Arab Journal of Administrative Sciences

2025, Vol. 32, No. 2, 435-454
Doi: 10.34120/ajas.v32i2.1289

Cyber Threats and Vulnerabilities in Industry 5.0: A Review

Raja W. Anwar
Yasmine Souissi
German University of Technology (GUtech)
Sultanate of Oman
Saqib Ali
Sultan Qaboos University
Sultanate of Oman

Abstract

Purpose: This study aims to explore the cybersecurity threats and vulnerabilities unique to Industry 5.0, emphasizing the need for a robust security framework to protect human-machine interactions and industrial systems.

Study design/methodology/approach: This review adopts a systematic analysis of existing literature, identifying security risks, challenges, and potential countermeasures within Industry 5.0. The study synthesizes findings from peer-reviewed journals, industry reports, and case studies to provide a comprehensive assessment of cybersecurity concerns in this emerging paradigm.

Sample and data: The study evaluates cybersecurity trends and vulnerabilities based on recent empirical research, industry reports, and case studies from multiple sectors implementing Industry 5.0 technologies.

Results: The review identifies key cybersecurity challenges, including an expanded attack surface, privacy risks, and the exploitation of intelligent systems. It underscores the need for adaptive and proactive security strategies tailored to the human-centric nature of Industry 5.0. Additionally, it presents actionable recommendations for securing industrial ecosystems, ensuring data integrity, and mitigating potential cyber threats.

Originality/value: This study contributes to the growing body of knowledge on cybersecurity in Industry 5.0 by offering a structured framework for analyzing threats and vulnerabilities. It provides valuable insights for policymakers, industry leaders, and researchers, facilitating the development of secure, resilient, and ethically grounded industrial ecosystems.

Research limitations/implications: While this review provides a comprehensive assessment of cybersecurity risks in Industry 5.0, future research should focus on empirical validations, real-world case studies, and the practical implementation of recommended security measures.

Keywords: Cyber Security, Industry 5.0, Threat, Privacy, Risk, Artificial Intelligence (AI).
JEL classification: Y9

Submitted: 17/12/2024, revised: 10/1/2025, accepted: 19/3/2025.

To cite: Anwar, R. W., Souissi, Y., & Ali, S. (2025). Cyber threats and vulnerabilities in Industry 5.0: A review. *Arab Journal of Administrative Sciences*, *32*(2), 435-454. https://doi.org/ 10.34120/ajas.v32i2.1289

الملخص
التهديدات السيبرانية ونقاط الضعف في الصناعة 5.0: مراجعة

رجا وسيم أنور **ياسمين السويسي**
الجامعة الألمانية للتكنولوجيا (جيوتك)
سلطنة عمان

ساقب علي
جامعة السلطان قابوس
سلطنة عمان

هدف الدراسة: تهدف هذه الدراسة إلى استكشاف التهديدات والثغرات السيبرانية الفريدة من نوعها في الصناعة 5.0، مع التركيز على الحاجة إلى إطار عمل قوي لحماية التفاعلات بين الإنسان والآلة والنُظم الصناعية.

تصميم/ منهجية/ طريقة الدراسة: اعتمدت الدراسة على مراجعة منهجية للأدبيات القائمة؛ لتحديد الأخطار الأمنية والتحديات وإجراءات المواجهة. جُمعت النتائج من المجلات المحكمة والتقارير الصناعية ودراسات الحالة؛ لتقييم المخاوف المتعلقة بالأمن السيبراني تقييماً شاملاً.

عينة الدراسة وبياناتها: قيّمت الدراسة اتجاهات الأمن السيبراني ونقاط ضعفه؛ باستخدام أبحاث تجريبية حديثة وتقارير صناعية ودراسات حالة، من القطاعات التي تعتمد تقنيات الصناعة 5.0.

نتائج الدراسة: تشمل التحديات الرئيسية توسع سطح الهجوم، وأخطار الخصوصية، واستغلال الأنظمة الذكية. وتؤكد المراجعة على الحاجة إلى استراتيجيات أمنية تكيفية واستباقية مصممة وفقاً للطبيعة البشرية في الصناعة 5.0، وتُقدم توصيات عملية لتأمين النظم الأيكولوجية، وضمان سلامة البيانات، والتخفيف من التهديدات السيبرانية.

أصالة الدراسة: تسهم هذه الدراسة بإطار عمل منظم لتحليل التهديدات والثغرات في الصناعة 5.0؛ مما يوفر رؤى قيمة لصنّاع القرار، وقادة الصناعة، والباحثين لتطوير نظم صناعية آمنة ومرنة وأخلاقية.

حدود الدراسة وتطبيقاتها: على الرغم من شموليتها، تتطلب هذه المراجعة بحوثاً مستقبلية حول التحقق التجريبي، ودراسات الحالة الواقعية، وتطبيق الإجراءات الأمنية بما يشمل العوائق، والتكاليف، والفعالية. عملياً، تتيح النتائج لصناع القرار وضع إرشادات أقوى، ومساعدة المنظمات على تحديد أولويات الاستثمارات الأمنية، وإرشاد المهنيين لتصميم استراتيجيات مخصصة لبيئات الصناعة 5.0.

الكلمات المفتاحية: الأمن السيبراني، الصناعة 5.0، التهديد، الخصوصية، المخاطر، الذكاء الاصطناعي (AI).

الإشارة المرجعية: أنور، رجا وسيم، والسويسي، ياسمين، وعلي، ساقب. (2025). التهديدات السيبرانية ونقاط الضعف في الصناعة 5.0: مراجعة. *المجلة العربية للعلوم الإدارية، 32*(2)، 435-454.
https://doi.org/10.34120/ajas.v32i2.1289

Introduction

Rapid technological improvements and changes have a significant impact on many facets of our lives. To develop an intelligent, connected, and adaptable production environment, Industry 5.0, the most recent industrial revolution, emphasizes the integration of IoT, AI, and cyber-physical systems. Industry 5.0 is the newest development in industrial production, with the goal of creating more efficient and flexible production processes by integrating human knowledge with state-of-the-art technology. In addition, Industry 5.0 focuses on digitalizing manufacturing practices as the next stage of the artificial revolution. Building on earlier artificial revolutions, Industry 5.0 integrates cutting-edge technology such as robots, automation, Artificial Intelligence (AI), and the Internet of Things (IoT) to create a highly intelligent and interconnected production environment (Adi et al., 2020). Also, unprecedented levels of data flow across the value chain and automation distinguish these businesses. Changes in traditional industrial processes and enhanced organizational management have also resulted from the development of information and communication technology and its incorporation into production processes.

Industry 5.0 marks a transformative evolution in industrial practices, building on the advancements of previous industrial revolutions. The First Industrial Revolution (Industry 1.0) brought mechanization powered by water and steam, while the Second Industrial Revolution (Industry 2.0) introduced mass production enabled by the advent of electricity. The Third Industrial Revolution (Industry 3.0) introduced electronics and IT into manufacturing, paving the way for automation. Building on this, Industry 4.0 focused on cyber-physical systems, IoT, and AI, enabling the development of smart factories with real-time data exchange capabilities. In contrast, Industry 5.0 prioritizes human-centricity, resilience, and sustainability, blending advanced technologies with human creativity and intelligence to create a more adaptive, collaborative, and sustainable production ecosystem (Sharma & Singh, 2020).

The First Industrial Revolution began in the late 18th century, around the 1780s, with the advent of mechanical power generated using basic resources such as water, steam, and fossil fuels. The Second Industrial Revolution (Industry 2.0) emerged in the 1870s, characterized by the adoption of electrical energy and mass production, particularly in assembly line manufacturing. The Third Industrial Revolution (Industry 3.0), which started in the 1970s, introduced automation into manufacturing processes through the integration of electronics and Information

Technology (IT). The Fourth Industrial Revolution (Industry 4.0) builds on these advancements by leveraging artificial intelligence (AI), cloud computing, and the Internet of Things (IoT) to create intelligent cyber-physical systems (CPS). These systems enable real-time interaction and integration between the virtual and physical worlds, revolutionizing industrial practices (Rashid & Kausik, 2024). Industry 5.0 is a futuristic concept that blends precision, intelligence, and efficient technology with the creative thinking of human professionals (Ivascu, 2020). In the most recent industrial revolution, known as the fifth industrial revolution, resilience and sustainability in production systems combine with the advantages of networked automation to foster both prosperity and sustainability. Experts now see Industry 5.0 as fusing powerful, intelligent, and precise technology with the extraordinary inventiveness of human workers. However, many digital visionaries believe Industry 5.0 will bring back the human element in the manufacturing industry (George, 2024). The industrial revolution has increased productivity of industrial activities at the same time as it has increased the complexity of the industrial systems themselves (ElFar et al., 2021). The development of these qualities has been hastened by advances in artificial intelligence (AI) and systems that use human and machine collaboration as resources to build a network that can execute orders with near-human intelligence.

The Industry 5.0 Revolution is characterized by the collaboration of humans and machines to increase industrial production efficiency. Industry 5.0 is rapidly expanding into various exciting technologies and applications that enhance production and enable the spontaneous distribution of customized products. Security is crucial in Industry 5.0, as it directly impacts an enterprise's success. A security assessment is necessary, as threats can compromise availability, integrity, confidentiality, and non-repudiation by exploiting software and hardware vulnerabilities. Additionally, the core values of Industry 5.0 enhance the current Industry 4.0 paradigm by focusing on research and innovation to transition towards a sustainable, human-centric, and resilient industrial framework. In Industry 5.0, the term "human-centric" refers to the fusion of human knowledge, intelligence, and creativity with machinery to enhance productivity. This approach ensures that manufacturing technology is adaptable to the diverse needs of the workforce. Technology aims to benefit people and societies. Industry 5.0 fosters a culture of security awareness by educating employees, reducing the likelihood of successful social engineering attacks that capitalize on human error. This approach helps organizations build a proactive workforce dedicated to safeguarding systems and data

(Kour et al., 2024). Resilience involves strengthening industrial production to withstand disruptions and ensure the continuous support of critical infrastructure. Key components of resilience include intrinsic redundancy and adaptability, enabling systems to recover from malfunctions. Industry 5.0 emphasizes sustainability and resilience as fundamental design elements, utilizing data-driven projects like closed-loop manufacturing and interconnected supply chains. However, this interconnectedness creates a complex cybersecurity landscape that necessitates robust security controls (Abuhasel, 2023).

The main objective of this review paper is to analyze the current cybersecurity threats, vulnerabilities and challenges facing organizations embracing Industry 5.0. The following research questions are addressed in this study:

- What are the key-enabling technologies and major applications for Industry 5.0?
- How to protect the industry 5.0 from the current cybersecurity threats and challenges?

The remainder of the paper is organized as follows: The next section describes the key enabling technologies, followed by a discussion on the major applications in the Industry 5.0 environment. The subsequent section focuses on the security requirements. Then, the paper highlights the various security threats in Industry 5.0, explores the future of cybersecurity in Industry 5.0, and finally concludes with some suggestions for future directions.

Key Enabling Technologies for Industry 5.0

With the advent of Industry 5.0, the industrial revolution gained human-centric, resilient, and sustainable characteristics. By saving human workers from having to perform repetitive activities, it will completely transform production processes across the globe. There are a lot more applications in Industry 5.0 than in Industry 4.0. Having a broad, industry-spanning perspective is essential when evaluating the strategic significance of Industry 5.0 (Ghobakhloo et al., 2023; Rehman et al., 2022). The exponential growth of the Internet and related technologies is projected to drive the global number of social media users from 4.59 billion in 2022 to an estimated 5.85 billion by 2027 (Murteira & Antunes, 2024). Nonetheless, manufacturing principles, control, and intelligent behavior are the foundation upon which experts have created the industry 5.0 vision. Industry 5.0 places people at the center of processes and focuses on three ever-more-important

areas: sustainability, inclusivity, and quality of life. Industry 5.0 aims to regulate technological growth and systematically solve the social and environmental flaws of Industry 4.0. It is a natural continuation of the present digital industrial revolution. Additionally, Industry 5.0 relies on the integration of several technologies, techno-functional concepts, and intelligent components to achieve a transition towards a productive, human-centric, sustainable, and resilient future industry. Several major technologies are used in Industry 5.0, such as digital twins (DT), AI and extended reality (XR) technologies, 6G systems, cyber-physical systems (CPS), intelligent healthcare, and the Internet of Things (IoT) (Alabdulatif et al., 2022; Moustafa et al., 2019). These major technologies are explained as follows:

- **6G:** 6G will represent the new generation of wireless communication, enabling low latency, a higher volume of data transfer rates, and connectivity. This new communication is going to bring revolutionary changes to Industry 5.0: seamless integration of AI-driven systems, real-time processing of big data, and a much higher degree of automation. More particularly, 6G-amazing IoT networks and hyper-connectivity will drive innovation in such fields as smart manufacturing, autonomous systems, and immersive technologies like AR and VR (Mantri et al., 2024).
- **Digital Twins (DT):** Digital twins are virtual replicas of physical systems that facilitate real-time monitoring, simulation, and optimization. Integrating AI, IoT, and edge computing, DT thus enables predictive maintenance, improves system efficiency, and enhances decision-making processes in various industries (Hozdić & Jurković, 2023).
- **Cyber-Physical Systems (CPS):** CPS perfectly represents the integration of physical processes with digital computation and communication. These systems connect physical devices and machinery to intelligent software for real-time monitoring, control, and automation. CPS acts as the backbone for Industry 5.0 because it will enable adaptive manufacturing, improve the resiliency of systems, and thus facilitate efficient collaboration between humans and machines (Huang et al., 2022).
- **Internet of Things (IoT):** IoT is a network of connected devices and sensors that continuously monitor data, share information, and analyze it. In the case of Industry 5.0, IoT provides smart manufacturing with a backbone when machines, systems, and humans freely communicate with each

other. Integrated with AI and edge computing, IoT enables predictive analytics to improve operational efficiencies and extend support for personalized, human-centric innovations across industries (Chander et al., 2022).

- **AI and Extended Reality (XR):** Virtual reality (VR) is a computer-generated simulation that replicates a real-world environment or creates an entirely new, imaginary realm (Gkatzola & Papadopoulos, 2023).
- **Intelligent Healthcare (IHC):** Intelligent healthcare is a key application in the era of Industry 5.0, signaling a paradigm shift in patient care and medical services (Gkatzola & Papadopoulos, 2023).

Major Applications in Industry 5.0

Cutting-edge technologies such as cloud computing, robotics, artificial intelligence (AI), and the Internet of Things (IoT) are used in Industry 5.0, or the fifth generation of industrial production. Industry 5.0 places a strong emphasis on the manufacturing sector's integration of people, equipment, and technology. However, specialists have built the industry 5.0 vision on a foundation of manufacturing principles, control, and intelligent behavior. Some of the major applications of Industry 5.0 are highlighted in Table 1.

Table 1
Major Applications of Industry 5.0

Technology	Description
Collaborative Robotics (Cobots)	Collaborative robot (cobot) systems play a transformative role in enhancing workplace safety, efficiency, and collaboration across the workforce. Designed to operate alongside human employees, cobots excel at performing repetitive tasks such as assembly, quality control, and material handling with exceptional precision. By handling these monotonous and physically demanding activities, cobots not only reduce the risk of workplace injuries and minimize human error but also free employees to concentrate on more creative and strategic responsibilities (Rahman et al., 2024).
Human-Centric Workplaces	Industry 5.0 creates more interactive and ergonomically designed workplaces by leveraging digital twins, virtual reality, and augmented reality (Maddikunta et al., 2022).

Cont. Table 1
Major Applications of Industry 5.0

Technology	Description
Healthcare Innovation	Robotic surgery, wearable health monitoring devices, and personalized medicine are some of the healthcare solutions that are being developed using Industry 5.0 technologies (Grybauskas et al., 2022).
Agriculture 5.0	Agriculture 5.0 optimizes crop yields, minimizes resource consumption, and advances sustainable farming practices through the application of drone technology, AI, and precision farming techniques (Raffik et al., 2023)
Smart Manufacturing	While smart manufacturing technology has hugely revolutionized industrial processes, in the context of Industry 5.0, they would be efficient, sustainable, and human-centric in nature. Industry 5.0 applies IoT devices to connect machines, sensors, and systems for real-time collection and analysis of data. In such an ecosystem, predictive maintenance is facilitated, thus minimizing downtime and operational disruption owing to the identification of any forthcoming equipment failure in advance. AI and machine learning further enhance this by providing advanced analytics and decision-making capabilities that enable manufacturers to optimize production schedules, reduce waste, and improve resource allocation (Sarkar et al., 2024).
Edge Computing (EC)	Edge computing is essential to Industry 5.0 because it moves data processing closer to the sources of data generation, which include IoT devices and sensors utilized in production and manufacturing processes (Dalal et al., 2023).

With an emphasis on sustainability, personalization, and improved collaboration, these aforementioned Industry 5.0 applications are crucial in balancing human brilliance with cutting-edge technologies. Furthermore, these applications highlight Industry 5.0's dedication to improving human capacities, encouraging environmental sustainability, and customizing goods and services across a range of industries.

Security Requirements for Industry 5.0

Many industries are currently witnessing a significant improvement in the quality of industrial production because of digitizing an increasing number of industrial processes, utilizing automated big data collection from sensors and

actuators, conducting inference, trend analysis, and employing AI-based future event prediction. However, these developments also raise the demands on industrial processes' dependability, including resilience to both intentional and unintentional failures and cyberattacks (Anwar & Qureshi, 2023). Although significant efforts were made to harness the technological revolution through simple evolutionary activities, the variety of technologies underlying Industry 5.0, on the other hand, produces an undesirable speed of change since firms must expend enormous efforts to adapt them to the current organizational framework. Modern technologies like artificial intelligence (AI), machine learning, cloud computing, analytics, and the Internet of Things (IoT) are forcing businesses to integrate their production processes. Industry 5.0 describes a new degree of smooth and harmonious integration between people, automation, and robots in organizations like distribution networks. Automation refers to the administration, enhancement, and deployment of procedures and technological systems. Because the ubiquity of these information and operation technologies has altered the appearance of cyber dangers, cyber security risks are vital (Anwar & Abdullah, 2023).

Industry 5.0 is composed of multiple interdependent components that form complex architectures. A significant security risk to the system could arise from the jeopardizing of any one of these parts, which could then cause disruptions in the way the system operates. Because of their interconnectivity, the system is extremely vulnerable to attacks since if one link in the chain becomes compromised, the entire system could fail. If the system is not designed to prevent such attacks, it could lead to an abrupt end of all network operations. The primary objective of security in Industry 5.0 is to protect data, networks, and physical assets from known and undiscovered threats, vulnerabilities, and assaults. Numerous gadgets produce large amounts of data that are utilized as decision-making tools. To maintain the availability and integrity of the collected data, experts view it as the most precious asset and need sufficient protection. Integrity ensures that only those who are authorized and expected to take action actually do so. It is the guarantee of the correctness of the resources within a system. Table 2 enumerates the security requirements that authentication procedures and designers must consider (Black et al., 2023; Boisrond et al., 2024; Liu et al., 2022).

Table 2
Industry 5.0 Security Requirements

Security Requirements	Description
Confidentiality	With data related to trade secrets, customer information, and industrial processes accessible only to those with the appropriate permission, the goal is to avoid unauthorized access to or exposure of sensitive information.
Integrity	The guarantee that information and procedures are correct, dependable, and unaltered is known as integrity.
Availability	Availability means the capability and ability to ensure that industrial systems, networks, or data are regularly accessible to authorized users when required. The challenge of this concept assumes extensive importance in the frame of Industry 5.0. In Industry 5.0, advanced technologies such as IoTs, AI, collaborative robotics, and edge computing will result in wide integration into the industrial environment, thereby increasing dependency on digital infrastructure. The robust strategy of Industry 5.0 involves avoiding downtime and ensuring continuous access to critical resources (Boisrond et al., 2024).
Authentication	Authentication becomes crucial to be implemented in the Industry 5.0 area, allowing the secure access of industrial networks, sensitive data, and operational technologies. In cases where advanced technologies like IoT, AI, and collaborative robots are being introduced into the ecosystems by Industry 5.0, the surge in complexity and interconnectivity of systems jumps to a whole new dimension. This brings in broader attack surfaces where robust authentication mechanisms become intrinsic needs for maintaining security (Boisrond et al., 2024).
Authorization	Industry 5.0 requires authorization to be instantiated as the backbone in maintaining operational integrity, especially in environments where human-machine collaboration and advanced technologies are deeply ingrained. With smart systems, collaborative robots, and IoT devices interacting. In connected ecosystems involving smart systems, collaborative robots, and IoT devices, it is crucial to ensure that only authorized individuals, devices, and processes have access to critical resources, thereby protecting sensitive data and operations (Hassan et al., 2024).
Non-repudiation	Non-repudiation provides the verifiability and traceability of acts, data exchanges, or transactions conducted digitally within Industry 5.0 standards.
Anonymity	Data security and inaccessibility to potential adversaries are provided through anonymity.
Attack Resistance	It is the ability of industrial systems, networks, and devices to defend against cybersecurity threats and attacks effectively.

Industry 5.0 is currently facing cyberattacks targeting not only devices directly but also their communication networks, associated applications, and underlying hardware and software systems. Increases in devices, infrastructure availability, integrity, scalability, and interoperability have led to the creation of new vulnerabilities.

Security Threats to Industry 5.0

Within the context of Industry 5.0, a "Cyber Threat" is any potential threat, danger or harmful activity directed at the digital systems, networks, and data utilized in sophisticated industrial processes (Natalia et al., 2024). On the other hand, "Vulnerabilities" in the context of Industry 5.0 refer to shortcomings or imperfections in digital systems, networks, or devices that could be used by cyber threats as a means of harm or disruption (Kour et al., 2024). Industry 5.0 is vulnerable to many cyber risks and attacks due to its integration with human intelligence and smart technology (Siddharth et al., 2021; Tallat et al., 2023). A summary of these threats is provided in Table 3.

Table 3
Security Threats to Industry 5.0

Threat	Description
Advance Persistent Threats (APTs)	Industry 5.0 infrastructure is often vulnerable to complex stealthy cyberattacks known as advanced persistent threats (APTs).
IoT Device Attacks (IoT)	Industry 5.0 is heavily dependent on IoT devices, making them an easy target for cybercriminals.
Supply Chain Attacks	The interconnected supply chains of Industry 5.0 are susceptible to cyberattacks that aim to compromise the integrity of goods and services.
Man-in-the-Middle Attack (MitM)	In Industry 5.0, Man-in-the-Middle (MitM) attacks occur when an attacker intercepts and monitors communications between two systems, such as an IoT device and its control system.
Ransomware Attacks	Attacks like Ransomware have the potential to stop production and cause significant financial losses.
Impersonation Attack	The attacker may try to fabricate fake communications as part of this assault that seems to have originated from a source entity.
Guessing (on-of-fline) Attack	A malicious party can effectively guess a registered user's credentials (password and biometrics) in an access control scheme by using intercepted messages (Turner & Oyekan, 2023).

Table 3 highlights the security requirements unique to Industry 5.0, addressing the distinct challenges posed by this advanced industrial landscape. For instance:

Authorization: In Industry 5.0, authorization must go beyond simply verifying users' access rights. It should dynamically adapt to evolving roles and responsibilities within highly collaborative environments. The primary challenge lies in implementing fine-grained access controls that consider real-time context and user behavior.

Data Integrity: Ensuring data integrity is vital in Industry 5.0, where vast amounts of data are generated by interconnected devices. Key challenges include safeguarding data from unauthorized alterations by malicious actors and maintaining its authenticity during transmission across multiple platforms.

Authentication: The integration of diverse technologies and human operators in Industry 5.0 necessitates robust authentication mechanisms to accurately verify identities while maintaining seamless workflow. This involves overcoming challenges associated with implementing multi-factor authentication in environments where speed and efficiency are critical.

Resilience: The interconnected nature of Industry 5.0 systems demands a strong focus on resilience against cyberattacks and operational disruptions. Organizations must implement adaptive security measures capable of addressing evolving threats while ensuring uninterrupted operations.

Each requirement highlights the unique complexities brought about by the human-centric focus of Industry 5.0, calling for a redefinition of traditional security paradigms.

Because Industry 5.0 depends so heavily on new technology and interconnected systems, it is vulnerable to many cyber threats and attacks. A strong cybersecurity strategy, including safe system design, vulnerability assessments, and ongoing monitoring, is required to counter these attacks.

Cyber Security for Industry 5.0

The adoption of Industry 5.0 technologies has become essential for maintaining competitiveness in today’s market. A smart, open manufacturing platform aims to establish a human-centric, sustainable, and resilient foundation for the interconnected industrial networks of Industry 5.0 (Kolosnjaji et al., 2018). On the

other hand, this increased connectedness and complexity of Industry 5.0 systems created new challenges in cybersecurity, thereby making them more vulnerable and prone to various kinds of attacks. Every connected device, sensor, actuator or cobot becomes a potential entry point for malicious actors. Cybersecurity breaches can cause a significant impact- namely, economic damage, production loss, injury, and death. With the rising frequency and severity of cyberattacks, cybersecurity professionals face increasingly complex and challenging threats to manage (Corallo et al., 2022).

The new attack vectors brought by emerging technologies like AI, IoT, and 5G require innovative cybersecurity solutions. Furthermore, the vast volumes of data generated and exchanged in Industry 5.0 raise significant concerns about data privacy and confidentiality, particularly in the event of unauthorized access or security breaches. In addition, the integration of AI and machine learning in industrial processes, while improving operational efficiency, also poses cybersecurity threats and risks. The complexity of these technologies can be exploited if not properly secured, leading to potential breaches and operational disruptions (Santos et al., 2024).

Industry 5.0, as an interconnected ecosystem, introduces numerous cybersecurity challenges that must be addressed to ensure system safety and security. The proliferation of connected devices—such as machines, sensors, and robots—creates multiple potential entry points for attackers. Additionally, the vast amounts of sensitive data generated and collected within Industry 5.0 systems, including production data, customer information, and AI models, underscore the critical need for robust data security measures. Industry 5.0 extends its influence beyond the factory floor, encompassing suppliers and partners within its ecosystem. Any vulnerabilities in the supply chain can be exploited to infiltrate core systems. Furthermore, the intricate interactions between humans and machines in Industry 5.0 heighten the risk of social engineering attacks and the manipulation of human operators, posing critical challenges that demand careful attention (Kour et al., 2024).

Industry 5.0 increases connectivity and devices, and the need for growing data protection will increase in consequence. The manufactured devices of today's era should consider cybersecurity as a core building block. This will ensure a better, strong operational resiliency in Industry 5.0 against any cyber threats or attacks. Additionally, AI-powered security solutions will give a new direction to threat detection and incident response capabilities. The tools and devices that assure

cybersecurity are crucial elements for Industry 5.0 systems; the sooner these technologies are in place, the longer it takes to unlock its full potential. With proper countermeasures in place, an organization can ensure that its cybersecurity posture is improved to such an extent that the advancements of Industry 5.0 are realized without compromising security (Lechachenko et al., 2023).

Future of Cyber Security for Industry 5.0

Cybersecurity is a growing concern since more sectors incorporate cutting-edge technologies like robotics, IoT, and artificial intelligence into their daily operations. Industry 5.0's cybersecurity landscape is expected to undergo significant changes. Along with increased personalization and efficiency, this integration also presents difficult cybersecurity issues. Future cybersecurity efforts will likely concentrate on creating more complex defenses, using AI to analyze threats in advance, and improving data privacy by using cutting-edge encryption methods to solve them. Securing the Industry 5.0 ecosystem against new cyber threats will also depend on the proactive cooperation of industry stakeholders, ongoing innovation in cybersecurity technologies, and adherence to strict norms and laws (Tuptuk & Hailes, 2018).

The systems in Industry 5.0's intelligence and interconnection increase production, but they also increase the attack surface area that cybercriminals can target. For instance, the incorporation of IoT devices increases operational efficiency but also creates vulnerabilities because of their sometimes-inadequate security features. As new and dynamic cyber threats emerge in Industry 5.0, a proactive and comprehensive approach to cybersecurity is required. Although traditional cybersecurity measures are in place and are still relevant, they may not be sufficient to address the sophisticated and evolving nature of these threats. The integration of advanced cybersecurity technologies, along with the development of robust security protocols and continuous monitoring, is imperative. In addition, fostering a culture of cybersecurity awareness among the workforce is equally important and crucial to mitigating the risks associated with human error. To protect industrial innovation and productivity in the future, it is imperative that we comprehend and address these cyber dangers and vulnerabilities as we progress further into the era of Industry 5.0. The digital infrastructure of Industry 5.0 is susceptible to cyberattacks, which pose a risk of disrupting industrial operations, gaining unauthorized access, and compromising data. The installation phase of Industry 5.0 technologies is still in progress. However, adopting Industry 5.0 re-

quires collaboration with smart machines and cobots while adhering to industrial standards and regulations. The three future directions for Industry 5.0 are quantum computing, cognitive computing, and human-machine interaction.

Conclusion and Directions for Future Research

This review-based study focuses on analyzing the various cybersecurity threats and vulnerabilities Industry 5.0 is facing. Industry 5.0 ushers in a new era of technology integration and human-centered innovation, yet it also unveils a multitude of cyberthreats and vulnerabilities, necessitating robust and advanced cybersecurity defenses. Industry 5.0's unique combination of IoT, AI, and collaborative robotics improves operational efficiency and personalization while posing challenging security issues. These challenges to the integrity and resilience of industrial systems include advanced persistent attacks, data privacy breaches, and the exploitation of Internet of Things vulnerabilities. Developing a culture of cybersecurity awareness, establishing robust legislative frameworks, and introducing cutting-edge technological solutions are all necessary components of a multipronged strategy to tackle these issues. To ensure that cyberthreats do not jeopardize the potential benefits of this technical advancement, the underlying approaches to safeguarding these networked systems must also evolve in tandem with Industry 5.0.

References

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

Adi, E., Anwar, A., Baig, Z., & Zeadally, S. (2020). Machine learning and data analytics for the IoT. *Neural Computing and Applications, 32*, 16205–16233. https://doi.org/10.1007/s00521-020-04874-y

Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). Security of blockchain and AI-empowered smart healthcare: Application-based analysis. *Applied Sciences, 12*(21), 11039. https://doi.org/10.3390/app122111039

Anwar, R. W., & Abdullah, T. (2023). DBTS: Distributed blockchain-based trust scheme for data privacy and security in smart cities. In K. Arai (Ed.), *Proceedings of the Future Technologies Conference (FTC) 2023, Volume 1. FTC 2023. Lecture Notes in Networks and Systems* (Vol. 813, pp. 423–436). Springer. https://doi.org/10.1007/978-3-031-47454-5_30

Anwar, R. W., & Qureshi, K. N. (2024). Attack detection mechanisms for Internet of Everything (IoE) networks. In K. Naseer Qureshi, T. Newe, G. Jeon, & A. Chehri (Eds.), *Cybersecurity vigilance and security engineering of Internet of Everything. Internet of Things* (pp. 33–48). Springer. https://doi.org/10.1007/978-3-031-45162-1_3

Black, N. L., Neumann, W. P., Noy, I., & Dewis, C. (2023). Applying ergonomics and human factors to congress organization in uncertain times. *Applied Ergonomics, 106*, 103862. https://doi.org/10.1016/j.apergo.2022.103862

Boisrond, K., Tardif, P. M., & Jaafar, F. (2024). Ensuring the integrity, confidentiality, and availability of IoT data in Industry 5.0: A systematic mapping study. *IEEE Access*, *12*, 107017–107045. https://doi.org/10.1109/ACCESS.2024.3434618

Chander, B., Pal, S., De, D., & Buyya, R. (2022). Artificial intelligence-based Internet of Things for Industry 5.0. In S. Pal, D. De, & R. Buyya (Eds.), *Artificial intelligence-based Internet of Things systems* (pp. 3–45). Springer. https://doi.org/10.1007/978-3-030-87059-1_1

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the industrial Internet of Things: A systematic literature review. *Computers in Industry, 137*, 103614. https://doi.org/10.1016/j.compind.2022.103614

Dalal, S., Seth, B., & Radulescu, M. (2023). Driving technologies of Industry 5.0 in the medical field. In B. Akkaya, S. A. Apostu, E. Hysa, & M. Panait (Eds.), *Digitalization, sustainable development, and Industry 5.0: An organizational model for twin transitions* (pp. 267–292). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83753-190-520231014

ElFar, O. A., Chang, C.-K., Leong, H. Y., Peter, A. P., Chew, K. W., & Show, P. L. (2021). Prospects of Industry 5.0 in algae: Customization of production and new advance technology for clean bioenergy generation. *Energy Conversion and Management: X, 10*, 100048. https://doi.org/10.1016/j.ecmx.2020.100048

George, A. S. (2024). Bridging the digital divide: Understanding the human impacts of digital transformation. *Partners Universal International Innovation Journal (PUIIJ), 2*(3), 1–34. https://doi.org/10.5281/zenodo.11287684

Ghobakhloo, M., Iranmanesh, M., Foroughi, B., Tirkolaee, E. B., Asadi, S., & Amran, A. (2023). Industry 5.0 implications for inclusive sustainable manufacturing: An evidence-knowledge-based strategic roadmap. *Journal of Cleaner Production, 417*, 138023. https://doi.org/10.1016/j.jclepro.2023.138023

Gkatzola, K., & Papadopoulos, K. (2023). Social media actually used by people with visual impairment: A scoping review. *British Journal of Visual Impairment, 42*(3), 832–848. https://doi.org/10.1177/02646196231189393

Grybauskas, A., Stefanini, A., & Ghobakhloo, M. (2022). Social sustainability in the age of digitalization: A systematic literature review on the social implications of Industry 4.0. *Technology in Society, 70*, 101997. https://doi.org/10.1016/j.techsoc.2022.101997

Hassan, M. A., Zardari, S., Farooq, M. U., Alansari, M. M., & Nagro, S. A. (2024). Systematic analysis of risks in Industry 5.0 architecture. *Applied Sciences, 14*(4), 1466. https://doi.org/10.3390/app14041466

Hozdić, E., & Jurković, Z. (2023). Cognitive cyber-physical production systems: A new concept of manufacturing systems on the route to Industry 5.0. In I. Karabegovic, A. Kovačević, & S. Mandzuka (Eds.), *New technologies, development and application VI. NT 2023. Lecture Notes in Networks and Systems* (Vol. 687, pp. 201–212). Springer. https://doi.org/10.1007/978-3-031-31066-9_21

Huang, S., Wang, B., Li, X., Zheng, P., Mourtzis, D., & Wang, L. (2022). Industry 5.0 and Society 5.0—Comparison, complementation, and co-evolution. *Journal of Manufacturing Systems, 64*, 424–428. https://doi.org/10.1016/j.jmsy.2022.07.010

Ivascu, L. (2020). Measuring the implications of sustainable manufacturing in the context of Industry 4.0. *Processes, 8*(5), 585. https://doi.org/10.3390/pr8050585

Kolosnjaji, B., Demontis, A., Biggio, B., Maiorca, D., Giacinto, G., Eckert, C., & Roli, F. (2018). Adversarial malware binaries: Evading deep learning for malware detection in executables. In *Proceedings of the 26th European Signal Processing Conference (EUSIPCO)* (pp. 533–537). https://doi.org/10.48550/arXiv.1803.04173

Kour, R., Karim, R., Dersin, P., & Venkatesh, N. (2024). Cybersecurity for Industry 5.0: Trends and gaps. *Frontiers in Computer Science, 6*, 1434436. https://doi.org/10.3389/fcomp.2024.1434436

Lechachenko, T., Kozak, R., Skorenkyy, Y., Kramar, O., & Karelina, O. (2023). Cybersecurity aspects of smart manufacturing transition to Industry 5.0 model. *IT-TAP*, 416–424. https://ceur-ws.org/Vol-3628/short15.pdf

Liu, Z., Liu, Q., Xu, W., Wang, L., & Zhou, Z. (2022). Robot learning towards smart robotic manufacturing: A review. *Robotics and Computer-Integrated Manufacturing, 77*, 102360. https://doi.org/10.1016/j.rcim.2022.102360

Maddikunta, P. K. R., Pham, Q.-V., Prabadevi, B., Deepa, N., Dev, K., Gadekallu, T. R., Ruby, R., & Liyanage, M. (2022). Industry 5.0: A survey on enabling technologies and potential applications. *Journal of Industrial Information Integration, 26*, 100257. https://doi.org/10.1016/j.jii.2021.100257

Mantri, D. S., Pawar, P. M., Kulkani, N. P., Prasad, N. R., & Prasad, R. (2024). Industry 5.0 and 6G: Human-centric approach. In *6G connectivity-Systems, technologies, and applications* (pp. 21–37). River Publishers. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003515920-2/industry-5-0-6g-human-centric-approach-dnyaneshwar-mantri-pranav-pawar-nandkumar-kulkani-neeli-prasad-ramjee-prasad

Moustafa, N., Hu, J., & Slay, J. (2019). A holistic review of network anomaly detection systems: A comprehensive survey. *Journal of Network and Computer Applications, 128*, 33–55. https://doi.org/10.1016/j.jnca.2018.12.006

Murteira, C. S. R., & Antunes, A. C. (2024). All users are equal, but some users are more equal than others: Exploring the psychology of users that follow social media influencers. In *Using influencer marketing as a digital business strategy* (pp. 89–111). IGI Global. https://doi.org/10.4018/979-8-3693-0551-5.ch004

Natalia, T., Pathani, A., Dhaliwal, N., Rajasekhar, N., & Khatkar, M. (2024). Blockchain integration in Industry 5.0: A security experiment for resilience assessment. *BIO Web of Conferences*, *86,* 01070. https://doi.org/10.1051/bioconf/20248601070

Raffik, R., Sathya, R. R., Vaishali, V., & Balavedhaa, S. (2023). Industry 5.0: Enhancing human-robot collaboration through collaborative robots—A review. In *Proceedings of the 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICAECA56562.2023.10201120

Rahman, M. M., Khatun, F., Jahan, I., Devnath, R., & Bhuiyan, M. A.-A. (2024). Cobotics: The evolving roles and prospects of next-generation collaborative robots in Industry 5.0. *Journal of Robotics, 2024(1)*, 2918089. https://doi.org/10.1155/2024/2918089

Rashid, A. B., & Kausik, A. K. (2024). AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications. *Hybrid Advances*, *7,* 100277. https://doi.org/10.1016/j.hybadv.2024.100277

Rehman, A., Abbas, S., Khan, M., Ghazal, T. M., Adnan, K. M., & Mosavi, A. (2022). A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. *Computers in Biology and Medicine, 150*, 106019. https://doi.org/10.1016/j.compbiomed.2022.106019

Santos, B., Costa, R. L. C., & Santos, L. (2024). Cybersecurity in Industry 5.0: Open challenges and future directions. In *Proceedings of the 21st Annual International Conference on Privacy, Security and Trust (PST)* (pp. 1–6). IEEE. https://doi.org/10.1109/PST62714.2024.10788065

Sarkar, B. D., Shardeo, V., Dwivedi, A., & Pamucar, D. (2024). Digital transition from Industry 4.0 to Industry 5.0 in smart manufacturing: A framework for sustainable future. *Technology in Society, 78*, 102649. https://doi.org/10.1016/j.techsoc.2024.102649

Sharma, A., & Singh, B. J. (2020). Evolution of industrial revolutions: A review. *International Journal of Innovative Technology and Exploring Engineering, 9*(11), 66–73. https://www.ijitee.org/wp-content/uploads/papers/v9i11/I7144079920.pdf

Siddharth, D., Saini, D. K., & Kumar, A. (2021). Precision agriculture with technologies for smart farming towards Agriculture 5.0. In *Unmanned aerial vehicles for Internet of Things (IoT) concepts, techniques, and applications* (pp. 247–276). Wiley. https://doi.org/10.1002/9781119769170.ch14

Tallat, R., Hawbani, A., Wang, X., Al-Dubai, A., Zhao, L., Liu, Z., Min, G., Zomaya, A. Y., & Alsamhi, S. H. (2024). Navigating Industry 5.0: A survey of key enabling technologies, trends, challenges, and opportunities. *IEEE Communications Surveys & Tutorials, 26*(2), 1080–1126. https://doi.org/10.1109/COMST.2023.3329472

Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems, 47*, 93–106. https://doi.org/10.1016/j.jmsy.2018.04.007

Turner, C., & Oyekan, J. (2023). Manufacturing in the age of human-centric and sustainable Industry 5.0: Application to holonic, flexible, reconfigurable, and smart manufacturing systems. *Sustainability, 15*(13), 10169. https://doi.org/10.3390/su151310169

Raja W. Anwar is an Assistant Professor of Cybersecurity at the German University of Technology (GUtech). His research focuses on cybersecurity, machine learning, wireless sensor networks, and the Internet of Things (IoT). He has published extensively in top-tier peer-reviewed journals in these domains. (raja.anwar@gutech.edu.om)

Yasmine Souissi is the Director of the Research and Consultancy Office (RCO) at the German University of Technology (GUtech) and an Assistant Professor in the Department of Engineering. Her research focuses on bio-hydrogen production, wastewater treatment, and biofertilizer development. She has published extensively in leading peer-reviewed journals in these fields. (yasmine.souissi@gutech.edu.om)

Saqib Ali is a Professor of Information Systems at Sultan Qaboos University. His research interests include cybersecurity for cyber-physical systems, information systems security, and e-business communication. He has published extensively in leading peer-reviewed journals in these fields. (saqib@squ.edu.om)