Forging the Future: Pioneering Approaches in Business, Management and Economics Engineering to Overcome Emerging Global Challenges - 2024

https://doi.org/10.24867/FUTURE-BME-2024-076 Original scientific paper

CYBERSECURITY IN INDUSTRIAL INTERNET OF THINGS AND COLLABORATIVE ROBOTS: INDUSTRY 5.0 PERSPECTIVE

Dragana Slavic[1] [0000-0002-5834-889X], Aleksa Komosar[2] [0000-0003-4366-9014], Darko Stefanovic[3] [0000-0002-4360-7676], Slavko Rakic[4] [0000-0002-9021-8585]

Abstract

Industry 5.0 is leading important transformative changes in today's world. Through human-centric, sustainable, and resilient practices, these changes are answering challenges identified on a global level. In the manufacturing sector, the shift from technology-oriented production to people-oriented production is being made. Industry 5.0 enhances the importance of people, their role in Industrial Internet of Things, and working in a symbiosis with Collaborative Robots. These practices require obtaining sensitive data, which makes strengthening and maintaining firms' Cybersecurity measures necessary. In order to show how Cybersecurity pervades Industrial Internet of Things and Collaborative Robots, authors of this paper have applied the PRISMA framework. The main findings of this paper show how Cybersecurity is used in Industrial Internet of Things and Collaborative Robots from the Industry 5.0 perspective.

Key words: *Industry 5.0, Cybersecurity, Industrial Internet of Things, Collaborative Robots.*

1. Introduction

Digital technologies have emerged in the scope of the Industry 4.0 strategy, which was initiated in 2011 (Lasi et al., 2014). Ever since, digitalisation and digital transformation are changing the ways of doing business, resulting in the creation of digital product-service systems (Rakic et al., 2023; Vuckovic et al., 2022). As digital technologies of the Fourth industrial revolution, cybersecurity, industrial internet of things (IIoT), and collaborative robots (cobots) are intertwined with an aim to

[1] University of Novi Sad, Faculty of Technical Sciences, Serbia, slavic.draganaa@uns.ac.rs
[2] University of Novi Sad, Faculty of Technical Sciences, Serbia, aleksakomosar@uns.ac.rs
[3] University of Novi Sad, Faculty of Technical Sciences, Serbia, slavkorakic@uns.ac.rs
[4] University of Novi Sad, Faculty of Technical Sciences, Serbia, darko.stefanovic

ensure a proper functioning of cyber-physical systems (Komosar et al., 2024; Lezzi et al., 2018). However, with the introduction of Industry 5.0, human-cyber-physical systems have appeared (Chen et al., 2021). The human factor in the human-cyber-physical systems resembles main Industry 5.0 pillars – human-centricity, sustainability, and resilience (Chen et al., 2021; Slavic et al., 2024). When compared with Industry 4.0 which is identified as a technology-driven strategy, Industry 5.0 is identified as a value-driven strategy (Crnobrnja et al., 2023; Golovianko et al., 2023). In other words, Industry 5.0 goes beyond firms' needs and tends towards answering societal needs on a global level (Slavic et al., 2024).

In this paper, a systematic literature review is conducted with an aim to investigate the use of Cybersecurity in (Industrial) Internet of Things and Collaborative Robots from the Industry 5.0 perspective. Consequently, authors propose following research questions:

RQ1: How are Cybersecurity and Internet of Things intertwined in the context of Industry 5.0?

RQ2: How are Cybersecurity and Collaborative Robots intertwined in the context of Industry 5.0?

To answer the research questions, the paper is structured in the following way: Section 2 gives an overview of the research methodology, Section 3 consists of a review of extracted research, Section 4 includes a discussion on the given topic, and Section 5 concludes the paper.

2. Research methodology

In this paper, a systematic literature review (SLR) was conducted to investigate the use of Cybersecurity in (Industrial) Internet of Things and Collaborative Robots in the context of Industry 5.0. Aim of this study is to identify and interpret recent literature in the mentioned field. Preferred Reporting Items for Systematic reviews and Meta-Analyses, also known as the PRISMA framework was used in this study. The PRISMA framework consists of three stages: (1) identification, (2) screening, and (3) inclusion. Figure 1 shows a PRISMA flow chart which resembles phases of this SLR study.

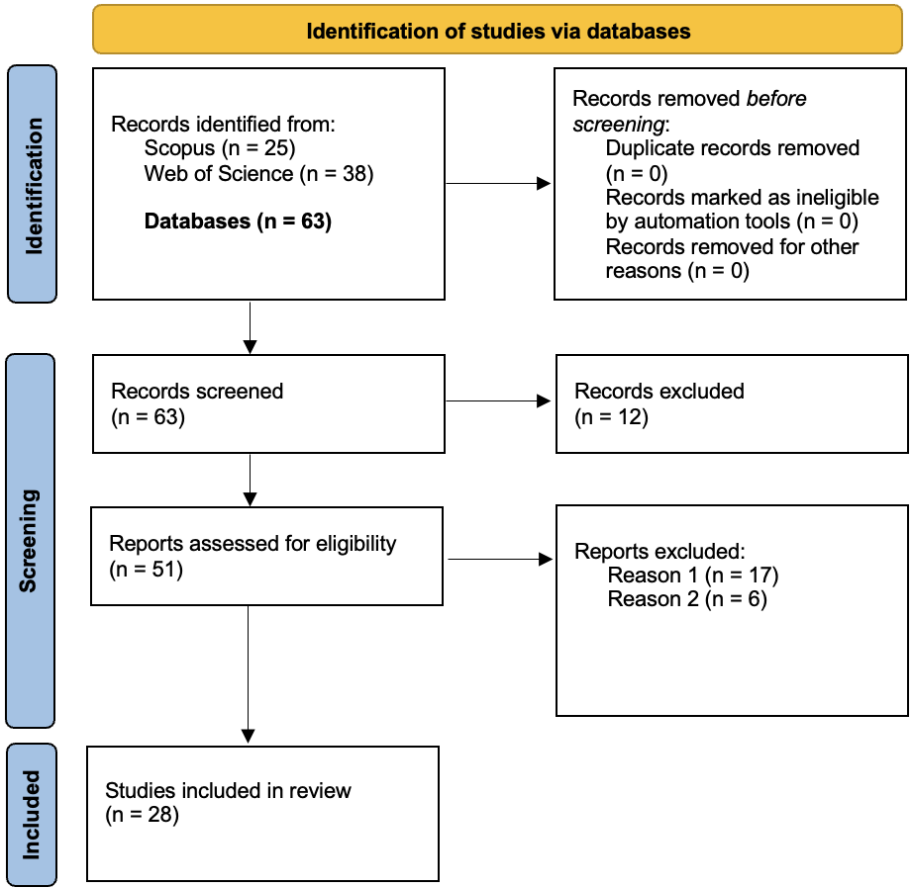

Figure 1: PRISMA flow diagram presenting the results of the systematic research

This SLR study was conducted in September 2024. Data collection and screening were done in the Scopus and Web of Science databases using the following research string for researching titles, abstracts, and keywords: "cybersecurity" AND "internet of things" OR "collaborative robots" AND "Industry 5.0". This research string gathered 106 results. Only conference papers and articles written since 2020 were further included in the SLR, resulting in 63 records for further screening. After the screening process, 12 records were excluded due to inaccessibility. Next, 51 reports were assessed for eligibility – 17 were excluded after examining the titles (Reason 1), and 6 were excluded after examining the abstracts (Reason 2). Finally, 28 studies were included in the systematic literature review.

3. Review of extracted research

As Internet of Things represents a network of interconnected systems, software, data storage, and services, it also represents a target for cyberattacks due to sensitive and important data it storages (Ahmed et al., 2023; Alkhudaydi et al., 2023). With the transition to Industry 5.0 and enhanced collaboration between humans and robots, more personal data is included (Nelufule et al., 2024). Additionally, educating the end-users of these systems about potential threats plays a crucial role in maintaining responsible usage and cybersecurity practices (Ganji & Afshan, 2024). By introducing regular staff training, cybersecurity awareness increases, and the impact of cyberattacks on performance, intellectual capital, and organisational knowledge minimises (Corallo et al., 2022).

Cybersecurity attack, threats, and vulnerabilities which are found in IoT environments are Denial of Service (DoS), Distributed Denial of Service (DDoS), malicious, ransomware, blackhole, sinkhole, reconnaissance, and wormhole attacks (Abdullahi et al., 2022). Methodologies for predicting these attacks are usually based on artificial intelligence and deep learning/machine learning, and blockchain (Alrowais et al., 2023; Mughaid et al., 2024; Rudenko et al., 2022; Tariq et al., 2023). Industrial machines and devices are particularly vulnerable to cyberattacks due to their design which emphasizes functionality rather than security (Alnajim et al., 2023). The vulnerability increases as the dependence on technology grows (Díaz, 2022). To encounter this risk, cybersecurity models tailored specifically for Industry 5.0 connectivity needs are designed (Babbar et al., 2024).

However, Internet of Things has proven to be useful in different fields, such as medicine (Internet of Medical Things), and manufacturing (Industrial Internet of Things) (Casarosa, 2024; Corallo et al., 2022). The use of IoT systems in medicine implies gathering very sensitive data needed for patients' survival, which should be organised according to legal frameworks (Casarosa, 2024). Nonetheless, there are several security certifications schemes which address cybersecurity issues in the IoT environment (Matheu et al., 2019, 2021). Except for fulfilling the security certification schemes requirements, when designing cybersecurity solutions, design guidelines should be followed as well (Boukerche & Coutinho, 2021).

Open-source tools and materials are important for understanding how Internet of Things and collaborative robots work – testbeds which provide simulations of these technologies represent a great source for education and research in these fields (Thom et al., 2021). Also, as working with collaborative robots requires trust, including employees in simulations strengthens the relationship one has with the cobot (Liao et al., 2023). Since cobots do not require any safety net between the machine and the human, the whole network of connected smart objects needs to be both safe and secure (Raimundo & Rosário, 2022).

4. Discussion

4.1. Cybersecurity and Internet of Things

In the context of Industry 5.0 and the connectivity between suppliers, employees, consumers, and technologies it provides, cybersecurity attacks represent a great threat to any digitalised business. Education and research play an important role when defining preventive and corrective strategies in the scope of cybersecurity. Through employee training, cybersecurity awareness is increased, and firm's human-centricity and resilience are strengthened. Additionally, new employee profiles, such as Cybersecurity Professional, are introduced in companies with an aim to focus on cybersecurity attacks, threats, and vulnerabilities.

Internet of Things gathers and stores big amounts of data, some of it being sensitive and personal, especially when IoT is applied in the health sector. Additionally, leading automotive companies use mandatory established cybersecurity implementation in development and manufacturing of products such as airbag systems, and breakes. In order to keep the data secure, different cybersecurity methods are developed. Also, cybersecurity certifications schemes and legal frameworks are designed with an aim to keep the Internet of Things systems as secure as possible.

Accordingly, the answer to **RQ1:** *How are Cybersecurity and Internet of Things intertwined in the context of Industry 5.0?* is that *Cybersecurity and Internet of Things are intertwined in a way which prioritizes keeping personal data safe, and emphasizes the importance of employee education and training*.

4.2. Cybersecurity and Collaborative Robots

Compared to industrial robots, collaborative robots require a higher level of human-machine interaction. This represents a challenge, due to the fear many employees have when faced with collaborative robots which have an anthropomorphistic design. The new human-machine interaction requires further digital forensic analyses. When integrated with artificial intelligence, collaborative robots can predict the way a certain employee will perform its tasks. Due to the close collaboration, the workspace needs to be both safe and secure.

In the context of collaborative robots, which represent one of smart objects which are connected through the Internet of Things, cybersecurity secures the data about human-robot interaction and tasks they have performed together.

Correspondingly, the answer to **RQ2:** *How are Cybersecurity and Collaborative Robots intertwined in the context of Industry 5.0?* is that *Cybersecurity and Collaborative Robots are intertwined in a way that secures the data and IT systems which represent the "machine" part in human-machine interaction*.

5. Conclusions

This manuscript has investigated the connection between Cybersecurity and Internet of Things, and Cybersecurity and Collaborative Robots, both from the perspective of Industry 5.0. The research was done using the PRISMA framework for conducting a systematic literature review. The study included 28 papers from Scopus and Web of Science databases.

With an aim to contribute to Industry 5.0 practices through a human-centric use of digital technologies, more specifically Internet of Things, Collaborative Robots, and Cybersecurity, companies should invest in developing organisational knowledge related to these fields through education, research, and training. Except for gaining and sharing knowledge inside the company, this data should also be secured. Additionally, next to security stands safety, important for maintaining employees' health and well-being.

The transition to Industry 5.0 implies a human-centric, sustainable, and resilient approach towards doing business. In Internet of Things environments and human-robot collaborations, cybersecurity prioritizes minimising risks and addressing attack, threats, and vulnerabilities associated with data and IT systems. Also, education and training of employees, as well as designing new employee profiles contributes to strengthening cybersecurity in the whole Internet of Things network.

Future research on the given topic should include other scientific databases, such as Science Direct or MDPI. Additionally, case studies which include investigating best practices regarding cybersecurity methodologies in IoT and collaborative robots should be conducted.

Acknowledgments

This research has been supported by the Ministry of Science, Technological Development and Innovation (Contract No. 451-03-65/2024-03/200156) and the Faculty of Technical Sciences, University of Novi Sad through project "Scientific and Artistic Research Work of Researchers in Teaching and Associate Positions at the Faculty of Technical Sciences, University of Novi Sad" (No. 01-3394/1).

REFERENCES

[1] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics*, *11*(2), 198. https://doi.org/10.3390/electronics11020198

[2] Ahmed, A. A., Malebary, S. J., Ali, W., & Alzahrani, A. A. (2023). A Provable Secure Cybersecurity Mechanism Based on Combination of Lightweight Cryptography and Authentication for Internet of Things. *Mathematics*, *11*(1), 220. https://doi.org/10.3390/math11010220

[3] Alkhudaydi, O. A., Krichen, M., & Alghamdi, A. D. (2023). A Deep Learning Methodology for Predicting Cybersecurity Attacks on the Internet of Things. *Information*, *14*(10), 550. https://doi.org/10.3390/info14100550
[4] Alnajim, A., Habib, S., Islam, M., Thwin, S., & Alotaibi, F. (2023). A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things. *Technologies*, *11*(6), 161. https://doi.org/10.3390/technologies11060161
[5] Alrowais, F., Althahabi, S., S. Alotaibi, S., Mohamed, A., Ahmed Hamza, M., & Marzouk, R. (2023). Automated Machine Learning Enabled Cybersecurity Threat Detection in Internet of Things Environment. *Computer Systems Science and Engineering*, *45*(1), 687–700. https://doi.org/10.32604/csse.2023.030188
[6] Babbar, H., Rani, S., & Boulila, W. (2024). Fortifying the Connection: Cybersecurity Tactics for WSN-driven Smart Manufacturing in the Era of Industry 5.0. *IEEE Open Journal of the Communications Society*, 1–1. https://doi.org/10.1109/OJCOMS.2024.3428531
[7] Boukerche, A., & Coutinho, R. W. L. (2021). Design Guidelines for Machine Learning-based Cybersecurity in Internet of Things. *IEEE Network*, *35*(1), 393–399. https://doi.org/10.1109/MNET.011.2000396
[8] Casarosa, F. (2024). Cybersecurity of Internet of Things in the health sector: Understanding the applicable legal framework. *Computer Law & Security Review*, *53*, 105982. https://doi.org/10.1016/j.clsr.2024.105982
[9] Chen, X., Eder, M. A., Shihavuddin, A., & Zheng, D. (2021). A Human-Cyber-Physical System toward Intelligent Wind Turbine Operation and Maintenance. *Sustainability*, *13*(2), 561. https://doi.org/10.3390/su13020561
[10] Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*, 103614. https://doi.org/10.1016/j.compind.2022.103614
[11] Crnobrnja, J., Stefanovic, D., Romero, D., Softic, S., & Marjanovic, U. (2023). Digital Transformation Towards Industry 5.0: A Systematic Literature Review. In E. Alfnes, A. Romsdal, J. O. Strandhagen, G. Von Cieminski, & D. Romero (Eds.), *Advances in Production Management Systems. Production Management Systems for Responsible Manufacturing, Service, and Logistics Futures* (Vol. 689, pp. 269–281). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-43662-8_20
[12] Díaz, J. E. M. (2022). Cybersecurity and Internet of Things. Outlook for this decade. *Computación y Sistemas*, *26*(3). https://doi.org/10.13053/cys-26-3-3925
[13] Ganji, K., & Afshan, N. (2024). A bibliometric review of Internet of Things (IoT) on cybersecurity issues. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/JSTPM-05-2023-0071

[14] Golovianko, M., Terziyan, V., Branytskyi, V., & Malyk, D. (2023). Industry 4.0 vs. Industry 5.0: Co-existence, Transition, or a Hybrid. *Procedia Computer Science*, *217*, 102–113. https://doi.org/10.1016/j.procs.2022.12.206
[15] Komosar, A., Stefanović, D., & Sladojević, S. (2024). An overview of image processing in biomedicine using U-Net convolutional neural network architecture. *Journal of Computer and Forensic Sciences*, *3*(1), 5–20. https://doi.org/10.5937/jcfs3-48848
[16] Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, *6*(4), 239–242. https://doi.org/10.1007/s12599-014-0334-4
[17] Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004
[18] Liao, S., Lin, L., & Chen, Q. (2023). Research on the acceptance of collaborative robots for the industry 5.0 era—The mediating effect of perceived competence and the moderating effect of robot use self-efficacy. *International Journal of Industrial Ergonomics*, *95*, 103455. https://doi.org/10.1016/j.ergon.2023.103455
[19] Matheu, S. N., Hernandez-Ramos, J. L., & Skarmeta, A. F. (2019). Toward a Cybersecurity Certification Framework for the Internet of Things. *IEEE Security & Privacy*, *17*(3), 66–76. https://doi.org/10.1109/MSEC.2019.2904475
[20] Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2021). A Survey of Cybersecurity Certification for the Internet of Things. *ACM Computing Surveys*, *53*(6), 1–36. https://doi.org/10.1145/3410160
[21] Mughaid, A., Obeidat, I., Abualigah, L., Alzubi, S., Daoud, M. Sh., & Migdady, H. (2024). Intelligent cybersecurity approach for data protection in cloud computing based Internet of Things. *International Journal of Information Security*, *23*(3), 2123–2137. https://doi.org/10.1007/s10207-024-00832-0
[22] Nelufule, N., Singano, T., Masemola, K., Shadung, D., Nkwe, B., & Mokoena, J. (2024). An Adaptive Digital Forensic Framework for the Evolving Digital Landscape in Industry 4.0 and 5.0. *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, 1686–1693. https://doi.org/10.1109/IDCIoT59759.2024.10467482
[23] Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the Internet of Things in Industrial Management. *Applied Sciences*, *12*(3), 1598. https://doi.org/10.3390/app12031598
[24] Rakic, S., Medic, N., Leoste, J., Vuckovic, T., & Marjanovic, U. (2023). Development and Future Trends of Digital Product-Service Systems: A Bibliometric Analysis Approach. *Applied System Innovation*, *6*(5), 89. https://doi.org/10.3390/asi6050089
[25] Rudenko, R., Pires, I. M., Oliveira, P., Barroso, J., & Reis, A. (2022). A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity. *Electronics*, *11*(11), 1742. https://doi.org/10.3390/electronics11111742

[26] Slavic, D., Marjanovic, U., Medic, N., Simeunovic, N., & Rakic, S. (2024). The Evaluation of Industry 5.0 Concepts: Social Network Analysis Approach. *Applied Sciences*, *14*(3), 1291. https://doi.org/10.3390/app14031291

[27] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

[28] Thom, J., Das, T., Shrestha, B., Sengupta, S., & Arslan, E. (2021). Casting a Wide Net: An Internet of Things Testbed for Cybersecurity Education and Research. *2021 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, 1–8. https://doi.org/10.23919/SPECTS52716.2021.9639278

[29] Vuckovic, T., Stefanovic, D., Dionisio, R., Dakic, D., & Havzi, S. (2022, April). Learning Environment Digital Transformation: Systematic Literature Review. *Proceedings on 18th International Conference on Industrial Systems – IS'20*. Conference on Industrial Systems – IS'20. https://doi.org/10.1007/978-3-030-97947-8_12