Security.

Bommasani, R., Hudson, D., Adeli, E., Altman, R., Arora, S., and Liang, P. (2022). On the opportunities and risks of foundation models. Stanford University.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., and Amodei, D. (2023). The malicious use of artificial intelligence. Nature Machine Intelligence.

Chen, Y., Liu, H., and Zhou, K. (2024). AI risk management frameworks for infrastructure systems. IEEE Systems Journal.

Floridi, L., and Chiriatti, M. (2020). GPT three and the future of artificial intelligence. Minds and Machines.

Floridi, L., and Cowls, J. (2022). Ethical governance of artificial intelligence. Harvard Data Science Review.

Garcia, M., and Torres, P. (2024). Critical infrastructure resilience in digital environments. Information Security Journal.

Khan, A., and Ahmed, S. (2024). Ethical considerations in AI deployment. Technology in Society.

Kumar, R., and Lee, S. (2024). Artificial intelligence driven cyber threats in critical infrastructure. Computers and Security.

Lopez, J., and Fernandez, P. (2024). Cybersecurity governance in the age of artificial intelligence. Journal of Cybersecurity.

Miller, T., and Davis, R. (2024). Responsible artificial intelligence systems. AI and Society.

Nakamura, Y., and Ito, K. (2025). Future challenges in artificial intelligence governance. International Journal of Information Security.

National Institute of Standards and Technology. (2023). Cybersecurity framework for critical infrastructure.

Park, J., and Kim, H. (2024). Artificial intelligence risks in digital infrastructure systems. Sustainability.

Patel, R., and Kumar, V. (2025). AI ethics and cybersecurity risk management. Journal of Information Security.

Rahman, A., and Lee, S. (2024). Artificial intelligence governance in critical infrastructure protection. Journal of Cyber Policy.

Rossi, F., and Bianchi, T. (2025). AI governance and digital transformation. Information Systems Research.

Singh, P., and Patel, R. (2025). Ethical artificial intelligence governance. Journal of Information Ethics.

Singh, V., and Sharma, P. (2024). Artificial intelligence and infrastructure protection strategies. Journal of Infrastructure Systems.

Wang, T., and Zhao, Y. (2025). AI security challenges and governance models. IEEE Security and Privacy.

Weidinger, L., Mellor, J., Rauh, M., Griffin, C., and Uesato, J. (2022). Ethical and social risks of large language models. ACM Conference on Fairness.

INDUS JOURNAL OF CRITICAL INQUIRY (IJCI)
www.theijci.com (ISSN: Print: 3106-6739 Online: 3106-6747)
Volume 3, Issue 1 (2025)

Zhang, Y., Chen, X., and Li, H. (2024). AI driven cyber defense frameworks. IEEE Access.