Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Cyber Security Challenges in Industry 4.0: A Review

Farah Sami Khoshaba, Shavan Askar, Soran Abdulrahman Hamad, Sozan Sulaiman Maghdid
farah.xoshibi@epu.edu.iq, shavan.askar@epu.edu.iq,
[1]Information System Engineering, Technical Engineering College, Erbil Polytechnic University, Erbil, Iraq
[2]College of Engineering, Erbil Polytechnic University, Erbil, Iraq

Article Information

Submitted : 21 Mar 2024
Reviewed: 25 Mar 2024
Accepted : 8 Apr 2024

Keywords

Industry 4.0, cyber-security, Cyber-physical, Internet of Things (IOT)

Abstract

In the era of Industry 4.0, when smart factories and networked systems are reshaping the landscape of industrial production, the protection of important data and information security is a top priority. Cyber-physical systems and the technology that supports it are the keys to Industry 4.0. It is founded on four essential design principles: interoperability, availability of information, technological assistance, and decentralized decision-making. These design principles, however, provide new weaknesses that could be exploited by bad people. To protect these systems from emerging dangers, great consideration should be given to the proactive and adaptive security measures, which will consequently enable the continuing growth and success of Industry 4.0 technologies. This paper will delve into the multifaceted challenges that Industry 4.0 presents in terms of data security and the emerging solutions and strategies required protecting vital information in this brave new world of manufacturing. The exploration of these challenges and the proposed solutions are essential for businesses and policymakers alike to navigate the complexities of data security and ensure the resilience of critical information in the digital age of Industry 4.0.

A. Introduction

Industry 4.0, first stated in 2011, has recently gained attention as the fourth industrial revolution. It has been defined as "a name for the current trend that is changing the way industry works [1]. It may be seen as an industrial stage when information and communication technologies are integrated with production processes [2]. Some examples of I4.0 technologies are: artificial intelligence, augmented/virtual reality, big data, blockchain technology, cloud computing, digital platforms, and the Internet of Things [3]. While the implementation of Industry 4.0 appears to solve many of production issues, new cyber-security concerns may be introduced. The use of sensors and remote access may provide entry points for hackers, cybercriminals or industry competitors to gain access to the systems. The main security challenges identified in this domain include data privacy and security, access control, attack mitigation, and detection for anomalies [4]. With industries depending more and more on networked systems, protecting vital data has become a top priority to defend against cyberattacks and guarantee the stability of industrial processes. The goal of this thorough analysis is to examine the intricacies of data security within the framework of Industry 4.0. In addition to stressing the presence of hype and inflated estimates within the Industry 4.0 discourse, the research issues a warning against having high expectations. Executives are under tremendous pressure to change and stay competitive in the face of Industry 4.0 market projections that are expected to be worth trillions of dollars and potentially create enormous amounts of value [5]. In response to critics, it is imperative to recognize that, even though computing technology has been around for more than 50 years, the extraordinary rate of change, along with improvements in hardware and software capabilities, signals the start of a new phase of the industrial revolution. Industry 4.0 has a revolutionary potential that goes beyond simple technology improvements; it can positively reshape humankind's destiny. The paper's later sections outline the essential components of Industry 4.0 and focus on the challenges that Industry 4.0 may face from two different points of view: main challenges and security challenges. The goal is to offer a comprehensive picture of the situation and aid in the creation of plans that safeguard vital data against changing cyber threats by examining the issues and potential solutions. Although there is a growing corpus of material addressing the problems associated with data security in Industry 4.0, there is still a discernible lack of synthesis and consolidation of the existing information. Reviews that now exist tend to concentrate on particular areas, such as technology or human factors, rather than offering a thorough analysis of the issues and solutions of Industry 4.0 data security as a whole. By providing an in-depth analysis of the issues and solutions related to data security in Industry 4.0, this paper seeks to close this gap. Figure (1), depicts a general overview of Industry 4.0's components, including the three main components.

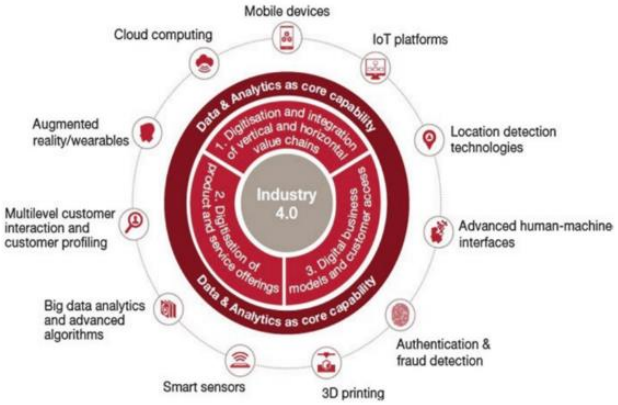

Figure 1. The components of Industry 4.0 [6]

The goal of the review is to offer useful insights for industrial cybersecurity researchers, practitioners, and policymakers by summarizing and critically evaluating the body of existing research. This review's primary goal is to perform a thorough analysis of the state of data security today within the framework of Industry 4.0. Through a review of the literature, this goal seeks to offer a comprehensive picture of the current state of data security, highlighting major issues and weaknesses in the Industry 4.0 framework. The review aims to establish a foundation for a comprehensive assessment of the effectiveness of current security measures using this investigation. The evaluation of suggested frameworks, best practices, and solutions aimed at resolving the noted data security issues in Industry 4.0 is the second goal. This goal is to extract useful insights into practical methods for reducing risks and strengthening data by examining successful implementations and their influence on safeguarding vital information. security within the industrial landscape.

B. Industry 4.0 Components

Industry 4.0 encompasses the digitization and integration of basic technical-economic networks, turning them into complex entities. It integrates three or more interconnected factors. Along with the adoption and integration of new market models, this integration also entails the digitization of goods and services. These three elements embody a range of concepts and technologies that can be broadly classified as elements of Industry 4.0 [7].

Industry 4.0 Components or Reference Architecture Model Industry 4.0 (RAMI 4.0) models serve as the foundation for these components. A three-dimensional understanding of the relationship between technical and economic elements is provided by the RAMI 4.0 model. RAMI 4.0 essentially states that Industry 4.0 is made up of business, functional, information, communication, asset, and integration levels; each of these layers contributes to the creation, upkeep, or use of elements meant to improve production efficiency. Along with considering connections to the outside world, this system also considers enterprise operations and prospects, work units and stations, and device control. However, big data, Smart factories, Cyber-Physical Production Systems (CPPSs), and Internet of Things (IoT) technologies and concepts can be used to categorize the components

included in the RAMI 4.0 model. These four elements clarify Industry 4.0's primary functions and possible commercial uses, even though the platform's main objective is often manufacturing process automation. Figure 2 illustrates how different applications of Industry 4.0 principles and the three main functions are connected via big-data-related technologies. Big data includes information created both inside and outside of the corporate setting. In terms of technology, it could include machine learning and other data analytics methods intended for corporate intelligence and anti-fraud security measures [7]. By emphasizing all cyber computing processes and communication technologies within the context of people and gadgets, the CPPS can also actively participate in big data analytics. To understand and monitor data, the CPPS combines physical processes that carry out directives with computation, networking tools, and technology. The Internet of Things (IoT) interconnection within the factory and the ensuing network application and process alignments give rise to the idea of the Smart Factory as a component of Industry 4.0. It is imperative to acknowledge that a Smart Factory consists of multiple CPPSs and emphasizes the fact that the Smart Factory offers numerous attack surfaces. Any part of a system that is vulnerable to attack is known as its attack surface. Attack surfaces expand along with threats, making them harder to control.

In computing parlance, cloud computing is the Internet-based provisioning of computer services such servers, storage, databases, networking, software, analytics, and intelligence—collectively, "the cloud." This promotes economies of scale, flexible resource allocation, and quicker innovation. By 2018, it is expected that 3.6 billion people will have used cloud computing services. Email, online searches, and financial transactions are just a few of the many online activities that have made cloud computing essential. Big Data is a term that is strongly related to Industry 4.0 and refers to the unprecedented amounts of data that are generated, saved, and shared online. The combined data storage capacity of major internet storage businesses such as Google, Amazon, Microsoft, and Facebook are at least 1,200 petabytes, while exact figures are difficult to determine due to continuously fluctuating volumes. With the advent of technologies like 3D printers, laser machines, and robotic automation, digital manufacturing, also known as factory 2.0, has completely changed traditional production processes. Case examples demonstrate the transition from traditional production lines with large numbers of industrial people to automated processes that use robotics and other technologies. This trend is particularly evident in the automotive industry. Supply Chain Management 4.0 and Logistics 4.0 are the results of Industry 4.0's substantial impact on logistics. Industry 4.0 technology enablers have transformed traditional warehouse operations. This is exemplified by Amazon's sophisticated computer systems and robots that oversee warehouse and delivery operations. Cyber-Physical Systems (CPS) integrate networking, computation, and physical processes.

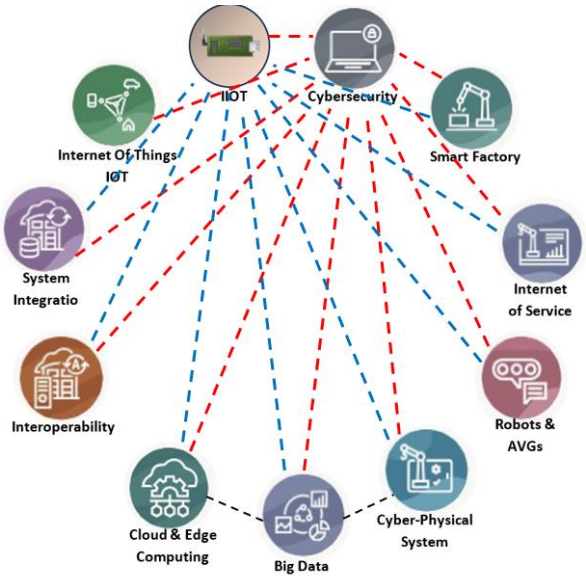

Figure (2). Different Applications of Industry 4.0

C. Industry 4.0 Challenges

In recent years, with the increasing advancement in the applications of the Internet of Things (IoT), the volume of applications and requested data has rapidly increased. In addition, the demand for real-time data processing and analysis is increasing [8]. The convergence of IoT devices with Industry 4.0 has initiated a new era of advanced connectivity and data-driven decision-making. However, this integration also introduces significant security risks, as the main threats to industrial processes become intricately tied to the vulnerabilities associated with interconnected IoT devices. The main security risks associated with IoT devices include vulnerabilities to cyber-attacks, data breaches, privacy concerns, and lack of standard security protocols. Without addressing these risks; the industry 4.0 processes and systems become potential targets for malicious activities. Furthermore, the interconnected nature of IoT devices means that a security breach in one device can have cascading effects on an entire network, leading to significant disruptions and potential harm. It is therefore important to address these security risks to protect critical data, ensure privacy, and maintain the integrity of IoT systems. [9]

These challenges are caused by the distributed design and massive data throughput in edge computing, whereby traditional information security protection strategies used in Industry 4.0 cannot be fully deployed for protecting such information within it. In order to address the above-mentioned challenges, two important dimensions have been selected from prior research [4], [10], and [12] that are discussed in separate tables, which show the complexities based on Industry 4.0. Complex security challenges, are examined in Table 1, focusing on Industry 4.0 security problems such as secure communication, access management, attack mitigation, anomaly detection, and possible solutions. The focal point is information security protection from cyberattacks. As a result, issues in the fields of technology, HR, finance, and policy are analyzed in Table 2. Standards-less environment, lack of technology, and handling liability for products

based on the Internet of Things are some of these difficulties. It is then possible to see the problem with these issues facing Industry 4.0 being so intricate, meaning that all-inclusive solutions are needed in order to navigate this revolutionary industrial terrain successfully.

Table 1. Industry 4.0 Security Challenges

Title	Information
Enhancing privacy and security of data	Edge computing requires effective tools and technologies to ensure data privacy and security. This includes providing users with privacy and security awareness and implementing security protocols for Wi-Fi networks.
Secure communication	To maintain data security in edge computing, ensuring secure communication from data center to edge is critical in edge computing. This includes the use of secure communication protocols and encryption techniques to protect data during transmission.
Access control	Implementing robust user monitoring tools to manage and control access to data and resources in edge computing environments. This includes authentication, authorization and identity management solutions to ensure that only authorized entities have access to sensitive data.
Attack mitigation	Developing strategies and technologies to mitigate potential cyber-attacks targeting edge computing devices and networks. This may involve intrusion detection systems, firewalls, and other security measures to detect and prevent malicious activities.
Anomaly detection	Applying anomaly detection techniques to detect and respond to unusual behavior or security threats in edge computing environments. This includes using machine learning and artificial intelligence to identify and respond to security anomalies.
Proposed Solutions	These proposed solutions aim to address the security challenges in edge computing and pave the way for more secure and resilient edge computing environments.

Table 2. Industry 4.0 Main Challenges

Title	Information
Lack of IT/OT Security Expertise	This challenge stems from individuals' lack of expertise in changing production and securing digital assets associated with them Lack of information security professionals is a major obstacle to effectively

	managing IT and operational technology (OT) security.
Lack of Policies and Funds to Focus on Security	Poor planning and limited funding allocation pose significant challenges in strengthening the security environment in Industry 4.0. This critical cybersecurity infrastructure increases the risk of gaps, while insufficient funding prevents the implementation of comprehensive security measures. Addressing these issues is critical to establishing a strong security foundation in Industry 4.0.
Liability over Products	Many stakeholders are involved in connecting smart objects to the Internet of Things (IoT). These challenges pose challenges related to manufacturing accountability, and clear policies and guidelines are needed to assume responsibility for the development and management of IoT-related devices in Industry 4.0
Lack of Uniform Standardization Science	Unlike IoT or other technologies with established standards, Industry 4.0 security does not have uniform standards. The lack of comprehensive standards complicates the implementation of security measures, creating challenges for users looking to follow standard practices in their Industry 4.0 projects
Technical Constraints of the Devices	Industry 4.0, which focuses on the digitization of existing production processes, faces technological obstacles related to the tools involved. These constraints can affect the ease of digital integration and functionality in the manufacturing process, requiring solutions to overcome technological constraints.

D. Literature Review

The technological landscape has changed due to Industry 4.0, which is defined by the integration of digital technologies in manufacturing processes [13]. These changes have created unprecedented powers and problems. This literature review sheds light on the security implications of Industry 4.0 through the interactions between big data, cyber- physical systems, the Industrial Internet (IIoT), and other sophisticated technologies. Selected articles cover Industry 4.0-related security intelligence, hazards, and challenges and provide details of the solutions. Paper [14] acknowledges the challenges associated with healthcare protection and infrastructure, including the need for rapid response and efficiency, protection of data privacy, and energy consumption of IoT devices internal control. This highlights the need to address these challenges to ensure the safety and efficiency of IoT-enabled healthcare systems. Additionally, the paper highlights the significant impact of IoT and machine learning in the healthcare industry and the critical need to address security and infrastructure challenges for successful integration of these technologies. In [15], Industry 4.0 highlights the key point that safety intelligence and big data converge in the context of healthcare. As businesses enter the fourth technological revolution, the authors highlight the need for robust security measures to protect sensitive health information. The purpose of the chapter is to provide insights into how enhanced security intelligence can be used to protect the privacy, integrity, and general security of health information in Industry 4.0 by integrating big data into health and examining the policy. The chapter focuses on security threats related to

technological services in [16] highlighting the importance and implications of healthcare services while exploring the potential changes of using big data to improve security measures. The authors examine the challenges and risks associated with integrating state-of-the-art technologies into industrial environments. The review covers a wide range of security threats, including potential risks to privacy, data integrity, and the complexity of digitized industrial systems in general by method upon analysis of these threats the article makes an important contribution to understanding and addressing security issues in a rapidly changing Industry 4.0 environment. The paper emphasizes the need for a better understanding of the security environment in order to develop strategies to effectively mitigate the risks associated with Industry 4.0 operations. It is a useful tool for practitioners, academics, and regulators seeking to understand the complexities of digital transformation in manufacturing while maintaining the security and integrity of critical operations. Within the larger framework of Industry 4.0, the thorough assessment by the authors gives practical implications for protecting the manufacturing sector and lays the groundwork for future research efforts. In the Industry 4.0 model, [17] focuses on solving cybersecurity challenges. The authors acknowledge that, in the context of Industry 4.0, where industrial systems face increasing cyber threats as sophisticated technologies merge, insights into specific vulnerabilities emerging at the fourth industrial revolution in is derived from the paper's approach to explore key issues that industry and cybersecurity. They also provide policies and ideas for effectively addressing these cybersecurity issues. The paper provides a comprehensive overview of the changing threat landscape and outlines proactive steps to improve the resilience of industrial systems, serving as a guide for practitioners and policymakers in the industry. In [9] the paper discusses the importance of protecting IoT devices and the potential of blockchain technology to provide secure solutions. It highlights security risks associated with IoT devices and emphasizes the importance of addressing them. The authors propose that blockchain technology can provide a decentralized and secure way to secure IoT applications. The paper also explores the real-world application of blockchain in securing IoT devices and outlines the potential benefits for businesses and consumers. Overall, it provides insights into the intersection of blockchain and IoT security and gives a comprehensive overview of the topic. To improve Industry 4.0 production processes, the authors in [18] propose a new system that blends blockchain technology and cyber-physical processes (CPS). It emphasizes the use of blockchain technology for security and transparency to address data integrity, traceability, and reliability in industrial processes, including the integration of blockchain into the larger system of cyber-physical systems, and to create a secure and efficient basis for Industry 4.0 production. In [19] in which the author explores the practical relationship between IIOT and Industry 4.0 focusing on the contribution of networked devices to industrial development strategy. In its master plan, IIOT provides a thorough integration analysis, providing information for technological developments, applications, and sectoral results. [20] The authors examine how the Internet interacts with the Fourth Industrial Revolution, with special emphasis on integrating IoT technologies into industrial systems In Industry 4.0, the study provides insights into how they can has addressed the role

and implications of IoT, focusing on how networked devices evolve technology systems development. This paper provides a comprehensive view of the interplay between these two disruptive technologies, making it a great resource for understanding how the IoT impacts the Industry 4.0 landscape.

E. Introduction Discussion and Analysis

Industry 4.0 represents a transformational step in technology evolution, and its success depends on how well key data security issues are resolved. Data security becomes paramount as enterprises increasingly rely on network infrastructure to protect against cyberattacks and maintain their operational reliability [45-47]. Comes to the issue of protecting data from threats. The important task of finding an ideal balance between safety and innovation is evident. This paper outlines several research projects on various aspects of Industry 4.0 security, illustrating a multifaceted approach to risk understanding and mitigation. Table 2 provides a summary of several research articles on Industry 4.0, describing their individual objectives and areas of application and presenting them in comparison. The wide range of topics addressed illustrates the nature of multifaceted research efforts in understanding and developing Industry 4.0 technologies and applications[48,49,50].

Table 3. A Comparative Analysis of Objectives and Applications between different studies of Industry 4.0 Research

Ref. No.	year	Field of Application	Objective	Achievement	Critical Analysis
[21]	2010	Industry 4.0 technologies	Classify and advance Industry 4.0 technologies with a layered model, addressing data privacy and IT security	Reviewed RAMI 4.0 as a comprehensive coordinate system	RAMI 4.0 Layered Model for Technology
[22]	2017	Automation technology, IoT	Focus on real-time performance, security, and communication in automation technology	Explored transition from ISA-95 to IoT-based solutions	Real-time Exploration Approach
[23]	2017	Industry 4.0 healthcare	Safeguard healthcare data using enhanced security intelligence in the context of Industry 4.0	Emphasized security intelligence and big data in Industry 4.0 healthcare	Security Intelligence and Big Data Safeguarding Approach
[24]	2018	Industry 4.0	Enhance security and resilience using machine learning and data analytics for threat detection and response	Developed MHMM for threat intelligence in Industry 4.0	Machine Learning Threat Intelligence Approach

[25]	2019	Industry 4.0 framework	Address cybersecurity and safety challenges in Industry 4.0	Explored Integrated Cyber Safety & Security Management System	Cyber Security Management System Approach
[26]	2019	Industrial environments	Analyze wireless data for latency performance and physical-layer security techniques	Discussed challenges of deploying wireless communication for critical control applications	Wireless Data Analysis and Security Challenges Approach
[27]	2019	Industrial Internet of Things (IIoT)	Propose cloud-fog- device storage framework with edge intelligence for data security	Highlighted role of IIoT in advancing industrial productivity	Cloud-Fog- with Edge Intelligence for Data Security Technology
[28]	2019	Industry 4.0	Provide insights into vulnerabilities, recommend strategies for increasing resilience	Addressed cybersecurity challenges in Industry 4.0	Insights into Vulnerabilities and Strategies for Resilience in Industry 4.0 Approach
[29]	2019	Requirement analysis for cybersecurity in Industry 4.0	Conduct a requirement analysis for cybersecurity solutions in Industry 4.0 platforms	Explored requirement analysis for cybersecurity solutions in Industry 4.0 platforms	Cybersecurity Platforms Approach
[30]	2020	Smart factories, Industrial cyber- security	Derive design requirements, propose cryptographic solutions, and recommend secure architecture for low-power OT devices	Used QFD to explore security challenges in smart factories	Cryptographic QFD Exploration Approach

F. Conclusion

With the integration of cutting-edge digital technologies, Industry 4.0 represents a major shift in the evolution of the industry and brings unheard of growth and innovation. This paradigm shift is not without its challenges, especially when it comes to data security. As businesses increasingly rely on networked systems, protecting sensitive data is key to preventing cyber-attacks and ensuring trust in engineering operations. Thus, this comprehensive analysis highlights the importance of maintaining a balanced approach to increasing expectations and market forecasting associated with Manufacturing 4.0. Industry 4.0 has transformative potential that goes beyond simple technological advances to change the course of human history. Focusing on the importance of the Internet of Things (IoT), computer-physical systems (CPS), and other enabling technologies, the paper provides a comprehensive survey of materials and key features of Industry 4.0.

Many scholarly works explore important areas, such as classifying cybersecurity assets, analyzing blockchain applications, assessing supply chain

impacts, and querying data security issues at the edge of the Intelligent Industrial Internet of Things (IIoT). By providing a comprehensive analysis of data security concerns in the larger context of Industry 4.0, the paper seeks to close the gaps in the body of existing products. Properly addressing data security issues is critical to the success of Industry 4.0. Striking a balance between innovation and strong cybersecurity measures is essential for businesses in this transition phase to continue to grow and prosper. To ensure a secure and profitable technological future, ongoing research, interdisciplinary collaboration, and a commitment to cybersecurity education will take precedence.

G. References

[1] Xu, X., Lu, Y., Vogel-Heuser, B., & Wang, L. (2021). Industry 4.0 and Industry 5.0—Inception, conception and perception. Journal of Manufacturing Systems, 61, 530-535.

[2] Dalenogare, L. S., Benitez, G. B., Ayala, N. F., & Frank, A. G. (2018). The expected contribution of Industry 4.0 technologies for industrial performance. International Journal of production economics, 204, 383-394.

[3] Strazzullo, S., Cricelli, L., Grimaldi, M., & Ferruzzi, G. (2022). Connecting the path between open innovation and industry 4.0: a review of the literature. IEEE Transactions on Engineering Management.

[4] Husain, B. H., & Askar, S. (2021). Survey on edge computing security. International Journal of Science and Business, 5(3), 52-60.

[5] Ijaz Ahmad, Felipe Rodriguez, Tanesh Kumar, et al. Communications Security in Industry X: A Survey. TechRxiv. February 23, 2023. DOI: 10.36227/techrxiv. 22128380.v1

[6] Oztemel, E., & Gursev, S. (2020). Literature review of Industry 4.0 and related technologies. Journal of intelligent manufacturing, 31, 127-182.

[7] Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. Procedia manufacturing, 13, 1253-1260.

[8] Ibrahim, M. A., & Askar, S. (2023). An Intelligent Scheduling Strategy in Fog Computing System Based on Multi-Objective Deep Reinforcement Learning Algorithm. IEEE Access, 11, 133607-133622.

[9] Askar, S. (2021). Blockchain For Securing IoT Devices: A Review. Available at SSRN 3962701.

[10] El Hamdi, S., Abouabdellah, A., & Oudani, M. (2019, June). Industry 4.0: Fundamentals and main challenges. In 2019 International Colloquium on Logistics and Supply Chain Management (LOGISTIQUA) (pp. 1-5). IEEE.

[11] Peres, R. S., Jia, X., Lee, J., Sun, K., Colombo, A. W., & Barata, J. (2020). Industrial artificial intelligence in industry 4.0-systematic review, challenges and outlook. IEEE Access, 8, 220121-220139.

[12] Furstenau, L. B., Sott, M. K., Kipper, L. M., Machado, E. L., Lopez-Robles, J. R., Dohan, M. S., ... & Imran, M. A. (2020). Link between sustainability and industry 4.0: trends, challenges and new perspectives. Ieee Access, 8, 140079-140096.

[13] Alani, M. M., & Alloghani, M. (2019). Security challenges in the industry 4.0 era. Industry 4.0 and engineering for a sustainable future, 117-136.

[14] Mohammed, C. M., & Askar, S. (2021). Machine learning for IoT healthcare applications: a review. International Journal of Science and Business, 5(3), 42-51.
[15] Aceto, G., Persico, V., & Pescapé, A. (2020). Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. Journal of Industrial Information Integration, 18, 100129.
[16] Prinsloo, J., Sinha, S., & von Solms, B. (2019). A review of industry 4.0 manufacturing process security risks. Applied Sciences, 9(23), 5105.
[17] Humayun, M. (2021). Industry 4.0 and cyber security issues and challenges. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 2957-2971.
[18] Eyeleko, A. H., & Feng, T. (2023). A Critical Overview of Industrial Internet of Things Security and Privacy Issues Using a Layer-Based Hacking Scenario. IEEE Internet of Things Journal.
[19] Ghadge, A., Er Kara, M., Moradlou, H., & Goswami, M. (2020). The impact of Industry 4.0 implementation on supply chains. Journal of Manufacturing Technology Management, 31(4), 669-686.
[20] Prause, M. (2019). Challenges of industry 4.0 technology adoption for SMEs: the case of Japan. Sustainability, 11(20), 5807.
[21] Hankel, M., & Rexroth, B. The reference architectural model Industrie 4.0 (rami 4.0). ZVEI (2015). URL: https://przemysl-40. pl/wp-content/uploads/2010-The-Reference-Architectural-Model-Industrie-40. pdf.
[22] Delsing, J. (2017). Local cloud internet of things automation: Technology and business model features of distributed internet of things automation solutions. IEEE Industrial Electronics Magazine, 11(4), 8-21.
[23] Manogaran, G., Thota, C., Lopez, D., & Sundarasekar, R. (2017). Big data security intelligence for healthcare industry 4.0. Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing, 103-126.
[24] Moustafa, N., Adi, E., Turnbull, B., & Hu, J. (2018). A new threat intelligence scheme for safeguarding industry 4.0 systems. IEEE Access, 6, 32910-32924.
[25] Kharchenko, V., Dotsenko, S., Illiashenko, O., & Kamenskyi, S. (2019, June). Integrated cyber safety & security management system: industry 4.0 issue. In 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 197-201). IEEE.
[26] Jiang, X., Pang, Z., Luvisotto, M., Pan, F., Candell, R., & Fischione, C. (2019). Using a large data set to improve industrial wireless communications: Latency, reliability, and security. IEEE Industrial Electronics Magazine, 13(1), 6-12.
[27] Svaigen, A. R., Boukerche, A., Ruiz, L. B., & Loureiro, A. A. (2023). Security in the Industrial Internet of Drones. IEEE Internet of Things Magazine, 6(3), 110-116.
[28] Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 cybersecurity challenges. IEEE Engineering Management Review, 47(3), 79-86.
[29] İlhan, İ., & Karaköse, M. (2019, September). Requirement analysis for cybersecurity solutions in industry 4.0 platforms. In 2019 International Artificial Intelligence and Data Processing Symposium (IDAP) (pp. 1-7). IEEE.

[30] Mantravadi, S., Schnyder, R., Møller, C., & Brunoe, T. D. (2020). Securing IT/OT links for low power IIoT devices: design considerations for industry 4.0. IEEE Access, 8, 200305-200321.

[31] Nagorny, K., Scholze, S., Colombo, A. W., & Oliveira, J. B. (2020). A DIN Spec 91345 RAMI 4.0 compliant data pipelining model: An approach to support data understanding and data acquisition in smart manufacturing environments. IEEE Access, 8, 223114-223129.

[32] Dalzochio, J., Kunst, R., Pignaton, E., Binotto, A., Sanyal, S., Favilla, J., & Barbosa, J. (2020). Machine learning and reasoning for predictive maintenance in Industry 4.0: Current status and challenges. Computers in Industry, 123, 103298.

[33] Liu, X. L., Wang, W. M., Guo, H., Barenji, A. V., Li, Z., & Huang, G. Q. (2020). Industrial blockchain based framework for product lifecycle management in industry 4.0. Robotics and computer-integrated manufacturing, 63, 101897.

[34] Rahman, Z., Khalil, I., Yi, X., & Atiquzzaman, M. (2021). Blockchain-based security framework for a critical industry 4.0 cyber-physical system. IEEE Communications Magazine, 59(5), 128-134.

[35] Hosseini, A. M., Sauter, T., & Kastner, W. (2021, June). Towards adding safety and security properties to the Industry 4.0 Asset Administration Shell. In 2021 17th IEEE International Conference on Factory Communication Systems (WFCS) (pp. 41-44). IEEE.

[36] Laghari, S. U. A., Manickam, S., Al-Ani, A. K., Rehman, S. U., & Karuppayah, S. (2021). SECS/GEMsec: A mechanism for detection and prevention of cyber-attacks on SECS/GEM communications in industry 4.0 landscape. IEEE Access, 9, 154380-154394.

[37] Rambabu, S., Rao, N. T., Ramakotaiah, M., Raju, J. S., & Venumurali, J. (2021). Security Vulnerabilities Affecting on Addititve Manufacturing Systems in the Era of Industry 4.0: An Extensive Review. 2021 Emerging Trends in Industry 4.0 (ETI 4.0), 1-5.

[38] Golec, M., Gill, S. S., Bahsoon, R., & Rana, O. (2020). BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and industry 4.0. IEEE Consumer Electronics Magazine, 11(2), 51-56.

[39] Rahman, A., Hasan, K., & Jeong, S. H. (2022, October). An Enhanced Security Architecture for Industry 4.0 Applications based on Software-Defined Networking. In 2022 13th International Conference on Information and Communication Technology Convergence (ICTC) (pp. 2127-2130). IEEE.

[40] Singh, G., Bhardwaj, G., Singh, S. V., & Chaudhary, N. (2022, February). Artificial intelligence led Industry 4.0 application for sustainable development. In 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM) (Vol. 2, pp. 339-343). IEEE.

[41] Gao, J., Zhang, B., Guo, X., Baker, T., Li, M., & Liu, Z. (2022). Secure partial aggregation: Making federated learning more robust for industry 4.0 applications. IEEE Transactions on Industrial Informatics, 18(9), 6340-6348.

[42] Sauter, T., & Treytl, A. (2023). IoT-Enabled Sensors in Automation Systems and Their Security Challenges. IEEE Sensors Letters, 7(12), 1-4.

[43] Hammad, M., Badshah, A., Abbas, G., Alasmary, H., Waqas, M., & Khan, W. A. (2023). A provable secure and efficient authentication framework for smart manufacturing industry. IEEE Access.
[44] Kurdistan Ali & Shavan Askar, 2021. "Security Issues and Vulnerability of IoT Devices," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 101-115.
[45] Kosrat Dlshad Ahmed & Shavan Askar, 2021. "Deep Learning Models for Cyber Security in IoT Networks: A Review," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 61-70.
[46] Omar Shirko; Shavan Askar , "A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking" IEEE Access, Volume 11, 2023.
[47] D. H. Abdulazeez and S. K. Askar, "A Novel Offloading Mechanism Leveraging Fuzzy Logic and Deep Reinforcement Learning to Improve IoT Application Performance in a Three-Layer Architecture Within the Fog-Cloud Environment," in IEEE Access, vol. 12, pp. 39936-39952, 2024,
[48] Zhala Jameel Hamad & Shavan Askar, 2021. "Machine Learning Powered IoT for Smart Applications," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 92-100.
[49] Shavan Askar & Kurdistan Ali & Tarik A. Rashid, 2021. "Fog Computing Based IoT System: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 183-196.
[50] D. H. Abdulazeez and S. K. Askar, "A Novel Offloading Mechanism Leveraging Fuzzy Logic and Deep Reinforcement Learning to Improve IoT Application Performance in a Three-Layer Architecture Within the Fog-Cloud Environment," in IEEE Access, vol. 12, pp. 39936-39952, 2024.