Innovations in Environmental Economics

www.iee.reapress.com

Innov. Environ. Econ. Vol. 1, No. 1 (2025) 81–95.

Paper Type: Original Article

From Protection to Progress: Linking Cybersecurity Strategies with Global Sustainability Goals

Kaosar Hossain*

Department of Management, International American University, The United States; mkhs795@gmail.com.

Citation:

Received: 15 April 2024 *Revised: 23 July 2024* *Accepted: 25 September 2024*	Hossain, K. (2025). From protection to progress: Linking cybersecurity strategies with global sustainability goals. *Innovations in Environmental Economics, 1* (1), 81-95.

Abstract

This study investigates the intersection between cybersecurity and sustainable development, emphasizing how robust digital security measures can accelerate progress toward the United Nations (UN) Sustainable Development Goals (SDGs). Using a Systematic Literature Review (SLR) of peer-reviewed studies, policy reports, and international frameworks published between 2010 and 2024, the paper synthesizes evidence on the role of cybersecurity in safeguarding critical infrastructure, enhancing institutional resilience, and protecting data systems vital for economic, social, and environmental sustainability. The findings highlight the transformative potential of emerging technologies—such as blockchain, Artificial Intelligence (AI), and Machine Learning (ML)—in strengthening cybersecurity while simultaneously advancing SDGs related to health, education, innovation, climate action, and governance. However, persistent challenges—including regulatory gaps, capacity constraints, and the global asymmetry in digital access—pose barriers to integrating cybersecurity into sustainability strategies. The paper recommends fostering international cooperation, expanding cybersecurity education, and developing inclusive governance frameworks to ensure digital resilience. Overall, the study underscores that embedding advanced cybersecurity practices into sustainable development pathways is essential for achieving a secure, equitable, and sustainable digital future.

Keywords: Cybersecurity, Sustainable development goals, Digital infrastructure, Blockchain, Artificial intelligence.

1 | Introduction

The 2030 Agenda for Sustainable Development (SD), established by the United Nations (UN), set out 17 Sustainable Development Goals (SDGs) as a universal call to action to end poverty, protect the planet, and promote peace and prosperity. These goals highlight the interconnectedness of economic growth, social inclusion, and environmental protection, while emphasizing the crucial role of technological innovation in

Corresponding Author: mkhs795@gmail.com

https://doi.org/10.48313/iee.vi.43

advancing global sustainability. In recent years, the rapid digitalization of societies has reshaped the pathways toward achieving the SDGs by expanding access to education, healthcare, financial inclusion, and smart urban development [1], [2]. However, the growing reliance on digital networks has also exposed vulnerabilities that threaten the integrity of sustainable development efforts. Cybersecurity has therefore emerged as a critical component of modern development, ensuring the protection of digital infrastructure, key services, and sensitive data that underpin economic and social systems [3], [4]. Without robust cybersecurity measures, the continuity and reliability of digital technologies—essential for sectors such as healthcare, financial markets, education, and climate monitoring—remain at significant risk of disruption. The potential of emerging technologies to support both digital security and sustainability has gained increasing scholarly attention. For instance, blockchain-based systems have been proposed to enhance transparency and accountability in governance, contributing directly to SDG 16 on peace, justice, and strong institutions [5], [6]. Similarly, innovations in Artificial Intelligence (AI) and Machine Learning (ML) are recognized as transformative tools in strengthening cybersecurity, while also enabling efficient progress toward multiple SDGs [7], [8]. These technological synergies underscore that cybersecurity is no longer a purely technical issue but a foundational pillar for building resilient, inclusive, and sustainable societies.

Despite the recognized importance of digital transformation in advancing sustainable development, the lack of robust cybersecurity frameworks poses a serious threat to achieving the SDGs. Increasing cyberattacks, data breaches, and weak governance mechanisms undermine trust in digital platforms and disrupt essential services, ranging from healthcare to financial systems [9], [10]. Such vulnerabilities not only cause economic losses but also hinder social inclusion, education, and environmental monitoring efforts that are central to the global sustainability agenda [11], [12].

Moreover, the existing literature on SDGs often underemphasizes the role of cybersecurity, treating it as a peripheral issue rather than a central enabler of sustainable development. While research highlights the potential of digital technologies to accelerate progress, limited attention is paid to the risks associated with cyber threats and the mechanisms required to safeguard digital infrastructures [13], [14]. This omission creates a significant gap in understanding how to integrate cybersecurity measures into sustainability frameworks. Emerging technologies provide opportunities to enhance resilience, yet they also introduce new challenges. For example, blockchain and AI can improve transparency, accountability, and threat detection, but their deployment is often constrained by issues of scalability, regulatory gaps, and uneven digital access [15], [16]. Without a systematic approach to integrating cybersecurity into sustainability agendas, digital risks will continue to jeopardize the achievement of multiple SDGs, particularly those related to economic growth (SDG 8), innovation and infrastructure (SDG 9), and sustainable cities and communities (SDG 11).

Positioning cybersecurity as a central pillar of sustainable development is essential for ensuring the continuity and resilience of digital systems that drive progress toward the SDGs. As societies transition into increasingly data-driven economies, the security of digital infrastructure becomes a prerequisite for inclusive growth, equitable access to services, and long-term environmental sustainability [4], [17]. Cybersecurity safeguards not only protect critical sectors such as healthcare, education, and financial systems, but also enable the effective functioning of governance and democratic institutions by preventing fraud, corruption, and cyber-enabled crimes [18], [19]. Furthermore, recent studies highlight that cybersecurity is closely linked to the realization of broader sustainability outcomes. For example, robust cybersecurity measures enhance trust in e-learning platforms, directly supporting SDG 4 on quality education [20], [21].

Similarly, protecting digital fundraising schemes and financial inclusion initiatives contributes to SDG 8 on economic growth and SDG 10 on reducing inequalities [22]. In addition, securing environmental data through advanced cybersecurity frameworks is vital for climate action and biodiversity conservation, directly addressing SDGs 13, 14, and 15 [23], [24]. The transformative role of emerging technologies further underscores the significance of this research. AI and ML enhance cybersecurity through predictive threat detection and automated response systems, while blockchain ensures transparency and accountability in governance and commerce [25]. These innovations demonstrate that cybersecurity is not merely a technical

safeguard but an enabling mechanism for sustainable economic, social, and environmental progress. Against this backdrop, this study is both timely and novel, as it systematically investigates how cybersecurity measures intersect with sustainability agendas. By synthesizing existing evidence and identifying challenges, opportunities, and policy pathways, this research contributes to bridging a critical gap in the literature and offers strategic insights for policymakers, practitioners, and researchers engaged in shaping a secure and sustainable digital future.

The primary aim of this study is to investigate the critical intersection between cybersecurity and sustainable development, emphasizing how robust digital security measures can accelerate progress toward the SDGs. Specifically, the research examines the role of cybersecurity in safeguarding digital infrastructures essential for healthcare, education, financial inclusion, and climate action. It also explores emerging technologies such as AI, ML, blockchain, and green cybersecurity as transformative tools for strengthening resilience and transparency in digital systems. In addition, the study evaluates key barriers—including governance deficits, regulatory gaps, and uneven digital access—that hinder the effective integration of cybersecurity into sustainability frameworks. Finally, the paper proposes strategic policy recommendations aimed at promoting international cooperation, advancing cybersecurity education, and fostering inclusive governance structures to ensure a secure and sustainable digital future.

The remainder of this paper is organized as follows. Section 2 outlines the methodology, including data sources, search strategies, and selection criteria applied in the systematic review. Section 3 presents the literature review, highlighting the role of cybersecurity in advancing SDGs, the contribution of emerging technologies, and sector-specific perspectives. Section 4 provides an in-depth discussion and analysis, including case studies, identification of challenges, and strategic recommendations. Section 5 explores future directions by examining innovative approaches, global cooperation frameworks, and technological pathways for enhancing cybersecurity in sustainable development. Finally, Section 6 concludes with key insights and policy implications, emphasizing the importance of integrating cybersecurity as a foundational element for achieving the SDGs.

2 | Literature Review

2.1 | Understanding Cybersecurity within the Framework of Sustainable Development Goals

Cybersecurity has become an indispensable component of the global effort to achieve the SDGs. As digitalization accelerates, critical infrastructure, communication networks, and data systems form the backbone of economic, social, and environmental progress. Protecting these systems from cyber threats is therefore essential for advancing inclusive growth, fostering innovation, and ensuring resilient communities [3]. Within the SDG framework, cybersecurity plays a cross-cutting role. It underpins SDG 4 (quality education) by safeguarding digital learning platforms, SDG 8 (decent work and economic growth) by securing financial systems, SDG 9 (industry, innovation, and infrastructure) by protecting digital infrastructure, and SDG 11 (sustainable cities and communities) by ensuring resilience in urban systems. In addition, it contributes to SDG 16 (peace, justice, and strong institutions) through the prevention of fraud, corruption, and cyber-enabled crime [26–28]. Scholars emphasize that effective cybersecurity requires comprehensive national strategies tailored to specific contexts.

Raihan et al. [29] argue that developing countries in particular must design adaptive strategies that integrate governance, public–private partnerships, and compliance mechanisms to secure digital infrastructures. Similarly, Melaku [30] stresses the need for dynamic governance frameworks that address rapidly evolving cyber threats while ensuring the ethical and responsible use of technology. Sector-specific approaches further highlight the importance of cybersecurity in sustainable development. For example, in the construction industry, a tailored cybersecurity framework ensures the protection of information, materials, and systems,

reinforcing the resilience of the built environment [31]. Such examples illustrate that cybersecurity is not merely a technical safeguard but a strategic enabler across sectors critical to sustainable development.

2.2 | The Role of Cybersecurity in Promoting Sustainable Economic Growth

Cybersecurity is fundamental to building the trust and stability required for sustainable economic growth. Modern economies increasingly depend on digital infrastructures to facilitate trade, financial transactions, and service delivery, making them vulnerable to cyber threats. Safeguarding these systems ensures the reliability of economic activities and protects them from disruptions that can undermine development outcomes [18], [32]. Secure digital platforms also enable innovative financing mechanisms that support community-level development. For instance, digital fundraising models such as zakat, sukuk, and waqf can significantly contribute to social welfare and economic growth when protected against cyber risks [14]. Cybersecurity in this context is not only about defense but also about enabling digital finance to serve as a reliable driver of sustainable development [33], [34]. Empirical evidence further demonstrates the positive correlation between pursuing SDGs and fostering economic growth. In Morocco, for example, initiatives toward financial inclusion and institutional quality have promoted economic resilience, with cybersecurity playing a central role in ensuring the stability and trustworthiness of financial systems [35]. This illustrates how robust digital security measures protect financial stability and institutional credibility, both of which are critical for sustainable economic performance.

2.3 | Cybersecurity's Impact on Sustainable Industrialization and Innovation

Sustainable industrialization and innovation, central to SDG 9, depend heavily on the security and resilience of digital infrastructures. Cybersecurity ensures the protection of critical industrial systems, Intellectual Property Rights (IPR), and technological innovations that drive long-term industrial growth. Without adequate protection, cyber threats can disrupt production networks, compromise sensitive data, and weaken innovation ecosystems, undermining progress toward sustainability [3]. Intellectual property is particularly vulnerable in the digital era.

Denoncourt [36] highlights how corporate longevity and social responsibility are closely tied to the safeguarding of IPR assets, which not only foster innovation but also ensure sustainable business practices. Cybersecurity thus serves as both a defensive mechanism and an enabler of transparent, responsible, and innovation-driven industrial development. The Fourth Industrial Revolution (4IR) further intensifies the need for robust cybersecurity. Advanced technologies such as autonomous robots, smart sensors, and data-driven systems can significantly enhance sustainable industrialization but are simultaneously exposed to cyber vulnerabilities. Studies reveal that comprehensive cybersecurity strategies are required to protect these innovations and allow them to contribute effectively to inclusive and sustainable industrialization [37]. In this regard, cybersecurity acts as a backbone of modern industrial ecosystems, safeguarding intellectual property, protecting critical infrastructures, and enabling the safe adoption of advanced technologies. By reinforcing resilience and trust in innovation processes, cybersecurity directly supports sustainable industrialization, helping societies achieve long-term growth aligned with SDG 9.

3.4 | The Importance of Cybersecurity in Ensuring Sustainable Cities and Communities

Urban sustainability, reflected in SDG 11, increasingly relies on digital technologies that support governance, infrastructure, and service delivery. As cities adopt smart systems for transport, housing, waste management, and public safety, ensuring cybersecurity becomes essential to protect against disruptions that could threaten urban resilience. Cybersecurity thus acts as a safeguard for inclusive, safe, and sustainable urban development [38], [39]. Case studies highlight that weak urban infrastructure, such as precarious housing in Algeria, demonstrates the importance of integrating sustainable planning with secure digital systems. Bouteche and Bougdah [40] argue that cybersecurity-enabled technologies can strengthen urban planning, allowing for better monitoring, risk assessment, and policy implementation. Similarly, the use of remote sensing technologies in city planning and environmental monitoring requires strong cybersecurity measures to protect

data integrity and ensure reliable decision-making [41]. As smart cities expand, the threat of cyberattacks on critical infrastructure grows, posing risks to energy grids, transportation systems, and emergency services. Cybersecurity, therefore, plays a dual role: Protecting urban systems from immediate threats while enabling the long-term resilience of sustainable cities and communities. By embedding digital resilience into urban planning, cybersecurity becomes a cornerstone of sustainable urban development and a critical driver for achieving SDG 11.

3.5 | Cybersecurity Strategies for Climate Action: Protecting Environmental Data

Climate action and environmental sustainability, central to SDGs 13, 14, and 15, depend on the accuracy and security of environmental data. Digital systems are increasingly used to monitor climate change, biodiversity, and pollution levels, but these systems are highly vulnerable to cyber threats. Protecting environmental databases is therefore essential to ensure reliable decision-making and effective climate policies [42]. In archival and knowledge management, cybersecurity plays a key role in preserving climate-related records and ensuring their accessibility. Robinson [23] emphasizes that professional ethics and digital security are vital in protecting environmental archives, which form the foundation for long-term climate action strategies. Similarly, in the financial sector, sustainable banking initiatives that integrate environmental risk assessments require secure data systems to avoid manipulation or misuse.

Niedziółka [43] demonstrates how cybersecurity safeguards financial stability while supporting environmental protection goals. By integrating cybersecurity strategies into climate action frameworks, governments and organizations can prevent data breaches, strengthen environmental monitoring, and secure financing mechanisms that support sustainability. Cybersecurity thus not only protects sensitive environmental information but also acts as a catalyst for achieving climate resilience and advancing environmental sustainability.

3.6 | Emerging Trends in Cybersecurity for Sustainable Development

The evolving landscape of digital threats has accelerated the development of new cybersecurity trends that directly support sustainable development. Traditional defenses such as firewalls are no longer sufficient; instead, modern approaches incorporate cloud security, mobile protection, advanced encryption, and AI [44–47]. These innovations ensure that digital infrastructures remain secure while enabling broader progress toward the SDGs. AI and ML have emerged as transformative tools, enhancing early threat detection, predictive analytics, and automated responses to cyberattacks.

Salih et al. [7] highlight their effectiveness in extracting complex patterns from large datasets, thereby strengthening the resilience of digital systems essential for sustainability. Similarly, blockchain technologies are increasingly applied to secure transactions, enhance transparency, and protect digital platforms, enabling more reliable governance and economic activities [48]. Another significant trend is the rise of "green cybersecurity," which focuses on protecting environmental technologies and inter-organizational networks, especially in the Environmental Goods and Services Sector.

Sulich et al. [49] emphasize that integrating cybersecurity with environmental management helps safeguard data systems that are vital for addressing climate change and biodiversity loss. Overall, these emerging trends show that cybersecurity is not static but adaptive, continuously aligning with the demands of sustainable development. By embracing advanced technologies and integrating them into sustainability strategies, societies can build secure, innovative, and resilient digital ecosystems that directly support the achievement of the SDGs.

3 | Methodology

3.1 | Research Design

This study adopts a Systematic Literature Review (SLR) design, complemented by content analysis, to examine the intersection of cybersecurity and sustainable development. A systematic review was considered the most suitable approach because it allows for a comprehensive and unbiased synthesis of existing scholarly and policy-oriented knowledge. Unlike narrative reviews, which may be selective, the SLR process ensures transparency, replicability, and rigor by following a structured methodology that clearly defines data sources, search strategies, and selection procedures. The purpose of using an SLR in this context is twofold. First, it enables the identification of how cybersecurity contributes to the advancement of the SDGs, including its role in safeguarding digital infrastructures, enhancing institutional trust, and supporting inclusive innovation. Second, it highlights the challenges and opportunities that emerge from the integration of cybersecurity into sustainability frameworks, particularly in light of rapid digitalization and evolving technological trends. In addition to systematically reviewing the literature, content analysis was applied to classify and interpret recurring themes. This involved coding the selected publications into thematic categories such as the role of cybersecurity in achieving specific SDGs, emerging technologies (e.g., AI, blockchain, ML), sector-specific applications (e.g., healthcare, education, financial systems), and policy recommendations. This dual approach ensured that the analysis not only synthesized existing knowledge but also offered insights into patterns, gaps, and future research needs.

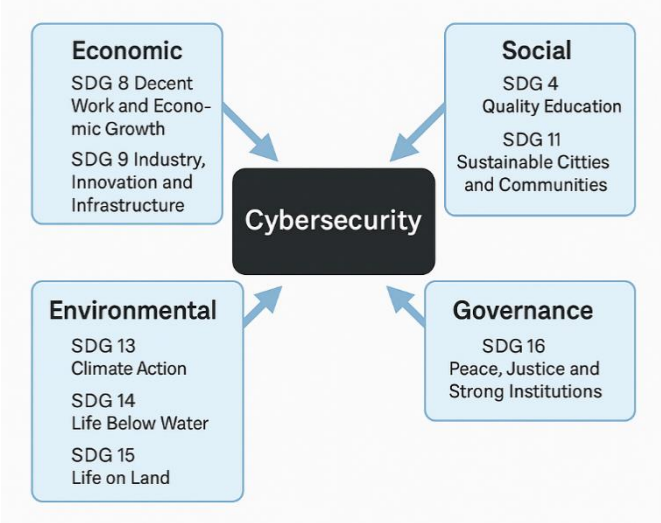

Fig. 1. Cybersecurity and SDGs.

3.2 | Data Sources

To ensure comprehensive coverage of relevant scholarship, this study drew on a wide range of academic and institutional sources. The primary materials included peer-reviewed journal articles, conference proceedings, and high-quality reports produced by reputable international organizations. Such sources were selected because they provide validated, credible, and policy-relevant insights into the intersection of cybersecurity and sustainable development. The academic databases consulted were IEEE Xplore, ScienceDirect, JSTOR, and Web of Science. These platforms were chosen because they contain an extensive collection of high-impact publications in the fields of computer science, information systems, sustainability studies, and interdisciplinary research. IEEE Xplore was particularly useful for accessing technical studies on cybersecurity frameworks and emerging digital technologies, while ScienceDirect and JSTOR provided access to sustainability-oriented articles linking digital transformation with the SDGs. Web of Science, with its broad

indexing of multidisciplinary journals, was instrumental in capturing both technical and policy-focused perspectives.

In addition to scholarly databases, reports and working papers were retrieved from international organizations such as the UN, the World Bank, and the International Telecommunication Union (ITU). These institutions are at the forefront of shaping global policy and practice in areas directly related to digitalization, governance, and sustainable development. Their reports often provide authoritative discussions of global trends, challenges, and best practices, making them essential for situating academic findings within broader policy debates. The integration of both scholarly and institutional sources ensured that the dataset reflected not only theoretical and empirical evidence but also practical insights and policy considerations. This diversity of sources strengthened the reliability of the review. It supported the aim of capturing the multifaceted role of cybersecurity in advancing sustainable development across economic, social, and environmental dimensions.

3.3 | Search Strategy

A carefully designed search strategy was employed to ensure that the literature review captured the most relevant and high-quality studies on the relationship between cybersecurity and sustainable development. The strategy combined keywords, Boolean operators, and filters to systematically locate publications that directly aligned with the research objectives. The initial set of keywords included "cybersecurity," "sustainable development," "SDGs," "digital infrastructure protection," "emerging technologies in cybersecurity," and "cybersecurity for sustainability." These terms were selected based on preliminary scoping of the literature and refined iteratively during the search process to maximize coverage. Boolean operators (e.g., "AND," "OR") were applied to connect terms and broaden or narrow the search.

For example, combinations such as "cybersecurity AND sustainable development" or "cybersecurity AND SDGs AND blockchain" helped identify studies that explicitly examined the intersection of digital security and sustainability. To maintain decency and relevance, the search was restricted to literature published between January 2010 and December 2024, a period during which the global digital transformation has significantly accelerated and the SDG framework has been widely adopted. Only publications in the English language were considered to ensure consistency in interpretation and accessibility.

The search was conducted across multiple databases, including IEEE Xplore, ScienceDirect, JSTOR, and Web of Science. In addition, targeted searches were performed on the websites of international organizations such as the UN, World Bank, and ITU to capture reports and policy documents. Reference lists of key articles were also examined through backward and forward citation tracking to identify additional relevant studies. This systematic and multi-layered search strategy ensured a comprehensive and representative dataset. By combining technical, interdisciplinary, and policy-oriented sources, the strategy provided a robust foundation for analyzing how cybersecurity measures contribute to the achievement of the SDGs.

3.4 | Inclusion and Exclusion Criteria

To ensure the quality and relevance of the literature reviewed, this study applied carefully defined inclusion and exclusion criteria. The inclusion criteria covered peer-reviewed journal articles, conference proceedings, and authoritative reports from organizations such as the UN, World Bank, and ITU that offered empirical evidence, conceptual insights, or policy recommendations on the nexus between cybersecurity and sustainable development. Only studies that explicitly addressed cybersecurity within the framework of the SDGs, or linked digital security to specific goals such as education, economic growth, innovation, urban resilience, and climate action, were considered. To capture the most relevant developments, the timeframe was restricted to publications between 2010 and 2024, reflecting the period in which digitalization has become central to sustainable development discourses.

Furthermore, only English-language publications were included to maintain consistency and avoid misinterpretation. On the other hand, exclusion criteria filtered out non-peer-reviewed materials such as blogs, editorials, or opinion pieces, as well as studies that focused exclusively on cybersecurity without

reference to sustainability, or on sustainability without a discussion of digital security. Duplicated studies were removed to avoid redundancy, while works with insufficient methodological detail or vague connections between cybersecurity and sustainability were also excluded. This systematic application of inclusion and exclusion criteria allowed the review to focus on a high-quality and thematically relevant body of literature, thereby ensuring that the findings reflect both the academic rigor and the policy significance of cybersecurity in advancing sustainable development.

3.5 | Selection Process

The selection of studies followed a systematic and transparent process to ensure the reliability and credibility of the review. First, an initial pool of publications was identified through database searches using predefined keywords and Boolean combinations. Titles and abstracts of these records were screened against the inclusion and exclusion criteria to remove clearly irrelevant or low-quality materials. This initial screening eliminated studies that did not explicitly address the intersection of cybersecurity and sustainable development or those that lacked methodological rigor. The second phase involved a full-text review of the remaining studies to determine their suitability for detailed analysis. During this stage, particular attention was given to whether the publication provided meaningful insights into the role of cybersecurity in achieving SDGs, discussed emerging technological trends such as AI, blockchain, or green cybersecurity, or highlighted sector-specific applications in areas like healthcare, education, finance, or climate action. Studies offering substantive discussion of barriers, opportunities, or policy recommendations were prioritized to strengthen the depth of the analysis.

In addition to database searches, reference lists of key articles were examined through backward and forward citation tracking to identify further relevant works that may not have appeared in the initial search. This iterative process ensured comprehensive coverage of the literature while avoiding duplication. By combining database screening, full-text assessment, and citation tracking, the selection process produced a curated dataset of high-quality publications that provided a robust foundation for synthesizing evidence and identifying gaps in the existing body of knowledge.

3.6 | Data Analysis

The final stage of the methodology involved a systematic analysis of the selected literature using a thematic content analysis approach. Each publication was carefully reviewed and coded to extract relevant information on how cybersecurity contributes to, or interacts with, the SDGs. The coding process was guided by predefined categories such as the role of cybersecurity in supporting specific SDGs, the adoption of emerging technologies like AI, blockchain, and green cybersecurity, sector-specific applications in areas including healthcare, AI education, finance, and environmental protection, as well as challenges, barriers, and policy responses. Through this structured process, recurring patterns and cross-cutting themes were identified, which allowed for a clearer understanding of the ways in which cybersecurity both enables and constrains progress toward sustainability.

At the same time, gaps and inconsistencies in the existing literature were highlighted, providing a basis for outlining areas in need of further research. Quantitative measures, such as the frequency of certain themes and qualitative insights derived from contextual interpretation, were integrated to ensure a balanced and comprehensive analysis. Furthermore, the synthesis process placed particular emphasis on aligning findings with broader global sustainability discourses and policy frameworks, thereby ensuring both academic and practical relevance. By combining systematic coding with interpretive synthesis, the analysis generated a nuanced understanding of the intersection between cybersecurity and sustainable development, laying the foundation for the subsequent discussion of case studies, challenges, and strategic recommendations presented in the later sections of the paper.

4 | Discussion and Analysis

4.1 | Analyzing the Impact of Cybersecurity Measures on Achieving Sustainable Development Goals

Cybersecurity has become a foundational enabler of the SDGs, given that digital infrastructures now underpin economic growth, social inclusion, and environmental sustainability. Secure digital systems contribute directly to SDG 8 (decent work and economic growth) by protecting financial platforms, enabling secure e-commerce, and fostering trust in digital fundraising mechanisms such as zakat, sukuk, and waqf, which can expand community welfare when safeguarded against cyber threats [22]. In the context of SDG 9 (industry, innovation, and infrastructure), cybersecurity plays a crucial role in protecting critical infrastructures, IPR, and innovative technologies that drive industrial development and competitiveness [47]. Similarly, robust cybersecurity is central to SDG 11 (sustainable cities and communities) as it ensures the resilience of smart city systems—such as transportation, energy grids, and environmental monitoring platforms—against potential cyberattacks [40], [41]. The importance of cybersecurity also extends to governance and institutional frameworks. By preventing fraud, corruption, and cyber-enabled crime, it strengthens SDG 16 (peace, justice, and strong institutions), fostering public trust in governance processes [50].

Additionally, the protection of digital education platforms supports SDG 4 (quality education) by safeguarding access to remote learning and knowledge-sharing systems [20]. Cybersecurity further contributes to environmental sustainability goals—particularly SDGs 13, 14, and 15—by ensuring the integrity of environmental databases and climate monitoring systems that inform global responses to climate change [23].

4.2 | Case Studies and Practical Insights

Examining practical experiences across different regions and sectors illustrates how cybersecurity directly supports sustainable development outcomes. In the financial sector, Morocco provides a useful case where institutional quality and financial inclusion have been strengthened through secure digital platforms. Ziky and El-Abdellaoui [51] demonstrate that the promotion of inclusive finance initiatives, supported by effective cybersecurity, not only enhances economic resilience but also contributes to broader sustainability goals. Similarly, digital fundraising mechanisms such as zakat and waqf have gained prominence as tools for financing social welfare projects, yet their success depends heavily on cybersecurity measures that prevent fraud, protect donor trust, and ensure transparency [22]. Urban sustainability also benefits from secure digital infrastructures. In Algeria, studies on precarious housing and weak urban systems highlight the importance of integrating cybersecurity into sustainable urban planning.

Bouteche and Bougdah [40] argue that smart city initiatives must embed digital resilience into their governance structures to ensure long-term inclusivity and safety. Remote sensing technologies, increasingly used in environmental monitoring and city management, also require robust cybersecurity to maintain the integrity of data and support informed decision-making [52]. From an environmental perspective, securing digital archives and climate databases is critical for long-term climate action. Robinson [42] emphasizes that without adequate cybersecurity, the reliability of environmental data is at risk, undermining global efforts to address climate change. Moreover, the integration of sustainable banking practices into environmental governance demonstrates how financial institutions can promote sustainability when supported by strong digital safeguards [43], [53].

4.3 | Challenges and Barriers to Integrating Cybersecurity with Sustainability

While cybersecurity has the potential to accelerate progress toward the SDGs, several challenges hinder its effective integration into sustainability frameworks. One of the most critical barriers is the regulatory and governance gap. Many countries, particularly in the Global South, lack comprehensive national cybersecurity strategies or the institutional capacity to implement existing policies. As Ridwan et al. [54] argue, without well-defined governance frameworks and compliance mechanisms, digital infrastructures remain exposed to

significant vulnerabilities. Similarly, Melaku [30] notes that governance systems must evolve dynamically to respond to rapidly changing cyber threats, yet many governments struggle to adapt their institutional structures to the pace of technological advancement. Another challenge lies in resource and capacity constraints. Building robust cybersecurity systems requires significant financial investments, skilled human capital, and advanced technological infrastructure.

However, developing countries often face competing development priorities and limited budgets, which reduce their ability to invest adequately in cybersecurity. This imbalance creates a digital divide in global cyber readiness, leaving vulnerable populations disproportionately exposed to risks. In addition, unequal digital access poses a barrier to inclusive and sustainable cybersecurity strategies. Populations without reliable internet access or digital literacy are often excluded from secure platforms, deepening existing inequalities in education, finance, and governance. Emerging technologies such as AI and blockchain, while promising, also introduce new risks related to scalability, ethical considerations, and regulatory uncertainty [55].

4.4 | Strategic Recommendations for Policymakers and Institutions

To overcome existing barriers and harness the full potential of cybersecurity in advancing the SDGs, a set of strategic recommendations is essential for policymakers and institutions. First, there is a need for comprehensive national cybersecurity frameworks that integrate sustainability objectives. Raihan et al. [46] highlight that developing countries should design adaptive strategies that not only safeguard digital infrastructure but also align with broader governance and development priorities. These frameworks should be supported by regulatory mechanisms that ensure compliance while remaining flexible to address evolving technological threats [46]. Second, policymakers must invest in capacity building and education. Expanding training programs, digital literacy campaigns, and higher education curricula in cybersecurity will help close the human capital gap.

Al-Sherideh et al. [20] emphasize that cybersecurity education not only enhances resilience but also ensures continuity in areas such as digital learning, directly contributing to SDG 4 on quality education. In addition, fostering a culture of digital ethics and professional responsibility can strengthen institutional trust. Third, international cooperation and multistakeholder partnerships are crucial. Cyber threats are global in nature, and effective responses require cross-border collaboration between governments, private firms, and civil society organizations. Initiatives such as secure digital finance systems or climate monitoring platforms can benefit from shared resources, technical expertise, and standardized practices [56].

Finally, institutions should leverage emerging technologies responsibly. AI and blockchain can significantly enhance cybersecurity, but their adoption must be accompanied by ethical guidelines, transparency measures, and accountability mechanisms [20], [27]. By embedding these recommendations into policy and practice, nations can build secure digital ecosystems that not only protect against threats but also actively enable sustainable, inclusive, and resilient development pathways.

4.5 | Future Prospects and Pathways

Looking ahead, the integration of cybersecurity into sustainable development strategies is expected to become even more critical as digital transformation accelerates globally. One promising direction is the growing adoption of AI and ML in cybersecurity. These technologies enhance predictive threat detection and automated response systems, enabling institutions to safeguard sensitive infrastructures more effectively. Salih et al. [20] argue that AI-driven models will play a transformative role in strengthening resilience across multiple sectors, from healthcare and finance to education and environmental monitoring. Similarly, blockchain technologies are anticipated to expand their role in ensuring transparency, traceability, and trust in governance and economic transactions, thereby directly supporting SDGs on strong institutions and economic growth [12]. Another emerging pathway is the rise of green cybersecurity, which integrates environmental considerations into digital protection strategies.

Sulich et al. [49] highlight how this approach can safeguard environmental technologies and inter-organizational networks, ensuring the security of systems used for climate action, biodiversity monitoring, and renewable energy transitions. Such innovations demonstrate the potential for cybersecurity to contribute not only to digital resilience but also to environmental sustainability. At the policy level, the future will likely see greater emphasis on international cooperation and harmonized governance frameworks. As cyber threats transcend borders, collective responses involving governments, private actors, and civil society will be necessary to build inclusive and resilient digital ecosystems [56]. Strengthening collaboration across regions can also help bridge the digital divide, ensuring that developing economies are not left behind in the cybersecurity–sustainability nexus.

5 | Conclusion

This study has examined the vital role of cybersecurity in advancing the SDGs, demonstrating that secure digital systems are not merely protective mechanisms but fundamental enablers of sustainable development. Through a systematic review of scholarly and institutional sources, the research highlighted how cybersecurity supports multiple SDGs by safeguarding digital infrastructures, fostering economic growth, enabling innovation, strengthening governance, and protecting environmental and educational systems. The findings underscore that cybersecurity is indispensable for building resilient and inclusive societies in an era of rapid digital transformation. The analysis revealed several key contributions. First, cybersecurity underpins critical economic functions, from securing financial systems and digital fundraising initiatives to protecting industrial innovation and intellectual property. Second, it plays a central role in urban sustainability and climate action by ensuring the integrity of smart city systems, environmental databases, and remote sensing technologies. Third, emerging trends such as AI, blockchain, and green cybersecurity offer promising pathways for enhancing resilience and transparency, though their deployment must be accompanied by robust governance and ethical oversight. At the same time, the study identified significant challenges, including regulatory gaps, limited institutional capacity, unequal access to digital resources, and the complexity of integrating advanced technologies into sustainability frameworks. These barriers highlight the need for comprehensive national strategies, capacity-building initiatives, and stronger international cooperation to ensure that the benefits of cybersecurity are equitably shared.

Conflict of Interest

The authors have no relevant financial or non-financial interests to disclose.

Data Availability

The research data supporting this study are available upon reasonable request from the corresponding author.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] Ridwan, M., Akther, A., Dhar, B. K., Roshid, M. M., Mahjabin, T., Bala, S., & Hossain, H. (2025). Advancing circular economy for climate change mitigation and sustainable development in the Nordic Region. *Sustainable development*, 1–20. https://doi.org/10.1002/sd.3563

[2] Mozumder, M. A. S., Nguyen, T. N., Devi, S., Arif, M., Ahmed, M. P., Ahmed, E., … & Uddin, A. (2024). Enhancing customer satisfaction analysis using advanced machine learning techniques in fintech industry. *Journal of computer science and technology studies*, *6*(3), 35–41. https://www.academia.edu/download/120386146/Paper_03.pdf

[3] Odumesi, J. O., & Sanusi, B. S. (2023). Achieving sustainable development goals from a cybersecurity perspective. *Proceedings of the cyber secure nigeria conference.* (pp. 1–10). Nigerian Army Resource Centre (NARC) Abuja, Nigeria. https://www.csean.org.ng/

[4] Raihan, A., Voumik, L. C., Ridwan, M., Akter, S., Ridzuan, A. R., Wahjoedi, … & Ismail, N. A. (2024). Indonesia's path to sustainability: Exploring the intersections of ecological footprint, technology, global trade, financial development and renewable energy. In *Alareeni, B. & Elgedawy, I. (Eds.), Opportunities and risks in AI for business development: volume 1* (pp. 1–13). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-65203-5_1

[5] Uddin, M. K., Akter, S., Das, P., Anjum, N., Akter, S., Alam, M., … & Pervin, T. (2024). Machine learning-based early detection of kidney disease: A comparative study of prediction models and performance evaluation. *international journal of medical science and public health research*, *5*(15), 58–75. https://doi.org/10.37547/ijmsphr/Volume05Issue12-05

[6] Ridzuan, A. R., Rahman, N. H. A., Singh, K. S. J., Borhan, H., Ridwan, M., Voumik, L. C., & Ali, M. (2024). Assessing the impact of technology advancement and foreign direct investment on energy utilization in malaysia: An empirical exploration with boundary estimation. *Technology and business model innovation: challenges and opportunities* (pp. 1–12). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-55911-2_1

[7] Salih, A., Zeebaree, S. T., Ameen, S., Alkhyyat, A., & Shukur, H. M. (2021). A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection. *2021 7th international engineering conference "Research & innovation amid global pandemic" (IEC)* (pp. 61–66). IEEE. https://doi.org/10.1109/IEC52205.2021.9476132

[8] Sweet, M. M. R., Arif, M., Uddin, A., Sharif, K. S., Tusher, M. I., Devi, S. (2024). Credit risk assessment using statistical and machine learning: Basic methodology and risk modeling applications. *International journal on computational engineering*, *1*(3), 62–67. https://doi.org/10.62527/comien.1.3.21

[9] Shak, M. S., Uddin, A., Rahman, M. H., Anjum, N., Al Bony, M. N. V., Alam, M., … & Pervin, T. (2024). Innovative machine learning approaches to foster financial inclusion in microfinance. *International interdisciplinary business economics advancement journal*, *5*(11), 6–20. https://doi.org/10.55640/business/volume05issue11-02

[10] Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cybersecurity at the grassroots: American local governments and the challenges of internet security. *Journal of homeland security and emergency management*, *15*(3), 20170048. https://doi.org/10.1515/jhsem-2017-0048

[11] Toapanta, S. M. T., Jaramillo, J. M. E., & Gallegos, L. E. M. (2020). Cybersecurity analysis to determine the impact on the social area in latin america and the caribbean. *Proceedings of the 2019 2nd international conference on education technology management* (pp. 73–78). New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3375900.3375911

[12] Rahat, S. K. R. U. I., Rahman, M. D. H., Arafat, Y., Rahaman, M., Hasan, M. M., & Amin, M. Al. (2025). advancing diabetic retinopathy detection with AI and deep learning: Opportunities, limitations, and clinical barriers. *British journal of nursing studies*, *5*(2), 01–13. https://doi.org/10.32996/bjns.2025.5.2.1

[13] Rahman, M. H., Anwar, M. M., & Hossain, F. (2025). AI-driven big data and business analytics: Advancing healthcare, precision medicine, supply chain resilience, energy innovation and economic competitiveness. *Journal of medical and health studies*, *6*(3), 205–215. https://doi.org/10.32996/jmhs.2025.6.3.30

[14] Akhter, A., Al Shiam, S. A., Ridwan, M., Abir, S. I., Shoha, S., Nayeem, M. B., & Bibi, R. (2024). Assessing the impact of private investment in AI and financial globalization on load capacity factor: Evidence from United States. *Journal of environmental science and economics*, *3*(3), 99–127. https://doi.org/10.56556/jescae.v3i3.977

[15] Akther, A., Tahrim, F., Voumik, L. C., Esquivias, M. A., & Pattak, D. C. (2025). Municipal solid waste dynamics: Economic, environmental, and technological determinants in Europe. *Cleaner engineering and technology*, *24*, 100877. https://doi.org/10.1016/j.clet.2024.100877

[16] Arif, M., Hasan, M., Al Shiam, S. A., Ahmed, M. P., Tusher, M. I., Hossan, M. Z. (2024). Predicting customer sentiment in social media interactions: Analyzing Amazon help Twitter conversations using machine learning. *International journal of advanced science computing and engineering*, *6*(2), 52–56. https://doi.org/10.62527/ijasce.6.2.211

[17] Hossain, M. N., Anjum, N., Alam, M., Rahman, M. H., Taluckder, M. S., Al Bony, M. N. V., … & Jui, A. H. (2024). Performance of machine learning algorithms for lung cancer prediction: a comparative study. *International journal of medical science and public health research*, *5*(11), 41–55. https://doi.org/10.37547/ijmsphr/Volume05Issue11-05

[18] Rahman, M., Al Amin, M., Hasan, R., Hossain, S. M. T., Rahman, M. H., & Rashed, R. A. M. (2025). A predictive AI framework for cardiovascular disease screening in the us: Integrating EHR data with machine and deep learning models. *British journal of nursing studies*, *5*(2), 40–48. https://doi.org/10.32996/bjns.2025.5.2.5

[19] Voumik, L. C., & Ridwan, M. (2023). Impact of FDI, industrialization, and education on the environment in Argentina: ARDL approach. *Heliyon*, *9*(1), 1–12. https://doi.org/10.1016/j.heliyon.2023.e12872

[20] Al-Sherideh, A. S., Maabreh, K., Maabreh, M., Al Mousa, M. R., & Asassfeh, M. (2023). Assessing the impact and effectiveness of cybersecurity measures in e-learning on students and educators: A case study. *International journal of advanced computer science and applications*, *14*(5), 158–164. https://www.academia.edu/download/111068817/Paper_16-Assessing_the_Impact_and_Effectiveness_of_Cybersecurity_Measures.pdf

[21] Urbee, A. J., Hasan, M. A., Ridwan, M., & Dewan, M. F. (2025). Adaptation and resilience in the face of climate-induced migration: Exploring coping strategies in the urban economy of barishal metropolitan city. *Environment, innovation and management*, *1*, 2550005. https://doi.org/10.1142/S306090112550005X

[22] Wibowo, A. (2023). Enhancing economic growth for the achievement of sustainable development goals through digital era fundraising schemes for sustainable community development: A policy analysis from the islamic economic perspective. *Proceeding of international conference on Islamic philantrophy* (Vol. 1, pp. 26–37). Islamic Philantrophy. https://proceedings.uinsaizu.ac.id/index.php/icip/article/download/301/273

[23] Robinson, G. (2021). Come hell or high water: Climate action by archives, records and cultural heritage professionals in the United Kingdom. *Records management journal*, *31*(3), 314–340. https://doi.org/10.1108/RMJ-10-2020-0036

[24] Ridwan, M., Urbee, A. J., Voumik, L. C., Das, M. K., Rashid, M., & Esquivias, M. A. (2024). Investigating the environmental Kuznets curve hypothesis with urbanization, industrialization, and service sector for six South Asian countries: Fresh evidence from Driscoll Kraay standard error. *Research in globalization*, *8*, 100223. https://doi.org/10.1016/j.resglo.2024.100223

[25] Zawaideh, F. H., Abu-Ulbeh, W., Mjlae, S. A., El-Ebiary, Y. A. B., Al Moaiad, Y., & Das, S. (2023). Blockchain solution for smes cybersecurity threats in e-commerce. *2023 international conference on computer science and emerging technologies (CSET)* (pp. 1–7). IEEE. https://doi.org/10.1109/CSET58993.2023.10346628

[26] Ridwan, M., Aspy, N. N., Bala, S., Hossain, M. E., Akther, A., Eleais, M., & Esquivias, M. A. (2024). Determinants of environmental sustainability in the United States: Analyzing the role of financial development and stock market capitalization using LCC framework. *Discover sustainability*, *5*(1), 319. https://doi.org/10.1007/s43621-024-00539-1

[27] Orthi, S. M., Rahman, M. H., Siddiqa, K. B., Uddin, M., Hossain, S., Al Mamun, A., & Khan, M. N. (2025). Federated learning with privacy-preserving big data analytics for distributed healthcare systems. *Journal of computer science and technology studies*, *7*(8), 269–281. https://doi.org/10.32996/jcsts.2025.7.8.31

[28] Rahman, M. H., Hossin, M. E., Hossain, M. J., Uddin, S. M. M., Faruk, M. I., Anwar, M. M., & Hossain, F. (2024). Harnessing big data and predictive analytics for early detection and cost optimization in cancer care. *Journal of computer science and technology studies*, *6*(5), 278–293. https://doi.org/10.32996/

[29] Raihan, A., Bala, S., Akther, A., Ridwan, M., Eleais, M., & Chakma, P. (2024). Advancing environmental sustainability in the G-7: The impact of the digital economy, technological innovation, and financial accessibility using panel ARDL approach. *Journal of economy and technology*, In Press. https://doi.org/10.1016/j.ject.2024.06.001

[30] Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of cybersecurity and privacy*, *3*(3), 327–350. https://doi.org/10.3390/jcp3030017

[31] Turk, Ž., García de Soto, B., Mantha, B. R. K., Maciel, A., & Georgescu, A. (2022). A systemic framework for addressing cybersecurity in construction. *Automation in construction*, *133*, 103988. https://doi.org/10.1016/j.autcon.2021.103988

[32] Ridwan, M., Akther, A., Tamim, M. A., Ridzuan, A. R., Esquivias, M. A., & Wibowo, W. (2024). Environmental health in BIMSTEC: The roles of forestry, urbanization, and financial access using LCC theory, DKSE, and quantile regression. *Discover sustainability*, *5*(1), 429. https://doi.org/10.1007/s43621-024-00679-4

[33] Raihan, A., Ibrahim, S., Ridwan, M., Rahman, M. S., Bari, A. B. M. M., & Guneysu Atasoy, F. (2025). Role of renewable energy and foreign direct investment toward economic growth in Egypt. *Innovation and green development*, *4*(1), 100185. https://doi.org/10.1016/j.igd.2024.100185

[34] Rahman, J., Rahman, H., Islam, N., Tanchangya, T., Ridwan, M., & Ali, M. (2025). Regulatory landscape of blockchain assets: Analyzing the drivers of NFT and cryptocurrency regulation. *BenchCouncil transactions on benchmarks, standards and evaluations*, *5*(1), 100214. https://doi.org/10.1016/j.tbench.2025.100214

[35] Chouraik, C. (2024). Enhancing cybersecurity in Moroccan banking: A strategic integration of AI, blockchain, and business intelligence. *International journal of science and research archive*, *13*(02), 1723–1734. https://doi.org/10.30574/ijsra.2024.13.2.2312

[36] Denoncourt, J. (2020). Companies and UN 2030 sustainable development goal 9 industry, innovation and infrastructure. *Journal of corporate law studies*, *20*(1), 199–235. https://doi.org/10.1080/14735970.2019.1652027

[37] binti Sulaiman, N., binti Mahmud, N. P. N., Nazir, U., Abid, S. K., & others. (2021). The role of autonomous robots in fourth industrial revolution (4IR) as an approach of sustainable development goals (sdg9): industry, innovation and infrastructure in handling the effect of covid-19 outbreak. *IOP conference series: Earth and environmental science* (Vol. 775, p. 12017). IOP Publishing. 10.1088/1755-1315/775/1/012017

[38] Shahid, R., & Ahmed, B. (2022). Embedding four indicators of resilience to make cities and communities sustainable in Pakistan. *Global journal for management and administrative*, *3*(2), 63–73. https://pdfs.semanticscholar.org/3df7/01e4b4732134f0a79b61f37bccf13d52ec57.pdf

[39] Fallah Shayan, N., Mohabbati-Kalejahi, N., Alavi, S., & Zahed, M. A. (2022). Sustainable development goals (SDGs) as a framework for corporate social responsibility (CSR). *Sustainability*, *14*(3), 1222.

[40] Bouteche, B., & Bougdah, H. (2023). Sustainable cities and precarious housing: The case of Algeria. *Management of sustainable development*, *15*(2), 28–35. http://dx.doi.org/10.54989/msd-2023-0014

[41] Ridwan, M., Akther, A., Al Absy, M. S. M., Tahsin, M. S., Bin Ridzuan, A. R., Yagis, O., & Mukhta, K. P. (2024). The role of tourism, technological innovation, and globalization in driving energy demand in major tourist regions. *International journal of energy economics and policy*, *14*(6), 675–689. 10.32479/ijeep.17344.

[42] Ridwan, M., Tahsin, M. S., Al-Absy, M. S. M., Eleais, M., Ridzuan, A. R., & Mukthar, K. P. J. (2025). Economic Alchemy: Unraveling the nexus between trade openness, inflation, exchange rates, and economic growth in bangladesh. *International journal of economics and financial issues*, *15*(3), 244. https://doi.org/10.32479/ijefi.17779

[43] Niedziółka, P. (2020). Polish banking sector facing challenges related to environmental and climate protection. *Problemy zarządzania*, *18*(4 (90)), 32–47. https://www.ceeol.com/search/article-detail?id=991838

[44] Jerbi, D. (2023). Beyond firewalls: Navigating the jungle of emerging cybersecurity trends. *Journal of current trends in computer science research*, *2*(2), 191–195. https://www.opastpublishers.com/open-access-articles/beyond-firewalls-navigating-the-jungle-of-emerging-cybersecurity-trends.pdf

[45] Rahman, M. D. H., Rahaman, M., Arafat, Y., Rahat, S. K. R. U. I., Hasan, R., Rimon, S. M. T. H., & Dipa, S. A. (2025). Artificial intelligence for chronic kidney disease risk stratification in the USA: Ensemble vs. deep learning methods. *British journal of nursing studies*, *5*(2), 20–32. https://doi.org/10.32996/bjns.2025.5.2.3

[46] Raihan, A., Hasan, M. A., Voumik, L. C., Pattak, D. C., Akter, S., & Ridwan, M. (2024). Sustainability in Vietnam: Examining economic growth, energy, innovation, agriculture, and forests' impact on CO2 emissions. *World development sustainability*, *4*, 100164. https://doi.org/10.1016/j.wds.2024.100164

[47] Raihan, A., Zimon, G., Ridwan, M., Rahman, M. M., & Salehi, M. (2025). Role of mineral resource rents, renewable energy, and energy efficiency toward carbon neutrality in China. *Energy nexus*, *17*, 100394. https://doi.org/10.1016/j.nexus.2025.100394

[48] Rahman, M. H., Das, A. C., Shak, M. S., Uddin, M. K., Alam, M. I., Anjum, N., … & Alam, M. (2024). Transforming customer retention in fintech industry through predictive analytics and machine learning. *The american journal of engineering and technology*, *6*(10), 150–163. https://doi.org/10.37547/tajet/Volume06Issue10-17

[49] Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. *Procedia computer science*, *192*, 20–28. https://doi.org/10.1016/j.procs.2021.08.003

[50] Rahman, M. H., Dipa, S. A., Hasan, K., & Hasan, M. M. (2025). Health at Risk: Respiratory, cardiovascular, and neurological impacts of air pollution. *Innovations in environmental economics*, *1*(1), 56–69. https://doi.org/10.48313/iee.v1i1.41

[51] Ziky, M., & El-Abdellaoui, L. (2023). Can sustainable development goals go hand in hand with economic growth? Evidence from Morocco. *Problems and perspectives in management*, *21*(3), 656. 10.21511/ppm.21(3).2023.51

[52] Ekmen, O., & Kocaman, S. (2023). From pixels to sustainability: Trends and collaborations in remote sensing for advancing sustainable cities and communities (SDG 11). *Sustainability*, *15*(22), 16094. https://doi.org/10.3390/su152216094

[53] Onwe, J. C., Ridzuan, A. R., Uche, E., Ray, S., Ridwan, M., & Razi, U. (2024). Greening Japan: Harnessing energy efficiency and waste reduction for environmental progress. *Sustainable futures*, *8*, 100302. https://doi.org/10.1016/j.sftr.2024.100302

[54] Ridwan, M., Al Jubayed, A., Kayser, K. A., Ahmed, M. E., Chowdhury, R. R., Hassan, M. R., … & Kanij, H. N. (2025). Examine the role of political stability and education toward green economy: An empirical evidence for Bangladesh. *Environment, innovation and management*, *01*, 2550011. https://doi.org/10.1142/S3060901125500115

[55] Etemadi, N., Van Gelder, P., & Strozzi, F. (2021). An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity. *Sustainability*, *13*(9), 4672. https://doi.org/10.3390/su13094672

[56] Chisty, N. M. A., Baddam, P. R., & Amin, R. (2022). Strategic approaches to safeguarding the digital future: insights into next-generation cybersecurity. *Engineering international*, *10*(2), 69–84. https://pdfs.semanticscholar.org/1b58/6859a65c542ca2d501be4d0bf0768bca7ae0.pdf