frontiers | Frontiers in Computer Science

TYPE Review
PUBLISHED 26 July 2024
DOI 10.3389/fcomp.2024.1434436

OPEN ACCESS

EDITED BY
Saqib Saeed,
Imam Abdulrahman Bin Faisal University,
Saudi Arabia

REVIEWED BY
Polinpapilinho F. Katina,
University of South Carolina Upstate,
United States
Neda Azizi,
Torrens University Australia, Australia

*CORRESPONDENCE
Ravdeep Kour
ravdeep.kour@ltu.se

RECEIVED 17 May 2024
ACCEPTED 15 July 2024
PUBLISHED 26 July 2024

CITATION
Kour R, Karim R, Dersin P and Venkatesh N (2024) Cybersecurity for Industry 5.0: trends and gaps.
Front. Comput. Sci. 6:1434436.
doi: 10.3389/fcomp.2024.1434436

Cybersecurity for Industry 5.0: trends and gaps

Ravdeep Kour*, Ramin Karim, Pierre Dersin and Naveen Venkatesh

Division of Operation and Maintenance Engineering, Luleå University of Technology, Luleå, Sweden

Industry 5.0 promises to revolutionize the industry by focusing on human-centric, sustainability, and resilience empowered by emerging technologies such as Artificial Intelligence (AI) and digitalization. This paradigm shift is expected to bring significant advancements in sustainability, resilience, productivity, effectiveness, efficiency, customization, reliability, safety, security, maintainability etc. However, this shift of the industrial paradigm introduces substantial cybersecurity challenges due to the increased attack surface and data sensitivity. Therefore, the objective of this paper is to conduct a thorough literature review of the recent research on cybersecurity in Industry 5.0, highlighting emerging trends, gaps, and potential solutions. To conduct this research, the authors have applied the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology to investigate cybersecurity solutions in Industry 5.0. The findings reveal that conceptual research dominates, with AI, Blockchain, and Internet of Things (IoT) most prevalent but highlights a gap in linking cybersecurity to resilience and sustainability. Furthermore, the paper aims to present trends in cybersecurity research with more relevant results from 2022 to 2024. It conducts a thorough review of the literature, highlighting the evolving landscape of cybersecurity applications in Industry 5.0.

KEYWORDS

cybersecurity, Industry 5.0, human-centric, resilient, sustainable

Introduction

Industry 4.0 revolutionized industries with automation, interconnectivity, and data-driven decision-making. Industry 5.0 builds upon these foundations by introducing human-centric collaboration with intelligent machines (Breque et al., 2021). This collaborative environment leverages Artificial Intelligence (AI), big data analytics, and advanced robotics to achieve mass customisation, real-time optimisation, and self-learning processes. The interconnected nature of Industry 5.0 may introduce various cybersecurity-related aspects that need to be addressed, to ensure the required level of system safety and security. Some of these aspects are:

- Increased Attack Vectors: The proliferation of connected devices (machines, sensors, robots) creates numerous entry points for attackers.
- Data Security Concerns: The vast amount of sensitive data generated and collected in Industry 5.0 systems (production data, customer information, AI models) necessitates robust data security measures.
- Supply Chain Vulnerabilities: The interconnectedness of Industry 5.0 extends beyond factory walls, encompassing suppliers and partners. Vulnerabilities in any part of the supply chain can be exploited to gain access to core systems.

- AI Security Risks: The integration of AI introduces new attack vectors. Malicious actors can target AI algorithms to manipulate outputs, disrupt operations, or steal intellectual property.
- Human-Machine Collaboration Risks: The close collaboration between humans and machines necessitates secure authentication protocols to prevent unauthorized access or manipulation by either party.

According to Orange cyberdefense Security Navigator 2024 Report (Orangecyberdefense, 2023), most of the targeted industry in the year 2023 was Manufacturing (See Figure 1).

Figure 2 shows timeline of some of the occurrences of cyberattacks happened in past in various industries including nuclear, manufacturing, water facility, pipeline, transportation, aviation, Information Technology (IT), and so on.

The impacts of these cyberattacks are briefly discussed below:

- *Iran's nuclear facilities attack (2010)*: Stuxnet a computer worm that infected computer networks through USB-flash drives and switched off safety devices, causing centrifuges to spin out of control (Langner, 2011).
- *WannaCry Ransomware Attack (2017)*: It damaged worth more than $4 billion with 300,000 infected computers (Akbanov et al., 2019).
- *Norsk Hydro (2019)*: A trusted customer's email tricked a Norsk Hydro employee, causing a ransomware attack that shut down plants, forced manual operations, and cost the company $40 million (Salviotti et al., 2023).
- *The Florida water plant attack (2021)*: Attacker changed the chemical levels of the water supply by increasing the amount of sodium hydroxide, but it was thwarted by a watchful operator before it could cause harm (Cervini et al., 2022).
- *Colonial Pipeline Ransomware Attack (2021)*: Leading to fuel delivery disruption and panic buying across the United States, the company paid the ransom demanded by the hacker group (75 bitcoin, or approximately $4.4 million USD; Beerman et al., 2023).
- *Toyota (2022 and 2023)*: A cyberattack in 2022 halted Toyota production in Japan, while a 2023 ransomware attack on their financial services in Germany exposed data and demanded an $8 million ransom (Arctic Wolf, 2024).
- *Bridgestone Americas (2022)*: A LockBit cyberattack forced Bridgestone to shut down manufacturing across North and Latin America for days, compromising customer and employee data (Arctic Wolf, 2024).
- *Johnson Controls (2023)*: A ransomware attack by The Dark Angels stole over 27 Terabyte of data and demanded a $51 million ransom (Arctic Wolf, 2024).
- *Scandinavian Airlines website hit by cyberattack (2023)*: SAS website was down for a few hours and customer details exposed to customers who are active during the attack (SAS, 2023)
- *IT company Tietoevry's hit by ransomware (2024)*: This cyberattack affected several customers and forced several stores to close across Sweden (Tietoevry, 2024).

Cyberattacks can compromise people's safety, because system failures, damage organizational reputations, lead to monetary losses, and compromise data accuracy. They also impact a system's Reliability, Availability, Maintainability, and Safety (RAMS), ultimately threatening its dependability. Since dependability encompasses availability, reliability, maintainability, and maintenance support

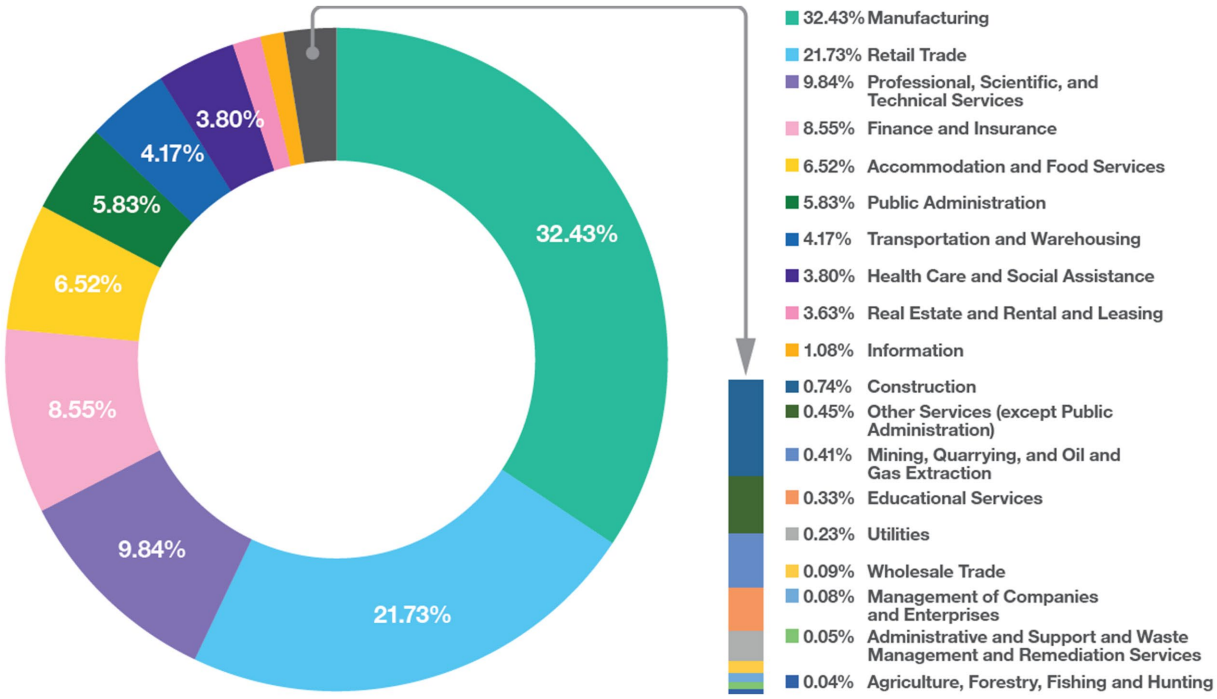

FIGURE 1
Cyberattack targeted industry in the year 2023 (Orangecyberdefense, 2023).

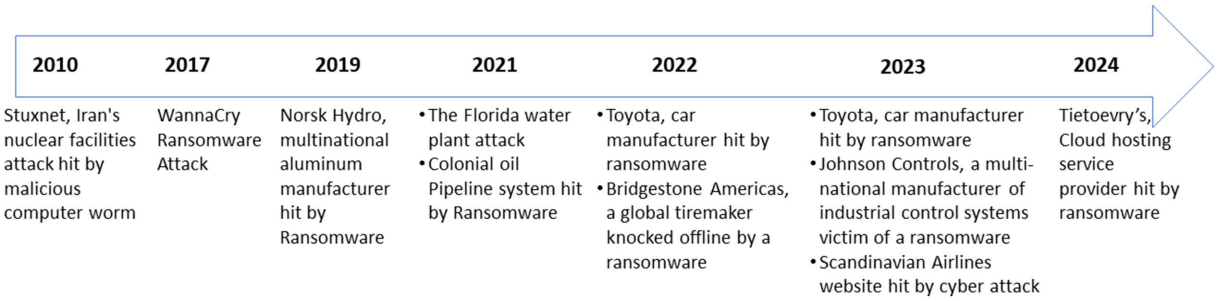

FIGURE 2
Timeline of some of the occurrences of cyberattacks in industries.

(International Electrotechnical Commission, 2015), improved cybersecurity will have direct positive impact on the overall dependability of the system.

Several efforts have been undertaken to protect data, including the introduction of regulations like the European Union's General Data Protection Regulation (GDPR) (European Union, 2016). To stay secure, industries must be vigilant about emerging cybersecurity trends and threats. The European Union (EU) has implemented the Network and Information Security (NIS 2) Directive specifically to safeguard critical infrastructure (European Commission, 2022). Another available series of standards for industrial communication networks and systems security include IEC 62443 (Industrial Society of Automation, 2020). Industry 5.0 lacks specific regulations, but existing frameworks like GDPR (European Union, 2016), IEC 62443 (Industrial Society of Automation, 2020), and ISO 27001 (ISO/IEC 27001:2022, 2022) can be leveraged for security until dedicated standards emerge.

After this introduction section, Research Methodology, outlines the methods used to conduct this review process. Results present the overall trend of cybersecurity research within Industry 5.0, analyzing publications by year, geographic location, and technology. It also covers the aspects of Industry 5.0 related to cybersecurity along with a comparative analysis and discussions of the reviewed literature. Next comes the Conclusion, followed by Acknowledgments.

Research methodology

The research methodology employed in this paper has followed PRISMA methodology (Page et al., 2021). PRISMA promotes transparent reporting of systematic reviews, it does not inherently address limitations of included studies or assess all potential biases. These aspects require additional methodological considerations during the review process. PRISMA encompasses the following components: Eligibility Criteria, Information Sources, Search Process, Study Selection, and Data Collection & Analysis of Results.

Eligibility criteria

Articles considered for this review must meet the following criteria:

- Publication within last 5 years.
- Availability of the full-text manuscript on Google Scholar and Scopus
- Publication in a peer-reviewed or scholarly journal or conference, or thesis.
- Availability in the English language.

Information sources

To extract relevant literature pertaining to the cybersecurity within Industry 5.0, the authors of this paper explored two databases: Google Scholar and Scopus.

Search strategy

To recognize the initial scope of cybersecurity in Industry 5.0, the authors of this paper have conducted a web-based search. The study used popular databases, including Scopus and Google Scholar. The search query used were "industry 5.0" AND cybersecurity OR secure OR privacy OR security OR threats OR hacking. All the literature were merged to delete duplicate entries, and authors were left with 30 papers to carry out the review.

Study selection

This review paper has focused on the study of cybersecurity research within Industry 5.0. From an initial pool of 30 papers, 18 were selected based on eligibility criterion and their relevance to Industry 5.0. These 18 papers were then analyzed in detail, with a specific focus on technologies, research method, and industrial aspect.

Data collection and analysis of results

The search strategy applied for web-based exploration within these databases is outlined in Figure 1. The search strings have been defined in section 2.3. The majority of the identified literature sources were obtained from the Scopus database. All literature considered for inclusion in this study underwent independent evaluation by three researchers to determine its relevance. Only literature aligning with

the study's criteria was retained. Any literature that did not meet these criteria, as determined by at least two researchers, was excluded. Subsequently, after eliminating redundant or unrelated materials, a total of 18 papers were selected for review. These selected reviewed papers are from 2022 to 2024. Our initial search focused on papers published within the past 5 years. We found that the most relevant papers fall within the range of 2002 to 2024. Additionally, as Industry 5.0 is an emerging concept, there is limited existing literature on the topic. A visual representation of the literature review process using PRISMA method is presented in Figure 3.

The scope of this paper is limited to addressing cybersecurity in the context of Industry 5.0's focus on resilience, human-centricity, and sustainability, rather than providing a critical or exhaustive literature review, we primarily utilized two databases. For future, more comprehensive reviews, we will consider including additional resources such as Web of Science and IEEExplore.

Results

Trends in cybersecurity research in Industry 5.0

A literature review has been conducted of 18 papers from internationally recognized academic journals and conferences published between 2022 and 2024, addressing cybersecurity in the context of Industry 5.0's focus on resilience, human-centricity, and sustainability. Figure 4 presents statistics on literature related to cybersecurity research within Industry 5.0. Of these, most were published in 2023 (67%). The distribution of publication venues leans toward conferences (50%) with journals following at (39%). Geographically, the studies originated primarily from India (33%), followed by Pakistan (11%) and Russia (11%).

Among the 18 reviewed papers, the most common research method is conceptual (39%) (See Figure 5). Comparative analysis follows at 33%, with experimental methodology (22%) and multi-criteria analysis (5%) also being used. Blockchain technology and Internet of Things (IoT) are the most prevalent technologies employed in the reviewed literature (See Figure 5). The datasets used include Edge-IIoTset and ToN-IoT dataset (Dey et al., 2024), Empirical data collected from 50 people (Dmitrieva et al., 2024), Hybrid dataset (Sharma et al., 2023), FEMINIST and CIFAR-10 (Singh et al., 2023), CIC-DDOS2019 and CSE-CIC-IDS2018 (Wu et al., 2023), and Kaggle (Siddique et al., 2023).

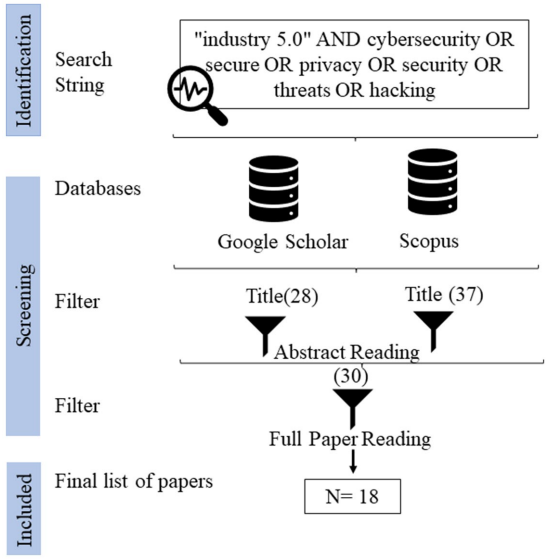

FIGURE 3
Research Methodology based on PRISMA method.

Industry 5.0 and cybersecurity

Industry 5.0 marks a significant shift in manufacturing, placing humans back at the center alongside intelligent machines. While this human-centric collaboration unlocks immense potential, it also introduces new cybersecurity challenges. To ensure a secure and sustainable future, cybersecurity needs to be woven into the very fabric of Industry 5.0, considering its core principles: human-centricity, sustainability, and resilience. Figure 6 represents a proposed schematic of cybersecurity considerations within industry 5.0.

Human-centricity and cybersecurity

According to the "Human Risk Review 2023," (SoSafe, 2023) the human element remains a critical factor in cybersecurity. The report emphasizes the rise of social engineering tactics and a surge in cyber threats powered by geopolitics and the remote work landscape. These factors elevate the vulnerability of human actors. Additionally, the report explores the risks associated with security gaps in supplier systems and the dominance of ransomware attacks. To address these challenges, the report concludes by offering recommendations (Kour, 2020), including security awareness training, implementation of remote work security measures, supplier security evaluations, and the development of robust incident response plans. In 1996 Zurko and Simon (Ellen et al., n.d.) proposed a user-friendly approach to security, where security features are designed with usability in mind. The authors highlight three key areas for user-friendly security:

- Usability testing: Applying usability testing techniques to security systems to ensure they are easy to understand and use.
- User-friendly security models and mechanisms: Developing security models and mechanisms that are user-friendly and do not require extensive technical knowledge.
- User needs as the primary goal: Prioritizing user needs throughout the security design process, ensuring security features integrate seamlessly with user workflows.

In Industry 5.0, user-friendly security makes security features clear and easy to use, empowering employees and minimizing the risk of human error in a human-machine collaboration environment. This reduces complexity and disruptions, creating a more secure and efficient system. Human-centric design principles encourage creating security features that are easy to understand and integrate into workflows. Complex procedures lead to workarounds and mistakes, increasing security vulnerabilities. Usable security reduces this risk.

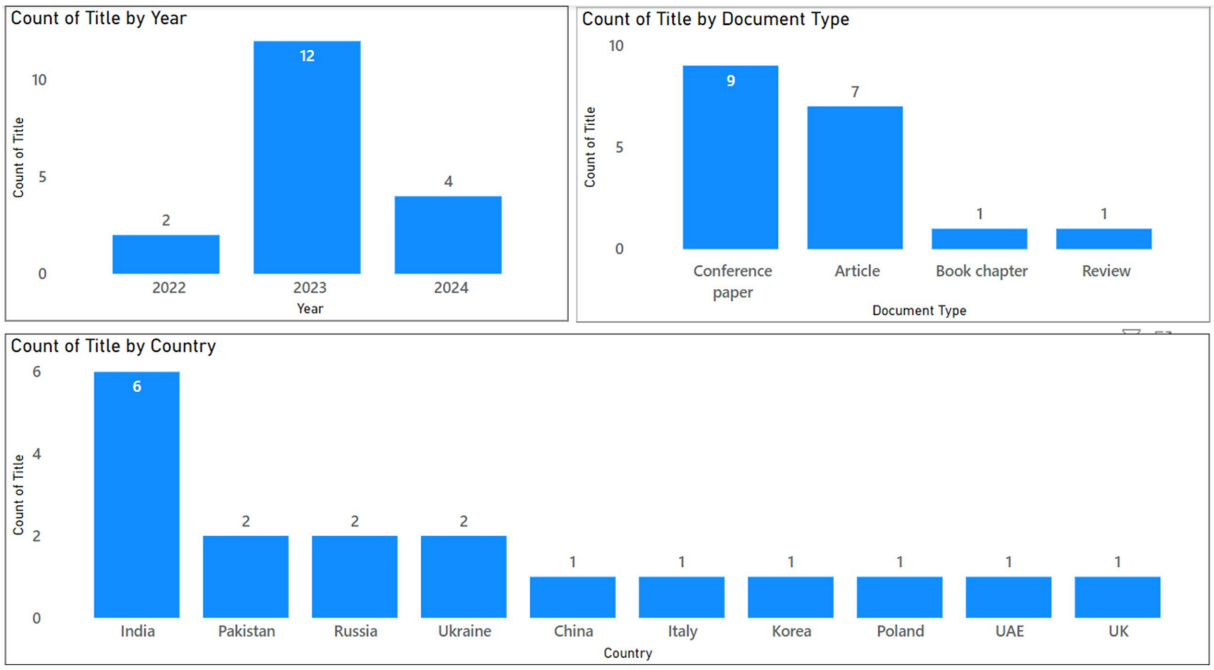

FIGURE 4
Statistics of current literature related to cybersecurity in Industry 5.0.

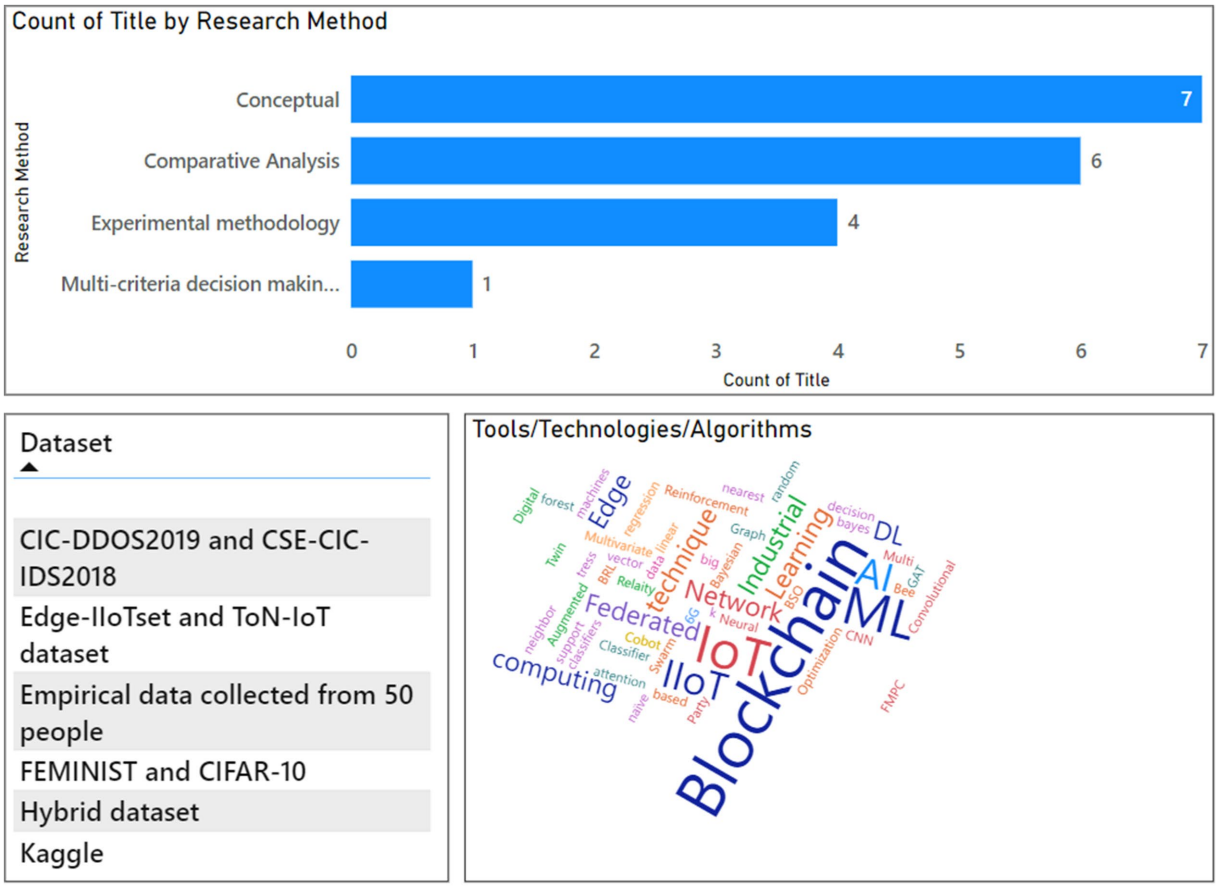

FIGURE 5
Research methods, technologies, and datasets used within the reviewed literature.

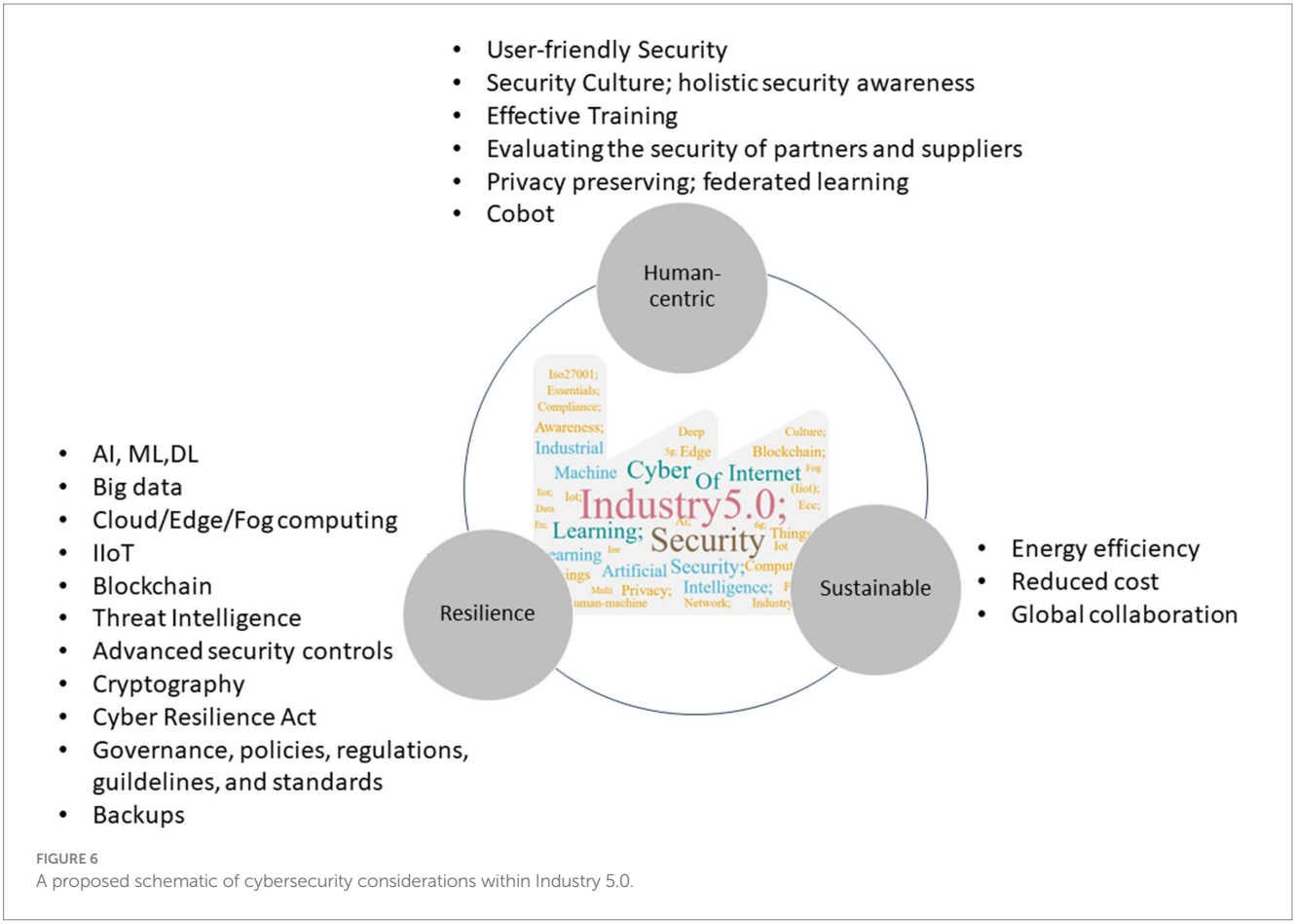

FIGURE 6
A proposed schematic of cybersecurity considerations within Industry 5.0.

A human-centric Industry 5.0 fosters a culture of security awareness. By educating employees, organizations can create a workforce actively involved in protecting systems and data. This reduces the success rate of social engineering attacks that prey on human error. The evolving nature of cyber threats necessitates ongoing training for employees. A human-centric approach ensures training programs are engaging and cater to different learning styles. This improves knowledge retention and promotes better security practices. Additionally, suppliers are the weak link in cyberattacks. According SoSafe - Human Risk Review 2023, 80% of security professionals agree their security relies on partners' security (SoSafe, 2023).

Solutions

To address the human element in cybersecurity, prioritizing cybersecurity awareness training is crucial. Equipping employees to recognize phishing attempts, social engineering tactics, and secure coding practices strengthens the organization's overall defense (Kour and Karim, 2020). Furthermore, implementing multi-factor authentication (MFA) and role-based access control (RBAC) strengthens access control measures. MFA and RBAC ensure that only authorized personnel have access to specific systems and data, minimizing the risk of unauthorized access. However, secure communication protocols for human-machine interaction require further research and development. As reliance on technology grows, robust protocols that safeguard communication channels are essential for comprehensive cybersecurity solutions.

Sustainability and cybersecurity

Industry 5.0 integrates sustainability into its core principles by utilizing interconnected supply chains and data-driven initiatives like closed-loop manufacturing. However, this interconnectedness creates a complex cybersecurity landscape including security controls. NIST recognized the most emissive security controls by applying qualitative methods. According to NIST, 50% of cybersecurity emissions are from the use of resilience activities (like, redundancy capabilities) and endpoints (Wavestone, 2024). While advancements like Industrial Internet of Things (IIoT) are crucial for environmental monitoring, they introduce resource limitations and potential vulnerabilities. Furthermore, with rising energy demands from data centers, exploring energy-efficient security solutions and mitigating vulnerabilities across interconnected ecosystems becomes paramount for building a sustainable future in Industry 5.0.

Solutions

Standardizing secure communication protocols across the supply chain can significantly minimize attack vectors. Optimizing the volume of logs collected and stored can help to reduce emissions (Wavestone, 2024). Sharing threat intelligence and implementing authentication methods that do not require dedicated physical equipment can contribute to fewer emissions (Wavestone, 2024). Additionally, strong data encryption and access controls ensure only authorized personnel can access sensitive data and help protect confidentiality while enabling valuable insights for sustainable

practices. As (Shaikh et al., 2024) suggests, AI-driven architectures with blockchain technology can optimize energy usage and secure data, bridging the gap between legacy industrial robustness and future productivity gains.

Resilience and cybersecurity

The Cyber Resilience Act (CRA) (European Union, 2022) mandates the integration of security features within manufacturing equipment, promoting the development of more secure hardware and software solutions. This aligns with the National Institute of Standards and Technology (NIST) definition of resilience (Ross et al., 2019), which emphasizes a system's capacity to anticipate, withstand, recover from, and adapt to cyber threats. As depicted in Figure 7 [adapted from Haque et al. (2021), Haque et al. (2021), Bodeau et al. (2015), and Bodeau et al. (2015)], a resilience curve illustrates system performance during a cyberattack over time. The five stages represent the entire resilience cycle, with the area under the curve serving as a quantitative measure of a system's cyber resilience (Haque et al., 2021). This value helps assess weaknesses and develop mitigation strategies (Haque et al., 2021). This approach, also known as functionality-based, allows for the creation of specific resilience metrics for Industrial Control Systems (ICS) as proposed by Haque et al., (2021).

Building upon these concepts, researchers have employed similar resilience stages to propose a cybersecurity approach (Kour et al., 2023) that predicts, prevents, and monitors cyberattack penetration probabilities at each stage of the Kill Chain Model (CKC) (Lockheed Martin, 2023). Additionally, studies have explored the potential of Blockchain technology (Zhang and Van Luttervelt, 2011; Leng et al., 2022, 2023a,b) and machine learning-based intrusion detection systems (Javeed et al., 2023) for enhancing resilience in manufacturing systems. Furthermore, AI-powered models have been proposed to analyze adversary behavior and predict vulnerabilities in critical infrastructure, enabling the implementation of targeted security measures and improved cyber resilience (Abuhasel, 2023).

Solutions

Industry 5.0's focus on interconnected, sustainable practices creates complex security challenges. While advancements like IIoT are crucial, they introduce resource limitations and vulnerabilities. Multi-layered security solutions are essential. Implementing robust intrusion and anomaly detection systems alongside research into secure AI can help prevent attacks. Network segmentation and resilient infrastructure are crucial, but Industry 5.0 also requires redundancy in critical systems and data backups for attack resilience. This redundancy can lead to increased emissions, as discussed in section 3.22. Therefore, a balanced solution is needed to trade-off between resilience and sustainability. This topic can be further explored in future research. Additionally, by adopting a culture of cybersecurity awareness alongside these technical solutions, we can build a human-centric, sustainable, and resilient Industry 5.0.

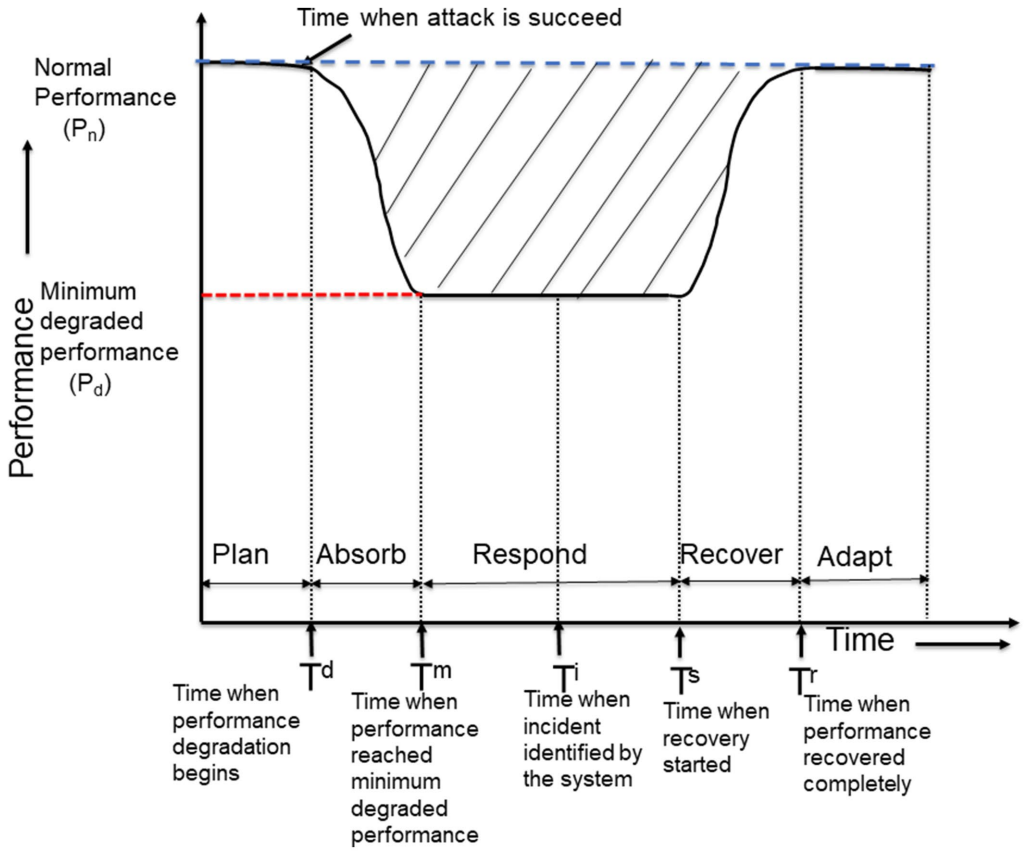

FIGURE 7
Resilience curve with different phases of action [adapted from Haque et al. (2021) and Bodeau et al. (2015)].

Comparative analysis and discussions

Several recent articles shed light on the evolving cybersecurity trends in Industry 5.0. (Bakkar, 2023) explores the cybersecurity landscape of Industry 5.0, examining prevalent attack methods, potential vulnerabilities, and the resulting challenges that industrial organizations face in this evolving technological era. The most discussed cyberattacks and methods in the literature are Distributed Denial of Service (DDOS), Shellcode, Spoofing, Tampering, Repudiation, Information Disclosure, Elevation of Privilege (STRIDE), brute force, cross site scripting (XSS), structured query language (SQL) injection, infiltration, port scanning, botnets, malware attacks, data breaches, and illegal access (Lechachenko et al., 2023; Sharma et al., 2023; Wu et al., 2023; Dmitrieva et al., 2024).

In addition to this, a systematic analysis by authors (Czeczot et al., 2023) outlines the increased attack surface due to the proliferation of connected devices like machines, sensors, IoT, IIoT, and robots. This vast network of interconnected systems creates numerous entry points for attackers, as highlighted in Kour et al., (2019); Czeczot et al., (2023); Dey et al., (2024). Furthermore, authors like (Lechachenko et al., 2023) emphasize the cybersecurity aspects in Industry 5.0. The vast amount of sensitive data generated (production data, customer information, AI models) necessitates robust cybersecurity measures to prevent breaches and unauthorized access.

The close collaboration between humans and machines in Industry 5.0 necessitates secure authentication protocols to prevent unauthorized access or manipulation by either party. This human-machine collaboration risk is addressed by Abishek et al., (2023). In a paper by Rawindaran et al., (2023), a security mindset was discussed that means constantly being aware of threats and taking steps to safeguard yourself and your surroundings. Humans have been the weakest links in cybersecurity. Therefore, their training and awareness are a must. This has been discussed by many researchers in papers (Bakkar, 2023; Czeczot et al., 2023; Rawindaran et al., 2023; Dmitrieva et al., 2024).

The Table 1 presents an analysis of research trends, gaps, and focus areas from various studies conducted between 2022 and 2024. The prevalent theme includes AI/ML/DL, which is frequently referenced across multiple studies, reflecting its central role in current research. Other prominent areas include blockchain distributed ledger technologies and Cloud/Edge/Fog computing, indicating a strong interest in decentralized and cloud-based solutions. IoT and Industrial IoT are also significant, highlighting the ongoing integration of connected devices in industrial applications. Cybersecurity aspects such as advanced security controls, cryptography, and cyber resilience appear consistently, emphasizing the growing importance of securing digital infrastructures. User-centric approaches like security training and collaboration are less frequently mentioned but still present, suggesting an awareness of the human factor in cybersecurity. User-friendly Security is notably absent from the studies, indicating a gap in research on accessible security solutions, while security cost and energy efficiency are scarcely addressed, suggesting room for further research in cost-effective measures and sustainable technology practices.

In summary, these 18 reviewed papers investigate into the critical issues of security and privacy within Industry 5.0. The papers range from advancements in core cryptographic techniques designed to strengthen overall security and privacy while minimizing computing resource usage (Shaikh et al., 2024), to the integration of blockchain technology for secure data management (Natalia et al., 2024). Researchers delve into explainable threat detection models, such as the BRL-ETDM (Bayesian reinforcement learning-based explainable threat detection model), to proactively identify and mitigate cyber threats in this new industrial landscape (Dey et al., 2024). Recognizing the increasing role of artificial intelligence (AI) in Industry 5.0, the papers explore both its benefits and drawbacks. Some studies examine AI's potential for threat prediction within the Industrial Internet of Things (IIoT) (Czeczot et al., 2023), while others highlight the need to address potential risks associated with AI adoption, such as job displacement, security vulnerabilities, and ethical considerations (Trunina et al., 2023). The human-centered approach of Industry 5.0 is reflected in research on securing Augmented Reality (AR) interfaces and patient privacy frameworks (Lechachenko et al., 2023). Furthermore, the reviewed papers explore novel methods for human-centric testing of IoT cybersecurity within Industry 5.0 (Waheed and Marchetti, 2023). Looking toward the future, the papers address data privacy concerns in Industry 5.0's decentralized environments, particularly those enabled by federated learning (Singh et al., 2023), and propose future research directions to optimize security and privacy for policymakers and practitioners (Navale et al., 2023).

Based on this conducted review following gaps have been identified in the literature.

- Few studies discuss cybersecurity in connection to big data, threat intelligence, advanced security technologies, cryptography, sixth generation (6G) cellular network, and governance.
- No literature addresses user-friendly security in Industry 5.0.
- A few studies discuss sustainability in terms of energy saving, cost reduction, and collaboration.
- The literature lacks in-depth discussion on the direct relationship between cybersecurity and Industry 5.0 aspects of resilience and sustainability.
- No literature discusses cybersecurity and all three aspects of Industry 5.0.

Additionally, literature shows a key gap in understanding how security concerns evolve from Industry 4.0 to Industry 5.0. By bridging this knowledge gap and fostering collaboration between researchers proposing different solutions, we can ensure comprehensive security for the human-centered future of Industry 5.0. This addition emphasizes the importance of understanding the changing security landscape between Industry 4.0 and 5.0. It highlights how collaboration can lead to more comprehensive security solutions for the future of industry.

Conclusion

This study conducted a thorough literature review of 18 academic papers published between 2022 and 2024, exploring cybersecurity considerations within the context of Industry 5.0's focus on resilience, human-centricity, and sustainability. Analysis of 18 papers revealed a strong emphasis on conceptual research and the prevalence of technologies like AI, blockchain and IoT. Studies highlighted the growing attack surface due to interconnected devices and the critical need for robust cybersecurity measures to protect sensitive data.

10.3389/fcomp.2024.1434436

TABLE 1 Cybersecurity literature in the context of Industry 5.0 technologies (presented in this study).

Year	References	AI/ML/DL	Big data	Cloud/Edge/Fog computing	IoT and industrial IoT	Blockchain distributed ledger	Threat intelligence	Advanced security controls	Cryptography	Cyber resilience	Governance	User-friendly security	Security culture	Security training	Suppliers security	Cobot	Federated learning	Energy efficiency	Security cost	Collaboration
2024	Dey et al. (2024)	x			x															
2024	Dmitrieva et al. (2024)	x												x						x
2023	Sharma et al. (2023)					x				x										
2023	Singh et al. (2023)			x	x	x														
2023	Wu et al. (2023)	x						x											x	
2023	Siddique et al. (2023)	x		x					x								x			x
2024	Shaikh et al. (2024)	x	x			x			x									x		
2023	Bakkar (2023)													x		x				x
2023	Lechachenko et al. (2023)				x		x													x
2023	Czeczot et al. (2023)	x		x	x	x	x			x			x	x						
2023	Abishek et al. (2023)															x				x
2023	Rawindaran et al. (2023)									x	x		x	x						x
2024	Natalia et al. (2024)					x				x										
2023	Trunina et al. (2023)	x													x		x			x
2023	Navale et al. (2023)	x	x	x	x	x							x	x	x					x
2023	Waheed and Marchetti (2023)				x						x			x	x					x
2022	Kohli et al. (2022)	x				x														
2022	Pant et al. (2022)	x			x	x														

However, the review also identified significant gaps in current research. Notably, limited attention has been paid to user-friendly security solutions and the intricate link between cybersecurity and Industry 5.0's core principles of resilience and sustainability. Furthermore, no existing literature comprehensively addresses cybersecurity across all three aspects of Industry 5.0.

These findings point toward important avenues for future research. Developing user-friendly security solutions and investigating the synergy between cybersecurity and industry 5.0's core values present exciting opportunities for advancing secure and sustainable industrial practices. Further exploration is also needed to understand how cybersecurity strategies can contribute to a more resilient and human-cantered Industry 5.0 future.

Author contributions

RavK: Conceptualization, Formal analysis, Investigation, Methodology, Visualization, Writing – original draft, Writing – review & editing. RamK: Funding acquisition, Project administration, Resources, Supervision, Writing – original draft, Writing – review & editing. PD: Writing – original draft, Writing – review & editing. NV: Writing – original draft, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. This work has been carried out within the framework, 'AI Factory'. The authors would like to express their gratitude to 'Sweden's innovation agency (VINNOVA)' for their financial support for 'AI Factory'. We would also like to thank JVTC (Luleå Railway Research Center) for their financial support.

Acknowledgments

We acknowledge the valuable support and resources provided by the eMaintenanceLAB in conducting this research.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Abishek, B. A., Kavyashree, T., Jayalakshmi, R., Tharunkumar, S., and Raffik, R. (2023). *Collaborative robots and cyber security in industry 5.0*. In: 2nd international conference on advancements in electrical, electronics, communication, computing and automation, ICAECA 2023. Institute of Electrical and Electronics Engineers Inc.

Abuhasel, K. A. (2023). A linear probabilistic resilience model for securing critical infrastructure in industry 5.0. *IEEE Access* 11, 80863–80873. doi: 10.1109/ACCESS.2023.3300650

Akbanov, M., Vassilakis, V. G., and Logothetis, M. D. (2019). WannaCry ransomware: analysis of infection, persistence, recovery prevention and propagation mechanisms. *J. Telecommun. Inform. Technol.* 1, 113–124. doi: 10.26636/jtit.2019.130218

Arctic Wolf. (2024). *The top 10 manufacturing industry cyber attacks*. Available at: https://arcticwolf.com/resources/blog/top-8-manufacturing-industry-cyberattacks/ (Accessed May 6, 2024).

Bakkar, M. N. (2023). *CyberSecurity essentials for industry 5.0*," in Advanced Research and Real-World Applications of Industry 5.0, (IGI Global), pp. 49–65.

Beerman, J., Berent, D., Falter, Z., and Bhunia, S. (2023). *A review of colonial pipeline ransomware attack*. In: Proceedings - 23rd IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing Workshops, CCGridW 2023.

Bodeau, D., Graubart, R., Heinbockel, W., and Laderman, E. (2015). *Cyber resiliency engineering aid: the updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques*. MITRE Corporation.

Breque, M., De Nul, L., and Petridis, A. (2021). Industry 5.0 - towards a sustainable, human- centric and resilient European industry. European Commission.

Cervini, J., Rubin, A., and Watkins, L. (2022). Don't drink the cyber: extrapolating the possibilities of Oldsmar's water treatment cyberattack. *Int. Conf. Cyber Warfare Secur.* 17, 19–25. doi: 10.34190/iccws.17.1.29

Czeczot, G., Rojek, I., Mikołajewski, D., and Sangho, B. (2023). AI in IIoT Management of Cybersecurity for industry 4.0 and industry 5.0 purposes. *Electronics (Switzerland)* 12:800. doi: 10.3390/electronics12183800

Dey, A. K., Gupta, G. P., and Sahu, S. P. (2024). BRL-ETDM: Bayesian reinforcement learning-based explainable threat detection model for industry 5.0 network. *Clust. Comput.* doi: 10.1007/s10586-024-04422-6

Dmitrieva, E., Balmiki, V., Bhardwaj, N., Kumar, K., Sharma, A., and Shruthi, C. H. M. (2024). *Security and privacy in AI-driven industry 5.0: experimental insights and threat analysis*. In: BIO Web of Conferences, (EDP Sciences).

Ellen, M., Org, Z. Z., and Simon, R. T. (n.d.). *User-centered security*.

European Commission. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the council of 14 December 2022 on measures for a high common level of cybersecurity across the union, amending regulation (EU) no 910/2014 and directive (EU) 2018/1972, and repealing directive (EU) 2016/1148 (NIS 2 directive)*.

European Union. (2016). *Regulation 2016/679 of the European parliament and the Council of the European Union. Official journal of the European Communities*.

European Union (2022). Cyber resilience act. France: European Union.

Haque, M. A., Shetty, S., Gold, K., and Krishnappa, B. (2021). Realizing cyber-physical systems resilience frameworks and security practices. *Stud. Syst. Decis. Control* 2021:361. doi: 10.1007/978-3-030-67361-1_1

Industrial Society of Automation. (2020). *ISA/IEC 62443 series of standards*. ISA/IEC 62443.

International Electrotechnical Commission. (2015). *IEC 60050-192:2015 international Electrotechnical vocabulary (IEV) - part 192: dependability*. IEC 60050–192:2015.

ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection – information security management systems – requirements*.

Javeed, D., Gao, T., Kumar, P., and Jolfaei, A. (2023). An explainable and resilient intrusion detection system for industry 5.0. *IEEE Trans. Consum. Electron.* 2023:704. doi: 10.1109/TCE.2023.3283704

Kohli, P., Sharma, S., and Matta, P. (2022). *Secured privacy preserving techniques analysis of 6G driven vehicular communication network in industry 5.0 internet-of-everything (IoE)* Applications., in 2022 international conference on SMART generation computing, communication and networking, SMART GENCON 2022, Institute of Electrical and Electronics Engineers Inc.

Kour, R., Aljumaili, M., Karim, R., and Tretten, P. (2019). eMaintenance in railways: issues and challenges in cybersecurity. *Proc. Inst. Mech. Eng. F J. Rail Rapid. Transit.* 233:2915. doi: 10.1177/0954409718822915

Kour, R., and Karim, R. (2020). Cybersecurity workforce in railway: its maturity and awareness. *J. Qual. Maint. Eng.* 27:59. doi: 10.1108/JQME-07-2020-0059

Kour, R. (2020). Cybersecurity in railway: a framework for improvement of digital asset security. Doctoral dissertation. (Sweden: Luleå University of Technology).

Kour, R., Patwardhan, A., Karim, R., Dersin, P., and Kumari, J. (2023). A cybersecurity approach for improved system resilience. Singapore: Research Publishing Services, 2514–2521.

Langner, R. (2011). Stuxnet: dissecting a cyberwarfare weapon. *IEEE Secur. Priv.* 9:67. doi: 10.1109/MSP.2011.67

Lechachenko, T., Kozak, R., Skorenkyy, Y., Kramar, O., and Karelina, O. (2023). *Cybersecurity aspects of smart manufacturing transition to industry 5.0 model.* In: 3rd International Workshop on Information Technologies: Theoretical and Applied Problems.

Leng, J., Chen, Z., Huang, Z., Zhu, X., Su, H., Lin, Z., et al. (2022). Secure Blockchain middleware for decentralized IIoT towards industry 5.0: a review of architecture, enablers, challenges, and directions. *Mach. Des.* 10:858. doi: 10.3390/machines10100858

Leng, J., Sha, W., Lin, Z., Jing, J., Liu, Q., and Chen, X. (2023a). Blockchained smart contract pyramid-driven multi-agent autonomous process control for resilient individualised manufacturing towards industry 5.0. *Int. J. Prod. Res.* 61:929. doi: 10.1080/00207543.2022.2089929

Leng, J., Zhu, X., Huang, Z., Xu, K., Liu, Z., Liu, Q., et al. (2023b). ManuChain II: Blockchained smart contract system as the digital twin of decentralized autonomous manufacturing toward resilience in industry 5.0. *IEEE Trans Syst Man Cybern Syst* 53:172. doi: 10.1109/TSMC.2023.3257172

Lockheed Martin (2023). Cyber kill chain® | Lockheed Martin. Bethesda, Maryland: Lockheed Martin.

Natalia, T., Pathani, A., Dhaliwal, N., Rajasekhar, N., and Khatkar, M. (2024). *Blockchain integration in industry 5.0: a security experiment for resilience assessment*. In: BIO Web of Conferences.

Navale, G. S., Madala, R., Managuli, M., Jayalakshmi, N., Kadiravan, G., and Rawat, R. (2023). *Research and innovation in next generation security and privacy in industry 5.0 Iot*. In: Proceedings of International Conference on Contemporary Computing and Informatics, IC3I 2023, (Institute of Electrical and Electronics Engineers Inc.), 1384–1390.

Orangecyberdefense. (2023). *Security navigator 2024*. Available at: www.orangecyberdefense.com.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ* 372:71. doi: 10.1136/bmj.n71

Pant, P., Rajawat, A. S., Goyal, S. B., Singh, D., Constantin, N. B., Raboaca, M. S., et al. (2022). *Using machine learning for industry 5.0 efficiency prediction based on security and proposing models to enhance efficiency*. In: Proceedings of the 2022 11th International Conference on System Modeling and Advancement in Research Trends, SMART 2022, (Institute of Electrical and Electronics Engineers Inc.), 909–914.

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., et al. (2023). Enhancing cyber security governance and policy for SMEs in industry 5.0: a comparative study between Saudi Arabia and the United Kingdom. *Digital* 3, 200–231. doi: 10.3390/digital3030014

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., and McQuaid, R. (2019). *Developing cyber resilient systems: Gaithersburg, MD*.

Salviotti, G., De Rossi, L. M., Abbatemarco, N., and Bjoernland, K. (2023). *Understanding the role of leadership competencies in cyber crisis management: a case study*. In: Proceedings of the Annual Hawaii International Conference on System Sciences.

SAS. (2023). *SAS cyber attack – update*. Available at: https://www.sasgroup.net/newsroom/press-releases/2023/sas-cyber-attack--update/ (Accessed May 6, 2024).

Shaikh, Z. A., Hajjej, F., Uslu, Y. D., Yuksel, S., Dincer, H., Alroobaea, R., et al. (2024). A new trend in cryptographic information security for industry 5.0: a systematic review. *IEEE Access* 12:1485. doi: 10.1109/ACCESS.2024.3351485

Sharma, A., Rani, S., Bashir, A. K., Krichen, M., and Alshammari, A. (2023). A low-rank learning-based multi-label security solution for industry 5.0 consumers using machine learning classifiers. *IEEE Trans. Consum. Electron.* 69:964. doi: 10.1109/TCE.2023.3282964

Siddique, A. A., Boulila, W., Alshehri, M. S., Ahmed, F., Gadekallu, T. R., Victor, N., et al. (2023). Privacy-enhanced pneumonia diagnosis: IoT-enabled federated multi-party computation in industry 5.0. *IEEE Trans. Consum. Electron.* 2023:565. doi: 10.1109/TCE.2023.3319565

Singh, S. K., Yang, L. T., and Park, J. H. (2023). FusionFedBlock: fusion of blockchain and federated learning to preserve privacy in industry 5.0. *Inform. Fusion* 90, 233–240. doi: 10.1016/j.inffus.2022.09.027

SoSafe. (2023). *Human risk review 2023. Lichtstrasse 25a 50825 Cologne, Germany*.

Tietoevry. (2024). *Ransomware attack in Sweden – restoration work progressing*. Available at: https://www.tietoevry.com/en/newsroom/all-news-and-releases/press-releases/2024/01/tietoevry-ransomware-attack-in-sweden--restoration-work-progressing/ (Accessed May 6, 2024).

Trunina, I., Bilyk, M., and Yakovenko, Y. (2023). *Artificial intelligence from industry 5.0 perspective: threats and challenges*. In: Proceedings of the 5th International Conference on Modern Electrical and Energy System, MEES 2023, (Institute of Electrical and Electronics Engineers Inc).

Waheed, T., and Marchetti, E. (2023). *The impact of IOT cybersecurity testing in the perspective of industry 5.0*. In: International conference on web information systems and technologies, WEBIST - proceedings, Science and Technology Publications, LDA, pp. 480–487.

Wavestone. (2024). *Can cybersecurity be made more sustainable?* Available at: https://www.wavestone.com/en/insight/cyber-sustainability-solutions/ (Accessed May 16, 2024).

Wu, Y., Nie, L., Xiong, X., Sadoun, B., Yang, L., and Ning, Z. (2023). Incremental update intrusion detection for industry 5.0 security: a graph attention network-enabled approach. *IEEE Trans. Consum. Electron.* 2023:1907. doi: 10.1109/TCE.2023.3331907

Zhang, W. J., and Van Luttervelt, C. A. (2011). Toward a resilient manufacturing system. *CIRP Ann. Manuf. Technol.* 60:41. doi: 10.1016/j.cirp.2011.03.041