Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 237 (2024) 80–87

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Industry Sciences and Computer Science Innovation

Digitalization and Cybersecurity in SMEs: A Bibliometric Analysis

Marta F. Arroyabe[a]*, Carlos F. A. Arranz[b], Juan Carlos Fernandez de Arroyabe[a], Ignacio Fernandez[c,d]

[a] *University of Essex, Elmer Approach, Southend on Sea SS1 1LW, UK*
[b] *University of Greenwich, Old Royal Naval College, Park Row, Greenwich SE10 9LS, UK*
[c] *Loughborough University Epinal Way, Loughborough LE11 3TU, UK*
[d] *Lloyds Banking Group, Gresham St, London EC2V 7HN, UK*

Abstract

This paper presents a bibliometric analysis of digitalization and cybersecurity in Small and Medium Enterprises (SMEs), using the R tool Bibliometrix, with a total of 417 papers. First, our paper contributes to academia by showing that research on this topic is grouped into four clusters corresponding to four research lines: Industry 4.0 and Smart Factory; Industry 4.0 and SME; SME and Cybersecurity; Digitalization, SMEs, and Entrepreneurship. Second, our paper contributes to the literature by highlighting the existing gaps. We see that the digital transformation of SMEs entails increasing exposure to possible cyberattacks, which can be a determining factor for digitalization and, additionally, can affect the future of the SME business. In this context, we see that this gap has not been covered, as research lines have been found that focus on these issues but are unconnected. Regarding future research, we can predict that cybersecurity in SMEs will be a particular case of cybersecurity in firms, separated from research on digitalization in SMEs, which addresses issues such as smart factories and Industry 4.0 objectives in these enterprises.

Keywords: Digitalization; Cybersecurity; SMEs; Bibliometric Analysis

* *E-mail address:* mf17255@essex.ac.uk

1877-0509
10.1016/j.procs.2024.05.082

1. Introduction

Digitalization is transforming economies, societies, forms of communication and jobs [1] [2]. The digitalization of companies is fundamentally based on adopting emerging technologies such as big data, cloud computing, artificial intelligence and machine learning (AI/ML), robotics, data analysis and blockchain [3] [4], which has a significant impact on innovation and business productivity [5].

Furthermore, digitalization supposes the interconnection of companies, allowing permeability of social agents to the environment, facilitating access to information or new markets and, as a consequence, increasing their competitiveness (see, for example, [6]). Thus, within the framework of the Internet of Things (IoT), computers, sensors and networks are combined to monitor and control devices, where the network, connectivity and computing capacity are extended to objects and sensors, allowing these devices to generate, exchange and consume data [7] [5]. The potential of the implementation of digitalization and the IoT supposes that the result is a hyperconnected world [8] [7].

However, digitalization and the implementation of the IoT mean greater exposure of companies to cyberattacks that are not only derived from vulnerabilities in the use of information technology, presenting additional security challenges [9] [10]. Thus, for the classic spyware, malware, denial of service (DoS), ransomware or phishing attacks, IoT devices can serve as potential entry points for cyberattacks. The connected nature of digitalization means that every poorly protected device that is linked online potentially impacts the security and resiliency of the internet [7]. For example, the implementation of digital technologies such as big data implies the storage of information, which can potentially be an object of attack. In addition, the incorporation of industrial robots connected to the Industrial Internet of Things (IIoT), or the use of cloud computing or smart devices, can be subject to potential attacks, for example, tampering attacks, which can distort the addresses of devices, or DoS, which affects wireless connections [11] [7]. Therefore, with the cyber epidemic gaining momentum, no companies or organizations are safe from potential attacks [12] [13]. Consequently, cybersecurity is emerging as a core critical competency for organizational survival and growth [14]. Tao et al. [15] and Alahmari and Duncan [16] point out that threats and incidents (IT security problems) have become vital in the digitalization process, taking into account the potential risks of interconnection to the IoT and the vulnerabilities of companies. In this context, cybersecurity appears in organizations as a key element to ensure the confidentiality and operability of these establishments in the current environment.

This work presents a bibliometric analysis of digitalization and cybersecurity, focusing on the case of small and medium-sized enterprises (SMEs). First, there are important works on digitalization in the literature; however, the connection between digitalization and cybersecurity is scarcely treated. In this sense, we understand that addressing a review of the literature of digitalization must be related to the problems of interconnection, and, therefore, the study of cybersecurity and vulnerabilities of companies in the digitalization process. Second, we focus on SMEs, considering the importance that these have in the economy and the inadequate treatment that has been given in the digitalization of them with respect to large companies [4] [17]. Moreover, from the point of view of cyber criminals, the rate of cyberattacks against SMEs is considerable; however, many SMEs do not believe that they are the target of these attacks [14]. In this context, there is an important gap: how SMEs are becoming digital, and how this digitalization affects their cybersecurity.

2. Methodology and Data

This study utilizes bibliometric analysis [18], to examine published research in the fields of digitalization, cybersecurity, and SMEs. The analysis employs the R package Bibliometrix [18] [19] to explore the collected data from the Web of Science (WoS) and Scopus databases. The methodology consists of several stages. The methodology followed is developed in various stages. First, we collect papers in digitalization, cybersecurity and SMEs, from the Web of Science (WoS) and Scopus databases. The bibliographical review uses the keywords and abstracts of the articles. As criteria for searching in the database, we introduce the keywords, using the combination (AND/OR).

- The first group of keywords refers to SMEs. As a result, this group has been determined by the following phrase: (“SMEs*” OR “SME*” OR “small and medium-sized enterprises” OR “small business” OR “small firm” OR “small enterprise” OR “small company” OR “medium-sized firm” OR “medium-sized business” OR “medium-sized enterprise” OR “medium-sized company”).

- The second group of keywords focuses on cybersecurity, which is determined by the following phrase: ("cybersecurity" OR "cyber security" OR "cyber" OR "cybercrime" OR "cyberattack" OR "cyber threat" OR "cyber risk" OR "cyber breaches"). The last group of keywords focuses on digital transformation ("digitalisation" OR "digitalization" OR "digital transformation" OR "digital technologies").

Second, after filtering the search, in terms of language and areas, the types of documents found are journals, books and proceedings. Furthermore, second filtering has been used to preserve the robustness of the analysis, eliminating informal literature surveys, duplicate documents, non-academic papers and technical descriptions. The results showed 417 documents, distributed in 231 journal articles, 168 proceedings and 18 book chapters and books. Third, using the tool Bibliometrix, we have conducted relational and prospective analyses.

3. Analysis and Results

As for the descriptive analysis, the temporary distribution of papers is shown in Figure 1. The figure shows that a growing significant number of papers between 2016 and 2021 (the revision was done in June 2022), showing that research in digitalization and cybersecurity in SMEs is incipient. Moreover, the descriptive results show the geographical dissemination of research, we see that this corresponds to a wide range of countries. More in detail, Germany (99) is the country with the highest number of papers, followed by Italy (70), the UK (49), France (36), India (35), Portugal (33), Spain (33), China (30), Finland (29), Malaysia (25), Poland (25), Romania (24), Netherlands (21), Canada (19), Indonesia (18), Austria (17), Sweden (17), Switzerland (14), and South Africa (14). In general, we observe that the topics of digitalization, cybersecurity and SME are recurring themes in all geographical areas, especially those that deal with Industry 4.0. Thus, this interest is shown in initiatives such as Industry 4.0 (I4.0), originating in Germany, Intelligent Manufacturing in the USA, Made in China 2025, Future of Manufacturing in the UK and Smart Factory in South Korea, among others [17] [4] [20].

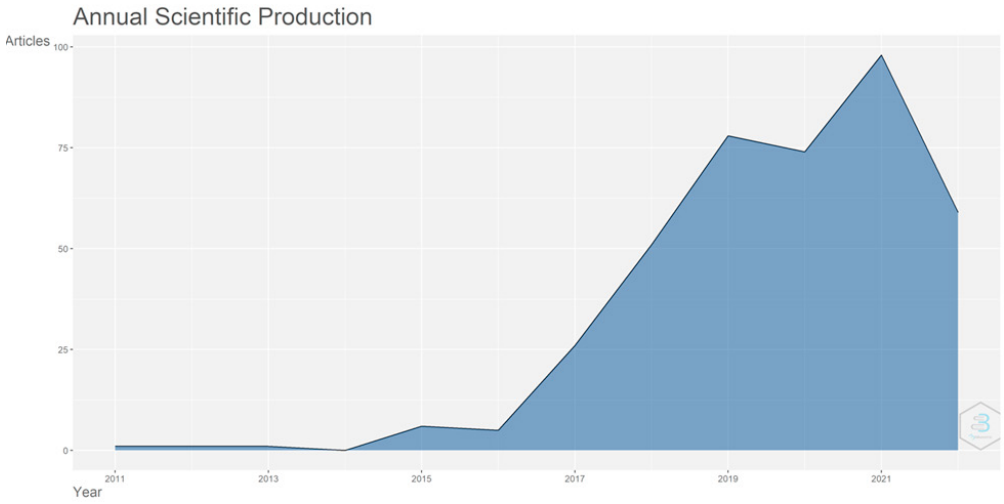

Fig. 1. Temporary scientific production.

The result of the bibliometric analysis shows the country collaboration clusters by country. In general, we observe the broad collaboration between European countries, and to a lesser extent with American countries (USA and Canada), showing the prevalence of Europe in this research. In this sense, Gruber [21] and Pianta et al. [22] have highlighted the importance of digitalization and industrialization policies for Europe, which serves as an incentive for research centers to focus on these topics. Moreover, Figure 2 shows the cloud of keywords, shown by those most used in the sample papers. Thus, we see that words like "Industry 4.0" and "SME" are the keywords with the highest frequency of appearance. At a second level, we find "digitalization" and "digital transformation". The figure also

includes other terms such as “cybersecurity”, “innovation”, “artificial intelligence”, “smart factory”, “sustainability”, “digital twins”, “Internet of Things (IoT)”, “machine learning”, “innovation” and “knowledge management”, among others, but with a lower level of frequency. In general, Figure 2 allows us to have an overview of the topics covered in our research, highlighted by frequency of use.

Fig. 2. Word Cloud of Keywords.

The relational analysis enables us to analyze the research areas. For this, bibliometric analysis has been executed using the keywords (Figure 3), exploring the network of research areas [18] [19]. The results show four research clusters.

- The first cluster is Industry 4.0 and Smart Factory (blue color). This cluster presents different topics, considering the smart factory as the result of the implementation of Industry 4.0 in firms. Industry 4.0 has been considered an industrial revolution with the objective of the digitalization of companies [23] [3] [24] [25] [26] [27]. Thus, in this cluster, the association between smart factories and Industry 4.0 has generated different groups of research: the importance for firms of the smart factory, the conceptualization of the smart factory, the connectivity of the smart factory with its environment, the challenges for firms to implement smart factories and the need to standardize companies’ processes and activities.
- The second cluster is Industry 4.0 and SMEs (purple color), which shows the relationship between Industry 4.0 and SMEs [28] [29] [30] [4] [3]. Thus, fundamentally, this cluster covers topics such as the adoption and models of digital technologies and the factors that influence the decision to adopt these technologies in SMEs.
- The third cluster is SMEs and cybersecurity (red color), emphasizing the relationship between SMEs and cybersecurity, and cybersecurity practices and activities in SMEs [31] [14] [10] [16].
- The fourth cluster is Digitalization, SMEs and Entrepreneurship (green color). This presents all aspects of the effect that digitalization has on entrepreneurial SMEs, and how they influence the business model. The association between digitalization, entrepreneurship and SMEs is evident in different groups of papers [32] [33] [34] [35].

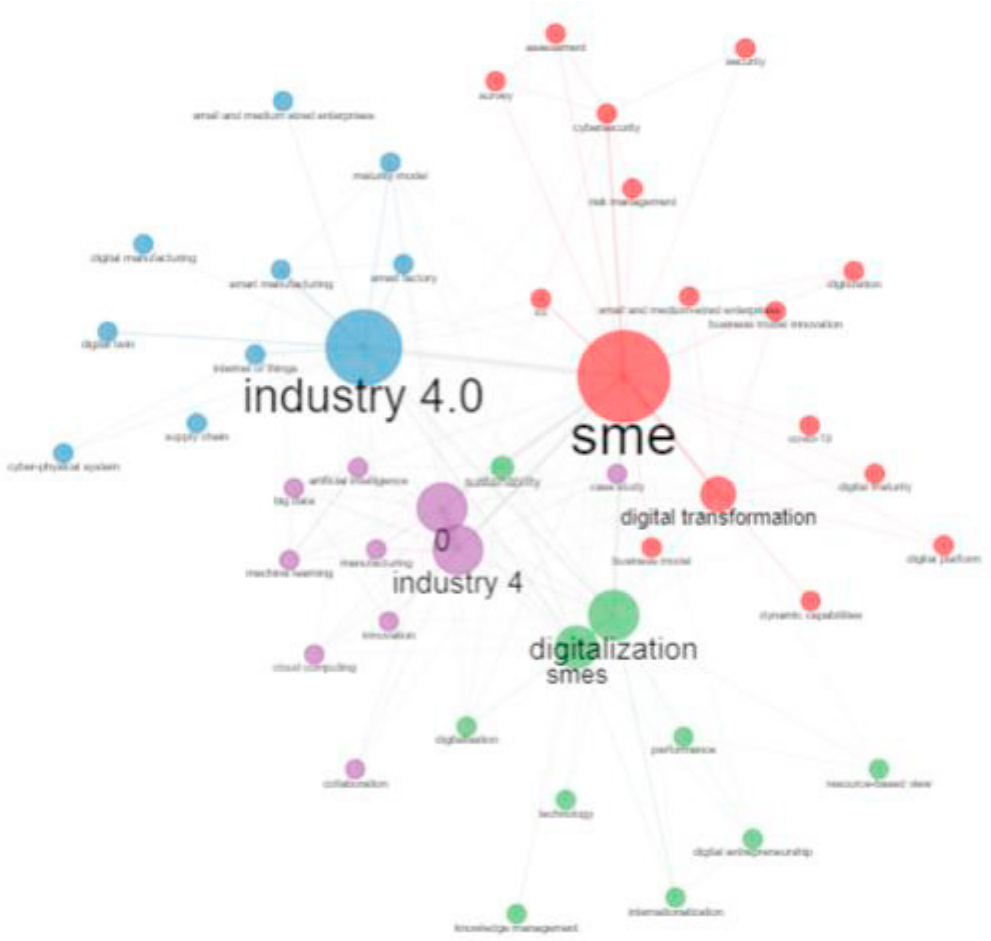

Fig. 3. Co-occurrence Keyword Network

A strategic map is used for prospective future research on digitalization and cybersecurity in SMEs (Figure 4). Following Aria and Cuccurullo [19], the map is a two-dimensional representation, using as variables the centrality and density of the network of scientific topics, producing a 2x2 quadrant (axes: centrality and density level in the network). These four quadrants are categorized as motor quadrant (upper right), transversal or basic quadrant (lower right), peripheral quadrant (upper left) and emerging or disappearing quadrant (lower left).

In the right-lower quadrant, we find base themes: SME digitalization and digital transformation, smart factories and the IoT, industry manufacturing, and cybersecurity assessment and risk management. These themes have low density and high centrality. The largest themes in terms of research size are industry and smart manufacturing with the IoT, and the digitalization of SMEs. Cybersecurity and industry manufacturing have fewer publications. These themes are loosely connected with other themes due to their diverse origin in literature from IT, operations management, supply chains, and strategy. Figure 1 shows the first line of investigation on SME digitalization, which is included in two research clusters. The second line focuses on smart factories and the IoT in the context of Industry 4.0, analyzing the benefits and challenges. The third line explores the relationship between SMEs and cybersecurity, while the last line addresses factors affecting manufacturing productivity. Overall, there is a research gap as these important issues are disconnected from SMEs, digitalization, and cybersecurity, despite the increasing exposure of SMEs to cyber threats and their lack of consideration for cybersecurity.

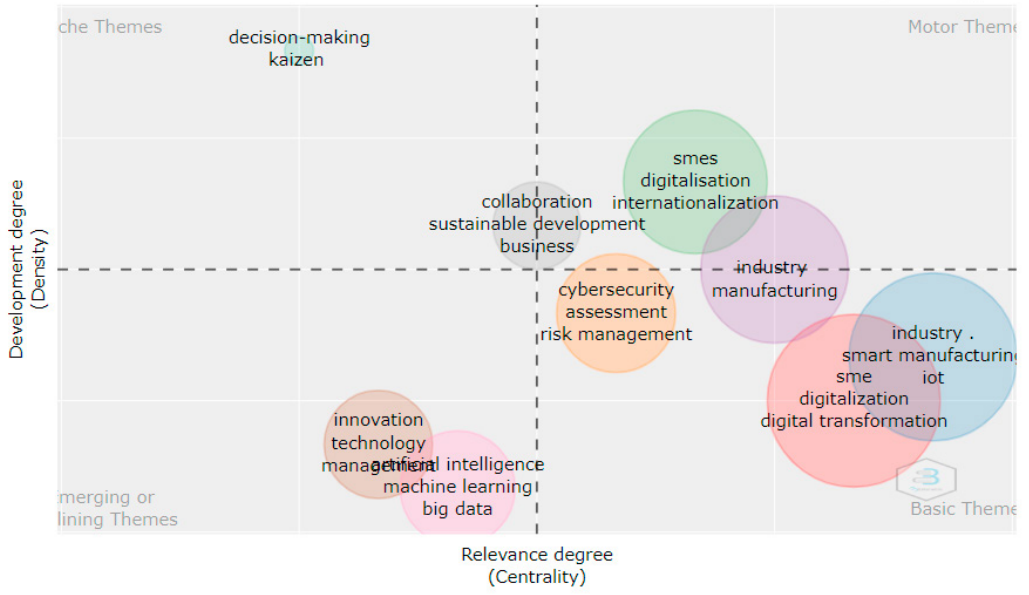

Fig. 4. Strategic Map.

In the upper quadrant, two themes emerge as the driving forces of the research, characterized by high density and centrality. The analysis reveals a range of topics, including SME digitalization and internationalization, as well as collaboration for business sustainability, albeit with fewer contributions. However, the explicit inclusion of cybersecurity is notably absent in this context. Some limited research links business sustainability with cybersecurity [36] [37]. It is noteworthy that cybersecurity research overlaps from the base quadrant to the motor quadrant, indicating its increasing importance (centrality) and interconnectedness (density), albeit at an early stage. This identifies a research gap that future studies could address: the integration of cybersecurity with SMEs and digitalization.

Lastly, quadrant three (niche topics) and quadrant four (emerging or missing topics) exhibit limited significance. Niche topics, such as decision-making and Kaizen, demonstrate high density but low centrality. These topics have received extensive coverage in the literature (Farris et al., 2008), yet there is no direct line focusing on SMEs, digitalization, and cybersecurity in the niche category. Emerging or disappearing themes encompass ethical machine learning, diversity of digital technologies, and innovation management. Research is starting to address ethical concerns related to the application of machine learning in organizations, as well as the longstanding topic of technological innovation. These topics are positioned in the fourth quadrant, indicating low importance (centrality) and interconnection (density). This suggests that they are either new, emerging, or in the final stages of the mainstream research cycle. Thus, the appearance of innovative technology management in this quadrant can be justified.

4. Conclusions

The objective of this paper was to carry out a bibliometric study on scientific research in the area of digitalization and cybersecurity in SMEs. The time horizon of the research was from 2006 to 2022, and 417 publications were obtained, distributed between empirical and theoretical studies, conferences, systematic literature reviews and books. Our study addresses the temporal evolution of research, scientific production by country and the distribution of research sources, among other things. In addition, we have described the main research areas, as well as the prospects for future research in digitalization and cybersecurity in SMEs, using both cluster analysis and strategy maps.

Through the bibliometric analysis of digitalization and cybersecurity in SMEs, the results provide important contributions to both academic research and policymakers. The first contribution is that we have identified four lines of investigation with a diverse research approach. The first research line covers topics such as the importance for companies of the smart factory, the conceptualization of the smart factory, the connectivity of the smart factory with

its environment, the challenges for companies to implement smart factories and the need to standardize their processes and activities. The second line emphasizes the adoption and models of digital technologies and the factors that influence the decision to adopt them in SMEs. The third research line covers the relationship between SMEs and cybersecurity, highlighting cybersecurity practices and activities in SMEs. The last line covers all aspects of the effect that digitalization has on entrepreneurial SMEs, and how they influence the business model.

The second contribution of the research has been the identification of important gaps and future challenges for research on SMEs, cybersecurity and digitalization. As we have seen previously, there is an important gap in the literature on the digitalization of SMEs regarding the consideration of cybersecurity. Thus, we see that the digital transformation of SMEs entails increasing exposure to possible cyberattacks, which can be a determining factor for digitalization and, on the other hand, can affect the future of SMEs. In this context, from our results, we see that this gap has not been covered, as research lines have been found that focus on these issues but are unconnected. In other words, cybersecurity research is carried out in the IT field, unlike the digital transformation of SMEs; it is carried out in fields closer to strategy and operations management, without there being obvious connections that tend to cover the gap. Regarding the future of research, our bibliometric analysis does not show a tendency to address this gap; rather, each research area develops separately. In fact, in the near future, we can predict that cybersecurity in SMEs will be a particular case of cybersecurity in firms, separated from research on digitalization in SMEs, which addresses issues such as smart factories and Industry 4.0 objectives in these enterprises. Thus, for example, the IoT, which is a fundamental element of the smart factory, is highlighted as an interconnected element in research on digitalization, but the IoT network, as well as potential threats, are investigated in the IT field, without there being a clear connection between them. Therefore, future work should address issues before the decision to digitally transform SMEs, considering the challenges that cybersecurity can pose at this stage. Likewise, work should be developed, in the digitalization management phase, taking account of the implications of cybersecurity management, attacks and contingency plans, among other things.

Regarding the implications for managers and policymakers, we consider there is a need to contemplate the importance of cybersecurity in the digitalization of SMEs. First, SME managers should forget the cybersecurity myopia by getting involved in cybersecurity decisions. Second, the digital transformation of SMEs must be accompanied by specific measures to mitigate vulnerabilities and potential cyber threats. Third, the adoption of cyber standards, such as ISO 27000s or Cyber Essentials (UK), must be a common practice in SMEs, eliminating internal vulnerabilities derived from the malpractice of the organization. Last, it must be considered that the digitalization of SMEs implies a connection to the IoT, with consequences for cyber management systems, derived from the necessity that smart devices and control systems have in terms of cybersecurity.

References

[1] Cassetta, E., Monarca, U., Dileo, I., Di Berardino, C., and Pini, M. (2020). "The relationship between digital technologies and internationalisation. Evidence from Italian SMEs". *Industry and Innovation*, **27(4):** 311-339.

[2] Amankwah-Amoah, J., Khan, Z., Wood, G., and Knight, G. (2021). "COVID-19 and digitalization: The great acceleration". *Journal of Business Research*, **136**: 602-611.

[3]. Ghobakhloo, M., and Ching, N. T. (2019). "Adoption of digital technologies of smart manufacturing in SMEs". *Journal of Industrial Information Integration*, **16**, 100107.

[4] Masood, T., and Sonntag, P. (2020). Industry 4.0: "Adoption challenges and benefits for SMEs". *Computers in Industry*, **121**, 103261.

[5] Chen, T., and Lin, Y. C. (2017). "Feasibility evaluation and optimization of a smart manufacturing system based on 3D printing: a review". *International Journal of Intelligent Systems*, **32(4)**: 394-413.

[6] Moeuf, A., Pellerin, R., Lamouri, S., Tamayo-Giraldo, S., and Barbaray, R. (2018). "The industrial management of SMEs in the era of Industry 4.0". *International Journal of Production Research*, **56(3):** 1118-1136.

[7] Boyes, H., Hallaq, B., Cunningham, J., and Watson, T. (2018). "The industrial internet of things (IIoT): An analysis framework". *Computers in Industry*, **101**: 1-12.

[8] Nayak, S., and Vijayalakshmi, M. N. (2016). "Analysis on IoT challenges, opportunities, applications and communication models". *International Journal of Advanced Engineering, Management and Science*, **2(4)**: 239393.

[9] Fernandez de Arroyabe, I., Arranz, C. F., Arroyabe, M. F., and Fernandez de Arroyabe, J. C. (2023). "Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019". *Computers & Security*, **124**, 102954.

[10] Benz, M., and Chatterjee, D. (2020). "Calculated risk? A cybersecurity evaluation tool for SMEs". *Business Horizons*, **63(4):** 531-540.

[11] Sahoo, S., and Lo, C. Y. (2022). "Smart manufacturing powered by recent technological advancements: A review". *Journal of Manufacturing Systems*, **64**: 236-250.

[12] Yan, D., Liu, F., Zhang, Y., and Jia, K. (2019). "Dynamical model for individual defence against cyber epidemic attacks". *IET Information Security*, **13(6):** 541-551.

[13] Manworren, N., Letwat, J., and Daily, O. (2016). "Why you should care about the Target data breach". *Business Horizons*, **59(3)**: 257-266.

[14] Fernandez De Arroyabe, I., and Fernandez de Arroyabe, J. C. (2021). "The severity and effects of Cyber-breaches in SMEs: a machine learning approach". *Enterprise Information Systems*, **17(3)**: 1-27.

[15] Tao, F., Qi, Q., Wang, L., and Nee, A. Y. C. (2019). "Digital twins and cyber–physical systems toward smart manufacturing and industry 4.0: Correlation and comparison". *Engineering*, **5(4)**: 653-661.

[16] Alahmari, A., and Duncan, B. (2020). "Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence". *In 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, 1-5. IEEE.

[17] Horváth, D., and Szabó, R. Z. (2019). "Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities?" *Technological Forecasting and Social Change*, **146**: 119-132.

[18] Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., and Lim, W. M. (2021). "How to conduct a bibliometric analysis: An overview and guidelines". *Journal of Business Research*, **133**: 285-296.

[19] Aria, M. and Corrado C. (2017). "Bibliometrix: An R-tool for comprehensive science mapping analysis". *Journal of Informetrics*, **11(4)**: 959-975.

[20] Nounou, A., Jaber, H., and Aydin, R. (2022). "A cyber-physical system architecture based on lean principles for managing industry 4.0 setups". *International Journal of Computer Integrated Manufacturing*, **35(8)**: 1-19.

[21] Gruber, H. (2019). "Proposals for a digital industrial policy for Europe". *Telecommunications Policy*, **43(2):** 116-127.

[22] Pianta, M., Lucchese, M., and Nascia, L. (2020). "The policy space for a novel industrial policy in Europe". *Industrial and Corporate Change*, **29(3)**: 779-795.

[23] Cañas, H., Mula, J., Díaz-Madroñero, M., and Campuzano-Bolarín, F. (2021). "Implementing industry 4.0 principles". *Computers & Industrial Engineering*, **158**, 107379.

[24] Sony, M., and Naik, S. (2020). "Key ingredients for evaluating Industry 4.0 readiness for organizations: a literature review". *Benchmarking: An International Journal*, **27(7):** 2213-2232.

[25] Dalenogare, L. S., Benitez, G. B., Ayala, N. F., and Frank, A. G. (2018). "The expected contribution of Industry 4.0 technologies for industrial performance". *International Journal of Production Economics*, **204**: 383-394.

[26] Mohamed, M. (2018). "Challenges and benefits of industry 4.0: An overview". *International Journal of Supply and Operations Management*, **5(3)**: 256-265.

[27] Rojko, A. (2017). "Industry 4.0 concept: Background and overview". *International Journal of Interactive Mobile Technologies*, **11(5)**: 77-90.

[28] Ramdani, B., Raja, S., and Kayumova, M. (2022). "Digital innovation in SMEs: a systematic review, synthesis and research agenda". *Information Technology for Development*, **28(1):** 56-80.

[29] Jung, W. K., Kim, D. R., Lee, H., Lee, T. H., Yang, I., Youn, B. D. and Ahn, S. H. (2021). "Appropriate smart factory for SMEs: concept, application and perspective". *International Journal of Precision Engineering and Manufacturing*, **22**: 201-215.

[30] Rozak, H. A., Adhiatma, A., Fachrunnisa, O., and Rahayu, T. (2021). "Social media engagement, organizational agility and digitalization strategic plan to improve SMEs' performance". *IEEE Transactions on Engineering Management*. **70(11)**: 3766-3775,

[31] Corallo, A., Lazoi, M., Lezzi, M., and Pontrandolfo, P. (2021). "Cybersecurity challenges for manufacturing systems 4.0: assessment of the business impact level". *IEEE Transactions on Engineering Management*. DOI: 10.1109/TEM.2021.3084687

[32] Papadopoulos, T., Baltas, K. N., and Balta, M. E. (2020). "The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice". *International Journal of Information Management*, **55**, 102192.

[33] Kraus, S., Palmer, C., Kailer, N., Kallinger, F. L., and Spitzer, J. (2019). "Digital entrepreneurship: A research agenda on new business models for the twenty-first century". *International Journal of Entrepreneurial Behavior & Research*, **25(2):** 353-375.

[34] Steininger, D. M. (2019). "Linking information systems and entrepreneurship: A review and agenda for IT-associated and digital entrepreneurship research". *Information Systems Journal*, **29(2)**: 363-407.

[35] Zaheer, H., Breyer, Y., and Dumay, J. (2019). "Digital entrepreneurship: An interdisciplinary structured literature review and research agenda". *Technological Forecasting and Social Change*, **148**, 119735.

[36] Salam, A. (2020). "Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends". In: *Internet of Things for Sustainable Community Development. Internet of Things*. Springer, Cham. https://doi.org/10.1007/978-3-030-35291-2_10

[37] Najaf, K., Mostafiz, M. I., and Najaf, R. (2021). "Fintech firms and banks sustainability: why cybersecurity risk matters?" *International Journal of Financial Engineering*, **8(02)**, 2150019.