Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.054150

REVIEW

A Review on Security and Privacy Issues Pertaining to Cyber-Physical Systems in the Industry 5.0 Era

Abdullah Alabdulatif[1], Navod Neranjan Thilakarathne[2,*] and Zaharaddeen Karami Lawal[3,4,*]

[1]Department of Cybersecurity, College of Computer, Qassim University, Buraydah, 51452, Saudi Arabia

[2]Department of ICT, Faculty of Technology, University of Colombo, Colombo, 00700, Sri Lanka

[3]Department of Computer Science, Federal University Dutse, Dutse, 720102, Nigeria

[4]Faculty of Integrated Technologies, Universiti Brunei Darussalam, Gadong, BE1410, Brunei Darusalam

*Corresponding Authors: Navod Neranjan Thilakarathne. Email: navod.neranjan@ict.cmb.ac.lk; Zaharaddeen Karami Lawal. Email: deenklawal13@gmail.com

Received: 20 May 2024 Accepted: 22 July 2024 Published: 12 September 2024

ABSTRACT

The advent of Industry 5.0 marks a transformative era where Cyber-Physical Systems (CPSs) seamlessly integrate physical processes with advanced digital technologies. However, as industries become increasingly interconnected and reliant on smart digital technologies, the intersection of physical and cyber domains introduces novel security considerations, endangering the entire industrial ecosystem. The transition towards a more cooperative setting, including humans and machines in Industry 5.0, together with the growing intricacy and interconnection of CPSs, presents distinct and diverse security and privacy challenges. In this regard, this study provides a comprehensive review of security and privacy concerns pertaining to CPSs in the context of Industry 5.0. The review commences by providing an outline of the role of CPSs in Industry 5.0 and then proceeds to conduct a thorough review of the different security risks associated with CPSs in the context of Industry 5.0. Afterward, the study also presents the privacy implications inherent in these systems, particularly in light of the massive data collection and processing required. In addition, the paper delineates potential avenues for future research and provides countermeasures to surmount these challenges. Overall, the study underscores the imperative of adopting comprehensive security and privacy strategies within the context of Industry 5.0.

KEYWORDS

Cyber-physical systems; CPS; Industry 5.0; security; data privacy; human-machine collaboration; data protection

1 Introduction

The industrial sector is an essential component of an economy, responsible for the production of material products that are highly mechanized and automated [1]. Since the Industrial Revolution's inception in the late 18th century (Industry 1.0), humankind has harnessed technology's power to drive progress. Industry 1.0 witnessed the rise of mechanical energy, while Industry 2.0, in the 1870s, focused more on electrical energy generation [2]. In addition, Industry 3.0, in the 1970s, focused on integrating electronics and information technologies into production, transforming manufacturing automation

[2,3]. Industry 4.0, the fourth iteration of the industrial revolution, leverages the collective potential of the Internet of Things (IoT), big data analytics, cloud computing, cognitive computing, robotics, and Artificial Intelligence (AI), among others, to establish smart Cyber-Physical Systems (CPSs). These CPSs effectively facilitate the integration of the virtual and physical worlds, enabling instantaneous communication and interaction [2,4].

The concept of Industry 4.0 pertains to integrating intelligent networking among machines and processes within the industrial sector [5,6]. This integration is facilitated by utilizing CPSs, which enables intelligent control by incorporating embedded networked systems [5]. The core concept behind Industry 4.0 is transforming the manufacturing sector into a "smart" industry, achieved through the interconnection of machines and gadgets capable of mutually controlling one another over their life cycles [7]. The main emphasis of Industry 4.0 is centered on the automation of processes, resulting in a decrease in human involvement within the manufacturing process. The primary objective of Industry 4.0 is to enhance overall productivity and performance by facilitating intelligent communication and interaction across various devices and applications, employing AI techniques [1,8–11].

Industry 4.0 is widely regarded as a revolution propelled by technology to enhance efficiency and productivity. It fosters the development of novel socio-technical infrastructures by reshaping various facets of a workplace, including health management and work organization, models for lifelong learning and career advancement, team structures, and knowledge management [5]. The socio-technical approach of the paradigm is characterized as a groundbreaking transformation in the interactions between humans, technology, and the environment [7]. Furthermore, Industry 4.0's focus on advanced automation and intelligence has overshadowed the consideration of human factors, potentially hindering sustainable human and societal development [9,10]. This necessitates greater attention and action from both industry experts and academia. While incorporating Industry 4.0 into frameworks like sustainability and sustainable supply chains can partially address this concern, a more comprehensive approach is needed to ensure a truly human-centric and sustainable future [9,11,12]. The advent of Industry 4.0 has brought about significant breakthroughs. Still, it has also posed issues that require a transition into Industry 5.0 to achieve sustainable growth and promote societal well-being [13–17]. Moreover, the promise for transformation, transparency, and connection inherent in Industry 4.0 brings cybersecurity threats, problems related to industrial espionage, and issues about data rights for organizations. Its complexity and associated costs sometimes hinder the adoption of integration, while compatibility concerns arise from partial implementation [1,12,13].

Furthermore, the effects of Industry 4.0 on the workforce, such as the displacement of jobs and the obsolescence of skills, necessitate strategic management to minimize resistance. In addition, the need for labor with advanced skills presents difficulties in recruiting and retaining such individuals [3,4,13,18–22]. Overall, the emergence of Industry 5.0 can be attributed to the concerns of humans and society during the industrial transition [23–27].

Overall, Industry 5.0 aims to rectify these limitations by strongly emphasizing human-centricity, sustainability, and resilience. It facilitates the establishment of a cooperative atmosphere in which humans and machines operate in synergy, promoting sustainable development and enhancing societal welfare [9]. Adopting Industry 5.0 allows enterprises to effectively address the limits of Industry 4.0 and achieve success in the evolving manufacturing landscape [14,15]. The inadequate focus on environmental preservation and sustainable technology within the framework of Industry 4.0 underscores the need for a transition towards Industry 5.0 [11,28–32].

The main objective of this study is to thoroughly examine and evaluate the security and privacy issues linked to CPSs within the context of Industry 5.0. Industry 5.0 represents the fifth iteration

of the Industrial Revolution, distinguished by integrating the physical, digital, and biological realms, resulting in extensively networked and intelligent systems named CPSs, which play a crucial function within the context of Industry 5.0 by facilitating instantaneous communication and interaction among diverse components [33–36]. Overall, CPS's growing integration and complexity in Industry 5.0 give rise to significant security and privacy concerns, endangering the underlying digital infrastructure and user data [28–32]. Industry 5.0 offers a paradigm shift with immense potential for organizations, governments, and society [37–40], whereas these challenges necessitate careful consideration and proactive measures to ensure the responsible and ethical implementation of Industry 5.0. On the other hand, to safeguard their crucial aspects and adhere to rules and regulations, organizations are compelled to prioritize cybersecurity, whereas policymakers must formulate all-encompassing frameworks for enhancing cybersecurity. In addition, policymakers must confront the societal ramifications associated with Industry 5.0, such as employment displacement, transparency, accountability, and sustainability. It is imperative for society to actively participate in the discourse regarding the ethical implementation of Industry 5.0 technologies while also ensuring that the advantages derived from these technologies are distributed in a fair manner. Thus, this study will examine the diverse security and privacy vulnerabilities associated with CPSs in Industry 5.0. The investigation will span several vital areas, analyzing security and privacy concerns, human interaction with CPSs, and providing solutions to the issues, which will contribute to developing effective mitigation methods and future research areas by providing a complete overview of the security and privacy landscape in Industry 5.0 CPSs. Researchers, industry practitioners, and policymakers involved in developing and deploying safe and privacy-preserving CPSs in Industry 5.0 will benefit from the findings of this research.

In this regard, the key contributions of the study can be outlined as follows:

- Provides an overview of the Industrial Revolution and a brief comparison of existing literature pertaining to the security and privacy aspect of the Industrial Revolution.
- Offers a brief overview of the role of CPSs in Industry 5.0 and the advantages of their integration.
- Provide a review of security and privacy concerns pertaining to the CPSs in Industry 5.0. Following the highlights of the security and privacy concerns provides insights into what countermeasures are available to tackle these concerns; furthermore, future prospects are also highlighted.

The methodology adopted in the study involves a keyword-based search for research and review articles in several scientific databases, including Web of Science, IEEE Xplore, Science Direct, and Google Scholar. The keywords used for the search were "Security", "Privacy," and "Security and Privacy" combined with one of the following terms: "Cyber-Physical Systems," "Industry 5.0 Era" and "Industry." Studies that referred to security or privacy but were not related to CPSs or Industrial eras were filtered out. The remaining studies were evaluated based on their relevance, key contributions, and proposed solutions, and they were utilized in the selection of the final studies for review.

The remainder of the study is organized in the following manner. Following the introduction, Section 2 provides an overview of the Industrial Revolution and then provides a summary of the latest state of the art to provide a comparison of our work with theirs. Section 3 provides a brief overview of Industry 5.0 and CPSs. Section 4 provides a brief discussion of security and privacy challenges pertaining to CPSs in Industry 5.0. Section 5 provides a brief overview of what countermeasures are available to overcome these challenges and highlight the future prospects. Finally, the study concludes with a conclusion.

2 Background and Related Work

The transition from agrarian and handicraft-based economies to industrial and machine-driven ones was symbolized by the Industrial Revolution, which was a pivotal era in human history [34–38]. A series of developments transpired throughout the 18th and 19th centuries, and their repercussions persisted well into the 20th century and beyond, paying the way towards a modernized world [34–38]. For a better understanding, the following briefly outlines the evolution of the Industrial Revolution:

1. *First Industrial Revolution (Late 18th to early 19th century)*
   During the first Industrial Revolution, the key innovations witnessed include the introduction of steam engines, mechanized textile production, and the development of factory systems. Overall, during this period, it led to significant growth in textile manufacturing, transportation (steam locomotives and steamships), and the coal and iron industries [34–38]. This revolutionized the way goods were produced and transported.
2. *Second Industrial Revolution (Mid to late 19th century)*
   During the Second Industrial Revolution, the key innovations witnessed include the widespread use of electricity, the internal combustion engine, and the expansion of the telegraph and telephone systems. Rapid industrialization, the rise of heavy industry (steel, chemicals, and machinery), urbanization, and the development of mass production techniques (assembly lines) were common during this period [34–38].
3. *Third Industrial Revolution (Late 19th to early 20th century)*
   During the Third Industrial Revolution, the key innovations witnessed include the rise of the automobile industry, aviation, and the development of new materials like plastics and synthetic chemicals. During this period, it transformed the way people lived, worked, and traveled, where the automobile made personal transportation more accessible, while aviation revolutionized long-distance travel and cargo transport [34–38].
4. *Fourth Industrial Revolution (Late 20th century to present)*
   The fourth Industrial Revolution is characterized by the digitalization of information, the Internet, robotics, AI, and biotechnology. Overall, during the period, it has led to automation, increased connectivity, the rise of e-commerce, and the proliferation of smartphones and personal computing devices [34–38].
5. *Current and future developments (21st century): Fifth Industrial Revolution*
   Continuing advancements in AI, renewable energy, 3D printing, and the IoT are driving the ongoing evolution of industry and society. These developments are likely to lead to further automation, increased efficiency, sustainable energy solutions, and new economic models. However, they also present challenges related to security and privacy, job displacement, and ethical concerns. According to [3,14,17,18], Industry 5.0 is highly dependent on the CPSs that were established during Industry 4.0. These CPSs, which facilitate the collaboration between humans and machines through the integration of computer intelligence and communication networks, serve as the foundation of Industry 5.0. Industry 5.0 revolutionizes automation through the integration of sophisticated AI into CPSs, facilitating extensive customization, a transition toward human proficiency, and an increased commitment to sustainability.

Overall, the Industrial Revolution has been a series of profound transformations in technology, economy, and society. Each phase has brought about new opportunities and challenges, and its effects are still felt today. The ongoing evolution of industry and technology is expected to continue shaping our world in ways we can only begin to imagine. Followed by the overview of the Industrial Revolution, the next section explains CPSs.

2.1 What Is CPS?

A CPS consists of many components that interact with the physical environment to develop intelligent solutions that address issues in various domains such as manufacturing, healthcare, transportation, smart city, and so on [39–43]. Overall, they emphasize the integration of software and hardware technologies, as well as the introduction of intelligent resources to automate utilization procedures [44–48]. In these systems, embedded computers and networks monitor and control the physical processes, with feedback loops, where physical processes affect computations and vice versa [48–51]. The key characteristic of CPS is the tight coupling of the cyber (computational) and physical elements. The typical structure of a CPS is shown in Fig. 1.

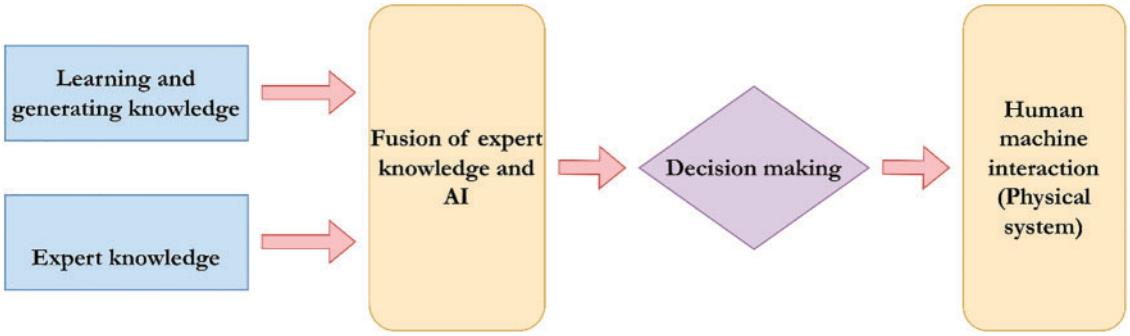

Figure 1: Structure of a CPS

Accordingly, CPS enriches its learning and knowledge-generation processes with expert knowledge using massive amounts of big data as input [40–44]. Consequently, decision-making for a specific issue within the entire CPS is facilitated by the fusion of AI and expert knowledge [45–48]. Overall, CPS is used in a wide range of applications, including industrial automation (smart manufacturing), transportation systems (autonomous vehicles, intelligent transportation systems), healthcare (robotic surgery, patient monitoring systems), energy systems (smart grids), and smart cities (urban infrastructure management) [42–46]. In summary, CPSs represent the fusion of digital computing and the physical world, enabling advanced monitoring, control, and automation across a wide range of applications and industries. Overall, they play a crucial role in the development of smart technologies and the advancement of industries in the era of Industry 5.0.

2.2 Summary of Related Research

Having provided a brief overview of the Industrial Revolution and CPSs, the main intention of this section is to summarize the latest available literature in terms of their attributes and prove that no previous research has been done on reviewing the security and privacy issues pertaining to CPSs in the context of Industry 5.0. Table 1 summarizes the recent literature, indicating whether the study presents Industry 5.0, CPSs, security and privacy concerns, and also the scope of the study.

Table 1: Summary of recent similar research

Reference	Present about Industry 5.0	Present about CPSs	Present about the security and privacy challenges	Present the countermeasures for overcoming security and privacy challenges	Scope of the study
[2]	✓	x	x	x	An analysis of the opportunities and challenges associated with the shift from Industry 4.0 to Industry 5.0 is presented.
[3]	x	✓	x	x	The design of intelligent CPSs that adhere to the cutting-edge smart factory framework for Industry 4.0 is highlighted.
[7]	✓	✓	x	x	The researchers analyze strategic methodologies to surmount the obstacles linked to Industry 4.0.
[8]	✓	✓	x	x	Conducts a survey about the possible uses and accompanying technologies of Industry 5.0.
[9]	✓	✓	x	x	Conducts a comparative bibliometric analysis to elucidate the interrelationships and distinctions between Industry 4.0 and Industry 5.0, as well as the ramifications of these developments on intelligent logistics.
[11]	✓	✓	x	x	The study presents Industry 5.0 as a potential resolution to the difficulties presented by the swiftly advancing digital technologies and artificial intelligence.
[12]	✓	✓	x	x	Humanization and sustainability-related aspects of the Industry 5.0 concept are discussed in the study.
[14]	✓	✓	x	x	A systematic analysis of Industry 5.0 is presented in order to provide an overview of its fundamental dimensions.
[17]	✓	✓	x	x	This research paper conducts a systematic literature review concerning CPSs and IoT.

(Continued)

Table 1 (continued)

Reference	Present about Industry 5.0	Present about CPSs	Present about the security and privacy challenges	Present the countermeasures for overcoming security and privacy challenges	Scope of the study
[18]	✓	✓	x	x	A heterogeneous architecture for Smart Cyber-Physical Systems (SCPS) was suggested by the researchers. This architecture allows for the integration of various electrical, pneumatic, and hydraulic processes in order to implement hybrid process dynamics.
[21]	✓	x	x	x	The authors present the challenges pertaining to Industry 5.0 implementation in the organizational context.
[22]	✓	x	x	x	This study introduces "The resilient Operator 5.0" concept, based on human operator resilience and human-machine systems resilience, providing a vision for the future of work in emerging Industry 5.0 hallmark.
[26]	✓	x	x	x	The study examines three defining characteristics of Industry 5.0—human-centricity, sustainability, and resiliency—along with its evolutionary trajectory.
[28]	✓	x	x	x	Upon implementing a personalized Industry 5.0 application that adheres to the conventional human-centered philosophy, the study identifies a number of ethical issues that must be resolved.
[31]	✓	x	x	x	This research paper conducts a bibliometric analysis in the Scopus database to support its tertiary examination of thirty-two literature reviews pertaining to Industry 5.0.
[34]	✓	✓	x	x	The authors provide a comprehensive analysis of Industry 5.0, detailing its philosophical and historical inception and development.

(Continued)

Table 1 (continued)

Reference	Present about Industry 5.0	Present about CPSs	Present about the security and privacy challenges	Present the countermeasures for overcoming security and privacy challenges	Scope of the study
[35]	✓	✓	x	x	The architecture of service-oriented digital twins in conjunction with metaverse-enabled platforms is described in this study. Furthermore, it offers recommendations for ambitious collaborations with the CPSs that extend beyond Industry 5.0 scenarios.
[36]	✓	✓	x	x	This research paper outlines the construction of a Human-Cyber-Physical System (HCPS) that utilizes a variety of sensing data to estimate operator risk within the framework of Industry 5.0.
[37]	✓	✓	x	x	An analysis is conducted to determine how systems in the manufacturing sector can benefit from the Industry 5.0.
[38]	✓	✓	x	x	The study examines the most recent Industry 5.0 applications and technologies and describes how Industry 5.0 appeared to surmount the obstacles posed by Industry 4.0.
[39]		✓	✓	x	A high-level overview of novel control-theoretic approaches for the security and privacy of CPSs is presented in this study.
[40]	x	✓	✓	x	Emerging security and privacy concerns in CPSs are discussed by the researchers, along with opportunities and challenges associated with the operation and development of such systems in a secure and privacy-preserving manner.
[41]	x	✓	✓	x	CPSs, cyber security challenges, characteristics, and associated technologies are described in thorough detail by the researchers.

(Continued)

Table 1 (continued)

Reference	Present about Industry 5.0	Present about CPSs	Present about the security and privacy challenges	Present the countermeasures for overcoming security and privacy challenges	Scope of the study
[42]	x	✓	✓	✓	The researchers analyze the differentiations that exist between CPSs' security and privacy and that of purely physical or cyber systems. They also propose potential strategies to strengthen these systems.
[43]	x	✓	✓	x	An overview of review studies conducted on the security and privacy of CPSs has been presented by the authors.
[44]	x	✓	✓	x	The authors have compiled a survey of concerns regarding the privacy and security of CPSs.
[46]	x	✓	✓	x	Showcasing limitations and future developments, the authors conduct an examination of the security and privacy of CPSs.
[47]	x	✓	✓	x	A comprehensive examination of the implementation of differential privacy techniques for CPSs is provided.
[48]	✓	x	✓	✓	The research paper provides an examination of the possible implementations of Industry 5.0, emphasizing obstacles and potential future developments.
[49]	✓	x	x	x	This study commences by analyzing the evolutionary path of Industry 5.0. It then proceeds to analyze three notable characteristics of Industry 5.0: an emphasis on human welfare and necessities, the capacity to endure and adapt, and the capability to recuperate.
[50]	x	✓	✓	x	The research examines security and privacy concerns at several levels within the architecture of a smart city. It specifically addresses domain-specific security challenges that arise from the implementation of CPSs in transportation, healthcare, smart grids, and smart homes.

(Continued)

Table 1 (continued)

Reference	Present about Industry 5.0	Present about CPSs	Present about the security and privacy challenges	Present the countermeasures for overcoming security and privacy challenges	Scope of the study
[51]	x	✓	✓	x	The primary aim of this study is to systematically compile and categorize the existing body of research concerning security and privacy concerns that emerge from the interface of the physical and digital realms, with a particular focus on diverse CPS applications.
Our study	✓	✓	✓	✓	Provide a review of security and privacy concerns pertaining to the CPSs in Industry 5.0 and also provide insights on what countermeasures are available to tackle these security and privacy concerns; further future prospects are also highlighted.

According to the summarized state of the art, it is evident that none of the research has been done in terms of reviewing the security and privacy concerns pertaining to CPSs in Industry 5.0, which has motivated us to conduct this review. Having provided background on the Industrial Revolution and CPSs, along with highlighting the summary of the related state of the art, the next section further explains Industry 5.0 and CPSs.

3 Industry 5.0 and Cyber-Physical Systems

The key intention of this section is to provide an overview of the key characteristics of Industry 5.0 and highlight the role and benefits of CPSs in Industry 5.0.

3.1 Characteristics of Industry 5.0

Industry 5.0 signifies the next phase of industrialization, emphasizing the synergistic cooperation between humans and machines to promote a more individualized and human-oriented interaction [34,35]. This concept is characterized by three fundamental pillars, as described below:

1. *Human-centric approach*
   Industry 5.0 focuses heavily on adopting a human-centric approach, wherein humans collaborate with robots and intelligent devices enabled by AI. This method aims to enhance human labor's abilities and potential, shifting away from an overreliance on technology to integrate critical thinking and adaptability [16,17].
2. *Resilience*
   The objective of Industry 5.0 is to bolster resilience by enabling human intervention when necessary, thereby supplementing the progress achieved in Industry 4.0 to provide assistance

rather than replace humans. This approach aims to foster the creation of employment opportunities that offer more excellent value, enhance the level of design autonomy for consumers, and promote the development of critical thinking skills and flexibility [16,18].

3. *Sustainability*
   Sustainability constitutes a core component of Industry 5.0, prioritizing comprehensive sustainability objectives and reintegrating human, environmental, and social aspects into one [11,19,20,34,35].

Fig. 2 below illustrates the intersection of the three pillars of Industry 5.0.

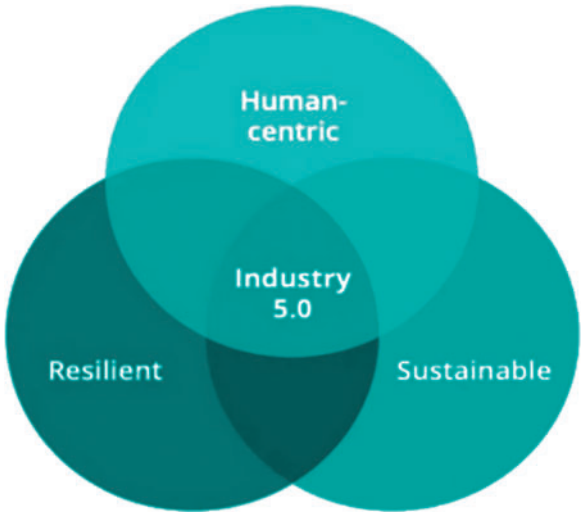

Figure 2: Three pillars of Industry 5.0

In general, the significance of Industry 5.0 resides in its capacity to create substantial transformations in organizational strategies and industrial practices. While CPS is a paradigm for Industry 4.0, Industry 5.0 places higher demands on human-centeredness and sustainability. This shift enables businesses and industries to proactively provide solutions for societal needs, conserve resources, and promote social stability. It fosters the creation of employment opportunities that offer greater value, enhances the level of creative autonomy for consumers, and promotes a work environment that prioritizes individualization and human-centered practices. In this context, some variants of CPS align more closely with the vision proposed by Industry 5.0. For example, Cyber-Physical-Social Systems (CPSS) proposed in [24] integrate social aspects into the cyber-physical framework, reflecting the human-centric and sustainable focus of Industry 5.0 [24].

Overall, Industry 5.0 holds significant importance due to its emphasis on the broader global context, encompassing not just productivity and profit but also the well-being of personnel, hence fostering interconnectedness. By prioritizing human and environmental considerations, Industry 5.0 aims to create more resilient and adaptable industrial ecosystems that contribute to overall societal advancement.

3.2 Role of Cyber-Physical Systems in Industry 5.0

CPSs are of paramount importance in Industry 5.0 as they facilitate secure and effective collaboration between humans and robots. They establish the groundwork for efficient collaboration between

human workers and robotic systems in the manufacturing industry by enabling real-time coordination, monitoring, safety protocols, data analysis, and adaptive processes. Overall, they facilitate human-robot collaboration by:

1. Adaptive and intelligent systems
   Integrating AI algorithms within CPSs enhances the adaptability and intelligence of these systems. Within the realm of human-robot collaboration, this cognitive ability empowers robots to acquire knowledge from human conduct, comprehend preferences, and modify their behaviors correspondingly [10].
2. Collaborative robotics (cobots)
   The CPS framework enables the advancement and implementation of collaborative robots, also known as cobots. These robotic systems are specifically engineered to collaborate with human operators, providing support and aid in various jobs. The role of CPS is to guarantee the safe operation of cobots, their ability to adapt to dynamic settings, and their efficient collaboration with human workers [21].
3. Integration of physical and digital systems
   CPSs combine physical processes with digital systems, establishing a cohesive linkage between the tangible realm and the virtual domain. Within the human-robot collaboration, CPSs facilitate the capability to monitor, control, and optimize physical processes in real-time, employing digital representations [22].
4. Real-time communication and data exchange
   The utilization of CPSs facilitates instantaneous communication and the exchange of data between human operators and robotic systems. This enables accelerated decision-making and adaptations to the production process in response to the changing manufacturing environment conditions [23].
5. Safety mechanisms
   Ensuring safety is of utmost importance in the context of human-robot collaboration. The implementation of safety measures, including collision detection, emergency stop systems, and predictive analytics, is of paramount importance in the functioning of CPSs, as they serve to identify potential dangers and mitigate accidents [23].
6. Sensing and perception
   Perception technologies and sophisticated sensors are essential elements of CPSs. These technological advancements enable robots to discern their environment, identify objects, and comprehend the gestures and actions of humans [16].
7. Skill augmentation
   Incorporating robotic systems in CPSs enables the enhancement of human talents. This symbiotic relationship between humans and robots has the potential to enhance production by leveraging their respective strengths. Humans contribute to their cognitive skills, while robots contribute to precision and efficiency [10].
8. Workflow optimization
   Using CPSs enables the enhancement of industrial processes in terms of efficiency and production. The integration of human-robot collaboration into workflows can be achieved seamlessly, wherein CPS is employed to analyze and adapt processes to improve overall performance constantly [10,11].

Overall, in various industries, the practical applications and benefits of CPSs are evident. For example, in automotive manufacturing, CPSs enable precise coordination between human workers and robots, where robots handle tasks requiring precision and strength, such as welding and component

assembly. In contrast, humans oversee quality control and complex decision-making processes, thus enhancing production efficiency and product quality [42–44]. On the other hand, in healthcare, CPSs facilitate advanced robotic surgeries, where robots assist surgeons with delicate procedures, and real-time data from sensors ensure precise movements, reducing the risk of failures [44–46]. In agriculture, smart farming systems utilize CPSs for precision agriculture, with drones and autonomous vehicles equipped with sensors gathering data on soil conditions, crop health, and weather patterns. This real-time information optimizes planting, irrigation, and harvesting processes, increasing yield and reducing resource consumption. In logistics and supply chain management, CPSs streamline operations by enabling real-time tracking and management of goods. Automated warehouses use collaborative robots to sort and move items efficiently, while real-time data analytics optimize inventory management, reducing delays and improving supply chain efficiency [42–46]. Overall, CPSs are essential for achieving the human-centric and sustainable goals of Industry 5.0, integrating advanced AI, real-time data processing, and robust safety mechanisms to enhance human-robot collaboration, improve productivity, and ensure safety in various industrial applications.

3.3 The Benefits of Cyber-Physical Systems Integration in Enhancing Industrial Processes

The incorporation of CPSs into manufacturing and industrial operations has an array of benefits. The utilization of real-time monitoring and control facilitates prompt decision-making and adaptability to alterations, whereas predictive maintenance detects and resolves prospective equipment malfunctions by reducing periods of idleness. The optimization of resource utilization is crucial for achieving optimal allocation of raw materials, energy, and workforce while also incorporating adaptive production factors [21]. The adaptability mentioned above encompasses the ability to enhance production flexibility, enabling the seamless reconfiguration of production lines to address evolving product specifications and market demands effectively [24]. Implementing CPS enables enhanced quality control through sophisticated monitoring and automated inspections, thereby guaranteeing elevated levels of product quality and uniformity. Integrating human and machine collaboration has facilitated a more fluid and efficient interaction, resulting in increased productivity and enhanced accuracy within the production environment [22].

Furthermore, the implementation of CPSs plays a pivotal role in enhancing energy efficiency through the continuous monitoring and optimization of energy usage. This proactive approach not only aids in mitigating the adverse environmental effects but also reduces operational expenses. This phenomenon's impact extends throughout the entire supply chain, resulting in enhanced visibility that facilitates improved coordination and efficiency among suppliers, manufacturers, and distributors [10,23]. By employing data-driven decision-making, CPSs effectively utilize generated data to conduct in-depth analysis, hence guiding decisions aimed at optimizing processes and enhancing overall business objectives. In general, the integration of CPSs leads to a reduction in costs, contributing to the establishment of a manufacturing environment that is both cost-effective and competitive [16,25].

4 Security and Privacy Challenges in Industry 5.0 CPSs

As mentioned above, Industry 5.0 represents the latest evolution in manufacturing and industry, characterized by increased automation and the integration of CPSs. While it offers numerous benefits, it also introduces various security challenges. The evolving threat landscape in Industry 5.0 is marked by the convergence of Information Technology (IT) and Operational Technology (OT), creating a larger attack surface for cybercriminals to play with. This convergence enables cyber criminals to

target both digital and physical components of industrial systems, posing a serious threat to critical infrastructure.

One of the primary security challenges in Industry 5.0 is the emergence of new and sophisticated threats [42–46]. Cyberattacks can lead to physical consequences, such as the manipulation of industrial processes or the disabling of safety systems. These threats include malware specifically designed to target CPS, ransomware attacks on manufacturing facilities, and supply chain vulnerabilities that can disrupt production [46–49]. Additionally, the proliferation of IoT devices and their often inadequate security measures can provide entry points for attackers looking to compromise CPS [50,51]. Further, the consequences of security breaches in Industry 5.0 can be severe [37–40]. They can lead to production downtime, equipment damage, loss of intellectual property, and even safety hazards for workers. For example, a cyberattack on a power grid or water treatment facility could result in widespread outages and public health risks. Nonetheless, the financial and reputational damage inflicted on organizations can be long-lasting, affecting their ability to remain competitive and recover from the breach.

Overall, the impact of security breaches in Industry 5.0 extends beyond individual organizations to society as a whole. Disruptions in critical infrastructure can have cascading effects on the economy and public safety. For instance, the 2015 cyberattack on Ukraine's power grid left hundreds of thousands of people without electricity during freezing temperatures, showcasing the real-world consequences of such attacks [52–54]. Furthermore, breaches can erode trust in emerging technologies like autonomous vehicles and smart cities, hindering their adoption and potential societal benefits. In Industry 5.0, where CPSs play a central role, security challenges are significant due to the increased interconnectivity and intelligence of these systems. Overall, the integration of advanced technologies and human-centric approaches in Industry 5.0 brings unique security challenges, which are outlined below:

1. Increased attack surface
   The extensive use of interconnected devices and systems in CPSs expands the attack surface, endangering the underlying infrastructure. Each sensor, actuator, and networked device can potentially be a point of vulnerability for cyber attackers to exploit [41–43]. For instance, in a smart grid system, sensors and smart meters are deployed to monitor and manage electricity usage in real-time. If a cyber attacker gains access to these sensors, they could manipulate the data being reported, leading to incorrect billing or even disruptions in electricity distribution [55–57].
2. Interconnected and interdependent systems
   The interconnected nature of CPSs means that a breach in one system can have cascading effects on others [44–46]. This interdependence can exacerbate the impact of cyberattacks if proper security measures are not in place, endangering the Industry 5.0 ecosystems. The interconnected nature of CPSs means that a breach in one system can have cascading effects on others [44–46]. This interdependence can exacerbate the impact of cyberattacks if proper security measures are not in place, endangering the Industry 5.0 ecosystems. For instance, in a smart manufacturing plant, various CPS components such as robotic arms, conveyor belts, and quality control sensors are interconnected to streamline production processes. If a cyber attacker breaches the network controlling the robotic arms, it could lead to malfunctions or shutdowns of the entire production line. This breach can further propagate to affect inventory management systems, logistics, and even external supply chains, causing significant operational and financial disruptions.

3. Complexity of systems
   The complexity of CPSs, integrating various technologies and layers, can make it challenging to identify and address vulnerabilities and predict how security breaches will impact the system [42–46]. The complexity of CPSs, integrating various technologies and layers, can make it challenging to identify and address vulnerabilities and predict how security breaches will impact the system [42–46]. This complexity arises from the diverse components involved, such as sensors, actuators, communication networks, and control systems, each potentially having its own security weaknesses. For example, consider a smart healthcare system where various devices like heart monitors, insulin pumps, and patient data management systems are interconnected. If a cyber attacker exploits a vulnerability in the communication protocol used by the heart monitors, it could lead to incorrect readings or malfunctions. This breach could then compromise patient safety and the integrity of the entire healthcare system.
4. Insider threats
   With a human-centric approach, Industry 5.0 increases the risk of insider threats, either unintentional (due to errors) or malicious. The involvement of more human operators and developers can introduce additional vulnerabilities, according to [42–46]. For example, in a smart factory setting, human operators might accidentally misconfigure a critical system or bypass security protocols, leading to vulnerabilities that could be exploited by cyber attackers.
5. Supply chain vulnerabilities
   CPS often involves complex supply chains. A single compromised component, such as a tainted software update or hardware with built-in vulnerabilities, can put the entire system at risk, according to [46–50].
6. Real-time operational constraints
   Many CPSs require real-time or near-real-time responses, limiting the time available to detect and respond to security incidents [43–47]. This can be particularly challenging for automated processes where human oversight is minimal. For example, in automated industrial control systems (ICS) used in manufacturing plants, processes such as assembly line operations and quality control need to occur in real time to ensure efficiency and product consistency. If a cyber attacker exploits a vulnerability in the ICS, they could disrupt the manufacturing process, causing defects or halting production entirely.
7. Emerging technologies and unknown vulnerabilities
   The rapid development of new technologies in Industry 5.0 (e.g., AI and advanced robotics) can introduce unknown vulnerabilities where the security implications of these technologies may not be fully understood or anticipated [42–46]. For instance, as AI and machine learning algorithms are increasingly integrated into CPSs for predictive maintenance and decision-making, they can become targets for adversarial attacks [57–59]. These attacks involve manipulating input data to deceive the AI systems into making incorrect decisions, potentially leading to malfunctions or security breaches.
8. Regulatory and compliance challenges
   Adhering to evolving regulatory standards and compliance requirements in different countries and sectors can be complex, especially when dealing with cross-border data flows and multinational operations [42–46]. For instance, organizations operating in the European Union must comply with the General Data Protection Regulation (GDPR), which imposes strict rules on data protection and privacy. However, these regulations can differ significantly from those in other regions, such as the United States' CCPA (California Consumer Privacy Act) or China's Cybersecurity Law.

9. Physical safety and cybersecurity interplay
   In CPSs, cybersecurity breaches can have direct physical consequences. Compromised systems can lead to physical harm [42–46], especially in contexts like manufacturing or critical infrastructure. For example, in a smart manufacturing plant, a cyber attacker could exploit vulnerabilities in the ICS to manipulate machinery operations. This could result in equipment malfunctions, production errors, or even catastrophic failures that endanger the safety of workers and the integrity of the plant.

To address these challenges, a multi-layered and holistic security approach is essential, including robust encryption, access control, continuous monitoring, incident response planning, and regular security audits [43–47]. Additionally, fostering a culture of security awareness and training among all stakeholders is crucial in mitigating these risks, which will be discussed in detail in upcoming sections. Some of the real-world examples that highlight the growing security challenges pertaining to the CPSs in Industry 5.0 include the Stuxnet worm, discovered in 2010, which is a famous instance of a cyberattack on industrial systems where it targeted Iran's nuclear facilities, causing physical damage to centrifuge by manipulating their control systems [53]. More recently, the Colonial Pipeline ransomware attack in 2021 disrupted fuel distribution across the U.S., underscoring the vulnerability of critical infrastructure to cyber threats [54]. These incidents serve as warnings of the need for robust cybersecurity measures and increased vigilance in the face of evolving threats in CPSs-integrated Industry 5.0. Based on real-world examples and available state-of-the-art, the following highlights some of the use cases of security challenges pertaining to CPSs in the context of Industry 5.0:

1. Smart manufacturing
   A smart manufacturing facility employs interconnected machines, robots, and sensors to optimize production processes. However, a cyberattack on the manufacturing line's control systems can result in production disruptions, product defects, and even safety hazards for workers [42–46].
2. Autonomous vehicles
   Industry 5.0 includes the development of autonomous vehicles for various purposes, such as self-driving cars and delivery drones. If these vehicles are compromised by hackers, it could lead to accidents, theft, or unauthorized access to sensitive data about transportation routes and passengers [43–47].
3. Smart grids
   Modern power grids are evolving into smart grids, incorporating digital communication and automation. A cyberattack on a smart grid can disrupt electricity supply, affecting homes, businesses, and critical infrastructure. Such an attack could lead to widespread outages and economic losses [43–47].
4. Healthcare IoT
   In the healthcare sector, IoT devices like connected medical devices and wearable health monitors are increasingly common. A security breach in these devices can compromise patient data privacy, disrupt healthcare services, and potentially put patient's lives at risk [43–47].
5. Smart cities
   Smart cities leverage CPSs to enhance urban services, such as traffic management, waste collection, and public safety. A cyberattack on a smart city's systems can disrupt these services, causing traffic congestion, delays in emergency response, and public inconvenience [50–54].
6. Industrial robots

Manufacturing industries rely on industrial robots for automation and efficiency. If these robots are compromised, they can be used for malicious purposes, causing damage to equipment or posing safety risks to workers [50–54].

7. Supply chain attacks
   Cybercriminals target the supply chains of manufacturers and logistics companies in Industry 5.0. By infiltrating these supply chains, attackers can introduce malware or manipulate products, compromising their integrity and safety [50–54].
8. 3D printing
   3D printing is increasingly used in Industry 5.0 for rapid prototyping and manufacturing, where a cyberattack on a 3D printer's control systems can lead to the production of defective or dangerous objects [50–54].

Overall, these use cases demonstrate the diverse range of applications in Industry 5.0 and the associated security challenges. Protecting against cyber threats in these scenarios requires a multi-layered approach, including robust cybersecurity measures, secure design practices, employee training, and ongoing monitoring and response strategies. As Industry 5.0 continues to evolve, addressing these security challenges will be critical to ensure the safety, efficiency, and reliability of CPSs.

4.1 Privacy Concerns in Industry 5.0 CPSs

Having provided a brief overview of security concerns pertaining to CPSs in the context of Industry 5.0, this section provides a brief overview of privacy concerns pertaining to CPSs in Industry 5.0.

1. Data privacy implications
   Industry 5.0 CPSs collect and process enormous quantities of sensitive data from human interactions, machines, sensors, and other sources. This data may contain sensitive information, including financial and personal details and trade secrets. Organizations must implement stringent data privacy measures to protect this sensitive information from unauthorized access, exploitation, and disclosure. Privacy infringement during data collection, storage, use, and sharing can significantly impact user trust and system acceptance, emphasizing the need for robust privacy protocols [23,25].
2. Challenges in human-robot collaboration
   Data privacy preservation is crucial in Industry 5.0, where there is significant integration of human and robotic collaboration within work contexts. This integration raises concerns about robots collecting and transmitting sensitive data about human employees, including their well-being, whereabouts, and conduct. It is essential for organizations to establish explicit norms and protocols governing human-robot interaction to safeguard human privacy. Addressing privacy concerns in human-computer interactions with robots is vital to maintaining user trust and ensuring system acceptance [17].
3. Ethical and legal considerations
   In addition to the aforementioned particular privacy concerns, organizations must also consider many broader privacy challenges while incorporating Industry 5.0 technology. These challenges include:
   i) The escalating intricacy and interconnectivity of CPSs pose challenges in effectively monitoring and managing data flow. This phenomenon could facilitate unauthorized entities in acquiring access to confidential information [2,18].

ii) The utilization of AI is frequently employed to analyze and process data inside Industry 5.0 systems. Nevertheless, AI systems possess a characteristic of opacity and complexity, rendering it challenging to comprehend the mechanisms by which data is utilized and ascertain its adherence to privacy norms.
iii) Presently, there is an absence of unambiguous and all-encompassing privacy regulations applicable to technology within the Industry 5.0 domain. This circumstance can pose challenges for enterprises in terms of understanding and adhering to privacy regulations and safeguarding individuals' privacy [19].

Organizations implementing Industry 5.0 technologies must undertake measures to tackle the privacy issues associated with such advancements effectively. This entails implementing comprehensive cybersecurity procedures to safeguard data against illegal access, abuse, and disclosure. One crucial step is to develop explicit norms and protocols governing data acquisition, manipulation, and dissemination [18,19]. Overall, the key objective is to ensure that individuals are granted transparency and autonomy in managing their personal data, and this can be achieved by collaborating with lawmakers to establish unambiguous and all-encompassing privacy rules. Moreover, organizations can adopt a series of measures to safeguard personal privacy while utilizing Industry 5.0 technology effectively. In this regard, the next section provides a brief overview of security and privacy attacks that could occur, endangering the CPSs in the context of Industry 5.0.

4.2 Security and Privacy Attacks

In the Industry 5.0 era, characterized by the advanced integration of CPSs, several types of security and privacy attacks can be expected, which are summarized in Fig. 3. To counter these attacks, a comprehensive and dynamic strategy for security and privacy is necessary, which includes the integration of cutting-edge technologies, ongoing employee education, and strong policies.

- Data breaches
  Increased data generation and exchange in CPSs can lead to sophisticated data breaches, where sensitive information such as trade secrets, personal data [57–59], or operational details could be stolen or exposed.
- Cyberattacks on physical systems
  As physical and digital systems are more closely integrated, cyberattacks could directly impact physical components [58–60]. This includes attacks on Industrial Control Systems (ICS) and critical infrastructure, potentially causing physical damage or disrupting manufacturing processes.
- Ransomware and malware attacks
  Ransomware and other malicious software can be used to lock out operators from controlling CPSs, demanding ransom for regaining access, or damaging systems and data [57–59]. In 2017, the WannaCry ransomware attack affected hundreds of thousands of computers worldwide, including critical infrastructure and industrial systems. It encrypted data and demanded ransom in bitcoin, showcasing the potential for ransomware to disrupt industrial operations [58–61].
- MITM (Man In The Middle) attacks
  These occur when attackers intercept communication between CPS components, potentially altering or stealing information. This is particularly risky in systems where data integrity is critical for operational safety [58–61].
- Supply chain attacks
  Given the interconnected nature of CPSs, vulnerabilities in one component can be exploited to

affect the entire system. Attackers may target less secure elements in the supply chain to gain access to more secure areas [58–61].

- AI-powered attacks
  Attackers may use AI to automate attacks or to create more sophisticated, adaptive attack methods that can learn and evolve to bypass security measures [61–65].
- Insider threats
  Employees or others with inside access could misuse their access rights to compromise CPSs, either maliciously or inadvertently [57–60].
- Eavesdropping
  Unauthorized access to CPSs could allow attackers to covertly monitor industrial processes, leading to industrial espionage [57–60].
- Privacy violations
  With vast amounts of data being processed, there is an increased risk of privacy violations, either through unauthorized access, misuse of personal data, or inadequate anonymization [58–61].
- IoT-targeted attacks
  Many CPSs rely on IoT devices as IoT made the backbone of them, which may have inherent security weaknesses, making them easy targets for attackers to enter larger systems [57–61].

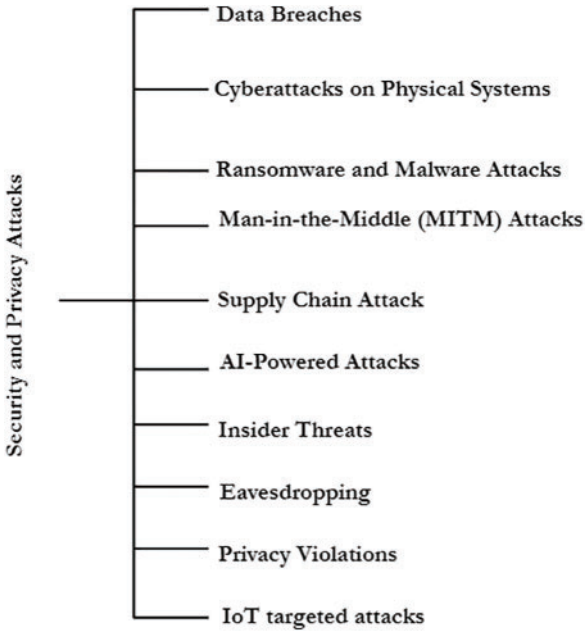

Figure 3: Security and privacy attacks

5 Countermeasures and Future Directions

Ensuring the security and privacy of CPSs in the context of Industry 5.0 involves a multi-layered approach that addresses various aspects of these systems. The following are the key countermeasures that can be taken:

1. Employing advanced encryption and authentication techniques
   Refers to utilizing state-of-the-art encryption and authentication methods to protect data in

transit and at rest. Integrating humans and machines in collaborative efforts is a fundamental characteristic of Industry 5.0, and establishing secure interactions between these entities is of utmost importance [37–40]. Thus, the successful implementation of effective authentication and encryption techniques is necessary in this context, where some of the techniques include:

i) Secure human authentication: Employ robust authentication procedures, such as multi-factor authentication, to authenticate the identity of human users engaging.
ii) Secure communication channels: It is advisable to utilize secure communication methods, such as encrypted protocols, to facilitate data transmission between humans and robots [27].

2. Robust access control mechanisms
Implementing stringent access control policies to ensure only authorized personnel and systems can access sensitive data and critical components. Nonetheless, implementing access control methods is necessary to restrict robots' access to sensitive data and systems, considering their given tasks and functions [28]. This can include the use of multi-factor authentication, biometric verification, and role-based access controls.
3. Network security solutions
Deploying firewalls, Intrusion Detection Systems (IDSs), and Intrusion Prevention Systems (IPSs) to protect network infrastructure. Securing wireless communication channels is particularly crucial [48–51].
4. Anomaly detection systems
Utilizing AI to monitor systems in real-time for unusual activities or deviations from normal operational patterns could indicate a security breach or system malfunction [46–50].
5. Regular compliance
Ensuring compliance with pertinent standards and regulations is critical in safeguarding the privacy and security of Industry 5.0 systems. This includes:
   i) Identify applicable regulations: The challenge at hand involves the identification and comprehension of the relevant cybersecurity and privacy legislation that governs the industry and operations of the company [31].
   ii) Implement compliance measures: In order to adhere to regulatory mandates, such as data breach notification laws and data protection rules, it is necessary to establish and enforce both technical and organizational controls [32].
   iii) Regularly review and adapt: It is imperative to consistently evaluate and modify compliance methods to remain aligned with the ever-changing regulatory landscape and technological improvements [28].
   iv) Seek expert guidance: It is advisable to consult with legal and cybersecurity professionals to ensure adherence to intricate and constantly evolving regulatory frameworks.
6. Data privacy policies and compliance
Adhering to international data protection regulations such as the General Data Protection Regulation (GDPR) and implementing policies for data minimization, consent management, and user data rights [46–51].
7. Secure software development practices
Emphasizing security in the software development lifecycle, including regular patching and updates to address security vulnerabilities [46–51].
8. Employee training and awareness programs
Educating employees and users about common cyber threats, safe practices, and the importance of security protocols [46–51].

9. Physical security measures
   Ensuring physical security of critical infrastructure and devices to prevent unauthorized physical access [46–51].
10. Resilient and redundant design
    Designing systems to be resilient to attacks and failures which can include redundant systems and fail-safe mechanisms [46–51].
11. Incident response and recovery plans
    Developing comprehensive incident response strategies to quickly address security breaches or privacy incidents and minimize their impact [43–47].
12. Ethical considerations and transparency
    Implementing ethical guidelines for the usage of data and AI and maintaining transparency about data usage and privacy practices with stakeholders [46–51].
13. Supply chain security
    Securing the supply chain against potential threats, including scrutinizing suppliers and implementing security standards for procured hardware and software [46–51].
14. Collaboration and information sharing
    Collaborating with other organizations, regulatory bodies, and security communities to share information about threats and best practices [46–51].
15. Employing privacy-preserving technologies
    The enormous quantity of data collected and processed in the context of Industry 5.0 gives rise to essential concerns regarding privacy. Privacy-preserving technologies present auspicious avenues for safeguarding individual privacy. Some of the privacy-preserving technologies that can be incorporated include:
    i) Differential privacy: Different differential privacy approaches are employed to introduce random alterations to sensitive data, enabling statistical analysis while safeguarding the privacy of individual information [29].
    ii) Secure multi-party computation: Secure multi-party computation techniques are employed to provide collaborative analysis of sensitive data while ensuring that no one participant gains access to the actual material.
    iii) Data anonymization: The application of data anonymization techniques is crucial in order to eliminate or obscure Personally Identifying Information (PII) from data sets, hence enabling analysis while safeguarding the privacy of individuals.
    iv) Federated learning: The utilization of federated learning algorithms enables the training of AI models on decentralized datasets, eliminating the need for centralized datasets/servers.

These countermeasures represent a holistic approach to security and privacy, combining technical strategies with organizational and human-centric practices. They require continuous evaluation and adaptation to stay effective against evolving threats in the dynamic landscape of Industry 5.0. Overall, by implementing these security and privacy measures, organizations may effectively address the complexities associated with Industry 5.0, ensuring the protection of vital infrastructure, securing sensitive information, and upholding individual privacy.

Anticipated Future Directions

The advent of Industry 5.0 brings a new wave of technological advancements in CPSs, blending human ingenuity with advanced digital technologies. However, this also raises significant security and privacy challenges. Thus, future directions in addressing these challenges must be comprehensive

and forward-thinking, encompassing both technological and regulatory aspects, which will be further discussed in the following:

1. Advanced threat detection and response
   As CPSs become more interconnected, they become more vulnerable to sophisticated cyber-attacks. Thus, future research should focus on developing advanced threat detection systems that leverage AI to identify and mitigate threats in real time [66]. Additionally, automated response systems capable of instantaneously reacting to breaches could significantly reduce the damage caused by cyber-attacks.
2. Enhanced data privacy technologies
   With Industry 5.0 emphasizing personalization and human-centric services, the amount of sensitive data processed by CPSs will increase. Innovations in encryption, such as homomorphic encryption, should be pursued to allow data processing while maintaining confidentiality. Thus, research into privacy-preserving data analytics will also be crucial. Nonetheless, blockchain technology can significantly enhance the privacy of CPSs by providing decentralized data management, ensuring data immutability, and leveraging cryptographic techniques for secure data transactions [67–69]. The use of smart contracts automates privacy controls, while anonymity and pseudonymity protect user identities. In addition, secure communication protocols facilitated by blockchain ensure that data in transit remains protected, addressing the growing privacy challenges in advanced CPSs.
3. Secure edge computing
   As CPSs often involve edge computing, ensuring the security of these distributed systems is essential [66]. Future developments could include secure data processing at the edge, robust authentication mechanisms, and secure communication protocols between edge devices and central systems.
4. Resilient design and engineering practices
   Incorporating security and privacy by design in CPSs is fundamental. This involves adopting resilient design practices that anticipate and mitigate potential security vulnerabilities right from the development phase. Additionally, regular security audits and updates must become an integral part of the CPSs lifecycle.
5. Regulatory and standardization efforts
   Industry 5.0 will require updated regulatory frameworks to address the unique challenges of CPSs. This includes international standards for data privacy, cross-border data flow, and cybersecurity measures. Collaboration among industry, academia, and governments will be vital in developing these regulations.
6. Human factor and training
   As human interaction with CPSs increases, understanding the human factor in cybersecurity becomes vital. This includes training employees in cybersecurity best practices and researching the impact of human behavior on CPSs security and privacy.
7. Ethical and responsible AI use
   The integration of AI in CPSs must be guided by ethical principles to ensure that decisions made by these systems do not violate privacy norms or ethical standards. Thus, developing guidelines for responsible AI use in CPSs will be a key challenge.

In conclusion, the security and privacy challenges in the Industry 5.0 era are multifaceted, requiring a holistic approach that combines technological innovation, regulatory frameworks, and a focus on the human elements of cybersecurity. Hence, the future direction should aim for a balanced approach that safeguards security and privacy while harnessing its full potential.

6 Conclusion

As we conclude this review on the security and privacy issues pertaining to CPSs in the era of Industry 5.0, several key insights emerge. The integration of advanced technologies with human-centric approaches, while offering immense potential for innovation and efficiency, also brings forth a complex array of challenges in terms of security and privacy. The expanded attack surface, the intricacies of system interdependencies, and the vulnerabilities introduced by real-time operational constraints underscore the need for robust, adaptive, and proactive security strategies. Moreover, the privacy concerns in CPSs, amplified by the extensive big data collection and processing inherent in these systems, call for a vigilant approach to data protection, compliance with global regulations, and a keen awareness of the ethical implications of data usage. The evolving landscape of Industry 5.0, characterized by its emphasis on human-machine collaboration, further complicates these issues, making it imperative to consider the human element in both the creation and mitigation of security and privacy risks. This review underscores the necessity of a multifaceted approach to address these challenges. Advanced technological solutions, such as sophisticated encryption methods, comprehensive access control, and intelligent anomaly detection systems, form the backbone of this approach. Equally important is the establishment of resilient and flexible frameworks that can adapt to evolving threats and technologies. The role of regulatory frameworks and standards cannot be overstated, as they provide essential guidelines and benchmarks for security and privacy practices in this new era. Looking forward, the field of CPSs in Industry 5.0 presents a fertile ground for research, particularly in the development of holistic security solutions that integrate technical, regulatory, and human-centric perspectives. The importance of fostering a culture of security awareness and the need to embed ethical considerations in the development and deployment of these systems is paramount. In conclusion, while the challenges are significant, the opportunities presented by CPSs in Industry 5.0 to revolutionize industrial practices are equally substantial. A concerted effort by researchers, practitioners, policymakers, and stakeholders is required to navigate these challenges effectively and harness the full potential of CPSs, ensuring a secure, privacy-conscious, and ethically sound future in Industry 5.0.

Acknowledgement: Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support.

Funding Statement: This research was funded by Qassim University (QU-APC-2024-9/1).

Author Contributions: Study conception and design: Navod Neranjan Thilakarathne and Zaharaddeen Karami Lawal; data collection: Navod Neranjan Thilakarathne and Zaharaddeen Karami Lawal; analysis and interpretation of results: Abdullah Alabdulatif, Navod Neranjan Thilakarathne and Zaharaddeen Karami Lawal; draft manuscript preparation: Abdullah Alabdulatif, Navod Neranjan Thilakarathne and Zaharaddeen Karami Lawal. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. Lasi, P. Fettke, H. G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Bus. Inform. Syst. Eng.*, vol. 6, no. 4, pp. 239–242, Aug. 2014. doi: 10.1007/s12599-014-0334-4.

[2] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "A literature review of the challenges and opportunities of the transition from Industry 4.0 to Society 5.0," *Energies*, vol. 15, no. 17, Sep. 1, 2022, Art. no. 6276. doi: 10.3390/en15176276.

[3] M. Ryalat, H. ElMoaqet, and M. AlFaouri, "Design of a smart factory based on cyber-physical systems and internet of things towards Industry 4.0," *Appl. Sci.*, vol. 13, no. 4, Feb. 2023, Art. no. 2156. doi: 10.3390/app13042156.

[4] M. Golovianko, V. Terziyan, V. Branytskyi, and D. Malyk, "Industry 4.0 vs. Industry 5.0: Co-existence, transition, or a hybrid," *Procedia Comput. Sci.*, vol. 217, pp. 102–113, 2022. doi: 10.1016/j.procs.2022.12.206.

[5] X. Xu, Y. Lu, B. Vogel-Heuser, and L. Wang, "Industry 4.0 and Industry 5.0—Inception, conception and perception," *J. Manuf. Syst.*, vol. 61, pp. 530–535, Oct. 2021. doi: 10.1016/j.jmsy.2021.10.006.

[6] A. Fay, F. Gehlhoff, B. Vogel-Heuser, and H. Baumgaertel, "Agents for the realization of Industrie 4.0-VDI status report," Aug. 2019. doi: 10.13140/RG.2.2.23998.84805.

[7] M. Khan, A. Haleem, and M. Javaid, "Changes and improvements in Industry 5.0: A strategic approach to overcome the challenges of Industry 4.0," *Green Technol. Sustain.*, vol. 1, no. 2, May 2023, Art. no. 100020. doi: 10.1016/j.grets.2023.100020.

[8] P. K. R. Maddikunta *et al.*, "Industry 5.0: A survey on enabling technologies and potential applications," *J. Ind. Inform. Integr.*, vol. 26, Mar. 1, 2022, Art. no. 100257. doi: 10.1016/j.jii.2021.100257.

[9] N. Jafari, M. Azarian, and H. Yu, "Moving from Industry 4.0 to Industry 5.0: What are the implications for smart logistics?" *Logistics*, vol. 6, no. 2, Jun. 1, 2022, Art. no. 26. doi: 10.3390/logistics6020026.

[10] G. F. Frederico, "From supply Chain 4.0 to supply Chain 5.0: Findings from a systematic literature review and research directions," *Logistics*, vol. 5, no. 3, Sep. 1, 2021, Art. no. 49. doi: 10.3390/logistics5030049.

[11] S. Nahavandi, "Industry 5.0—A human-centric solution," *Sustainability*, vol. 11, no. 16, Aug. 2019, Art. no. 4371. doi: 10.3390/su11164371.

[12] S. Grabowska, S. Saniuk, and B. Gajdzik, "Industry 5.0: Improving humanization and sustainability of Industry 4.0," *Scientometrics*, vol. 127, no. 6, pp. 3117–3144, Jun. 2022. doi: 10.1007/s11192-022-04370-1.

[13] M. Sony, "Pros and cons of implementing Industry 4.0 for the organizations: A review and synthesis of evidence," *Prod. Manuf. Res.*, vol. 8, no. 1, pp. 244–272, Jan. 2020. doi: 10.1080/21693277.2020.1781705.

[14] P. Pathak, P. R. Pal, M. Shrivastava, and P. Ora, "Fifth revolution: Applied AI & human intelligence with cyber physical systems," *Int. J. Eng. Adv. Technol.*, vol. 8, pp. 23–27, 2019.

[15] R. Sindhwani, S. Afridi, A. Kumar, A. Banaitis, S. Luthra and P. L. Singh, "Can Industry 5.0 revolutionize the wave of resilience and social value creation? A multi-criteria framework to analyze enablers," *Technol. Soc.*, vol. 68, Feb. 2022, Art. no. 101887. doi: 10.1016/j.techsoc.2022.101887.

[16] A. Adel, "Future of Industry 5.0 in society: Human-centric solutions, challenges and prospective research areas," *J. Cloud Comput.*, vol. 11, no. 1, Dec. 1, 2022. doi: 10.1186/s13677-022-00314-5.

[17] E. Valette, H. B. El-Haouzi, and G. Demesure, "Industry 5.0 and its technologies: A systematic literature review upon the human place into IoT- and CPS-based industrial systems," *Comput. Ind. Eng.*, vol. 184, Oct. 2023, Art. no. 109426. doi: 10.1016/j.cie.2023.109426.

[18] P. Thakur and V. Kumar Sehgal, "Emerging architecture for heterogeneous smart cyber-physical systems for Industry 5.0," *Comput. Ind. Eng.*, vol. 162, Dec. 2021, Art. no. 107750. doi: 10.1016/j.cie.2021.107750.

[19] K. P. Iyengar *et al.*, "Industry 5.0 technology capabilities in trauma and orthopaedics," *J. Orthop.*, vol. 32, pp. 125–132, Jul. 2022. doi: 10.1016/j.jor.2022.06.001.

[20] M. Ghobakhloo, M. Iranmanesh, M. L. Tseng, A. Grybauskas, A. Stefanini and A. Amran, "Behind the definition of Industry 5.0: A systematic review of technologies, principles, components, and values," *J. Ind. Prod. Eng.*, vol. 40, no. 6, pp. 432–447, 2023. doi: 10.1080/21681015.2023.2216701.

[21] A. Mukherjee, A. Raj, and S. Aggarwal, "Identification of barriers and their mitigation strategies for Industry 5.0 implementation in emerging economies," *Int. J. Prod. Econ.*, vol. 257, Mar. 2023, Art. no. 108770. doi: 10.1016/j.ijpe.2023.108770.

[22] D. Romero and J. Stahre, "Towards the resilient Operator 5.0: The future of work in smart resilient manufacturing systems," *Procedia CIRP*, vol. 104, pp. 1089–1094, 2021. doi: 10.1016/j.procir.2021.11.183.
[23] P. Coelho, C. Bessa, J. Landeck, and C. Silva, "Industry 5.0: The arising of a concept," *Procedia Comput. Sci.*, vol. 217, pp. 1137–1144, 2023. doi: 10.1016/j.procs.2022.12.312.
[24] J. J. Zhang *et al.*, "Cyber-physical-social systems: The state of the art and perspectives," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 3, pp. 829–840, Sep. 2018. doi: 10.1109/TCSS.2018.2861224.
[25] P. Sachsenmeier, "Industry 5.0—The relevance and implications of bionics and synthetic biology," *Engineering*, vol. 2, no. 2, pp. 225–229, Jun. 2016. doi: 10.1016/J.ENG.2016.02.015.
[26] J. Leng *et al.*, "Industry 5.0: Prospect and retrospect," *J. Manuf. Syst.*, vol. 65, pp. 279–295, Oct. 2022. doi: 10.1016/j.jmsy.2022.09.017.
[27] E. Coronado, T. Kiyokawa, G. A. G. Ricardez, I. G. Ramirez-Alpizar, G. Venture and N. Yamanobe, "Evaluating quality in human-robot interaction: A systematic search and classification of performance and human-centered factors, measures and metrics towards an Industry 5.0," *J. Manuf. Syst.*, vol. 63, pp. 392–410, Apr. 2022. doi: 10.1016/j.jmsy.2022.04.007.
[28] C. Murphy, P. J. Carew, and L. Stapleton, "Ethical personalisation and control systems for smart human-centred Industry 5.0 applications," *IFAC-PapersOnLine*, vol. 55, pp. 24–29, 2022. doi: 10.1016/j.ifacol.2022.12.005.
[29] M. Ghobakhloo, M. Iranmanesh, B. Foroughi, E. B. Tirkolaee, S. Asadi and A. Amran, "Industry 5.0 implications for inclusive sustainable manufacturing: An evidence-knowledge-based strategic roadmap," *J. Clean Prod.*, vol. 417, Sep. 2023, Art. no. 138023. doi: 10.1016/j.jclepro.2023.138023.
[30] W. D. Madhuka Priyashan and N. N. Thilakarathne, "IIoT framework for SME level injection molding industry in the context of Industry 4.0," *Int. J. Eng. Manage. Res.*, vol. 10, no. 6, pp. 61–68, Dec. 2020. doi: 10.31033/ijemr.10.6.9.
[31] J. Barata and I. Kayser, "Industry 5.0–past, present, and near future," *Procedia Comput. Sci.*, vol. 219, pp. 778–788, 2023. doi: 10.1016/j.procs.2023.01.351.
[32] Shruti, S. Rani, and G. Srivastava,"Secure hierarchical fog computing-based architecture for Industry 5.0 using an attribute-based encryption scheme," *Expert. Syst. Appl.*, vol. 235, Jan. 2024, Art. no. 121180. doi: 10.1016/j.eswa.2023.121180.
[33] N. N. Thilakarathn, G. Muneeswari, and V. Parthasarathy, "Federated learning for privacy-preserved medical Internet of Things," *Intell. Autom. Soft Comput.*, vol. 33, no. 1, pp. 157–172, 2022. doi: 10.32604/iasc.2022.023763.
[34] X. Wang *et al.*, "Steps toward Industry 5.0: Building '6S' parallel industries with cyber-physical-social intelligence," *IEEE/CAA J. Autom. Sinica.*, vol. 10, no. 8, pp. 1692–1703, Aug. 2023. doi: 10.1109/JAS.2023.123753.
[35] S. K. Jagatheesaperumal and M. Rahouti, "Building digital twins of cyber physical systems with metaverse for Industry 5.0 and beyond," *IT Prof.*, vol. 24, no. 6, pp. 34–40, Nov. 2022. doi: 10.1109/MITP.2022.3225064.
[36] A. Simeone, R. Grant, W. Ye, and A. Caggiano, "A human-cyber-physical system for Operator 5.0 smart risk assessment," *Int. J. Adv. Manuf. Technol.*, vol. 129, no. 5–6, pp. 2763–2782, Nov. 2023. doi: 10.1007/s00170-023-12481-z.
[37] N. Fazal, A. Haleem, S. Bahl, M. Javaid, and D. Nandan, "Digital management systems in manufacturing using Industry 5.0 technologies," in P. Verma, O. D. Samuel, T. N. Verma, and G. Dwivedi (Eds.), *Advancement in Materials, Manufacturing and Energy Engineering*, Singapore: Springer Nature Singapore, 2022, vol. II, pp. 221–234. doi: 10.1007/978-981-16-8341-1_18.
[38] A. Bécue, I. Praça, and J. Gama, "Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities," *Artif. Intell. Rev.*, vol. 54, no. 5, pp. 3849–3886, Jun. 2021. doi: 10.1007/s10462-020-09942-2.
[39] M. S. Chong, H. Sandberg, and A. M. H. Teixeira, "A tutorial introduction to security and privacy for cyber-physical systems," in *2019 18th Eur. Control Conf. (ECC)*, Naples, Italy, IEEE, Jun. 2019, pp. 968–978. doi: 10.23919/ECC.2019.8795652.

[40] M. Henze, J. Hiller, R. Hummen, R. Matzutt, K. Wehrle and J. H. Ziegeldorf, "Network security and privacy for cyber-physical systems," in H. Song, G. A. Fink, and S. Jeschke (Eds.), *Security and Privacy in Cyber-Physical Systems*, 1st ed. Wiley, 2017, pp. 25–56. doi: 10.1002/9781119226079.ch2.
[41] F. AlDosari, "Security and privacy challenges in cyber-physical systems," *J. Inform. Secur.*, vol. 8, no. 4, pp. 285–295, 2017. doi: 10.4236/jis.2017.84019.
[42] G. A. Fink, T. W. Edgar, T. R. Rice, D. G. MacDonald, and C. E. Crawford, "Security and privacy in cyber-physical systems," *Cyber Phys. Syst.*, vol. 22, pp. 129–141, 2017. doi: 10.1016/B978-0-12-803801-7.00009-2.
[43] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Des. Test.*, vol. 34, no. 4, pp. 7–17, Aug. 2017. doi: 10.1109/MDAT.2017.2709310.
[44] A. Nazarenko and G. Ali Safdar, "Survey on security and privacy issues in cyber physical systems," *AIMS Electron. Electr. Eng.*, vol. 3, no. 2, pp. 111–143, 2019. doi: 10.3934/ElectrEng.2019.2.111.
[45] A. Verma *et al.*, "Blockchain for Industry 5.0: Vision, opportunities, key enablers, and future directions," *IEEE Access*, vol. 10, pp. 69160–69199, 2022. doi: 10.1109/ACCESS.2022.3186892.
[46] J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocess. Microsyst.*, vol. 77, Sep. 2020, Art. no. 103201. doi: 10.1016/j.micpro.2020.103201.
[47] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 746–789, 2020. doi: 10.1109/COMST.2019.2944748.
[48] J. Hajda, R. Jakuszewski, and S. Ogonowski, "Security challenges in Industry 4.0 PLC systems," *Appl. Sci.*, vol. 11, no. 21, Oct. 2021, Art. no. 9785. doi: 10.3390/app11219785.
[49] M. Doyle-Kent and P. Kopacek, "Industry 5.0: Is the manufacturing industry on the cusp of a new revolution?" in *Proc. Int. Symp. Prod. Res. 2019*, Cham, Springer International Publishing, 2020, pp. 432–441. doi: 10.1007/978-3-030-31343-2_38.
[50] S. Rani, A. Kataria, M. Chauhan, P. Rattan, R. Kumar and A. K. Sivaraman, "Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: State-of-artwork," *Mat. Today: Proc.*, vol. 62, pp. 4671–4676, 2022. doi: 10.1016/j.matpr.2022.03.123.
[51] Z. Yu, Z. Kaplan, Q. Yan, and N. Zhang, "Security and privacy in the emerging cyber-physical world: A survey," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 3, pp. 1879–1919, 2021. doi: 10.1109/COMST.2021.3081450.
[52] Wikipedia, "2015 Ukraine power grid hack," Jul. 12, 2023. Accessed: Dec. 13, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=2015_Ukraine_power_grid_hack&oldid=1165079237
[53] Wikipedia, "Stuxnet," Dec. 12, 2023. Accessed: Dec. 13, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Stuxnet&oldid=1189546386
[54] Wikipedia, "Colonial pipeline ransomware attack," Nov. 29, 2023. Accessed: Dec. 13, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Colonial_Pipeline_ransomware_attack&oldid=1187489494
[55] Z. K. L. R. Y. Zakari, M. Z. Shuaibu, and A. Bala, "A review: Issues and challenges in big data from analytic and storage perspectives," *Int. J. Eng. Comput. Sci.*, vol. 5, Mar. 2016. doi: 10.18535/ijecs/v5i3.12.
[56] A. Alabdulatif, N. N. Thilakarathne, Z. K. Lawal, K. E. Fahim and R. Y. Zakari, "Internet of Nano-Things (IoNT): A comprehensive review from architecture to security and privacy challenges," *Sensors*, vol. 23, no. 5, Mar. 2023, Art. no. 2807. doi: 10.3390/s23052807.
[57] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, Feb. 2011. doi: 10.1080/00396338.2011.555586.
[58] A. Chowdhury, "Recent cyber security attacks and their mitigation approaches—An overview," in L. Batten, and G. Li (Eds.), *Applications and Techniques in Information Security*, Singapore: Springer Singapore, 2016, vol. 651, pp. 54–65. doi: 10.1007/978-981-10-2741-3_5.

[59] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu and P. Laplante, "Dimensions of cyber-attacks: Cultural, social, economic, and political," *IEEE Technol. Soc. Mag.*, vol. 30, no. 1, pp. 28–38, 2011. doi: 10.1109/MTS.2011.940293.

[60] J. Valuch, T. Gábriš, and O. Hamuľák, "Cyber attacks, information attacks, and postmodern warfare," *Baltic J. Law Polit.*, vol. 10, no. 1, pp. 63–89, Jun. 2017. doi: 10.1515/bjlp-2017-0003.

[61] S. Choudhary, P. P. Choudhary, and S. Salve, "A study on various cyber attacks and a proposed intelligent system for monitoring such attacks," in *2018 3rd Int. Conf. Inventive Comput. Technol. (ICICT)*, Coimbatore, India, IEEE, Nov. 2018, pp. 612–617. doi: 10.1109/ICICT43934.2018.9034445.

[62] G. Sabaliauskaite and A. P. Mathur, "Aligning cyber-physical system safety and security," in M. -A. Cardin, D. Krob, P. C. Lui, Y. H. Tan, and K. Wood (Eds.), *Complex Systems Design & Management Asia*, Cham: Springer International Publishing, 2015, pp. 41–53. doi: 10.1007/978-3-319-12544-2_4.

[63] P. Johri, J. N. Singh, A. Sharma, and D. Rastogi, "Sustainability of coexistence of humans and machines: An evolution of Industry 5.0 from Industry 4.0," in *2021 10th Int. Conf. Syst. Model. Adv. Res. Trends (SMART)*, Moradabad, India, IEEE, Dec. 2021, pp. 410–414. doi: 10.1109/SMART52563.2021.9676275.

[64] A. Alabdulatif, N. N. Thilakarathne, and K. Kalinaki, "A novel cloud enabled access control model for preserving the security and privacy of medical big data," *Electronics*, vol. 12, no. 12, 2023, Art. no. 2646. doi: 10.3390/electronics12122646.

[65] U. Bodkhe *et al.*, "Blockchain for Industry 4.0: A comprehensive review," *IEEE Access*, vol. 8, pp. 79764–79800, 2020. doi: 10.1109/ACCESS.2020.2988579.

[66] N. Ho, P. -M. Wong, R. -J. Soon, C. -B. Chng, and C. -K. Chui, "Blockchain for cyber-physical system in manufacturing," in *Proc. Tenth Int. Symp. Inform. Commun. Technol.-SoICT 2019*, Hanoi, Ha Long Bay, Viet Nam: ACM Press, 2019, pp. 385–392. doi: 10.1145/3368926.3369656.

[67] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018. doi: 10.1504/IJWGS.2018.095647.

[68] P. P. Groumpos, "A critical historical and scientific overview of all industrial revolutions," *IFAC-PapersOnLine*, vol. 54, pp. 464–471, 2021. doi: 10.1016/j.ifacol.2021.10.492.

[69] A. M. Alnajim, S. Habib, M. Islam, S. M. Thwin, and F. Alotaibi, "A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in industrial Internet of Things," *Technologies*, vol. 11, no. 6, Nov. 2023, Art. no. 161. doi: 10.3390/technologies11060161.