



This is a peer-reviewed, final published version of the following document and is licensed under Creative Commons: Attribution 4.0 license:

**Wynn, Martin G ORCID logoORCID: <https://orcid.org/0000-0001-7619-6079> and Bechkoum, Kamal (2024) Emerging Technologies, Sustainable Engineering and Cybersecurity in the Digital Age. *Sustainability*, 16 (17). p. 7364.  
doi:10.3390/su16177364**

Official URL: <http://dx.doi.org/10.3390/su16177364>

DOI: <http://dx.doi.org/10.3390/su16177364>

EPrint URI: <https://eprints.glos.ac.uk/id/eprint/14332>

#### **Disclaimer**

The University of Gloucestershire has obtained warranties from all depositors as to their title in the material deposited and as to their right to deposit such material.

The University of Gloucestershire makes no representation or warranties of commercial utility, title, or fitness for a particular purpose or any other warranty, express or implied in respect of any material deposited.


The University of Gloucestershire makes no representation that the use of the materials will not infringe any patent, copyright, trademark or other property or proprietary rights.

The University of Gloucestershire accepts no liability for any infringement of intellectual property rights in any material deposited but will remove such material from public view pending investigation in the event of an allegation of any such infringement.

PLEASE SCROLL DOWN FOR TEXT.

Editorial

# Emerging Technologies, Sustainable Engineering and Cybersecurity in the Digital Age

Martin Wynn <sup>1,\*</sup>  and Kamal Bechkoum <sup>2</sup><sup>1</sup> School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham GL50 2RH, UK<sup>2</sup> Faculty of Design, Informatics and Business, Abertay University, Dundee DD1 1HG, UK;  
kbechkoum@gmail.com

\* Correspondence: mwynn@glos.ac.uk

This Special Issue includes papers on various aspects of emerging technologies and cybersecurity, and the theme of sustainable engineering is also interwoven within some of these articles. As this Special Issue has been put together, global events have highlighted the pace and scale of technological change. ChatGPT has come to the fore in this period as educators, administrators, and the legal profession try to assess the potential of this tool [1], and the impact of other AI applications in industry and within society at large. The wars in Ukraine and the Middle East highlight the significance of advancements in technologies, with drones, guided bombs, and artillery utilising digital technologies as an integral component of modern warfare [2]. The CrowdStrike bug that brought down the Windows operating system in many organisations around the world [3] again highlighted the scale of cybersecurity threats and vulnerabilities. Meanwhile, the growing significance of the metaverse and quantum computing from beyond the technology horizon brings new possibilities and questions regarding digitalisation and its manifestation in business and society. As Rotolo et al. noted, these technologies have “the potential to exert a considerable impact on the socio-economic domain(s), which is observed in terms of the composition of actors, institutions and patterns of interactions, along with the associated knowledge production processes”, but that the “most prominent impact, however, lies in the future” [4] (p. 4).

The first three papers in this collection do indeed concern current and future applications of emerging technologies. The focus of the paper by Suleiman and Jung, however, is within the world of archaeology, and more specifically, on the detection of ancient artefacts. The authors identify the challenge of finding engraved characters on these objects and the need to develop tools that are accurately tailored to detect them. They examine different data augmentation techniques and conclude that Styleformer-ART-generated images perform better than other reviewed image-generation models. In the following paper, Tang, Cai, and Xiao put forward a method for the systematic and quantitative evaluation of emerging technologies. They use bibliometrics, most notably paper citation networks, to assess changes in knowledge across the evolutionary course of specific technologies. This represents a novel approach to measuring the technological progression of emerging technologies that will be of interest and value to IT practitioners and policymakers. This is followed by Mollajafari and Bechkoum’s seven-layer taxonomy of blockchain, which involves classification of the critical cybersecurity threats and vulnerabilities inherent in smart contracts. A seven-layer architecture is set out, in which the related security risks and corresponding countermeasures are specified. A taxonomy then establishes the inter-relationships between the vulnerabilities and attacks in a smart contract, and a model application is put forward that outlines the security risks within the contract layer.

Cybersecurity issues are considered in the following three articles: Mehdi Hosseinzadeh and his colleagues focus on IoT environments and suggest a new design for a secure authentication protocol, which is a critical part of access control for many applications.



**Citation:** Wynn, M.; Bechkoum, K. Emerging Technologies, Sustainable Engineering and Cybersecurity in the Digital Age. *Sustainability* **2024**, *16*, 7364. <https://doi.org/10.3390/su16177364>

Received: 6 August 2024

Accepted: 8 August 2024

Published: 27 August 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Building upon previous research, their protocol redesign is better able to withstand a range of vulnerabilities discussed in the paper. The Internet of Things is also the central theme in the paper by Zulfigar Ali and colleagues, but here it is studied in an urban environment, where smart cities rely on IoT devices as one of the key elements of their ICT infrastructure. The study identifies the key challenges involved in implementing existing IoT middleware and puts forward a novel IoT middleware product for smart city applications—the Generic Middleware for Smart City Applications (GMSCA). In a third paper on cybersecurity, Ozdemir, Wynn, and Metin examine the country-of-origin (COO) concept in the context of the import and export of digital products and the associated security risks. The article develops a 19-parameter framework for assessing the COO of digital products and concludes that new processes and policies are urgently required to enhance the cyber and information security of such products. This has been highlighted by a series of incidents in which national security has been threatened by the vulnerability of digital products developed or manufactured overseas, including recent concerns regarding new software developed in Belarus and deployed in the UK's nuclear-powered submarine fleet [5].

The two review papers in this Special Issue concern aspects of sustainable engineering and cybersecurity. First, Dharmendra Chauhan and colleagues examine the lifecycle of 6G wireless communication technology, pointing out that wireless communications have significantly increased energy consumption and resultant carbon emissions and lack appropriate disposal mechanisms for large amounts of electronic waste or measures for the effective recycling of electronic materials. The authors argue that such challenges must be urgently addressed and present a lifecycle analysis of 6G wireless communication technology, from production to disposal, focussing on electronic waste, energy consumption, and environmental impact. The article includes strategy recommendations and puts forward an ecological policy for all stakeholders for the sustainability of 6G. Finally, in a second review paper, Sarker, Yunus, and Deraman assess penetration testing concepts and develop a taxonomy for penetration domains, frameworks, standards, tools, and scoring methods. Recent penetration trends are discussed, and guidelines to aid organisations in selecting an appropriate item set for the penetration process are outlined.

The papers in this edition reinforce the view that emerging technologies are interwoven and are collectively pushing the boundaries of innovation. From enhancing cybersecurity with deep learning to revolutionising customer experience with AI, and from secure communication in smart grids with blockchain to the vast potential of quantum computing, these technologies are reshaping the future of various industries. The ongoing digital transformation promises to address critical global challenges, fostering a more connected, intelligent, and efficient world.

Of particular interest is the combined power of blockchain technology, Big Data and AI, constituting a powerful trio that amplifies their collective potential impact across various sectors. Blockchain provides a secure and immutable ledger for transactions, which, when infused with Big Data analytics, can offer deeper insights and enhanced decision-making capabilities. AI algorithms can analyse vast amounts of data stored on the blockchain to identify patterns, predict trends, and optimise operations in real-time. For instance, in smart grid networks, integrating blockchain with Big Data and AI can significantly enhance the management and security of energy distribution. Blockchain ensures the integrity and security of data collected from smart meters, while Big Data analytics processes this information to optimise energy usage and forecast demand. AI further enhances this system by predicting potential security breaches and optimising energy distribution to reduce waste and costs [6]. A further major application area is supply chain management, where this combination of these technologies can provide end-to-end transparency, improve traceability, and ensure the authenticity of products [7]. Blockchain secures transaction records, Big Data analytics provides insights into supply chain efficiency, and AI-driven predictive analytics enhances supply chain resilience by forecasting disruptions and optimising logistics.

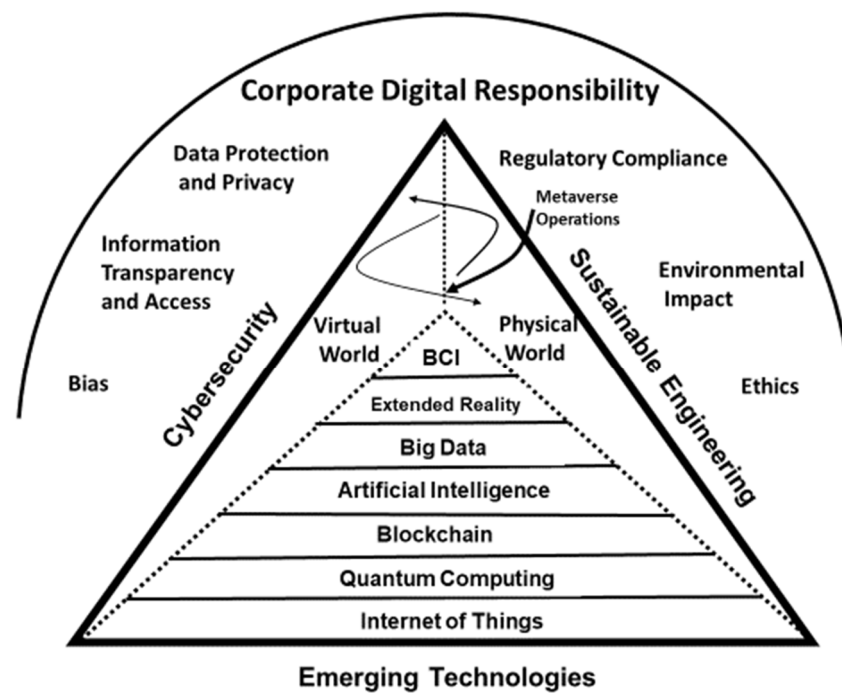
There are undoubtedly some strong indicators that the integration of blockchain with Big Data and AI represents a significant leap forward in leveraging these technologies' strengths. This synergy not only enhances the security, transparency, and efficiency of systems but also drives innovation and enables solutions to complex problems across various industries. However, this potential leap forward does not come without its risks and concerns. Chief among these concerns are the privacy and security risks. Combining Big Data and AI with blockchain can lead to potential privacy issues. Big Data involves collecting vast amounts of information, which can include sensitive personal data. Ensuring these data are anonymised and used ethically is critical to avoiding privacy violations. Blockchain is generally secure, but it is not immune to attacks, and the paper by Mollajafari and Bechkoum in this Special Issue highlights the vulnerabilities and security risks within existing blockchain architectures. Moving forward, quantum computing could potentially break the cryptographic algorithms used in blockchain. Additionally, the integration of AI introduces new attack vectors where malicious actors could exploit AI models to manipulate or infer sensitive data.

Another area that needs to be managed carefully with the growing impact of advanced emerging technologies is related to ethical and bias concerns. AI systems can inherit biases present in the data they are trained on. If the data on the blockchain is biased, AI algorithms might make unfair or unethical decisions. This is particularly concerning in applications such as hiring, law enforcement, and financial services, where biased decisions can have significant consequences. The use of AI and Big Data can also raise ethical questions around surveillance, consent, and data usage. Ensuring transparent and fair use of these technologies is crucial to maintaining public trust and compliance with regulations. There are also technical and operational challenges. Blockchain networks can face scalability issues due to the need for consensus mechanisms and the immutability of data. Integrating Big Data and AI requires substantial computational power and storage, which can exacerbate these scalability issues.

Making matters worse are the complexities surrounding the regulatory framework for these advanced emerging technologies. Different jurisdictions have varying regulations concerning data privacy, blockchain usage, and AI deployment. Ensuring compliance across different regions can be complex and resource-intensive. In this regard, several regulatory frameworks and guidelines have been developed globally. Existing frameworks, such as the General Data Protection Act (GDPR) or the California Consumer Privacy Act (CCPA), go a long way in addressing privacy and security concerns and have been strengthened by frameworks such as the European Union AI Act and the recently launched UAE AI Charter [8]. These regulatory frameworks should, collectively, address the key concerns, ensuring data privacy, security, ethical practises, and regulatory compliance across various sectors. However, as these technologies mature and become more pervasive, there remains a great deal of nervousness about the complexity of these frameworks and the practicalities of enforcing them.

This pace of change and associated uncertainty has served to increase the scrutiny on companies and organisations in their approach to corporate digital responsibility (CDR), which is increasingly seen as a significant component of overall corporate social responsibility (CSR) [9] (Figure 1). The advent of the metaverse [10]—and with it the potential new development of, for example, brain–computer interface (BCI) technologies [11]—plus the widening application of quantum computing [12]—will place greater pressure on corporations to adopt appropriate strategies and to be seen to be taking appropriate actions to manage the implications of increasingly rapid and wide-ranging digitalisation.

In conclusion, there is no doubt that advanced emerging technologies, such as those discussed in this Special Issue, hold immense potential for positive future advancements in organisations and across global society. They are accompanied, however, by significant risks that must be addressed through robust security measures, ethical considerations, regulatory compliance, the recognition of corporate digital responsibilities, and the proactive management of the wider social and economic impacts.



**Figure 1.** Corporate Digital Responsibility and Emerging Technologies.

**Author Contributions:** Both authors equally contributed to the published version of the editorial. All authors have read and agreed to the published version of the manuscript.

**Conflicts of Interest:** The authors declare no conflicts of interest.

**List of Contributions:**

1. Suleiman, J.T.; Jung, I.Y. Advancing Ancient Artifact Character Image Augmentation through Styleformer-ART for Sustainable Knowledge Preservation. *Sustainability* **2024**, *16*, 6455.
2. Tang, S.; Cai, M.; Xiao, Y. A Cross-Citation-Based Model for Technological Advancement Assessment: Methodology and Application. *Sustainability* **2024**, *16*, 435.
3. Mollajafari, S.; Bechkoum, K. Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy. *Sustainability* **2023**, *15*, 13401.
4. Hosseinzadeh, M.; Malik, M.H.; Safkhani, M.; Bagheri, N.; Le, Q.H.; Tighiz, L.; Mosavi, A.H. Toward Designing a Secure Authentication Protocol for IoT Environments. *Sustainability* **2023**, *15*, 5934.
5. Ali, Z.; Mahmood, A.; Khatoon, S.; Alhakami, W.; Ullah, S.S.; Iqbal, J.; Hussain, S. A Generic Internet of Things (IoT) Middleware for Smart City Applications. *Sustainability* **2023**, *15*, 743.
6. Ozdemir, S.; Wynn, M.; Metin, B. Cybersecurity and Country of Origin: Towards a New Framework for Assessing Digital Product Domesticity. *Sustainability* **2023**, *15*, 87.
7. Chauhan, D.; Mewada, H.; Gondalia, V.; Almalki, F.A.; Patel, S.; Modi, H.; Kavaiya, S.; Trivedi, Y.; Mohammed Mujlid, H.M. Balancing Technological Innovation and Environmental Sustainability: A Lifecycle Analysis of 6G Wireless Communication Technology. *Sustainability* **2024**, *16*, 6533.
8. Sarker, K.U.; Yunus, U.; Deraman, A. Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods. *Sustainability* **2023**, *15*, 10471.

**References**

1. Alawida, M.; Mejri, S.; Mehmood, A.; Chikhaoui, B.; Isaac Abiodun, O. A Comprehensive Study of ChatGPT: Advancements, Limitations, and Ethical Considerations in Natural Language Processing and Cybersecurity. *Information* **2023**, *14*, 462. [CrossRef]
2. Ozdemir, S.; Wynn, M.; Metin, B. The War in Ukraine: Why Knowing the Country of Origin of Tech Components Is Vital. 2023. Available online: <https://theacademic.com/why-knowing-the-country-of-origin-of-tech-components-is-vital/> (accessed on 4 August 2024).

3. Griffin, A. CrowdStrike Reveals How Huge Microsoft Outage That Led to Global Chaos Actually Happened. 2024. Available online: <https://www.independent.co.uk/tech/microsoft-crowdstrike-global-it-outage-b2585547.html> (accessed on 2 August 2024).
4. Rotolo, D.; Hicks, D.; Martin, B. What is an emerging technology? *Res. Policy* **2015**, *44*, 1827–1843. Available online: [http://sro.sussex.ac.uk/id/eprint/56071/1/2015RP\\_Rotolo\\_Hicks\\_Martin\\_Preprint.pdf](http://sro.sussex.ac.uk/id/eprint/56071/1/2015RP_Rotolo_Hicks_Martin_Preprint.pdf) (accessed on 6 August 2024). [[CrossRef](#)]
5. Turner, C. Ministers Urged to Carry Out Urgent Defence Review after Nuclear Submarine Fleet Revelations. 2024. Available online: <https://www.telegraph.co.uk/news/2024/08/03/russian-software-nuclear-submarines-defence-review/> (accessed on 4 August 2024).
6. Abdullah, A.K.; Asif, A.L.; Mamoon, R.; Hang, L.; Abdul Rehman, J.; Thippa, R.G. Artificial intelligence and blockchain technology for secure smart grid and power distribution Automation: A State-of-the-Art Review. *Sustain. Energy Technol. Assess.* **2023**, *57*, 103282. [[CrossRef](#)]
7. Naoum, T.; Roman, S.; Manoj, D.; Mukesh, K. Artificial intelligence and blockchain implementation in supply chains: A pathway to sustainability and data monetisation? *Ann. Oper. Res.* **2023**, *327*, 157–210. [[CrossRef](#)]
8. OneTrust Data Guidance. UAE: AI Office Launches Charter for Development and Use of AI. 2024. Available online: <https://www.dataguidance.com/news/uae-ai-office-launches-charter-development-and-use-ai> (accessed on 5 August 2024).
9. Wynn, M.; Jones, P. Corporate responsibility in the digital era. *Information* **2023**, *14*, 324. [[CrossRef](#)]
10. Wynn, M.; Jones, P. New technology deployment and corporate responsibilities in the metaverse. *Knowledge* **2023**, *3*, 543–556. [[CrossRef](#)]
11. Abdelghafar, S.; Ezzat, D.; Darwish, A.; Hassanien, A.E. Metaverse for Brain Computer Interface: Towards New and Improved Applications. In *The Future of Metaverse in the Virtual Era and Physical World*; Hassanien, A.E., Darwish, A., Torkey, M., Eds.; Studies in Big Data; Springer: Cham, Switzerland, 2023; Volume 123, pp. 43–58.
12. Wynn, M.; Jones, P. Corporate Digital Responsibility and the Business Implications of Quantum Computing. *Adv. Environ. Eng. Res.* **2023**, *4*, 53. [[CrossRef](#)]

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.