A UNIFIED ESG-ALIGNED AND CYBER SECURITY–AWARE GREEN AI MATURITY MODEL FOR SUSTAINABLE ARTIFICIAL INTELLIGENCE IN ACADEMIA

[1]Devina Vinod, [2]Akhija Lakshmi R, [3]Lekshmi M
[1,2,3]Assistant Professor
[1,2,3]Computer Science & Engineering (Cyber Security),
[1,2,3]St. Joseph's College of Engineering & Technology, Palai, Kottayam, Kerala, India

Abstract: The rapid expansion of artificial intelligence (AI) and digital infrastructures has intensified concerns related to environmental sustainability, ethical governance, and cyber security. Existing global frameworks such as SDGs, ESG standards, and cyber security models address these concerns in isolation, resulting in fragmented governance practices. This review critically examines major international guidelines, standards, and studies, focusing on their treatment of sustainability, AI governance, and cyber security. The analysis highlights significant gaps in AI lifecycle coverage, energy efficiency metrics, and integrated risk management, particularly in the context of academic and institutional environments. The review establishes the need for a unified, AI-centric sustainability and cyber security framework to support responsible and resilient digital transformation.

Index Terms **-** Artificial Intelligence, Green AI, ESG, Cyber Security, Sustainability, Academic Institutions, Maturity Model, Governance, Energy Efficiency, Digital Infrastructure.

I.INTRODUCTION

The increasing deployment of Artificial Intelligence (AI) across education, research, and institutional governance has transformed academic ecosystems into highly data-driven and compute-intensive environments. While AI-enabled systems improve efficiency, decision-making, and learning outcomes, they also introduce significant challenges related to energy consumption, carbon emissions, and cyber security risks. Early global sustainability initiatives such as the United Nations Sustainable Development Goals (SDGs) and climate-focused disclosure frameworks established high-level environmental and social objectives, but they did not consider the operational impact of AI technologies. As a result, AI-driven infrastructures in academic institutions have expanded without adequate alignment to sustainability metrics or security-by-design principles.

Subsequent frameworks addressing ethical and trustworthy AI emphasized transparency, fairness, and accountability, yet largely overlooked the environmental footprint and security resilience of AI systems. In parallel, the emergence of Green AI redirected attention toward energy-efficient model training and reduced computational cost, but its scope remained limited to algorithmic optimization without integration into institutional governance or risk management structures. At the same time, well-established cyber security standards such as NIST and ISO/IEC 27001 provided comprehensive controls for protecting information assets, but treated sustainability and ESG factors as external concerns. Recent interdisciplinary studies attempted to link cyber risk with sustainability outcomes; however, they lack AI-specific maturity models and fail to address the unique operational realities of academic institutions. This fragmented body of work clearly indicates the absence of a unified framework that simultaneously addresses AI sustainability, ESG alignment, and cyber security governance, thereby motivating the need for integrated maturity-based approaches.

II. LITERATURE SURVEY

A number of global initiatives and frameworks have shaped sustainability and governance practices over the past decade. The United Nations Sustainable Development Goals (SDGs) established a global framework integrating environmental, social, and governance objectives, promoting sustainable development worldwide [1]. However, the SDGs are high-level and do not provide operational guidance for AI systems or cyber security in academic institutions. Similarly, the Task Force on Climate-related Financial Disclosures (TCFD) enhanced climate risk reporting and organizational transparency [2], yet it primarily addresses financial risks, excluding AI sustainability and security considerations. Studies on AI and automation analyzed socio-economic impacts and governance implications [3], while the European Commission's Trustworthy AI guidelines proposed ethical principles such as transparency, accountability, and fairness for responsible AI deployment [4]. Nevertheless, both approaches overlook energy efficiency, environmental impacts, and integrated cyber security mechanisms.

The concept of Green AI emerged to emphasize energy-efficient model development and reduced carbon footprint [5]. While it focuses on computational efficiency, it does not incorporate ESG alignment or cyber security considerations. High-level ESG reporting frameworks, such as the World Economic Forum's Stakeholder Capitalism Metrics [6] and the UN Principles for Responsible Investment (PRI) [10], support comparability, transparency, and long-term resilience, but are either not tailored for AI systems or focus on investor perspectives. The Science Based Targets initiative (SBTi) aligns emission reduction targets with climate science [7], but it does not explicitly include AI operational energy consumption or cyber security impacts. Industry-specific reporting standards, including SASB [11] and GRI [12], enable disclosure of financial material and sustainability impacts, yet they fail to consider AI lifecycle and cyber risk integration.

Cyber security governance frameworks address technical and operational risks but often neglect sustainability concerns. The NIST Cyber Security Framework [8] defines best practices for managing cyber risks, and ISO/IEC 27001 [14] formalizes information security management systems. However, neither incorporates ESG alignment or energy efficiency metrics. Some recent studies attempt to link cyber risks with sustainability and environmental impact in digital infrastructures [9], but they lack AI-specific maturity models. Platforms such as CDP [11, 13] facilitate large-scale environmental disclosure, and the IPCC reports [15] provide authoritative evidence on climate change and industrial emissions. Nevertheless, AI-specific sustainability metrics, operational energy considerations, and academic governance contexts remain largely unaddressed. Collectively, these studies highlight a critical gap for a unified ESG-aligned, cyber-secure Green AI framework tailored for academic institutions.

Recent research highlights the growing integration of AI with ESG and sustainability principles, underlining the need for frameworks that consider ethical, environmental, and governance dimensions in AI systems. A comprehensive responsible AI assessment framework explicitly integrating ESG and AI principles has been proposed, providing practical metrics for responsible AI governance and sustainability reporting across sectors [21]. Surveys on the synergy between AI and information security further reveal that securing AI systems requires ethical design principles that align cyber security with broader governance goals [22]. Ethical sustainability frameworks emphasize the dual role of AI as both a contributor to climate challenges and a tool for climate mitigation, reinforcing the need for balanced governance approaches in research and policy [23]. Work on AI-driven sustainable finance demonstrates how machine learning and computational tools can improve ESG metric accuracy and implementation, informing institutional ESG strategies [24]. Conceptual reviews on the governance, regulatory readiness, and accountability of AI tools in sustainable finance stress gaps in transparency, bias management, and regulatory frameworks that hinder responsible deployment [25]. Furthermore, systematic reviews on AI ethics and sustainability highlight the paradox of AI's potential to advance sustainable development while simultaneously posing ethical and environmental risks, calling for integrated interdisciplinary oversight [26]. Collectively, these studies underscore the need for a unified model that integrates sustainability, governance, and security concerns within AI deployment, particularly in institutional contexts such as academia.

Table 1: Summary of Key Sustainability, ESG, and Cyber Security Frameworks and Studies

Sl. No.	Author(s) and Year	Focus Area	Key Contribution	Limitations Identified
1	United Nations, 2015	Sustainable Development Goals	The SDGs established a global framework integrating environmental, social, and governance objectives to promote sustainable development worldwide.	The framework is high-level and does not provide operational guidance for AI systems or cyber security in academic institutions.
2	TCFD, 2017	Climate Risk Disclosure	The TCFD recommendations introduced structured disclosure of climate-related financial risks, enhancing organizational transparency and strategic planning.	The framework focuses on financial risks and excludes AI sustainability and cyber security considerations.
3	Manyika et al., 2017	AI and Automation	The study analyzed the socio-economic impact of AI and automation across sectors, highlighting governance and workforce implications.	Environmental sustainability and cyber security risks associated with AI systems were not addressed.
4	European Commission, 2019	Trustworthy AI	The guidelines proposed ethical principles such as transparency, accountability, and fairness for responsible AI deployment.	Energy efficiency, environmental impact, and cyber security integration were not explicitly considered.
5	Schwartz et al., 2020	Green AI	The authors introduced Green AI, emphasizing energy-efficient model development and reduced carbon footprint of AI systems.	The work focuses on algorithmic efficiency and lacks ESG alignment and cyber security integration.
6	World Economic Forum, 2020	ESG Metrics	The Stakeholder Capitalism Metrics provided standardized ESG reporting indicators to improve sustainability disclosure and comparability.	The framework does not address AI lifecycle management or cyber security risks.
7	Science Based Targets Initiative, 2020	Climate Targets	The initiative aligned corporate emission reduction targets with climate science and the Paris Agreement.	AI operational energy consumption and security impacts are not included.
8	NIST, 2020	Cyber Security Framework	The framework established best practices for managing cyber security risks across information systems.	Environmental and ESG dimensions are not incorporated.

9	Radanliev et al., 2020	Cyber Risk and Sustainability	The study linked cyber risks with sustainability and environmental impact in digital infrastructures.	The work does not propose a maturity model or AI-specific framework.
10	UN PRI, 2021	ESG and Responsible Investment	The principles promoted ESG integration into governance and investment decisions, improving long-term resilience.	The framework is investor-focused and not tailored for AI systems or academia.
11	SASB, 2021	Industry-Specific ESG Standards	The standards enabled disclosure of financially material ESG issues across industries.	Academic institutions and AI systems are not explicitly addressed.
12	GRI, 2021	Sustainability Reporting	The standards provided a comprehensive structure for reporting environmental and social impacts.	Cyber security and AI energy efficiency metrics are absent.
13	CDP, 2022	Environmental Disclosure	The platform facilitated large-scale disclosure of emissions, water security, and deforestation risks.	AI-specific sustainability and cyber incident impacts are not captured.
14	ISO/IEC 27001, 2022	Information Security Management	The standard defined systematic governance mechanisms for information security management.	Sustainability and ESG alignment are not considered.
15	IPCC, 2023	Climate Change Assessment	The assessment provided authoritative evidence on accelerating global warming and industrial emission sources.	The report does not address AI systems or institutional cyber security governance.
16	AI and Ethics: Ethical, technical, and security challenges in AI,2024	AI Governance, Cyber Security	Highlights ethical and security issues of AI in real-world systems, supporting cyber-aware frameworks	Does not address environmental sustainability or ESG-aligned AI lifecycle management.
17	AI and Ethics: ESG-aligned AI assessment methods,2025	ESG Integration, Responsible AI	Proposes ESG-integrated AI evaluation, relevant for sustainable AI maturity models	Lacks operational cyber security controls and institutional implementation guidance.
18	Discover Artificial Intelligence: AI contribution to UN SDGs, 2025	Green AI, Sustainability	Discusses AI's role in achieving SDGs; informs ESG alignment and Green AI implementation	Focuses on strategic alignment; omits AI energy metrics and cyber risk considerations.
19	Journal of Environmental Management: Cyber threats and ESG performance,2025	Cyber Security, ESG	Shows how cyber risks affect environmental and governance outcomes, justifying integrated frameworks	Does not propose AI-specific governance or maturity assessment models.
20	Sustainability (MDPI): AI in ESG-oriented	AI, ESG, Sustainability	Case studies on AI-driven ESG strategies, supporting institutional framework design	Limited focus on cyber security and lacks standardized evaluation indicators.

	sustainable strategies,2026			
21	Artificial Intelligence Review: AI in ESG and sustainable finance,2024	AI Governance, ESG Integration	Surveys trends linking AI with ESG and sustainable finance, guiding Green AI models	Primarily finance centric; academic institutions and AI system security are not covered.
22	Int. Journal of Computer Engineering and Technology: ESG data management & cloud,2024	Digital Sustainability, ESG Data	Focuses on ESG data management and cloud platforms, relevant for institutional AI governance	Does not integrate AI model sustainability or cyber security maturity assessment.
23	International Journal of Social Impact: AI governance & regulatory readiness,2025	Governance, Regulatory Readiness	Conceptual review on AI governance frameworks in sustainability contexts	Remains conceptual and lacks technical validation or AI lifecycle integration.
24	IET Information Security: Cyber risk management, 2024	Cyber Security, Risk Management	Provides robust security frameworks applicable to AI and institutional systems	Environmental sustainability and ESG performance indicators are excluded.
25	IEEE Technology & Society Magazine: Social, ethical, and policy implications of AI, 2024	Technology Policy, Governance	Addresses societal, ethical, and governance impacts of AI, supporting ESG-aligned models	Does not offer measurable frameworks or operational security controls.
26	AI & Society: AI interaction with social systems,2024	AI Governance, Social Impact	Focuses on societal and ethical AI implications, relevant for ESG and academic institution alignment	Environmental efficiency and cyber security integration are not addressed.

III.CONCLUSION

This review reveals a clear disconnect between sustainability frameworks, AI governance principles, and cyber security standards. While each body of work contributes valuable insights, none offer a holistic framework that integrates environmental impact, ethical AI, and cyber resilience across the AI lifecycle. The absence of AI-specific sustainability metrics, energy-aware security controls, and institution-focused governance models remains a critical limitation. Addressing these gaps is essential for ensuring responsible AI deployment in increasingly digital and data-intensive environments. Future research must focus on developing integrated, measurable, and scalable frameworks that align sustainability objectives with cyber security and AI governance requirements.

REFERENCES

[1] R. Schwartz, J. Dodge, N. A. Smith, and O. Etzioni, “Green AI,” Communications of the ACM, vol. 63, no. 12, pp. 54–63, Dec. 2020.

[2] I. Goodfellow, J. Pouget-Abadie, M. Mirza, et al., “Generative adversarial nets,” Advances in Neural Information Processing Systems, vol. 27, pp. 2672–2680, 2014.

[3] European Commission, “Ethics guidelines for trustworthy AI,” High-Level Expert Group on Artificial Intelligence, Brussels, Belgium, 2019.

[4] World Economic Forum, "Measuring stakeholder capitalism: Towards common metrics and consistent reporting of sustainable value creation," Geneva, Switzerland, 2020.

[5] United Nations, "Transforming our world: The 2030 agenda for sustainable development," UN General Assembly, New York, NY, USA, 2015.

[6] United Nations Principles for Responsible Investment, "A practical guide to ESG integration for equity investing," PRI Secretariat, London, U.K., 2021.

[7] Task Force on Climate-related Financial Disclosures, "Final report: Recommendations of the TCFD," Financial Stability Board, Basel, Switzerland, 2017.

[8] Sustainability Accounting Standards Board, "SASB standards overview," SASB Foundation, San Francisco, CA, USA, 2021.

[9] Science Based Targets Initiative, "Foundations for science-based net-zero target setting in the corporate sector," SBTi, London, U.K., 2020.

[10] Global Reporting Initiative, "GRI sustainability reporting standards," GRI Secretariat, Amsterdam, The Netherlands, 2021.

[11] CDP, "Global climate change report," CDP Worldwide, London, U.K., 2022.

[12] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity," NIST Special Publication 800-53 Rev. 5, Gaithersburg, MD, USA, 2020.

[13] ISO/IEC, "ISO/IEC 27001: Information security management systems — Requirements," International Organization for Standardization, Geneva, Switzerland, 2022.

[14] A. Rai, "Explainable AI: From black box to glass box," Journal of the Academy of Marketing Science, vol. 48, no. 1, pp. 137–141, 2020.

[15] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed., Pearson, Boston, MA, USA, 2021.

[16] Intergovernmental Panel on Climate Change, "AR6 synthesis report: Climate change 2023," IPCC, Geneva, Switzerland, 2023.

[17] M. Radanliev, D. De Roure, and R. Nicolescu, "Sustainability and cyber risk in the Internet of Things," Journal of Cleaner Production, vol. 251, pp. 119–134, Apr. 2020.

[18] J. Manyika, M. Chui, B. Brown, et al., "Harnessing automation for a future that works," McKinsey Global Institute, 2017.

[19] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, Gaithersburg, MD, USA, 2011.

[20] A. van der Aalst, "Data science in action," Process Mining Handbook, Springer, Berlin, Germany, pp. 3–23, 2022.

[21] S. U. Lee, H. Perera, Y. Liu, B. Xia, Q. Lu, L. Zhu, J. Cairns, and M. Nottage, "Integrating ESG and AI: a comprehensive responsible AI assessment framework," *AI and Ethics*, vol. 5, pp. 5121–5148, June 2025.

[22] E. Hashmi, M. M. Yamin, and S. Y. Yayilgan, "Securing tomorrow: a comprehensive survey on the synergy of artificial intelligence and information security," *AI Ethics*, vol. 5, pp. 1911–1929, July 2024.

[23] "AI and climate: an ethical sustainability framework for balancing risks and responsibilities," *AI & Society*, Sept. 2025.

[24] "AI-driven sustainable finance: computational tools, ESG metrics, and global implementation," *Future Business Journal*, vol. 11, Art. 209, Aug. 2025.

[25] M. Bhakat, "Governance, regulatory readiness, and accountability of AI tools in sustainable finance: a conceptual review," *International Journal of Social Impact*, Oct. 2025.

[26] R. Dhiman et al., "Artificial intelligence and sustainability — a review," *Analytics*, vol. 3, no. 1, pp. 140–164, Mar. 2024.