Discover Sustainability

Research

Integrating sustainability into cybersecurity: insights from machine learning based topic modeling

Krishnashree Achuthan[1] · Sriram Sankaran[1] · Swapnoneel Roy[2] · Raghu Raman[3]

Received: 27 September 2024 / Accepted: 9 December 2024
Published online: 21 January 2025

Abstract

The increasing emphasis on sustainability in computing systems, ranging from small devices to large data centers, is fueled by environmental concerns. Moreover, ensuring cybersecurity in these interconnected networks demands the use of technologies such as resource-intensive cryptography and advanced intrusion detection systems. Our unique study investigates the integration of environmental sustainability into cybersecurity practices by identifying six pivotal themes through a textual analysis of related publications via machine learning based topic modeling. These themes highlight the convergence of cybersecurity with sustainable development goals (SDGs), particularly SDGs 7 (Affordable and Clean Energy), 9 (Industry, Innovation, and Infrastructure), and 8 (Decent Work and Economic Growth). These include the integration of sustainable cybersecurity measures in smart cities, sustainable digital protection strategies, the application of blockchain for cybersecurity in smart grids, and cybersecurity solutions for SMEs aimed at minimizing resource consumption. Additionally, the study explores multidisciplinary strategies and innovations across four perspectives: adaptive frameworks that prioritize resilience and environmental consciousness, policy shifts for coordinated protection, the power of AI in intelligent threat detection, and the impact of emerging technologies on both security and environmental efficiency. These strategies advocate for an evolved approach that incorporates advanced technologies such as AI, IoT, and blockchain into resilient, sustainable cybersecurity frameworks. This study not only provides a comprehensive overview of the intersection of cybersecurity and sustainability but also serves as a guide for future research and practical applications in creating robust, environmentally friendly cybersecurity practices.

Article highlights

- Explores sustainable cybersecurity aligned with SDGs 7, 8, and 9 using machine learning topic modeling.
- Highlights blockchain, AI, and IoT in cybersecurity for smart grids, SMEs, and resource-efficient systems.
- Advocates adaptive frameworks, AI-driven threat detection, and policy shifts for eco-conscious security solutions.

Keywords Sustainable development goal · Sustainable cybersecurity · Green cybersecurity · Digital economy · Smart city · Smart grids · Machine learning

✉ Krishnashree Achuthan, Krishna@amrita.edu; ✉ Raghu Raman, Raghu@amrita.edu | [1]Center for Cybersecurity Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam 690525, Kerala, India. [2]School of Computing, College of Computing, Engineering & Construction, University of North Florida, Jacksonville, USA. [3]Amrita School of Business, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam 690525, Kerala, India.

1 Introduction and related work

Cybersecurity is of paramount importance in computing systems, which generally range from tiny, embedded devices to computationally intensive data centers stored in the cloud [1–3]. This is due to the networked nature of devices coupled with the sensitivity of the data communicated through these devices [4]. However, cybersecurity increases the carbon footprint through the use of a number of crunching cryptographic algorithms, cryptocurrencies, attackers with advanced capabilities that deplete resources, and the development of high-overhead intrusion detection and prevention systems, thus resulting in energy—performance—security trade-offs [5–7]. Attackers with advanced capabilities further exacerbate this by depleting resources and necessitating the development of high-overhead intrusion detection and prevention systems. These activities lead to substantial energy-performance-security trade-offs, contributing to a larger carbon footprint. For instance, the energy consumption of cryptocurrencies such as Bitcoin can rival the annual power usage of small countries. These trade-offs need to be studied, and mechanisms need to be developed to balance them depending on the application requirements. Thus, the concept of sustainable or green cybersecurity is proposed not only to increase the lifetime of computing systems but also to incorporate sustainable practices into the cybersecurity lifecycle while being resilient to cyber threats [8, 9].

In this context, the United Nations Sustainable Development Goals (SDGs), a global framework of 17 interconnected goals designed to address the world's most pressing challenges, including poverty, inequality, climate change, environmental degradation, peace, and justice by 2030, are highly relevant [10]. Recent assessments indicate that progress on many of these targets is lagging, with significant shortfalls in areas critical to our collective future, underscoring the urgency of innovative and integrated solutions [11]. While advancements in computing and communication technologies have failed to compensate for improvements in sustainability, reducing the carbon footprint and maximizing the sustainability of computing systems have become imperative [12, 13]. Sustainable blockchain technology is revolutionizing various sectors, including supply chain management, engineering, energy, governance, and finance [14]. Its decentralized nature and transparency promote eco-friendly practices, renewable energy integration, and adherence to sustainability standards. While implementation costs exist, they are offset by long-term savings and environmental benefits [15]. Studying sustainable cybersecurity is essential because it intersects directly with goals such as SDG 11 (Sustainable Cities and Communities), SDG 9 (Industry, Innovation, and Infrastructure), and SDG 7 (Affordable and Clean Energy). Continued research and integration into regulations are crucial for its widespread adoption and contribution to global sustainability goals.

According to the World Economic Forum (WEF, 2024), cybercrime will cost $6 trillion in 2021 in terms of financial damage to the economy and $8 trillion in 2023, and the costs are expected to increase by 15% per year, thus reaching $10.5 million in 2025 [16]. Similarly, emerging threats such as Wannacry ransomware attacks cost an estimated $4 billion [17]. Thus, with the increasing capabilities of attackers along with the advent of things attached to everyday objects, referred to as the Internet of Things, the need to understand attacker motives, along with the corresponding impact on system operations and end users depending on application requirements, becomes necessary. In recent decades, the pervasive integration of digital technologies into nearly every aspect of modern society has transformed our world, offering unprecedented connectivity and efficiency. However, this digital transformation has also given rise to complex cybersecurity challenges, which threaten the integrity, privacy, and security of individuals, organizations, and nations [18]. In the context of smart cities, the relationship between cybersecurity and sustainability/resilience is crucial for achieving SDG11 [19] explored how cybersecurity threats impact various smart city domains, such as the transportation, healthcare, and residential sectors. As cybersecurity threats continue to evolve in terms of sophistication and scale, it becomes imperative to develop sustainable cybersecurity practices that can effectively mitigate these risks while fostering resilience and innovation [20, 21].

The sustainability of cybersecurity solutions in critical sectors such as healthcare, smart cities, and defense can indeed be a significant concern due to several key challenges and factors [23]. The issues that can lead to unsustainable practices include complexity and resource intensity, i.e., modern cybersecurity solutions often involve complex technologies, including advanced firewalls, intrusion detection systems, encryption tools, and endpoint protection [24]. Implementing and managing these technologies requires specialized skills and significant resources in terms of both financial investment and ongoing operational costs. This complexity can make cybersecurity unsustainable, especially for organizations with limited budgets or expertise.

Second, a rapidly evolving threat landscape enables attackers to become increasingly sophisticated in their methods [25]. This requires cybersecurity solutions to adapt continuously and update to address new vulnerabilities and attack vectors. Keeping up with these changes demands ongoing investments in research, development, and monitoring, which can strain resources over time.

Third, compliance and regulatory requirements in industries such as healthcare, smart cities, and defense are subject to stringent regulatory frameworks (e.g., HIPAA for healthcare, GDPR for data protection). Meeting these compliance standards often requires specific cybersecurity measures and audits. Compliance requirements can impose additional costs and administrative burdens on organizations, potentially making long-term sustainability challenging [26].

Fourth, we address data volume and privacy concerns. Healthcare and smart city initiatives generate vast amounts of sensitive data. Protecting these data requires robust cybersecurity measures, including encryption, secure storage, and access controls. The increasing volume and complexity of data add to the scalability challenges of cybersecurity solutions [27], particularly when considering data privacy laws and ethical considerations.

The fifth relates to risk assessment, such as with smart grids and smart cities, which are integral parts of critical infrastructure upon which many essential services and functions rely. Disruptions or attacks on these systems can have far-reaching consequences, including economic loss, public safety risks, and disruptions to daily life. As such, ensuring the resilience and sustainability of cybersecurity solutions for smart grids and smart cities requires a holistic approach that integrates cybersecurity into the design, development, and operation of these systems [28]. This includes proactive risk management, continuous monitoring and adaptation, collaboration between stakeholders, and investment in research, education, and innovation.

Sixth, budget constraints severely hamper many organizations, including those in healthcare and local governments (for smart cities). Allocating sufficient resources to cybersecurity amidst competing priorities can be difficult. This can lead to underinvestment in critical security measures [29], increasing the vulnerability of these sectors to cyber threats. Seventh, the interconnected nature of modern IT systems means that cybersecurity vulnerabilities can propagate across supply chains, which negatively impacts the digital economy. Supply chain vulnerabilities can expose digital businesses to cyber threats such as malware, ransomware, and data breaches [30]. Attackers may exploit weaknesses in third-party software, firmware, or hardware components to gain unauthorized access to systems, steal sensitive information, or disrupt operations. Managing these supply chain risks requires additional investments in monitoring and auditing, which can strain resources.

Finally, the scalability challenges in infrastructures that serve growing populations and technological advancements require scalable cybersecurity solutions to accommodate increased demand and complexity [31]. Legacy systems and infrastructure can further complicate scalability efforts, leading to potential gaps in cybersecurity coverage.

Addressing these sustainability challenges requires a comprehensive approach that integrates cybersecurity into the core of organizational strategy and operations. This may involve leveraging automation and AI-driven solutions to enhance threat detection and response, investing in workforce development to bridge cybersecurity skill gaps, and adopting risk-based approaches to prioritize security investments on the basis of the potential impact and likelihood of threats. Additionally, collaboration between the public and private sectors is essential for sharing threat intelligence and best practices, ultimately enhancing the resilience of cybersecurity solutions in critical sectors.

The concept of sustainable cybersecurity practices encapsulates a holistic approach to addressing cybersecurity challenges that not only focuses on immediate threat mitigation but also considers long-term impacts on society, the environment, and technological advancement [22]. This paper aims to explore the historical trends in cybersecurity practices by examining how past approaches have shaped our current cybersecurity landscape. Moreover, it seeks to forecast future directions for sustainable cybersecurity, outlining strategies and frameworks that can guide stakeholders toward more resilient and eco-conscious cybersecurity solutions.

Accordingly, the research questions explored in this study are as follows:

1. RQ1: Which primary SDGs and their associated subtargets are addressed in the literature on sustainable cybersecurity?
2. RQ2: What emerging themes in the sustainable cybersecurity literature are likely to significantly shape the future direction of the field?
3. RQ3: What theoretical foundations underlie emerging topics that could inform the creation of policies and strategies to advance sustainable cybersecurity practices?

Our paper is organized as follows. RQ1 is addressed through bibliometric analysis, and the study identifies key SDGs prominently featured within the literature. This analysis is visualized through graphical representations that highlight the frequency and depth of research topics aligned with these goals. RQ2 is answered by using advanced topic modeling

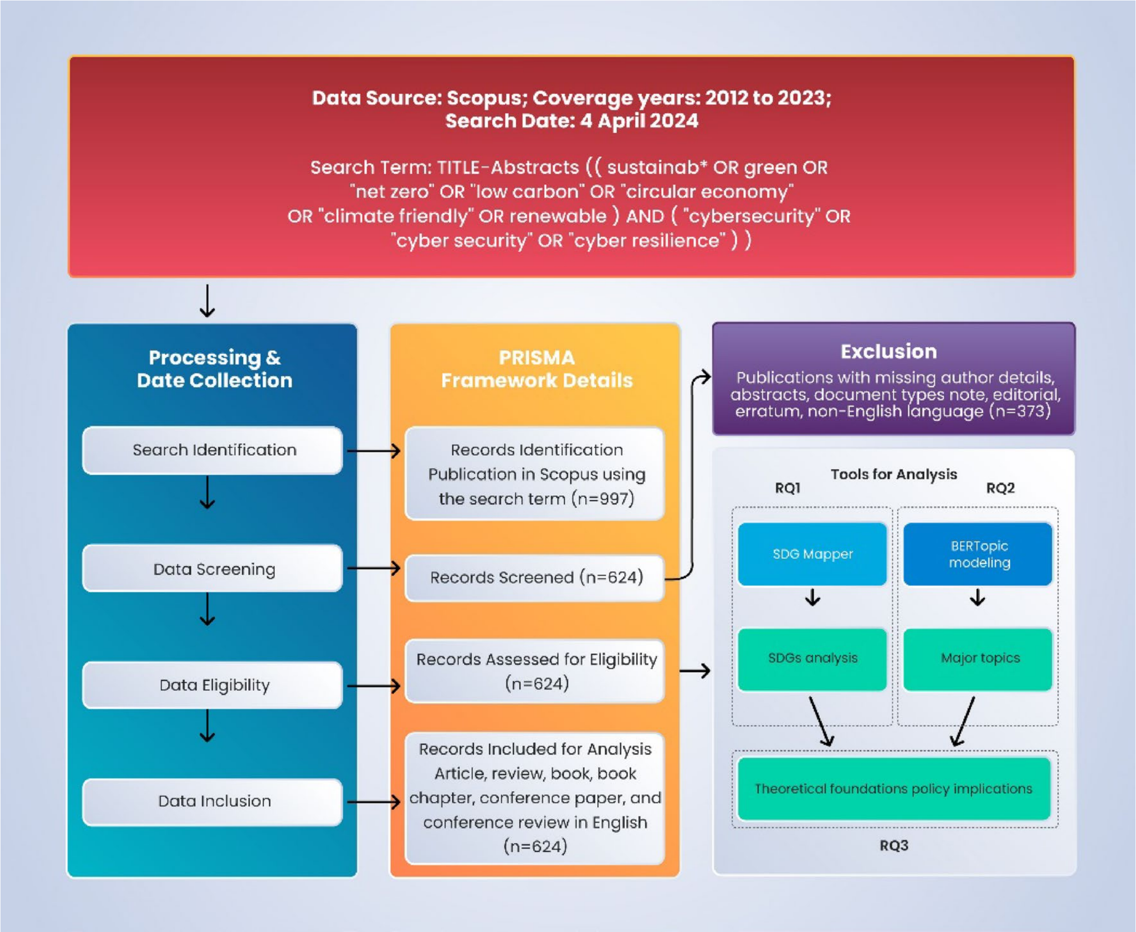
Data Source: Scopus; Coverage years: 2012 to 2023;
Search Date: 4 April 2024
Search Term: TITLE-Abstracts ((sustainab* OR green OR "net zero" OR "low carbon" OR "circular economy" OR "climate friendly" OR renewable) AND ("cybersecurity" OR "cyber security" OR "cyber resilience"))
Processing & Date Collection
Search Identification
Data Screening
Data Eligibility
Data Inclusion
PRISMA Framework Details
Records Identification Publication in Scopus using the search term (n=997)
Records Screened (n=624)
Records Assessed for Eligibility (n=624)
Records Included for Analysis Article, review, book, book chapter, conference paper, and conference review in English (n=624)
Exclusion
Publications with missing author details, abstracts, document types note, editorial, erratum, non-English language (n=373)
Tools for Analysis
RQ1
RQ2
SDG Mapper
BERTopic modeling
SDGs analysis
Major topics
Theoretical foundations policy implications
RQ3

Fig. 1 Research methodology

techniques. It provides a microscopic view, revealing specific discussions and their intricate relationships. RQ3 summarizes the literature from a theoretical perspective that could guide the development of policies and strategies for advancing sustainable cybersecurity practices.

2 Methods

This investigation was conducted in accordance with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines (Fig. 1), as outlined by [32]. These guidelines are recognized for their effectiveness in bibliometric research across various disciplines [33]. The literature search was performed via the Scopus database on April 4, 2024. Scopus is renowned for its comprehensive coverage of peer-reviewed literature, making it ideal for quantitative studies, and is considered the leading multidisciplinary database [34]. The initial search was set to start in the year 2012, aligning with the Rio + 20 summit that discussed the UN Sustainable Development Goals (SDGs). The search incorporated terms pertaining to cybersecurity and sustainable development in the title and abstract of the publications. Initially, 997 publications were identified, including articles, books, book chapters, conference papers, and reviews. After the exclusion of editorials, notes, errata, short surveys, and documents without authors or abstracts or not in the English language, 624 publications were selected for the final detailed analysis.

The search query used in Scopus is as follows: TITLE-ABS (Sustainab* OR Green OR "Net Z" OR "Low Carbon" OR "Circular Economy" OR "Climate Friendly" OR Renewable) AND TITLE-ABS ("cybersecurity" OR "cyber security" OR "cyber resilience") AND (PUBYEAR > 2012 AND PUBYEAR < 2024) AND LIMIT-TO (LANGUAGE, "English") AND LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "cp") OR LIMIT-TO (DOCTYPE, "re") OR LIMIT-TO (DOCTYPE, "cr") AND LIMIT-TO (SRCTYPE, "j") OR LIMIT-TO (SRCTYPE, "p") OR LIMIT-TO (SRCTYPE, "k").

The study employed machine learning based BERTopic, leveraging pretrained BERT embeddings to improve topic detection accuracy over traditional methods such as latent Dirichlet allocation [35–37]. BERTopic, a topic modeling tool employs advanced NLP methods to extract latent themes from textual data. It utilizes BERT (Bidirectional Encoder Representations from Transformers), a transformer-based language model that generates contextual embeddings, meaning each word's representation is sensitive to surrounding words, capturing complex contextual information. BERTopic further combines these embeddings with clustering algorithms like HDBSCAN to form coherent topic groups. This allows for dynamic topic discovery that can adapt to variations in language and terminology across texts, making it effective for uncovering patterns and themes in large datasets. When implemented in Python with transformers and a Class-Tf-idf-Transformer, the approach involved data preprocessing, NLP techniques, and tokenization. BERTopic analyzes the text corpus to extract and align topics while using probability analysis to enhance result interpretability. After processing the text, distinct topics were identified along with their probabilities, using parameters such as a minimum topic size of 20 and 20 keywords per topic. Six topics were selected through a combination of quantitative and qualitative evaluations, with a focus on intertopic distance and coherence scores. The 6-topic model provided optimal topic separation with minimal overlap and high coherence, whereas models with 4, 5, 7, 8, 9, or more topics presented greater overlap and reduced clarity. Therefore, the 6-topic model was chosen for its balance of data coverage and clarity. We then analyzed the five most-cited publications within each topic for further insights. This approach aligns with prior research attempting to map the research domain via BERTopic modeling [85–87, 91, 92].

For SDG mapping, the study utilized the SDG Mapper tool from the "Knowledge Base for the Sustainable Development Goals," provided by the European Commission [88]. This tool uses bubble charts to depict SDG interconnections and relevance among bibliometric records. The SDG Mapper tool uses natural language processing (NLP) and machine learning to map research content to specific SDGs. Leveraging a combination of keyword recognition, semantic analysis, and Named Entity Recognition (NER), the tool identifies SDG-related terms within text and assesses context through contextual embeddings. Trained on a large dataset of SDG-related documents, the SDG Mapper also applies clustering techniques, such as Latent Dirichlet Allocation (LDA), to detect thematic clusters aligned with SDGs. This allows it to capture associations and assigns a confidence score to each match, reflecting the probabilistic relevance of the text to specific SDGs. This process incorporates a rule-based approach for identifying keywords or phrases linked to each SDG, ensuring efficient and accurate mapping [38].

3 Results and discussion

3.1 Mapping sustainable cybersecurity research to SDGs

A textual analysis was conducted on a database containing 624 scholarly publications, which included the examination of document titles and abstracts. The SDG Mapper tool was utilized to align these publications with specific SDGs and their targets. Of the 169 available targets, 70 were identified as relevant through this process.

Figure 2 displays the associations between publications and the SDGs through a series of bubbles. The size of each bubble correlates with the proportion of associated keywords found, which is calculated as the number of goal-specific keywords divided by the total keyword count. As such, SDG 7, emphasizing affordable and clean energy, emerges as the most prominent, marked by 572 keyword occurrences. This is followed by SDG 9, concerning industry, innovation, and infrastructure, with 143 occurrences, and SDG 8, focused on decent work and economic growth, with 99 occurrences, underlining their relative prominence in the research database. Within SDG 7, there are several key subtargets that the research papers address: Subtarget 7.2 is shown as a distinct bubble within the larger SDG 7 circle, indicating focused research on renewable energy in cybersecurity. Subtarget 7.1, which aims to ensure universal access to affordable, reliable, and modern energy services, is another bubble within the SDG 7 area. This highlights the efforts in research to integrate energy access with cybersecurity. Subtarget 7.3 focuses on improving energy efficiency, signaling that ongoing research should be conducted to optimize energy use in cybersecurity solutions. Figure 2 shows that the size of the SDG 9 bubble implies that advancements in cybersecurity are being studied not only in isolation but also as a part of broader industrial and infrastructural applications that prioritize sustainability. Similarly, SDG 8 (Decent Work and Economic Growth) is also closely linked to SDG 7 and suggests that research should explore how sustainable energy is integral to promoting sustained, inclusive, and sustainable economic growth as well as full and productive employment within the context of cybersecurity.

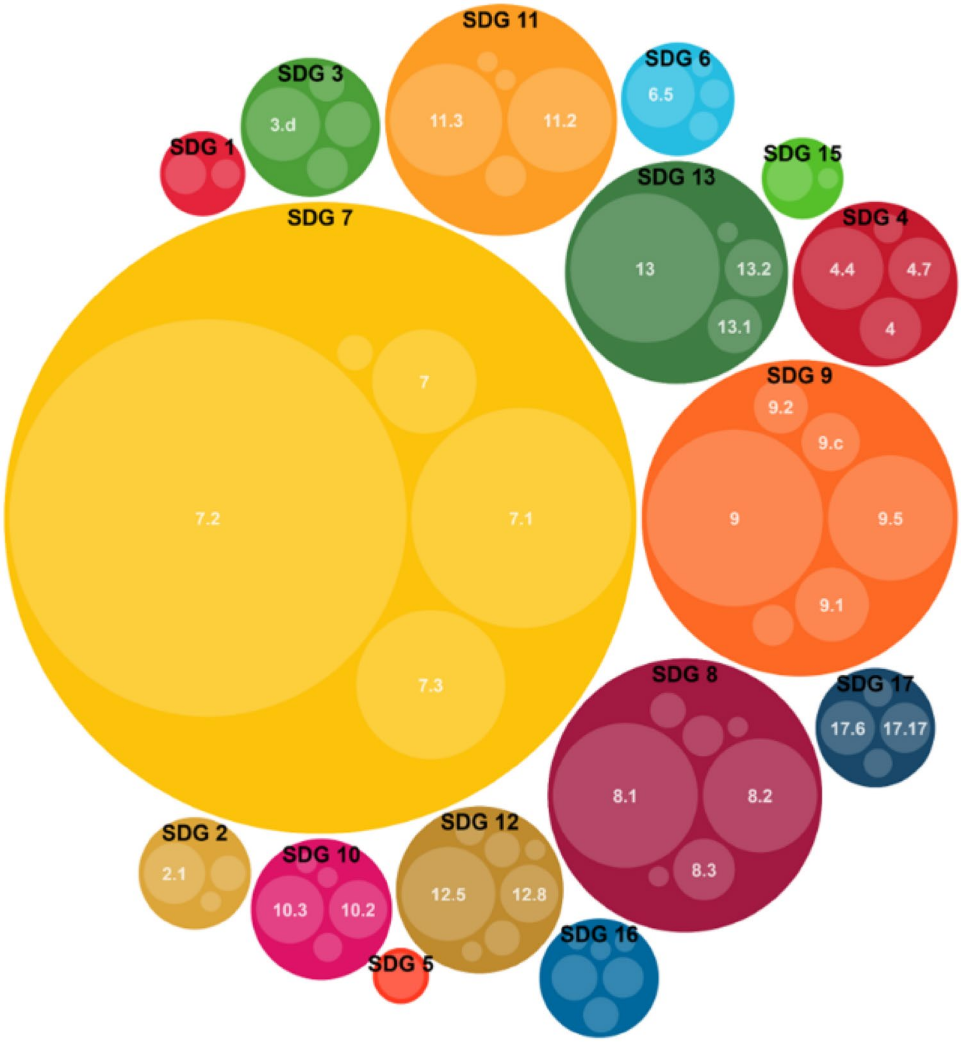

Fig. 2 Mapping sustainable cybersecurity research to SDGs

3.2 Major topics (RQ2)

BERTopic modeling identifies six key themes at the intersection of cybersecurity and sustainability, each contributing to various SDGs (Table 1). The integration of blockchain technology for sustainable cybersecurity emphasizes decentralization, fault tolerance, and energy efficiency, aligning with SDG 7, SDG 9, and SDG 13. Smart city development requires adaptable security frameworks that protect AI and IoT systems while optimizing energy use, supporting SDG 11. Digital protection strategies focus on energy-efficient machine learning models and resilient intrusion detection systems to reduce the environmental impact, addressing SDG 9 and SDG 12. In the energy and space sectors, cyber-resilience and AI-driven threat detection safeguard critical renewable energy infrastructures, aligning with SDG 7 and SDG 13. Smart grids benefit from cryptographic chips and dynamic security measures that ensure the resilience and efficiency of decentralized energy networks, contributing to SDG 7 and SDG 9. Finally, the digital economy's focus on data security and energy-efficient digital systems supports SDG 3 and SDG 12, particularly in areas such as healthcare and resource management. These themes illustrate how cybersecurity can evolve to meet both technological and environmental goals through innovative, resilient, and sustainable approaches.

Table 1 Major topics, their key sustainability and cybersecurity principles, and their SDG focus

Topic name	Key sustainability principles	Key cybersecurity concepts	SDG focus
Blockchain evolution for sustainable cybersecurity	Energy efficiency, Resilience	Decentralization, Data integrity, Fault tolerance, resource Control	7 AFFORDABLE AND CLEAN ENERGY 9 INDUSTRY, INNOVATION AND INFRASTRUCTURE 13 CLIMATE ACTION 16 PEACE, JUSTICE AND STRONG INSTITUTIONS
Green cybersecurity for smart city development	Low-power IoT, AI optimization, Energy-efficient data centers	Adaptable security frameworks, AI & IoT security, Privacy protection	11 SUSTAINABLE CITIES AND COMMUNITIES
Integrating sustainability into digital protection	Energy-efficient ML models, Sustainable intrusion detection	Resilience, Threat detection, Intrusion detection	9 INDUSTRY, INNOVATION AND INFRASTRUCTURE 12 RESPONSIBLE CONSUMPTION AND PRODUCTION
Securing energy in space and renewables	Energy-efficient technologies, AI for climate resilience	Cyber-resilience, AI in threat detection, Securing critical infrastructure	7 AFFORDABLE AND CLEAN ENERGY 12 RESPONSIBLE CONSUMPTION AND PRODUCTION 13 CLIMATE ACTION
Sustainable cybersecurity in smart grids	Renewable energy integration, Energy optimization	Cryptographic chips, Dynamic security, Resilient infrastructure protection	4 QUALITY EDUCATION 7 AFFORDABLE AND CLEAN ENERGY 9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
Digital economy and cybersecurity	Circular economy, Resource efficiency	Data security, AI in healthcare, Energy-efficient digital systems	3 GOOD HEALTH AND WELL-BEING 12 RESPONSIBLE CONSUMPTION AND PRODUCTION

3.2.1 Blockchain evolution for sustainable cybersecurity

The intersection of cybersecurity, blockchain technology, and sustainable development presents a promising avenue for achieving multiple SDGs and their specific targets. China's unique cybersecurity focus [39] offers a lens through which to explore blockchain's potential for enhancing both security and sustainability. This paper outlines a rigorous evaluation framework for popular platforms (Bitcoin, Ethereum, and Hyperledger), emphasizing that decentralization is key for reducing reliance on energy-intensive data centers. This approach supports SDG 7, particularly targets 7.2 and 7.3, by promoting energy-efficient technologies and potentially lowering the carbon footprint of the energy sector, thus aligning with SDG 13 (Climate Action). Moreover, the focus on fault tolerance, resource control, and recovery aligns with sustainable blockchain operations, which contribute to SDG 9, specifically 9.1 and 9.4. However, improvements in audits, access control, and data integrity are needed to meet national security infrastructure demands, ensuring compliance with SDG 16, particularly 16.6 and 16.10. The review by [40] further supports blockchain's role in creating a secure and sustainable energy infrastructure. They highlighted blockchain's applicability to peer-to-peer energy trading, enhanced cybersecurity, and enhanced renewable energy investment, all of which streamline power system operations. This aligns with SDG 7.1, SDG 9.1, and SDG 9.4 by fostering resilient infrastructure and sustainable industrialization. In the work of [41], the focus shifted to the specific needs of SMEs. Enhancing data integrity, combating fraud, and offering cost-effective security measures are crucial for SMEs in e-commerce, demonstrating how blockchain fosters security with environmental consciousness. This approach supports SDG 8.2 and SDG 12.

3.2.2 Green cybersecurity for smart city development

The development of a smart city that directly contributes to SDG 11 hinges on a nexus of cybersecurity, technology, and sustainability to build resilience against disruptions. Scholarly discussions emphasize cybersecurity's dual role: protecting information systems while supporting sustainable urban practices. Smart cities integrate AI and the IoT to optimize resources. However, this transformation increases their vulnerability [42]. A cyberattack on a city's power grid, for example, could cripple sustainable systems. Sustainable cybersecurity advocates for measures aligned with the SDGs, including energy-efficient data centers and low-power IoT devices. Sustainable cybersecurity advocates for measures aligned with SDG subtargets, such as 11.3, 11.5, and 11.b. By incorporating green principles into design, urban planners can ensure that security solutions do not negate environmental progress. Ref [43] emphasized the importance of safeguarding smart cities from evolving cyber threats. The complexity of AI and IoT systems demands adaptable cybersecurity frameworks that manage vast amounts of data while protecting privacy. This paper calls for innovation in security technologies and comprehensive cybersecurity legislation and policies to protect against breaches that could disrupt city operations and services. Ref [44] examined another dimension of smart cities by focusing on the potential of urban computing. Data analytics and intelligent automation can enhance smart city sustainability by optimizing energy use and transportation. This directly contributes to sustainable cybersecurity, as it ensures that security measures are environmentally sound. Urban computing must be a foundational element of sustainable smart city development, with cybersecurity practices aligning with environmental goals to prevent cyberattacks that undermine or disrupt efficient operations.

3.2.3 Integrating sustainability into digital protection

In this context, the studies delve into how cybersecurity is conceptualized within frameworks of sustainability and technological progress [45] address the vulnerability of IoT environments to data poisoning attacks. These attacks not only compromise security but also increase energy consumption because of frequent retraining and harm to IoT ecosystems. The authors advocate for ML models that are both robust against threats and energy efficient, reducing the carbon footprint associated with cybersecurity operations and thereby supporting SDG 12.6. Building resilience also involves ensuring a sustainable approach to network intrusion detection systems, as discussed by [46]. Traditional methods struggle with the volume and complexity of modern network traffic. Emerging ML techniques show promise because they efficiently process large datasets with lower computational demand, supporting energy-efficient cybersecurity. By proposing architectures that minimize energy use and enhance operational efficiency, these techniques reduce the environmental impact, aligning with SDG 9.4, which aims to upgrade infrastructure and retrofit industries to make them sustainable with increased resource-use efficiency. Ref. [47] further complemented this by using software-defined networking in conjunction with AI techniques to enhance cybersecurity. By optimizing the energy consumption of ML models used in detecting cyberattacks, such as in crypto mining, [47] addresses the high energy demands of conventional cybersecurity solutions. This effort supports SDG 12.2, which focuses on achieving sustainable management and efficient use of natural resources. Moreover, resilience against adversarial attacks requires adaptive security measures to cope with emerging threats. These studies stress the need to ensure resilience on both digital and ecological fronts while also supporting the aims of SDG 9 and SDG 12.

3.2.4 Securing energy in space and renewables

The use of renewable energy is one of the top enablers for SDG 7 and SDG 13. The emphasis on environmentally sound cybersecurity within the renewable energy sector highlights a move toward security measures that both protect and sustain energy infrastructure. This is essential for the long-term viability of renewable energy systems, where technological security and environmental sustainability intersect. The congressional research report by [48] focuses on transitioning toward energy solutions driven by the imperative of green cybersecurity for the use and maintenance of physical infrastructure. Modernizing the grid is inherently tied to enhancing its efficiency and reducing its environmental impact, aligning with SDG 7.3 and SDG 13.2. The Space 4.0 framework [49] parallels these concerns. In a world where space technologies monitor and manage Earth's environmental systems, cybersecurity is not just about data; it is about securing the tools we rely on to combat challenges such as climate change. The application of AI and energy-efficient technologies here underscores the importance of cyber-resilience, ensuring that these critical systems can withstand attacks and continue their environmental work. This finding supports SDG 13.3. Space cybersecurity was reinforced by [50], who focused on threats to systems integral to both national security and civilian applications such as environmental monitoring. This suggests that the sustainable approach to cybersecurity within space systems—emphasizing minimal resource consumption and a low carbon footprint—could serve as a model for renewable energy cybersecurity practices. This approach is in line with SDG 12.2.

3.2.5 Sustainable cybersecurity in smart grids

Within the electrical grid system, the evolution of the smart grid illustrates a significant shift toward integrating sustainable cybersecurity. This is crucial for ensuring the security, efficiency, and ecological impact of power delivery systems. The congressional report [51] focused on smart grid transformation and highlighted the integration of renewable energy sources (solar, wind). This modernization, including digital communication and information systems, enhances energy management and stability by leveraging advanced communication infrastructures, such as those integrating the IoT and cloud computing, which enable real-time data exchange for improved system resilience [93, 94]. These advancements are key for sustainable cybersecurity because they ensure infrastructure resilience against disruptive cyberattacks, aligning with SDG 9.1, which focuses on developing quality, reliable, sustainable, and resilient infrastructure. Ensuring the stability of renewable-based systems is vital, supporting SDG 7.2, which aims to increase the share of renewable energy in the global energy mix [52] presented innovative approaches to smart grid security through the incorporation of cryptographic chips and advanced communication mechanisms such as SCADA, enhancing system robustness [93]. Furthermore, the integration of distributed energy resources (DERs) and demand response (DR) programs, supported by Internet of Things (IoT)-enabled sensors and smart meters, ensures efficient load balancing, reduces peak energy demands, and strengthens energy security while reducing greenhouse gas emissions [93]. These goals align with sustainability goals, as they provide high levels of security with minimal energy consumption, supporting the smart grid's aim to optimize energy use, which corresponds with SDG subtarget 7.3. Notably, field programmable gate arrays offer flexibility and energy efficiency by allowing for dynamic reconfiguration of security measures without complete system overhauls. In addition to technological advances, [53] emphasized the need to integrate sustainable and secure practices into education. The smart grid course they developed demonstrated this shift, focusing not only on technical power systems but also on cybersecurity measures that protect increasingly decentralized energy networks. Hands-on projects addressing smart technologies, metering, and microgrids underscore the practical applications of sustainable cybersecurity, supporting SDG 4.7.

3.2.6 The digital economy and cybersecurity

The importance of protecting both digital infrastructures and sustainability goals is more important today than ever before [54] outline the institutional frameworks needed for sustainable development within the digital economy. It advocates for green cybersecurity measures that minimize environmental impacts while protecting digital systems.

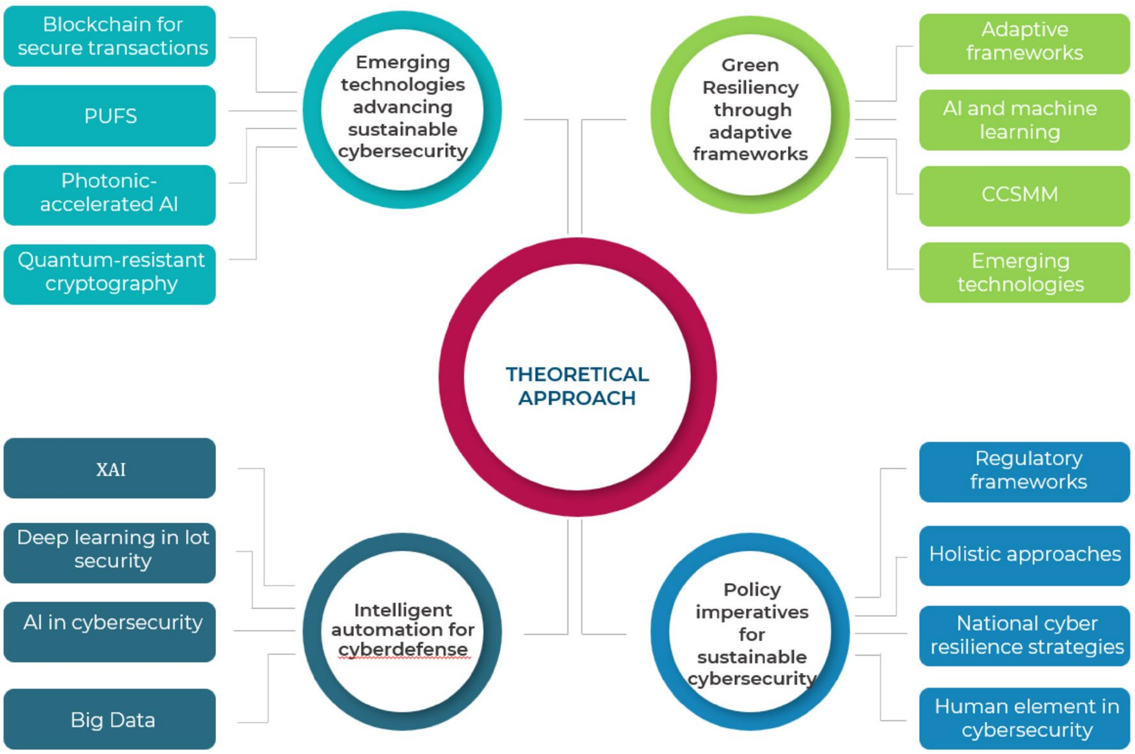
Blockchain for secure transactions
PUFS
Photonic-accelerated AI
Quantum-resistant cryptography
Emerging technologies advancing sustainable cybersecurity
Green Resiliency through adaptive frameworks
Adaptive frameworks
AI and machine learning
CCSMM
Emerging technologies
THEORETICAL APPROACH
XAI
Deep learning in Iot security
AI in cybersecurity
Big Data
Intelligent automation for cyberdefense
Policy imperatives for sustainable cybersecurity
Regulatory frameworks
Holistic approaches
National cyber resilience strategies
Human element in cybersecurity

Fig. 3 Theoretical approach

This includes building digital infrastructures with resilience in mind, using energy-efficient technologies, and reducing waste. Institutions such as the Institute of Digital Society play a vital role in regulating and guiding secure and resource-efficient practices. One of the crucial areas of relevance to the digital economy relates to healthcare, which in turn also impacts SDG 3. Digital health innovations demonstrate how technology can transform healthcare delivery into sustainable cybersecurity [55]. This includes the use of AI and electronic sensors to increase service efficiency and security while being environmentally sustainable, supporting SDG 3.8. The emphasis is on protecting health data and reducing the carbon footprint of traditional healthcare information systems. Challenges lie in ensuring accessibility and constant innovation to counter evolving cyber threats, delving into the methodologies of integrating security measures without adding environmental strain for digital transformations. They promote energy-efficient methods for securing data and network infrastructures, thereby reducing the cybersecurity carbon footprint, in line with SDG 12.6. It also highlights the role of cybersecurity in supporting the circular economy and promoting resource traceability and recycling through data integrity across digital product life cycles, aligning with SDG 12.5.

3.3 Theoretical approach (RQ3)

When the results of RQ1 and RQ2 are examined, the intersection of themes provides the following theoretical approaches for the sustainable cybersecurity landscape. We explore the multidisciplinary strategies and innovations needed to build robust digital defenses without compromising our sustainability goals from four perspectives. We will examine adaptive frameworks that prioritize resilience in a dynamic threat landscape, investigate policy shifts for coordinated protection, delve into the power of AI for intelligent threat detection, and explore how emerging technologies can offer both security and environmental efficiency, as shown in Fig. 3.

3.3.1 Green resiliency through adaptive frameworks

The rapid evolution of technology and the increasing complexity of cyber threats make it clear that traditional cybersecurity approaches are no longer sufficient. Sustainable cybersecurity frameworks are needed—frameworks that prioritize adaptability, resilience, and environmental consciousness. Studies exploring theoretical frameworks reveal several key strategies for achieving this goal. Studies [56, 57] advocate adaptive frameworks that embrace emerging technologies such as smart grids, the IoT, and blockchain—all of which are integrated in a way that supports sustainable development goals. The study by [56] motivated the need to develop a hybrid access control mechanism for realizing the vision of zero-trust for IoT-based systems. The notion of zero-trust offers an adaptive framework to ensure the sustainability and security of IoT systems. This framework leverages AI and machine learning for proactive threat defense. Moreover, the Community Cybersecurity Maturity Model offers a path for communities to improve their cybersecurity posture through systemic improvement and knowledge sharing. Sustainability also means protecting against environmental initiatives, making "green cybersecurity" vital. The study by [8] explores this link within the environmental goods and services sector, highlighting the threat to automation and interconnected systems within Industry 4.0. Robust cybersecurity has become a prerequisite for successfully integrating technological solutions with environmental strategies. Researchers propose a statistical—analytical approach to assess the current state of cybersecurity in this field and emphasize the need for policymakers to prioritize bridging the gap between current practices and those required for both sustainability and security. As organizations become increasingly complex, a unified and standardized approach to cybersecurity is crucial [58] built on established frameworks such as NIST and ISO 27001, emphasizing the need for integration, thorough risk assessments, synchronized people-process-technology management, and continuous adaptation. This comprehensive approach is essential for ensuring long-term security and resilience across large-scale environments.

Capability building is another cornerstone of sustainable cybersecurity. The Cybersecurity Capability Maturity Model (CM2) advocates advancing from basic to advanced capabilities, proactively evolving strategies to match threats, and prioritizing continuous education and awareness programs [59]. The development of standards and benchmarks for cybersecurity further strengthens this framework, ensuring proactive and well-informed protection. The rise of smart cities underscores the interconnected nature of technological advancement and cybersecurity [44] highlighted the need for comprehensive security protocols to safeguard data within these systems. Regulatory compliance and proactive participation in shaping new standards by key stakeholders such as governments, industry, and academia are critical to establishing the sustainable cybersecurity that smart cities require. Studies also suggest developing frameworks for adapting resilience concepts, applying assessment methods using reference metrics to monitor resilience against vulnerabilities and responses under stress [60]. This approach bolsters adaptability, a cornerstone of sustainable cybersecurity. Thus, there is an urgent need for sustainable cybersecurity frameworks. These frameworks must be adaptive, incorporate resilience concepts, consider environmental impact, balance technology with security, and promote standardization and knowledge sharing. The research provided offers valuable insights into building such frameworks better to safeguard our increasingly complex and interconnected digital world.

Adaptive cybersecurity frameworks address multiple sustainability challenges, aligning with various SDGs. By integrating smart grids and IoT systems securely, these frameworks contribute to SDG 7. Their emphasis on resilient digital infrastructure supports SDG 9 by enabling sustainable industrial practices. Furthermore, "green cybersecurity" protects environmentally focused systems, aiding SDG 13 through reduced energy usage and securing environmental initiatives. These adaptive systems also safeguard urban networks in smart cities, aligning with SDG 11. Finally, by fostering knowledge sharing and standardization (e.g., ISO 27001), they contribute to SDG 17 by enhancing global collaboration in cybersecurity standards.

3.3.2 Policy imperatives for sustainable cybersecurity

The sustainability of our digital world depends not only on technology but also on the policies that shape its use and protection. As cyber threats evolve, static approaches leave us vulnerable. Hence, a multifaceted approach that draws on studies that explore not only technological innovations but also the policy shifts vital for empowering organizations and individuals is necessary. One promising avenue lies in learning from the environmental movement. As suggested by [61], transparency and a shared responsibility approach can significantly strengthen cybersecurity practices. This perspective advocates for a holistic approach similar to environmental policy—building trust and resilience and ultimately contributing to long-term social and economic stability. The crucial role of coordinated policy is further highlighted by studies examining national cyber resilience strategies [62] revealed significant variances in the maturity and comprehensiveness of these strategies among Asia–Pacific countries. Their work argues that a "whole-of-society" approach, encompassing collaborative efforts from governments, the private sector, and individual citizens, is essential for building robust national cybersecurity frameworks. International collaboration to share knowledge and best practices is also seen as vital to strengthening collective cybersecurity postures.

The rise of e-commerce further emphasizes the urgency of securing the digital economy [63] underscore the need for a secure online environment to foster sustainable development and consumer trust. This requires integrating cybersecurity into the SDGs, with businesses actively contributing to creating safer digital spaces. This study highlights the need for policies that balance security, growth, and environmental sustainability across the digital economy. The human element is another crucial aspect of sustainable cybersecurity [64] emphasize the role that human capabilities play in achieving sustainable development. The study argues for integrating cybersecurity education and training programs into national and international security strategies. This approach recognizes cybersecurity as an interdisciplinary field encompassing not only technical expertise but also legal, organizational, procedural, and social dimensions. Continuous improvement in cybersecurity policy and practices is essential to keep pace with the dynamic nature of cyber threats and the increasing complexity of information and communication technologies. Additionally, [65] delves into policy formulation for renewable energy-focused smart grids—a critical component of sustainable energy systems. The study suggests multilayered policies informed by global experiences. These policies should encompass regulatory changes to foster innovation in cybersecurity technologies, establish strong cybersecurity governance strategies, and develop new business models that prioritize security and threat detection.

Importantly, the lack of standardization in cybersecurity risk, which is often difficult to quantify and report, consistently hinders informed decision-making [66] emphasized the need for regulatory frameworks with consistent disclosure requirements to enhance risk management. Furthermore, this study underscores the importance of integrating cybersecurity within the broader context of environmental, social, and governance factors to assess the full impact of these risks. In summary, sustainable cybersecurity policy necessitates an approach that prioritizes collaboration, transparency, and continuous improvement. Learning from environmental movements, integrating cybersecurity into the lifecycle of cybersecurity, and fostering human competencies are all crucial aspects of this endeavor. Policy frameworks must also evolve alongside technology, particularly in critical sectors such as renewable energy, to ensure secure and sustainable digital infrastructures for the future.

Policy shifts for sustainable cybersecurity play a transformative role in advancing the SDGs. Policies promoting transparency and accountability align with SDG 16 by building trust and ensuring equitable access to secure digital ecosystems. Regulatory frameworks for e-commerce enhance consumer trust, addressing SDG 8 by enabling secure economic transactions. Policies integrating cybersecurity in renewable energy grids bolster SDG 7 by fostering energy security. Furthermore, a "whole-of-society" approach to policy formulation strengthens global partnerships, directly contributing to SDG 17. Finally, by embedding cybersecurity education and training programs into national strategies, these policies support SDG 4, ensuring that cybersecurity competencies are widely disseminated.

3.3.3 Intelligent automation for cyberdefense

Artificial intelligence (AI) is redefining cybersecurity with its ability to learn and adapt to dynamic threat landscapes among evolving threats, seeking solutions that balance robust security with sustainability and adaptability. This section illustrates the capabilities achieved through the utilization of AI. A significant challenge in IoT security is the dynamic nature of the threat landscape and the devices themselves. Systems that can adapt to change are crucial. By using clustering algorithms for continuous learning, intrusion detection systems (IDSs) can maintain effectiveness against attack strategies while minimizing the need for energy-intensive retraining of models [67]. Similarly, machine learning algorithms can achieve approximately 90% accuracy in identifying malicious behavior within network traffic [68]. Further research into efficient algorithms holds the potential for greater sustainability by reducing the computational resources required for reliable threat detection. This focus on adaptability is central to sustainable security in the IoT. The hybrid AI-powered authorization model approach taken by [69] suggests the possibility of replacing traditional static security. This model continuously evaluates risk, empowering IoT systems to self-adjust their defenses in response to emerging cyberattacks and ensuring real-time protection without the need for frequent human intervention. The integration of big data analytics further enhances this adaptability, as advanced analysis of IoT and smart grid data enables predictive security measures. As highlighted in [97], the ability to manage large-scale data streams from smart grids allows for real-time monitoring and anomaly detection, a critical capability in protecting distributed systems from cascading failures.

In the complex landscape of smart cities, the need for both security and transparency is paramount. The integration of explainable AI (XAI) with machine learning models, as demonstrated by [70], addresses this duality. Techniques such as SHAP and LIME illuminate the decision-making processes within AI systems, fostering trust and allowing for the identification and correction of potential biases. This explainability becomes critical in applications tied to public infrastructure, where security failures can carry far-reaching consequences. Deep learning architectures are especially valuable in securing IoT environments. LSTM classifiers have an exceptional ability to detect cyberattacks targeting IoT devices in real time [71]. This proactive detection is essential given the sensitive nature of IoT data and the potential consequences of breaches. Moreover, the demonstrated efficiency of these AI-based approaches directly contributes to sustainability by minimizing resource consumption while ensuring responsiveness. Beyond the IoT, deep learning plays a key role in defending against advanced persistent threats (APTs), which are sophisticated attacks that often evade traditional detection [72]. Deep learning-based IDSs excel at this task, analyzing network traffic to identify subtle patterns indicative of APTs that less advanced methods would likely miss. The ability to optimize these systems for reduced power consumption and waste directly aligns with the goal of environmentally conscious cybersecurity.

Cybersecurity assessment is necessary to ensure that the systems work as desired and that no deviation from normal behavior due to attacks or faults is observed during the course of operations. Within the context of smart grids, cybersecurity assessments have been conducted for solar PV systems [73], renewable electricity markets [74], wind-integrated power systems [75], and nanogrids [76] via deep learning-based techniques. The ability to proactively ensure the resilience of these systems to cyberattacks through cybersecurity assessment is paramount to ensuring long-term sustainability.

Moreover, a crucial aspect of sustainable AI for cybersecurity is ensuring the robustness of machine learning models against data-driven attacks or unforeseen variations [77] explored strategies such as adversarial training and robust optimization to make models more resilient in the face of data manipulation or evolving threats. These techniques ensure that systems remain effective over time, furthering the sustainability of security solutions. In summary, the papers presented here showcase a strong trend toward sustainable, AI-powered cybersecurity. The emphasis on adaptability, cybersecurity assessment, real-time threat detection, resource efficiency, and explainability demonstrates a multifaceted approach to addressing cybersecurity challenges in a world where environmental concerns and digital threats intertwine.

The integration of AI and automation in cybersecurity solutions promotes multiple SDGs by advancing intelligent and resource-efficient cyber defense systems. AI-powered cybersecurity in renewable energy systems aligns with SDG 7 by optimizing energy usage and ensuring the resilience of smart grids. Real-time threat detection systems and resource-efficient AI models support SDG 12 by minimizing computational waste and enhancing operational efficiency. Deep learning architectures for protecting IoT devices also contribute to SDG 9 by fostering innovation and strengthening infrastructure. Explainable AI techniques improve transparency and accountability, supporting SDG 16 by addressing biases and building trust in critical systems. Finally, efficient cybersecurity mechanisms in smart cities bolster SDG 11 by ensuring secure, sustainable urban operations.

3.3.4 Emerging technologies and advancing cybersecurity

Without continuous hardware advancements, sustainable cybersecurity environments are impossible. Advances such as the use of photonically accelerated AI for cybersecurity in 6G networks [78] have led to improvements in speed and energy efficiency compared with traditional electronic systems, laying the foundation for sustainable high-performance threat detection [79] demonstrated the use of physically unclonable functions (PUFs). These exploit inherent manufacturing variations in hardware to create unique, tamper-resistant identifiers, protecting IoT devices in agriculture from cloning and unauthorized access. This approach aligns with sustainability goals by enhancing device longevity and security through intrinsic hardware properties. Building upon this, [79] introduces an architecture that leverages PUF-based trusted platform modules (TPMs)—secure hardware modules for storing cryptographic keys—alongside distributed ledger technology (DLT). This powerful combination ensures secure key storage, robust authorization, and a decentralized, tamper-proof record of system activity. The result is a secure-by-design approach that increases the resilience of IoT networks against a wide range of cyberattacks.

Blockchain exemplifies the potential of decentralized architectures in enhancing both security and operational efficiency. As highlighted in [95], blockchain facilitates trustless peer-to-peer systems, enabling secure and decentralized management of critical operations such as energy trading. This decentralized framework not only enhances security but also fosters economic and ecological benefits by supporting prosumer-driven energy transactions. By providing a secure platform for peer-to-peer (P2P) interactions, blockchain allows individuals and small-scale producers to actively participate in energy markets, creating value through transparency and reduced reliance on centralized systems [82]. Moreover, the integration of blockchain-based cryptocurrencies such as NRGcoin and SolarCoin, as discussed in [96], introduces innovative mechanisms for incentivizing renewable energy generation. These cryptocurrencies reward renewable energy producers, creating financial incentives to align energy production with sustainability goals. This approach also strengthens smart grid systems by promoting transparency and improving grid resilience through distributed, tamper-proof transaction records. By addressing challenges related to data privacy, transaction security, and system resilience, blockchain not only empowers a more localized and consumer-driven energy market but also positions itself as a critical technology for managing the complexities of decentralized energy systems.

Cloud computing offers scalability and advanced threat detection capabilities, but power consumption can be a significant concern. Several studies [80, 81] have explored strategies to optimize energy usage in cloud-based security systems, including smart scheduling algorithms for honeynets that maintain effective threat detection while minimizing resource usage. These innovations underscore the critical need for energy-conscious cybersecurity in the cloud era. As quantum computing matures, traditional cryptography may become vulnerable [83] advocated for a proactive stance by integrating quantum-resistant cryptography with blockchain. This future-focused approach aims to ensure that IoT networks remain secure against advanced decryption methods that quantum computers could enable.

Emerging technologies such as blockchain, quantum-resistant cryptography, and advanced hardware innovations directly align with several SDGs. Blockchain-powered decentralized systems for energy trading advance SDG 7 by fostering secure, localized renewable energy markets. Quantum-resistant cryptography secures future networks, aligning with SDG 9 by ensuring a resilient digital infrastructure. Hardware-based security innovations, such as PUF-based modules, protect IoT networks and enable systems such as secure agricultural monitoring systems that impact SDG 2. Cloud computing optimizations address SDG 12 by minimizing energy consumption in cybersecurity operations. Finally, by incentivizing renewable energy production through blockchain-based cryptocurrencies, these technologies promote SDG 13, a sustainable and secure digital ecosystem that aligns with environmental goals.

The research presented here highlights the multifaceted intersection of cybersecurity, technological innovation, and sustainability. By enhancing security at the hardware level, optimizing cloud-based defenses, leveraging the distributed trust of blockchain, and anticipating the challenges of quantum computing, smart systems can thrive safely and responsibly in the future. However, achieving net-zero goals demands a vigilant approach. The potential vulnerabilities [84] emphasize the need for the continuous development of robust cybersecurity measures. By prioritizing this two-pronged strategy—advancing capabilities and fortifying defenses—one can ensure that smart systems flourish in a secure and sustainable future without jeopardizing the environmental benefits they offer.

4 Implications and recommendations

4.1 Implications for practice

This research highlights the importance of integrating sustainable practices into daily cybersecurity operations. Professionals should focus on optimizing existing security systems to be more energy efficient, such as by configuring servers to enter low-power states when idle or adopting cloud services that are committed to using renewable energy sources. This could involve performing regular audits of energy usage across cybersecurity infrastructures to identify and address inefficiencies. Techno-security solution providers should be encouraged to innovate by designing inherently greener products. This includes creating software that requires less computational power, such as algorithms, cryptographic protocols, and hardware that has a smaller environmental footprint, such as energy-efficient firewalls or routers. Emphasizing the development of modular software that can be updated without significant energy costs could also contribute to more sustainable cybersecurity practices. Leaders within organizations should prioritize sustainability as a core aspect of their cybersecurity strategy. This means not only endorsing energy-efficient practices but also investing in training programs that raise awareness about the importance of sustainability in cybersecurity among employees. Encouraging the company-wide adoption of these practices can lead to significant reductions in the environmental impact of security operations. Practitioners should consider the implementation of system architectures that support sustainability, such as virtualization technologies that reduce the number of physical servers needed, thereby saving energy. Adopting a holistic approach to IT and network design that includes sustainability criteria in the decision-making process will help align cybersecurity practices with environmental objectives. By adopting these specific practices, professionals and leaders in the field can drive significant advancements in making cybersecurity operations more sustainable, which not only benefits the environment but also potentially reduces operational costs and enhances system performance.

4.2 Implications for policy

For policymakers, the implications of integrating sustainability into cybersecurity are significant and call for a proactive approach to legislating and incentivizing sustainable practices in the digital security field. Policymakers should work toward creating and enforcing standards that require cybersecurity products and practices to meet specific environmental criteria. This can include guidelines for energy efficiency, minimal use of hazardous materials, and extended product life cycles. Establishing clear standards will not only encourage the adoption of sustainable technologies but also ensure that environmental considerations are embedded in cybersecurity solutions from the ground up. Governments can play a crucial role by offering tax incentives, grants, or subsidies to organizations that implement sustainable cybersecurity measures. These incentives could be directed toward companies that invest in renewable energy sources for data centers, develop low-energy software solutions, or undertake significant efforts to reduce their carbon footprint in cybersecurity operations. Public funding should be allocated to research and development initiatives that focus on creating innovative, sustainable cybersecurity technologies. Supporting academic and private sector research can lead to breakthroughs in energy-efficient cybersecurity technologies and practices, which could set new industry standards. There should be wider and deeper collaborations between government bodies, private companies, and nonprofits to share knowledge, resources, and best practices related to sustainable cybersecurity. These partnerships can help standardize approaches to green cybersecurity across different sectors and geographies, ensuring the unified and effective implementation of sustainable practices. Policymakers should support educational programs and campaigns that raise awareness about the importance of sustainability in cybersecurity. This could involve updating the curriculum in educational institutions to include courses on energy-efficient IT and cybersecurity, as well as sponsoring conferences and workshops that focus on sustainable practices in the tech industry. Regulations that require cybersecurity hardware manufacturers to take responsibility for the end-of-life management of their products should be introduced. This can include mandates for recyclable materials, as well as take-back or recycling programs to ensure that cybersecurity hardware does not end up in landfills. Implementing these policy measures can significantly contribute to reducing the environmental impact of cybersecurity operations while fostering a market that values and promotes sustainability alongside security.

4.3 Recommendations for future research

To integrate a comprehensive roadmap for cybersecurity and sustainable cybersecurity practices, it is essential to adopt a structured, multidimensional approach that addresses the intricate interplay between technological advancements, environmental responsibilities, and organizational goals. This roadmap should serve as a guiding framework for aligning cybersecurity strategies with sustainability objectives, ensuring that digital systems are not only resilient against evolving threats but also operate in an environmentally conscious manner. Such an approach requires the integration of diverse elements, including the adoption of energy-efficient technologies, the formulation of forward-thinking policies, and the promotion of collaborative efforts among stakeholders. It also involves embedding sustainability principles into the lifecycle of cybersecurity measures, from design and implementation to evaluation and continuous improvement. By doing so, organizations can minimize their ecological footprint while safeguarding critical digital infrastructures. Furthermore, this roadmap should emphasize capacity building and foster a culture of awareness and engagement across all levels of society—policymakers, industry leaders, and the public. Research and innovation must play pivotal roles, with a focus on developing solutions that address both security challenges and environmental imperatives. Our recommendations include the following:

- Strategic assessment and alignment with the SDGs. This would involve the assessment of current cybersecurity practices and their impact on environmental sustainability. This would be followed by a focus on how cybersecurity initiatives can align with SDGs such as SDGs 7, 8, 9, 11, 12, 13, 16 and 17.
- Policy development and governance: Developing policies that encourage the use of green technologies and sustainable practices within cybersecurity frameworks. The government should establish governance structures that ensure compliance with both cybersecurity standards and environmental standards.
- Adopting sustainable technologies: Promotion of the adoption of energy-efficient hardware and software solutions. Research and development should be encouraged in new technologies that minimize environmental impact, such as blockchain, for energy-efficient transaction management.

- Capacity building and stakeholder engagement: Implement training programs focused on the importance of sustainable cybersecurity practices. Various stakeholders, including policymakers, industry leaders, and the community, should be encouraged to foster a collaborative approach to sustainable cybersecurity.
- Implementation of cybersecurity measures: Incorporate security at the design stage of products and infrastructure to ensure that they are robust against cyber threats and environmentally sustainable. Advanced monitoring tools are used to continually assess the effectiveness of cybersecurity measures and make adjustments on the basis of evolving threats and sustainability requirements.
- Evaluation and reporting: Regularly evaluate the impact of cybersecurity measures on organizational and environmental objectives. The outcomes and learning from cybersecurity initiatives should be documented, and improvements should be made on the basis of feedback and evolving conditions.

5 Conclusions

The advancement of sustainable cybersecurity practices promotes environmental sustainability and enhances computing system security and resilience. The textual analysis of the related corpus revealed significant alignment with SDGs, particularly SDG 7 (Affordable and Clean Energy), SDG 9 (Industry, Innovation, and Infrastructure), and SDG 8 (Decent Work and Economic Growth), highlighting key research focuses within cybersecurity's role in advancing sustainability and economic development. The analysis leveraging BERTopic modeling revealed six key themes that delineate the convergence of cybersecurity and sustainability, reflecting the relationship between securing digital infrastructures and advancing environmental goals. These themes include the integration of green cybersecurity measures in smart cities and the emphasis on sustainability within digital protection strategies. Particularly notable is the role of blockchain in enhancing cybersecurity for smart grids and SMEs, demonstrating its potential to reduce resource consumption and enhance data integrity in a decentralized manner. The dual necessity of smart cities highlights the need to safeguard digital systems while supporting sustainable urban development through energy-efficient practices. Furthermore, the emphasis on securing renewable energy sources and the modernization of smart grids illustrates the critical intersection of cybersecurity with energy sustainability. The theoretical underpinnings emphasize the necessity for adaptive cybersecurity frameworks that integrate advanced technologies such as AI, IoT, and blockchain, which are aligned with environmental sustainability goals. The role of intelligent automation and accelerated advancements in hardware in shaping future cybersecurity measures are evident in the literature. These technologies not only increase the speed and efficiency of cybersecurity systems but also enhance their sustainability by integrating secure, tamper-resistant hardware mechanisms that increase their longevity. Overall, the results presented in the study offer a robust foundation for future research and the implementation of sustainable cybersecurity practices that align with broader environmental and societal goals. This paper effectively bridges the gap between theoretical exploration and practical implications, setting a precedent for future studies in the field.

This study is not without limitations. First, the scope of literature from the selected database might not be comprehensive, potentially overlooking key research due to the exclusion of certain journals, conferences, or languages. Second, the reliance on literature and predefined keywords might have constrained the exploration of emerging or unclassified themes in sustainable cybersecurity. BERT topic modeling, despite its strengths in handling large datasets and uncovering themes, can be influenced by input data quality and its underlying assumptions. This study uses citations of publications within identified topics and topics as a proxy for impact, making it susceptible to the common limitations of citation analysis. These include citation biases such as affirmative citation bias, which can lead to the spread of misconceptions and overshadow critical or non-affirmative research [89]. To mitigate this, experts manually reviewed a subset of ten highly cited papers from each year, focusing on the introductions, methodologies, and results sections. Additionally, the complexities of SDG interconnections pose limitations in capturing them through a single mapping approach [90]. Future research could benefit from comparing our findings with results from multiple SDG mapping initiatives, such as the Aurora Network and the University of Auckland, offering a broader perspective and potentially strengthening future studies, although such a comparison falls outside the scope of this current review.

Acknowledgements We want to express our immense gratitude to our beloved Chancellor, Mata Amritanandamayi Devi (AMMA), for providing the motivation and inspiration for this research work.

Author contributions K.A.: Writing—original draft; review and editing. S.S.: Writing—original draft; review and editing. S.R.: Writing—original draft; review and editing. R.R.: Conceptualization, methodology, data curation, original draft, writing, review and editing.

Data availability Data is provided within the manuscript or supplementary information files.

Declarations

Competing interests The authors declare no competing interests.

References

1. Aftergood S. Cybersecurity: the cold war online. Nature. 2017. https://doi.org/10.1038/547030a.
2. Lu Y, Ma W, Shao L. Strategies to mitigate the environmental footprints of meat, egg and milk production in northern China. J Clean Prod. 2024;443:141027.
3. M. Mastroianni and F. Palmieri, "Energy-aware optimization of data centers and cybersecurity issues," in *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress*, 2022, pp. 1–7
4. Perkel J. How safe are your data? Many scientists want to keep their data and resources free; cybersecurity specialists want them under lock and key. Nature. 2010;464(7293):1260–2.
5. Bertino E, Casola V, Castiglione A, Susilo W. Security and privacy protection vs sustainable development. Comput Secur. 2018;76:250–1.
6. Li S, Tryfonas T, Li H. Future directions in cybersecurity research for IoT and cyber-physical systems: a focus on machine learning approaches. IEEE Internet Things J. 2018;5(6):4657–72.
7. Akana J, Islam BM, Patel K, Saini I, Chhipi-Shrestha G, Ruparathna R. Comparative eco-efficiency assessment of cybersecurity solutions. Environ Impact Assess Rev. 2023;100:107096.
8. Sulich A, Baird K, Rahman M, Bagis B. Corporate social responsibility and cybersecurity. Sustainability. 2021;13(2):718.
9. AL-Dosari K, Fetais N, Kucukvar M. A shift to green cybersecurity sustainability development: using triple bottom-line sustainability assessment in Qatar transportation sector. Int J Sustain Transp. 2023;17(12):1287–301.
10. Sachs JD, Lafortune G, Fuller G, Drumm E. Implementing the SDG stimulus. Dublin: Dublin University Press; 2023.
11. Leal Filho W, et al. When the alarm bells ring: why the UN sustainable development goals may not be achieved by 2030. J Clean Prod. 2023;407:137108.
12. D. S. Wall, "Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications for regulation and policing," *Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing*, 2017.
13. Hossain NUI, Rahman S, Liza SA. Cyber-susiliency index: a comprehensive resiliency-sustainability-cybersecurity index for healthcare supply chain networks. Decis Anal J. 2023;9:100319.
14. Rani P, Sharma P, Gupta I. Toward a greener future: a survey on sustainable blockchain applications and impact. J Environ Manage. 2024;354:120273.
15. de Bem Machado A, da Rocha FF, Dandolini GA, de Souza JA, Richter MF, de Moraes MTB. Blockchain as a technology for environmental sustainability: a bibliometric review. In: Sousa MJ, Workneh TC, Holtskog H, editors. Blockchain as a technology for environmental sustainability. Berlin: Springer; 2024. p. 133–59.
16. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. 2024.
17. J. Berr, WannaCry ransomware attack losses could reach 4 billion. 2017.
18. Humayun M, Niazi M, Jhanjhi NZ, Alshayeb M, Mahmood S. Cyber security threats and vulnerabilities: a systematic mapping study. Arab J Sci Eng. 2020;45:3171–89.
19. Andrade RO, Yoo SG, Tello-Oquendo L, Ortiz-Garcés I. Cybersecurity, sustainability, and resilience capabilities of a smart city. In: Visvizi A, del Hoyo RP, editors. Smart cities and the UN SDGs. Berlin: Springer; 2021. p. 181–93.
20. Polverini G, Gregorcic B. How understanding large language models can inform the use of ChatGPT in physics education. Eur J Phys. 2023. https://doi.org/10.1088/1361-6404/ad1420.
21. Ertmer PA, Ottenbreit-Leftwich AT, Sadik O, Sendurur E, Sendurur P. Teacher beliefs and technology integration practices: a critical relationship. Comput Educ. 2012;59(2):423–35.
22. Donnelly D, O'Reilly J, McGarr O. Enhancing the student experiment experience: visible scientific inquiry through a virtual chemistry laboratory. Res Sci Educ. 2013;43(4):1571–92. https://doi.org/10.1007/s11165-012-9322-1.
23. AlDaajeh S, Alrabaee S. Strategic cybersecurity. Comput Secur. 2024;141:103845.
24. Darem AA, Alhashmi AA, Alkhaldi TM, Alashjaee AM, Alanazi SM, Ebad SA. Cyber threats classifications and countermeasures in banking and financial sector. IEEE Access. 2023;11:125138–58.
25. Gugin NY, Villajos JA, Dautain O, Maiwald M, Emmerling F. Optimizing the green synthesis of ZIF-8 by reactive extrusion using in situ raman spectroscopy. ACS Sustain Chem Eng. 2023;11(13):5175–83. https://doi.org/10.1021/acssuschemeng.2c07509.

26. V. Ford, A. Siraj, A. Haynes, and E. Brown, "Capture the flag unplugged: An offline cyber competition," in *Proceedings of the Conference on Integrating Technology into Computer Science Education, ITiCSE*, Association for Computing Machinery, 2017, pp. 225–230. https://doi.org/10.1145/3017680.3017783.
27. Razaque A, Jararweh Y, Alotaibi B, Alotaibi M, Hariri S, Almiani M. Energy-efficient and secure mobile fog-based cloud for the internet of things. Futur Gener Comput Syst. 2022;127:1–13.
28. Mohammadpourfard M, Khalili A, Genc I, Konstantinou C. Cyber-resilient smart cities: detection of malicious attacks in smart grids. Sustain Cities Soc. 2021;75:103116.
29. Dinkova M, El-Dardiry R, Overvest B. Should firms invest more in cybersecurity? Small Bus Econ. 2023. https://doi.org/10.1007/s11187-023-00803-0.
30. Hammi B, Zeadally S, Nebhen J. Security threats, countermeasures, and challenges of digital supply chains. ACM Comput Surv. 2023;55(14):1–40.
31. Ali N, Ullah S, Khan D. Interactive laboratories for science education: a subjective study and systematic literature review. Multimod Technol Interaction. 2022. https://doi.org/10.3390/mti6100085.
32. Page MJ, et al. PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews. bmj. 2021. https://doi.org/10.1136/bmj.n160.
33. Achuthan K. Transactional distance theory in distance learning: past, current, and future research trends. Contemp Educ Technol. 2024;16(1):1–28. https://doi.org/10.30935/cedtech/14131.
34. Donthu N, Kumar S, Mukherjee D, Pandey N, Lim WM. How to conduct a bibliometric analysis: an overview and guidelines. J Bus Res. 2021;133:285–96. https://doi.org/10.1016/j.jbusres.2021.04.070.
35. Egger R, Yu J. A topic modeling comparison between lda, nmf, top2vec, and bertopic to demystify twitter posts. Front Sociol. 2022;7:886498.
36. Grootendorst M. BERTopic: neural topic modeling with a class-based TF-IDF procedure. arXiv preprint. 2022. https://doi.org/10.4855/arXiv.2203.05794.
37. Raman R, Pattnaik D, Lathabai HH, Kumar C, Govindan K, Nedungadi P. Green and sustainable AI research: an integrated thematic and topic modeling analysis. J Big Data. 2024;11(1):55.
38. Raman R, Lathabhai H, Mandal S, Kumar C, Nedungadi P. Contribution of business research to sustainable development goals: bibliometrics and science mapping analysis. Sustainability. 2023;15(17):12982.
39. Wang R, Liu C, Ma T. Evaluation of a virtual neurophysiology laboratory as a new pedagogical tool for medical undergraduate students in China. Adv Physiol Educ. 2018;42(4):704–10. https://doi.org/10.1152/advan.00088.2018.
40. Nour M, Chaves-Ávila JP, Sánchez-Miralles Á. Review of blockchain potential applications in the electricity sector and challenges for large scale adoption. IEEE Access. 2022;10:47384–418.
41. F. H. Zawaideh, W. Abu-Ulbeh, S. A. Mjlae, Y. A. B. El-Ebiary, Y. Al Moaiad, and S. Das, "Blockchain Solution For SMEs Cybersecurity Threats In E-Commerce," in *2023 International Conference on Computer Science and Emerging Technologies (CSET)*, Oct. 2023, pp. 1–7.
42. Dodge M, Kitchin R. Code and the city. London: Routledge; 2018.
43. Mijwil MM, Doshi R, Hiran KK, Al-Mistarehi AH, Gök M. Cybersecurity challenges in smart cities: an overview and future prospects. Mesop J Cybersec. 2022. https://doi.org/10.5849/MJCS/2022/001.
44. Hashem IAT, et al. Urban computing for sustainable smart cities: recent advances, taxonomy, and open research challenges. Sustainability. 2023;15(5):3916.
45. Dunn R, Carbo M. Modalities: an open letter to walter barbe, michael milone, and raymond swassing. Educ Leadersh. 1981;38(5):381–2.
46. K. C. Mouli, B. Indupriya, D. Ushasree, C. V Raghavendran, B. Rawat, and B. Madhu, "Network Intrusion Detection using ML Techniques for Sustainable Information System," in *E3S Web of Conferences*, EDP Sciences, 2023, p. 1064.
47. Mozo A, Karamchandani A, de la Cal L, Gómez-Canaval S, Pastor A, Gifre L. A machine-learning-based cyberattack detector for a cloud-based SDN controller. Appl Sci. 2023;13(8):4914.
48. R. J. Campbell. Electrical Power: Overview of Congressional Issues. 2013.
49. L. Petrovic. Motion planning in high-dimensional spaces. *CoRR*, vol. abs/1806.07457, 2018. http://arxiv.org/abs/1806.07457
50. K. Thangavel, J. J. Plotnek, A. Gardi, and R. Sabatini. Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity. in *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, Sep. 2022, pp. 1–10.
51. R. J. Campbell. The smart grid: Status and outlook. 2018.
52. D. N. Le, P. M. Kumar, and M. Kumar. Cybersecurity for smart cities: A brief review. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019, pp. 506–511.
53. M. Kuzlu, O. Popescu, and V. M. Jovanovic. Development of a Smart Grid Course in an Electrical Engineering Technology Program. 2021.
54. Zhidelev AV, Zhigun LA, Paytaeva KT. Institutional framework for the sustainable development of the digital economy. In: Ragulina JV, Khachaturyan AA, Abdulkadyrov AS, Zoya Sh, editors. Sustainable development of modern digital economy: perspectives from Russian experiences. Cham: Springer International Publishing; 2021. p. 275–83.
55. Barbazzeni B, Haider S, Friebe M. Engaging through awareness: purpose-driven framework development to evaluate and develop future business strategies with exponential technologies toward healthcare democratization. Front Public Health. 2022;10:851380.
56. S. Ameer, R. Krishnan, R. Sandhu, and M. Gupta, "Utilizing The DLBAC Approach Toward a ZT Score-based Authorization for IoT Systems," in *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*, 2023, pp. 283–285.
57. Sadik S, Ahmed M, Sikos LF, Islam AN. Toward a sustainable cybersecurity ecosystem. Computers. 2020;9(3):74.
58. J. Mtsweni, N. Gcaza, and M. Thaba, "A unified cybersecurity framework for complex environments," in *Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, 2018, pp. 1–9.
59. C. Barclay, "Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM 2)," in *Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world-Impossible without standards?*, 2014, pp. 275–282.

60. Serdar MZ, Koç M, Al-Ghamdi SG. Urban transportation networks resilience: indicators, disturbances, and assessment methods. Sustain Cities Soc. 2022;76:103452.
61. Shackelford SJ. Developing cyber peacefulness. Am Bus Law J. 2019;56(1):1–52.
62. D. I. Christine and M. Thinyane, "Comparative analysis of cyber resilience strategy in asia-pacific countries," in *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2020, pp. 71–78.
63. D'Adamo I, González-Sánchez R, Medina-Salgado MS, Settembre-Blundo D. E-commerce calls for cyber-security and sustainability: how European citizens look for a trusted online environment. Sustainability. 2021;13(12):6752.
64. Szczepaniuk EK, Szczepaniuk H. Analysis of cybersecurity competencies: recommendations for telecommunications policy. Telecomm Policy. 2022;46(3):102282.
65. Dehghani M, Liravi SM, Safdari M, Mozafari M, Rabiee M. Public policies for cyber security of sustainable dominated blockchain-based digital public services. Inf Process Manag. 2023;60(2):103187.
66. Karagozoglu AK. Novel risks: a research and policy overview. J Portf Manag. 2021;47(9):11–34.
67. M. M. Lopez, S. Shao, S. Hariri, and S. Salehi, "Machine learning for intrusion detection: Stream classification guided by clustering for sustainable security in IoT. In *Proceedings of the Great Lakes Symposium on VLSI 2023*. 2023, pp. 691–696.
68. Mouli KC, Indupriya B, Ushasree D, Raghavendran CV, Rawat B, Madhu B. network intrusion detection using ML techniques for sustainable information system. E3S Web Conf, EDP Sci. 2023. https://doi.org/10.1051/e3sconf/202343001064.
69. S. Ameer, R. Krishnan, R. Sandhu, and M. Gupta. Utilizing The DLBAC Approach Toward a ZT Score-based Authorization for IoT Systems. In *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*. 2023; 283–285.
70. Muna RK, Hossain MI, Alam MGR, Hassan MM, Ianni M, Fortino G. Demystifying machine learning models of massive IoT attack detection with explainable AI for sustainable and secure future smart cities. Internet of Things. 2023;24:100919.
71. Iwendi C, Rehman SU, Javed AR, Khan S, Srivastava G. Sustainable security for the internet of things using artificial intelligence architectures. ACM Trans Internet Technol (TOIT). 2021;21(3):1–22.
72. Oughannou Z, El Rhadiouini Z, Chaoui H, Bourekkadi S. Anomaly based intrusion detection system to detect advanced persistent threats: environmental sustainability. E3S Web Conf. 2023. https://doi.org/10.1051/e3sconf/202341201106.
73. Paul B, Murari KK, Patnaik U, Bahinipati CS, Sasidharan S. Sustainability transition for Indian agriculture. Sci Rep. 2023;13(1):7290.
74. D. T. Rizi, M. H. Nazari, M. Fani, and S. H. Hosseinian. Assessment of Cyber Security in Renewable Electricity Market Considering System Reliability Using Machine Learning. In *2023 8th International Conference on Technology and Energy Management (ICTEM)*, 2023, pp. 1–5. https://doi.org/10.1109/ICTEM56862.2023.10083662.
75. Liu X, Ospina J, Konstantinou C. Deep reinforcement learning for cybersecurity assessment of wind integrated power systems. IEEE Access. 2020;8:208378–94. https://doi.org/10.1109/ACCESS.2020.3038769.
76. Dafalla Y, Liu B, Hahn DA, Wu H, Ahmadi R, Bardas AG. Prosumer nanogrids: a cybersecurity assessment. IEEE Access. 2020;8:131150–64. https://doi.org/10.1109/ACCESS.2020.3009611.
77. Dunn C, Moustafa N, Turnbull B. Robustness evaluations of sustainable machine learning models against data poisoning attacks in the internet of things. Sustainability. 2020;12(16):6434.
78. Paolini G, Escorihuela MJ, Bellvert J, Merlin O, Pellarin T. PrISM at operational scale: monitoring irrigation district water use during droughts. Remote Sens. 2024;16(7):1116.
79. Bathalapalli VK, Mohanty SP, Kougianos E, Iyer V, Rout B. Pufchain 4.0: integrating PUF-based tpm in distributed ledger for security-by-design of IoT. Proc Great Lakes Symp VLSI. 2023;2023:231–6.
80. Pittman JM, Alaee S. A green scheduling algorithm for cloud-based honeynets. Front Sustain. 2023;3:1048606.
81. Riad K. Token-revocation access control to cloud-hosted energy optimization utility for environmental sustainability. Appl Sci. 2023;13(5):3142.
82. Moradi F, Abbaspour Asadollah S, Pourvatan B, Moezkarimi Z, Sirjani M. CRYSTAL framework: cybersecurity assurance for cyber-physical systems. J Log Algebraic Methods in Progr. 2024;139:100965. https://doi.org/10.1016/j.jlamp.2024.100965.
83. Muthukrishnan H, Suresh P, Logeswaran K, Sentamilselvan K. Exploration of quantum blockchain techniques towards sustainable future cybersecurity. In: Dhanaraj RK, Rajasekar V, Islam SKH, Balusamy B, Hsu C-H, editors. Quantum blockchain. Hoboken: John Wiley & Sons, Ltd.; 2022. p. 317–40.
84. H. Yuan and S. Li. Cyber Security Risks of Net Zero Technologies. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)*. 2022, pp. 1–11. https://doi.org/10.1109/DSC54232.2022.9888883.
85. Raman R, Gunasekar S, Dávid LD, Nedungadi P. Aligning sustainable aviation fuel research with sustainable development goals: trends and thematic analysis. Energy Rep. 2024;12:2642–52.
86. Raman R, Pattnaik D, Hughes L, Nedungadi P. Unveiling the dynamics of AI applications: a review of reviews using scientometrics and BERTopic modeling. J Innov Knowl. 2024;9(3):100517.
87. Raman R, Sreenivasan A, Suresh M, Nedungadi P. Mapping biomimicry research to sustainable development goals. Sci Rep. 2024;14(1):18613.
88. Borchardt, S., Barbero Vignola, G., Buscaglia, D., Maroni, M. and Marelli, L., Mapping EU Policies with the 2030 Agenda and SDGs, EUR 31347 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-60474-7, https://doi.org/10.2760/87754, JRC130904
89. Letrud K, Hernes S. Affirmative citation bias in scientific myth debunking: a three-in-one case study. PLoS ONE. 2019;14(9):e0222213.
90. Raman R, Nair VK, Nedungadi P. Discrepancies in mapping sustainable development goal 3 (good health and well-being) research: a comparative analysis of scopus and dimensions databases. Sustainability. 2023;15(23):16413.
91. Raman R, Sreenivasan A, Ma S, Patwardhan A, Nedungadi P. Green supply chain management research trends and linkages to UN sustainable development goals. Sustainability. 2023;15(22):15848.
92. Raman R, Martin H, Ray S, Das D, Nedungadi P. Exploring sustainable development goal research trajectories in small island developing states. Sustainability. 2024;16(17):1–25.

93. Ghorbanian M, Dolatabadi SH, Masjedi M, Siano P. Communication in smart grids: a comprehensive review on the existing and future communication and information infrastructures. IEEE Syst J. 2019;13(4):4001–14.
94. Singh, N., & Paliwal, P. (2022, December). Planning and monitoring of smart grid Architecture using Internet of Things. In *2022 IEEE 6th International Conference on Condition Assessment Techniques in Electrical Systems (CATCON)* (pp. 12–16). IEEE.
95. Yuan Y, Wang FY. Blockchain and cryptocurrencies: model, techniques, and applications. IEEE Trans Syst, Man, Cybern: Syst. 2018;48(9):1421–8.
96. Ghorbanian M, Dolatabadi SH, Siano P, Kouveliotis-Lysikatos I, Hatziargyriou ND. Methods for flexible management of blockchain-based cryptocurrencies in electricity markets and smart grids. IEEE Trans Smart Grid. 2020;11(5):4227–35.
97. Ghorbanian M, Dolatabadi SH, Siano P. Big data issues in smart grids: a survey. IEEE Syst J. 2019;13(4):4158–68.