International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0156
e ISSN: 2584-2854
Volume: 04 Issue: 04 April 2026
Page No: 1018 - 1023

Green Cybersecurity in Healthcare: Integrating Digital Security and Environmental Sustainability—A Narrative Review

Nisha Papachan[1], Tini F Peter Hose[2], Mallapalli Akanksha Reddy[3], Nihal nasim[4], Muhammed Shiras kk[5], Athira. S[6]

[1]Associate Professor, Dept of Hospital Administration, Yenepoya Deemed to be University, Bangalore

[2,3,4,5,6PG]MHA, Dept of Hospital Administration, Yenepoya Deemed to be University

Emails: *nishapapachan.blr@yenepoya.edu.in[1],39139@yenepoya.edu.in[2], 39143@yenepoya.edu.in [3],39170@yenepoya.edu.in[4], 39171@yenepoya.edu.in[5],39166@yenepoya.edu.in[6]*

Abstract

The accelerated digitalization of the healthcare industry has altered service delivery in healthcare. Such technologies as electronic health records, artificial intelligence (AI), telemedicine, and the Internet of Medical Things (IoMT) have a major role. These innovations are not only more effective and contribute to better patient outcomes but also introduce severe cybersecurity threats and environmental concerns. Cyberattacks are ideal targets for healthcare systems. These risks include data breaches, ransomware, and compromised medical devices due to the high sensitivity and value of the patient data. Simultaneously, as the digital base expands (data centers and AI), it consumes more energy, generates more carbon emissions, and more electronic waste, exacerbating environmental issues. This narrative literature review examines the concept of green cybersecurity in healthcare, a combination of security strategies and environmental sustainability principles. The results indicate that green approaches to cybersecurity, such as energy-efficient algorithms, AI-assisted threat detection, blockchain-based data protection, and green data center configurations, can help increase system resilience and minimize environmental impacts. Also, it is essential to bridge the gap between cybersecurity plans and global sustainability models, such as the United Nations Sustainable Development Goals, to ensure the sustainability of healthcare in the long term. The challenges mentioned above demand cross-disciplinary teamwork, policy-making, and sustainability by going digital. To sum up, green cybersecurity is a significant development in the healthcare sector. It enables the development of safe, effective and green systems. The future directions of research ought to be related to scalable, energy-efficient cybersecurity frameworks, balancing between sustainability and security performance objectives.

Keywords: *Digital sustainability, Energy-efficient computing, Green IT in healthcare, Healthcare cybersecurity, Sustainable cybersecurity*

1. Introduction

Sustainability is one of the most significant issues in the 21st century that we are witnessing. Ensuring good health and well-being is one of the primary Sustainable Development Goals (SDGs) designed to support the healthy lifestyle and well-being of all people, regardless of their age. This includes offering affordable, environmentally friendly healthcare to the larger community. Optimal health and wellness objectives are achieving equitable health outcomes and robust health systems. It also sheds light on the need to consider sustainable health concerns as part of policy frameworks in developing countries, in order to address the socioeconomic determinants of health. ICTs are important to improving patient access, quality of care and efficiency of the system in healthcare reform. This change of direction also demonstrates the importance of promoting digital leadership, cybersecurity, sustainability, creativity, and accessibility. The implementation of more sophisticated ICT, which is referred to as digital transformation, is a difficult task to carry out in healthcare systems. Nevertheless, integration, application design and security measures are a challenge. There was a lot of concern among the

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0156
e ISSN: 2584-2854
Volume: 04 Issue: 04 April 2026
Page No: 1018 - 1023

masses and even medical professionals regarding this true world epidemic of the digital age [4]. Hence, this situation, in addition to causing concern, gave the world nations the opportunity to improve their health care systems. Healthcare is faced with a twofold challenge to protect data against broad-scale cyber-attacks caused by the spread of Electronic Health Records (EHR), Internet of Medical Things, cloud-based health information systems, and telemedicine systems, as well as a surge in carbon emissions globally due to improved digital infrastructure and data centers. Intelligent healthcare has developed as a result of the global lack of health workers and the development of the latest technology in the medical sphere. Leadership in a healthcare setting is very important in the effective management of resources and the success of healthcare operations [10]. Healthcare management should be aware of the workforce requirements in order to improve the quality of clinical services and environmental sustainability. This is through the promotion of a corporate culture that places focus on social and environmental accountability and energy resource management. With effective green leadership being coupled with different technologies, this could influence behavioral change in all the patients in the hospital, which promotes a friendly and secure atmosphere and helps in maintaining the ecological balance. The purpose of this narrative review is to summaries the current knowledge of green cybersecurity, as well as to discuss a future in which the environment and digital security merge to achieve an improved future. The study reviews the latest articles, trying to determine the technology that enables green security of the cyber environment, analyses their success and evaluates the challenges and opportunities in this area.

1.1. Defining Cybersecurity

Green cybersecurity is the concept of integrating sustainability objectives with cybersecurity policy, emphasizing the provision of eco-friendly solutions, minimizing carbon footprint, and guaranteeing less energy consumption [1]. Artificial intelligence (AI) and machine learning (ML) can be incorporated into cybersecurity activities to provide effective means of improving cybersecurity and improving energy efficiency. Cybersecurity has been changing significantly because of AI and ML, allowing the creation of sophisticated algorithms capable of identifying and eliminating cyber threats [2]. The AI and ML may quickly process large volumes of information, identify trends and anomalies, and respond to possible risks automatically. This is not only effective in crafting sustainable and effective cybersecurity measures but it also encourages global sustainability. By following these measures, organizations will be able to manage electronic waste (e-waste) related to cybersecurity activities and reduce carbon emissions. Studies indicate that energy-efficient cybersecurity is an effective option when enhancing security and, at the same time, saving resources.

1.2. Importance of integrating sustainability into healthcare

Healthcare is experiencing serious challenges in the implementation of sustainable cybersecurity. Sustainable development is the global outlook of the national and local progress. The United Nations, the World Bank, and the United Nations Development Program (UNDP) are among the most successful organizations in the world that are avidly following the SDGs and formulating informed actions in this domain. Sustainable development is also affected by different external and internal factors in emerging and growing economies. The SDGs require the availability of accessible and quality public services, especially in developing and poor nations. Larsson [5] discussed the state governance and the policy making as one of the most important factors with respect to performance and delivery of services by institutions in South Asian countries. Berniak-Wozyn[3] also looked at how the ability of a state and prudent management of its resources could guarantee sustainable health and reduce the gap in development. In its universal approach to digital health care, the World Health Organization (WHO) suggests an understanding of the notions of accessibility, privacy, interoperability, confidentiality, transparency, security, scalability, and replicability. In order to improve the global

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0156
e ISSN: 2584-2854
Volume: 04 Issue: 04 April 2026
Page No: 1018 - 1023

healthcare system, the utilization of principle-based assessment criteria to various digital solutions (such as IoT, Blockchain Technology, and cloud) and the integration issues, including design and security, have to be explored. Therefore, in the current paper, we investigate the digital transformation in healthcare with regard to its aspects, applicability, and advantages. We also discuss the integration and design challenges and we categorize the security and privacy challenges. We further examined the use and application of various ICT technologies and blockchain in healthcare systems, as well as some unsolved problems that pose significant challenges.

1.3. Conformity to Sustainable Goals

ICT inclusion and related investments are currently trending topics in order to improve sustainable public services [2]. All countries, regardless of their level of development, have introduced IT implementation services since the SDGs first came into being. Research indicates that the wealthier countries are putting a lot of money into electronic governance systems. However, the capacity of the state and the development of ICT are crucial elements of this adoption. Developing or growing countries do not meet these requirements and do not have a working electronic governance system. The green cybersecurity helps in supporting different United Nations Sustainable Goals (SDGs), especially SDG 3 (Good Health and Well-being), SDG 9 (Industry, Innovation, and Infrastructure), SDG 12 (Responsible Consumption and Production), and SDG 13 (Climate Action). According to the case study presented by Sidii about Ghana, health systems facilitate the connection between digital security, resilience, and sustainability in the healthcare systems of low and middle-income countries. In designing sustainable security solutions, there is a need to consider the capacity of the personnel, the limits on infrastructure, and the need to ensure continuity of services in situations where there are limited resources. The development of cybersecurity in the healthcare industry resembles the ongoing battle against the constantly evolving threat environment. The issue of cybersecurity is extremely significant because the healthcare industry is embracing the use of digital technologies. Every stakeholder involved, which includes healthcare providers, technology companies, legislators, and the patients, should join forces to protect their information and healthcare systems. The future of cybersecurity in healthcare may be marked by a culture of cybersecurity awareness within the healthcare setting, a well-developed regulatory framework, and modern technologies.

2. Method

The selected articles were based on the topic of green cybersecurity in healthcare settings in terms of interventions and frameworks. Analysis based on cybersecurity and its environmental impact. The results of the synthesis were thoroughly formed based on qualitative and quantitative data to identify the emergence of common themes and gaps within existing literature and the problem of the overlap of cybersecurity and environmental responsibility in healthcare.

3. Results and Discussion

3.1. Digital Shift in Healthcare

Digital transformation is a widespread term in companies that refer to the integration of new data and technology to improve operations and customer experience. The adoption of innovative digital technologies in health systems has altered the ways the healthcare industry and its aspects (medicine, insurance, supply chain) process the management of urgent medical treatment and health issues. The interest of the UN system towards sustainable development, which involves the economic, social, and environmental dimensions of countries, is paying more attention to global health problems.

WHO defines e-health as the use of ICT in the healthcare sector to advance diagnosis and treatment. The digital health paradigm involves the application of ICT to healthcare and health-related purposes in all types of settings, including the healthcare industry and the broader community. Technological changes in the medical sector are not only solving issues related to medical care, economic development, and demands of the aging population but also opening new markets and business structures [6].

3.2. Healthcare Industry and its contribution

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0156
e ISSN: 2584-2854
Volume: 04 Issue: 04 April 2026
Page No: 1018 - 1023

to carbon emission and environmental waste

Since the healthcare business is a necessity and is 24/7, its energy needs are constant and substantial. Studies reveal that a significant percentage of carbon emissions to the world is caused by healthcare institutions. Lighting, heating, cooling, and IT infrastructure as well as medical devices, consume a lot of energy in hospitals, research, and healthcare IT systems. Data centres are among the most energy-consuming elements of healthcare systems when powered by non-renewable energy sources, and the consumption of large amounts of electricity is also necessary, which contributes to greenhouse gas emissions. The IT systems that use unsustainable energy sources also increase carbon emissions. The problem of controlling and reducing the environmental impact of the healthcare sector becomes more urgent with the expansion and introduction of more modern technologies into it. Innovative uses of cybersecurity [7]. Although cybersecurity has always been a very essential factor in the digital space, newer opportunities and challenges have emerged as sustainable digitalization has become a major topic of concern. The innovations in cybersecurity that follow are associated with sustainable digitalization

- Green cybersecurity: As people become more worried about the effects of technology on the environment, the concept of green cybersecurity is becoming an important part of sustainable digitalization. This entails coming up with cybersecurity solutions with low carbon emissions and those that consume low energy. [4]
- Smart city cybersecurity: Cybersecurity measures are crucial in the face of an even more connected and digitalized urban environment. Cybersecurity should be a priority in the smart city projects to ensure sustained digitalization of cities.
- The cybersecurity of renewable energy: The higher the adoption of renewable energy, the greater the demand for cybersecurity measures against cyber threats. Powerful cybersecurity solutions should be developed to safeguard renewable energy infrastructure in a sustainable way of digitalization.
- Sustainable supply chains in cybersecurity: As numerous customers shift to environmentally friendly products; sustainable supply chains are growing in significance. Cybersecurity is necessary to make these supply chains secure and sustainable.

Sustainable digitalization requires a comprehensive approach to cybersecurity, consideration of the environmental impact of technology and the effectiveness and sustainability of cybersecurity measures.

3.3. Overview of ongoing healthcare Green Cybersecurity initiatives

Cybercrimes in healthcare institutions are on the rise due to the sensitive nature of the information that encompasses patients and healthcare, which leads to negative consequences. All these cyber threats are often associated with high reliance on sophisticated technologies, wearable, implantable, gastrointestinal, and biomedical sensors, and smart devices, mobile healthcare applications, and smart medical devices aimed at enhancing healthcare services. It is therefore important to formulate, implement and invest towards robust cybersecurity measures in intelligent healthcare networks, owing to increased cyber-attacks. Mijwil et al. define cybersecurity in smart healthcare as actions taken, policies, processes, technologies, or processes used by healthcare organizations to defend their technological assets against cyber-attacks, unauthorized users, malpractices, leaking, or service disruptions, the confidentiality, integrity, and accessibility of healthcare data. Cybersecurity can provide secure communication, help with verification and authorization of users in the field of healthcare, help with risk analysis and management, prevent attacks and medical fraud, provide quality patient care, secure healthcare networks, manage complex treatments including better care of the patient, secure access to healthcare, improve services and patient outcomes, facilitate and manage activities daily in the

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0156
e ISSN: 2584-2854
Volume: 04 Issue: 04 April 2026
Page No: 1018 - 1023

healthcare field, and plan and supervise treatment procedures. Further, it has been used in network security, application security, information security, operational security, disaster recovery, business continuity and end user training. In order to ensure reliable and trustworthy exchange of healthcare information, some attention should be paid to business continuity, and cybersecurity principles (such as privacy, confidentiality, integrity, availability, authenticity, auditing, non-repudiation, secure data transfer, and access control) should be considered. SHS will comply with security regulations and implement protection measures that guarantee the security of the healthcare information, such as confidentiality, the integrity, the availability of security principles, privacy, authorization, etc.

3.4. Cybersecurity issues in Healthcare

According to the assessment, controlling endpoint devices, securing remote work, human errors, the lack of security awareness, ineffective risk assessment on senior levels, lack of business continuity plans, poor coordination in incident response, financial and resources constraints, and vulnerability of medical systems are the key cybersecurity issues in the health sector. The use of virtual private networks (VPN) and enterprise remote desktop protocols to access internal networks by healthcare professionals has become mandatory since remote work has become a necessity to provide healthcare services. But these are not without risks, which opponents are hoping to capitalize on. Many endpoint devices, such as many patient monitoring tools that connect to the outdated, dispersed networks or the internet, are not usually patched. With workers being concentrated on saving lives and adjusting to new settings and technologies, the chance of human error rises. Employees who experience prolonged stress due to abrupt changes in workplace procedures are more likely to engage in fraudulent behaviors and mistakes. The healthcare sector should improve its knowledge of cybersecurity to safeguard itself and its patients against potential cyber threats, including ransomware and phishing[8]. The health care workers also need additional training and support, including cybersecurity education about pandemics, laid out protocols and guidance about new procedures and technologies, since they were neither prepared or trained in situations of pandemics. Security is not provided by the vendors in the healthcare supply chain. According to current studies, the dependency on vendors, lack of encryption settings, and the failure to monitor the sharing and exchange of health information with third parties and international collaborators are the major security threats to the continuity of business activities. There is a deficit of incident response and recovery as healthcare organizations have not adopted an efficient and reliable backup system.

Conclusion

Sustainable development is an issue that has been analyzed in depth in the health sector ever since the 1972 United Nations Conference on the Human Environment in Stockholm. This industry is crucial to achieving the Sustainable Development Goal and targets of good health and well-being of the UN. Meanwhile, the healthcare industry contributes to 4.4 per cent of world greenhouse emissions. As a result, green and sustainable development of the health sector is a very complicated, interwoven and complicated issue. There is also a growing need of ecologically friendly healthcare in the past ten years due to the fact that hospitals and other medical institutions use a lot of resources to provide healthcare services (like water and electricity) and medical waste that is hazardous and pharmaceutical.
One of the most important issues of sustainable smart healthcare is cybersecurity. It is closely related to the details and fine points which are to be treated with the highest care and imagination. Researchers have highly delved into new techniques, developed a list of classification of cybersecurity threats in smart healthcare context methodically, discussed protection strategies, and outlined the essential purpose of cybersecurity in smart healthcare sustainability. The various aspects of cybersecurity in smart healthcare present improvements and some tough issues that are yet to be solved. The attacks and the risks of cyber threats increase along with intelligent healthcare technologies and demand constant modifications and careful attention However, despite all the complexity,

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0156
e ISSN: 2584-2854
Volume: 04 Issue: 04 April 2026
Page No: 1018 - 1023

there is still hope due to a promise of innovation, teamwork and the work towards a safer and more resilient future. Technology, knowledge, and social efforts are the sources that can help to build the foundations of intelligent healthcare and make it safe and sustainable at the same time. The researchers are of the opinion that the path to the sustainability of smart healthcare is associated with the attainment of cybersecurity excellence. With the knowledge gained out of this review and by acknowledging cybersecurity as an essential pillar of sustainable healthcare, the scientists will be able to cope with the issues of the digital age and ensure that the advantages of smart healthcare are brought safely, robustly, and equitably to all people.

Suggestions

Increase Investment in Sustainable Technologies: Governments and healthcare organizations should heavily invest in the implementation of renewable energy, energy-saving appliances, and building environmentally friendly buildings. Endorsing Sustainable Healthcare Policies: Faculty and healthcare management ought to offer specific subsidies and incentives to encourage the use of environmentally friendly technologies and buildings. Education on Climate Health: Improving knowledge about climate change: To improve advocacy and awareness of climate change among ordinary citizens and medical staff. Improve Climate-Resilient Healthcare Systems: Public health and healthcare organizations should introduce climate adaptation measures, such as planning to prevent climate-sensitive illnesses and making infrastructure resistant to storms and other adverse environmental effects.

References

[1]. Oluwabunmi Layode et al., The role of cybersecurity in facilitating sustainable healthcare solutions: Overcoming challenges to protect sensitive data, International Medical Science Research Journal, Volume 4, Issue 6, June 2024
[2]. Hafiz Syed et al., Impact of cybersecurity measures on improving institutional governance and digitalisation for sustainable healthcare, PLOSE ONE Journal
[3]. Berniak-Woźny J, Rataj M, Towards Green and Sustainable Healthcare: A Literature Review and Research Agenda for Green Leadership in the Healthcare Sector, International Journal of Environmental Research and Public Health, 04 Jan 2023
[4]. Ying He et al., Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review, Journal of Medical Internet Research
[5]. Shankha Shubhra Goswami et al., The role of cyber security in advancing sustainable digitalisation: Opportunities and challenges, Journal of Decision Analytics and Intelligent Computing, Vol. 3 issue 1, (2023)
[6]. Khizar Hameed et al., Digital transformation for sustainable health and well-being: a review and future research directions, Springer Nature Link
[7]. Guma Al et al., Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles, Mesopotamian journal of CybersecurityVol.4
[8]. Adam Thawbaan et al., Sustainable Cybersecurity in Healthcare An AI-Integrated Risk and Resilience Framework, American Journal of Research and Innovation (AJMRI), Volume 4 Issue 4, Year 2025