sensors

MDPI

Review

A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead

Vítor Pedreira [1], Daniel Barros [1] and Pedro Pinto [1,2,3,*]

[1] Instituto Politécnico de Viana do Castelo, 4900-347 Viana do Castelo, Portugal; vitorpedreira@ipvc.pt (V.P.); danielbarros@ipvc.pt (D.B.)
[2] Universidade da Maia, 4475-690 Maia, Portugal
[3] INESC TEC, 4200-465 Porto, Portugal
* Correspondence: pedropinto@estg.ipvc.pt

Abstract: The concepts brought by Industry 4.0 have been explored and gradually applied.The cybersecurity impacts on the progress of Industry 4.0 implementations and their interactions with other technologies require constant surveillance, and it is important to forecast cybersecurity-related challenges and trends to prevent and mitigate these impacts. The contributions of this paper are as follows: (1) it presents the results of a systematic review of industry 4.0 regarding attacks, vulnerabilities and defense strategies, (2) it details and classifies the attacks, vulnerabilities and defenses mechanisms, and (3) it presents a discussion of recent challenges and trends regarding cybersecurity-related areas for Industry 4.0. From the systematic review, regarding the attacks, the results show that most attacks are carried out on the network layer, where Denial of Service (DoS)-related and Man in the Middle (MITM) attacks are the most prevalent ones. Regarding vulnerabilities, security flaws in services and source code, and incorrect validations in authentication procedures are highlighted. These are vulnerabilities that can be exploited by DoS attacks and buffer overflows in industrial devices and networks. Regarding defense strategies, Blockchain is presented as one of the most relevant technologies under study in terms of defense mechanisms, thanks to its ability to be used in a variety of solutions, from Intrusion Detection Systems to the prevention of Distributed DoS attacks, and most defense strategies are presented as an after-attack solution or prevention, in the sense that the defense mechanisms are only placed or thought, only after the harm has been done, and not as a mitigation strategy to prevent the cyberattack. Concerning challenges and trends, the review shows that digital sovereignty, cyber sovereignty, and data sovereignty are recent topics being explored by researchers within the Industry 4.0 scope, and GAIA-X and International Data Spaces are recent initiatives regarding data sovereignty. A discussion of trends is provided, and future challenges are pointed out.

Keywords: cybersecurity; attacks; defenses; industry 4.0; vulnerabilities; survey; data sovereignty

Citation: Pedreira, V.; Barros, D.; Pinto, P. A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. *Sensors* **2021**, *21*, 5189. https://doi.org/10.3390/s21155189

Academic Editor: Rodrigo Román-Castro

Received: 22 June 2021
Accepted: 26 July 2021
Published: 30 July 2021

1. Introduction

Industry 4.0, or the fourth industrial revolution, advocates the automation of traditional practices of manufacturing and industrialization [1], with the use of smart technologies allowing machine-to-machine communication [2]. This concept of industry assumes machine-to-machine and human-to-machine communications, using the latest methods, techniques and tools, intended to transform digitally the industries manufacturing, production, and value creation processes.

Recent technologies have been integrated within Industry 4.0 implementations, bringing new challenges in the cybersecurity area [3]. Recent Industry 4.0 implementations include technologies such as cloud computing, Artificial Intelligence (AI), Cyber Physical Systems (CPSs) or Internet of Things (IoT). Industrial Internet of Things (IIoT) devices [4], IoT devices intended for industrial use, are typically small-sized, low-cost, efficient, capable of having sensors or actuators [5], but featuring low computing power micro-controllers [6].

A cluster of these devices can control entire manufacturing processes with great efficiency, making them useful in large manufacturing companies.

With the increase of devices connected to Industry 4.0-enabled networks, the surface of attack also expands. Malicious actors may find in any smart device an open door to exploit new vulnerabilities and perform attacks on them or on their infrastructure, with the intent of impacting financially a company or industry [7]. When compromised, these devices can cause serious damage to material goods, such as products on a manufacturing line, or immaterial goods, such as the leakage of sensitive information or industrial secrets. Several attacks have targeted industrial facilities and their devices, from the Stuxnet [8] in 2010, to the Trojan BlackEnergy [9] in 2015 and Mirai in 2016 [10], to recent ransomware attacks, such as the WannaCry [11] in 2017 or the LockerGoga [12] in 2019, resulting in operational and financial impact for affected companies. Thus, it is relevant to constantly monitor cybersecurity risks, the impact of attacks and the state of defense mechanisms in Industry 4.0 implementations [13]. A round of efforts, such as the one described in [14], are focused on good practices and prevention to keep Industry 4.0 implementations and Information Technology (IT) systems secure, while ensuring their normal operation and maintenance.

The contributions of this paper can be divided into three. First, a general systematic review of current cybersecurity attacks, vulnerabilities and defenses in Industry 4.0 and 5.0 scenarios is presented. Second, a detailed analysis and categorization regarding attacks, vulnerabilities and defenses of selected studies is presented. Third, a discussion is presented of recent challenges and trends regarding these areas on Industry 4.0 and Cybersecurity. This review is divided into three steps: (1) General Review, (2) Abstracts Review, and (3) Selected Papers Review.

This systematic review allows the identification of the most common attacks, vulnerabilities, and defense strategies. Additionally, a set of challenges and trends regarding Industry 4.0 are highlighted as an effort to enhance the detection and prediction of new vulnerabilities or zero-day attacks, and creating the necessary defense mechanisms to protect industry data. Digital, Cyber and Data Sovereignty concepts are discussed since challenges emerge regarding data sharing and ownership, and recent initiatives such as International Data Spaces (IDS) [15] and GAIA-X [16] are promoting data exchange, with the objective of ensuring data security and sovereignty.

The remainder of this document is organized as follows: Section 2 introduces the methodology used for the systematic review; Section 3 presents the results for the General Review; Section 4 presents the results for the Abstracts Review; Section 5 reviews the selected studies; Section 6 draws a discussion relative to the results obtained; lastly, in Section 7 conclusions are made.

2. Review Methodology

This review around the cybersecurity-related topics in Industry 4.0 intends to overview types of attacks, vulnerabilities and defense strategies. Additionally, this study aims to identify whether topics such as data sovereignty, digital sovereignty and cyber sovereignty are current trends for cybersecurity in the context of Industry 4.0, due to the appearance of the IDS and GAIA-X. Thus, a general systematic review was carried out, inspired by the methodology in [17], adapted for the current study context.

For the current study, we assume that the published paper progress over time (from 2014 to 2021) can be a possible approach to overview the cybersecurity-related topics and infer current trends and challenges. Thus, the following Research Questions (RQ) were formulated:

- RQ1 —What is the progress of the cybersecurity area for Industry 4.0, in number of papers related to vulnerabilities, defense and attacks topics?
- RQ2—What is the progress, in number of papers for the intersections of the topics of vulnerabilities, attacks and defense mechanisms for Industry 4.0?
- RQ3—What is the progress of the number of papers for challenges and trends related to data sovereignty, digital sovereignty and cyber sovereignty areas for Industry 4.0?

After defining the research questions, search engines were chosen. For this study, we selected the ACM Digital Library, Scopus and IEEExplore databases to receive the queries as input and to provide quantitative results of the number of papers.

The keywords used to perform the search queries were defined to include the results of Industry 4.0 and Industry 5.0 and to gather all recent matches regarding attacks, vulnerabilities, defenses, and sovereignty-related terms. The primary and secondary keywords used are presented in Table 1. The keywords were used in search queries, where the primary keywords were searched for in the abstract of the paper and the secondary keywords were searched for in the all the metadata of the paper. The search queries used for the three databases can be found in [18].

Table 1. Defined Keywords.

Primary Keywords	Secondary Keywords
Industry 4.0	Attack
Industry 5.0	Vulnerabilities
	Defense
	Data Sovereignty
	Digital Sovereignty
	Cyber Sovereignty

In Figure 1 the adopted systematic review process with the number of papers obtained in each stage is shown.

After the first search queries 1640 papers were selected, and duplicates were removed. For the remaining 855 papers, the StArt tool [19], a support tool for systematic reviews, was used. All 855 papers were imported and classified with a score assigned as follows: 20 points for each time one of the keywords appears in the title, 10 points for each time one of the keywords appears in the abstract and 5 points for each time one of the keywords appears in the full text. The application of the score resulted in a paper scores ranging from 0 to 260. Then, a set of exclusion criteria was used as presented in Table 2. The application of this criteria, which included the exclusion of all papers scoring under 100, resulted in the exclusion of 746 papers. The abstracts of the remaining 109 papers were evaluated and processed, and led to the exclusion 78 papers that were considered to be not relevant to this study. In the last step, the full texts of 31 papers were analyzed, in which 9 were discarded, 2 of them for being paid-for, for which reading was prevented. Thus, 22 papers were selected for a detailed review and categorization.

Table 2. Exclusion criteria.

(1) Papers that are not in English
(2) Papers with a score of less than 100
(3) Papers considered not relevant for this study
(4) Papers that required a special license to access their content

A detailed review was performed in three colored steps in Figure 1 as follows: general review, review of abstracts, and review of selected papers. The results of these detailed reviews are presented in the following sections.

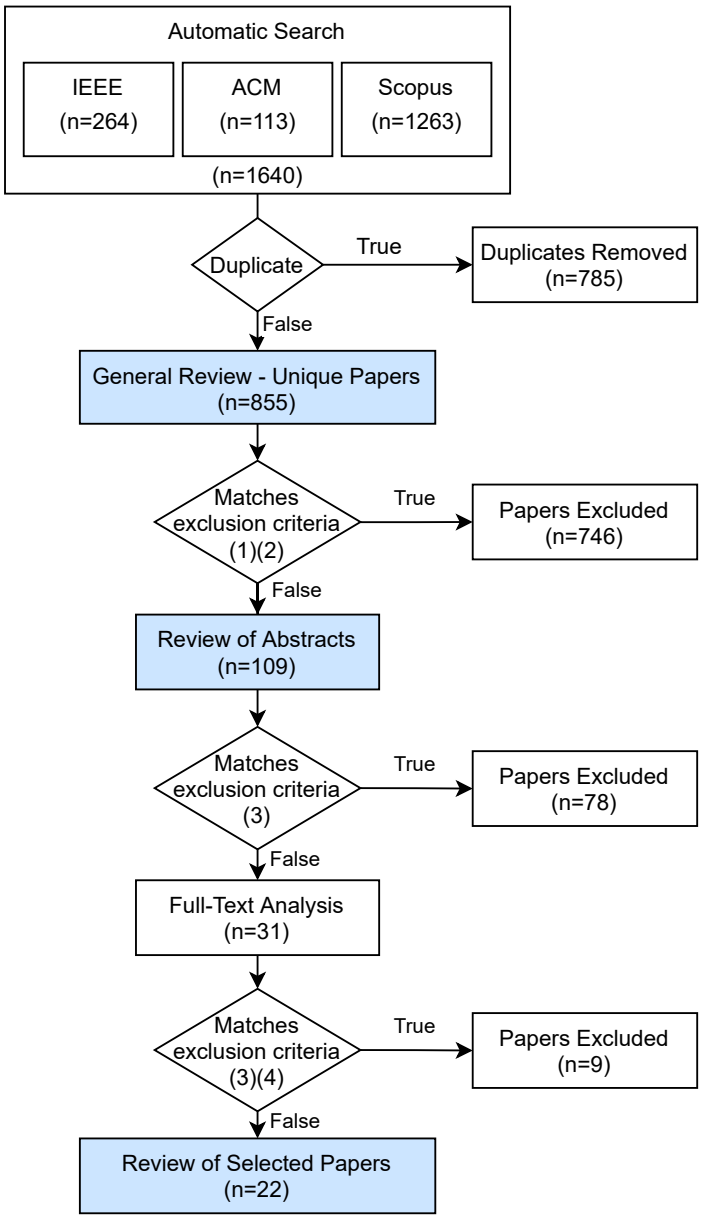

Figure 1. Systematic Review Methodology.

3. General Review

In this section, the results of the general review of search queries performed are presented. The number of papers referring to vulnerabilities, defenses, attacks, or the intersection of these three main topics is presented.

Figure 2 presents the number of papers for each year, with respect to security vulnerabilities, attacks and defenses strategies. In 2021, the current year, the number of papers was projected based on the temporal behavior of the types of papers. From the numbers obtained, it can be verified that:

- from 2014 to 2015 the number of papers regarding vulnerabilities where none;
- from 2014 to 2015 only one paper was published regarding defense strategies or mechanisms;
- the number of papers regarding attacks was constant until 2015, when it increased until now;
- papers about defense had a strong increase in number, per year, from all subjects analyzed, but the forecast for 2021 is to maintain, approximately, the previous year's number;

- the subject of attack presented the greatest number of papers, with 97 papers in 2020, and an estimate of 111 papers for 2021;
- the number of papers addressing vulnerabilities, despite growing over the years, has reduced compared to other subjects;
- the biggest year of growth in papers published was 2019, with a median factor of 2.3 times.

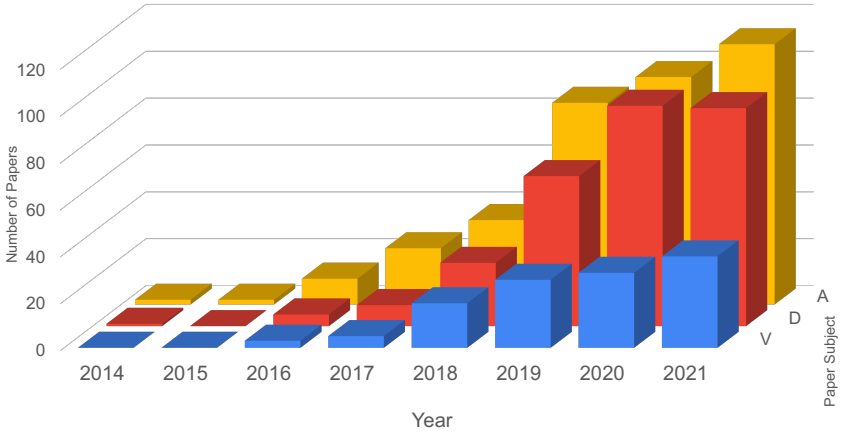

Figure 2. General Review—number of papers focusing on vulnerabilities, attacks and defenses.

Figure 3 displays the number of papers found per year, regarding vulnerabilities and defenses, attacks, and regarding the intersection of these three main topics, Vulnerabilities and Defenses (V&D), Defenses and Attacks (D&A), and Vulnerabilities and Attacks (V&A). From the results obtained, it can be verified that:

- the number of papers addressing attacks is the largest, followed by the number of papers including defense mechanisms.
- the number of papers talking about attacks has been growing significantly
- the number of papers talking about vulnerabilities has grown over the years, despite being small, compared to attacks and defenses
- the number of papers for both topics is twenty five (35) from 2014 to 2016.
- between 2017 and 2021 it is possible to identify that the number of papers increase, for all topics, except for the topic of V&D, in which there is a small increase.

Since the queries were extended to included recent areas and possible trends, the results of search queries including data, digital and cyber sovereignty were processed and analyzed. These results are presented in Figure 4. From these results, it can be verified that:

- from 2014 to 2017 for the categories of data, digital and cyber sovereignty, no papers were found.
- in 2018, the number of papers found was only 1 for the category of cyber sovereignty, which did not have papers found again until 2021 (projection).
- in 2019, no papers were found for the three categories.
- for digital sovereignty papers were found only in 2020.
- for data sovereignty, from 2014 to 2019 the number of papers is zero, but an increase is seen in 2020 and 2021 (projection).

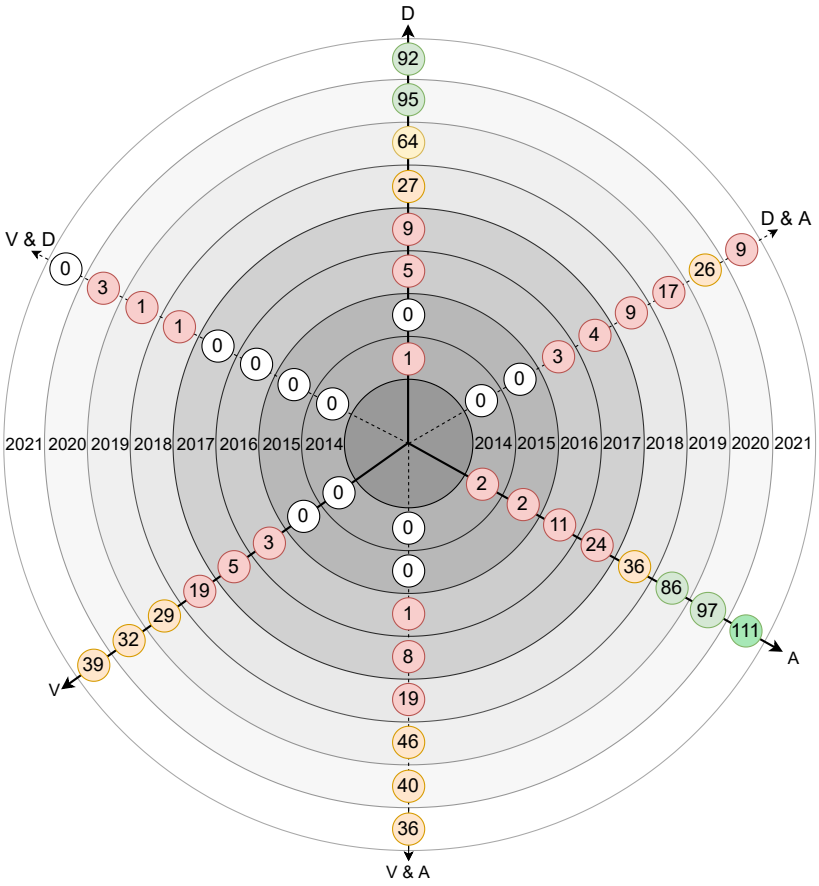

Figure 3. Number of attacks, vulnerabilities and defenses-related papers on multiple axis per year.

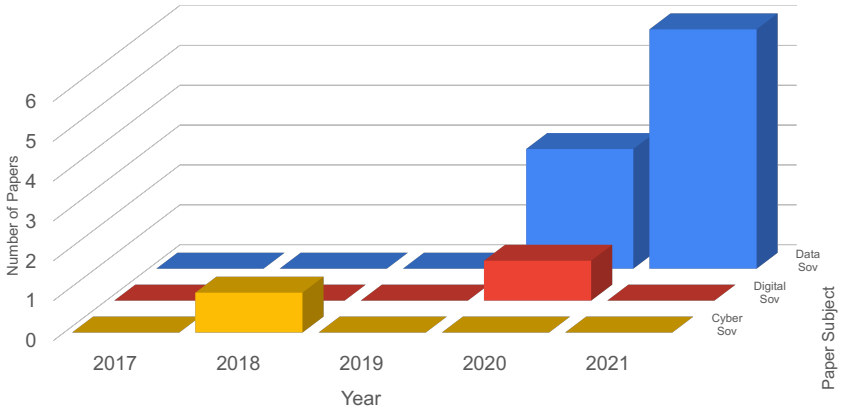

Figure 4. Data sovereignty, digital sovereignty and cyber sovereignty papers results.

From the 11 papers referring to data, digital or cyber sovereignty, two of them focus on particular initiatives, namely the GAIA-X and the IDS. In [20] the authors claim that a war for industrial data is starting, Europe is the main battleground, and future platforms need to be built to harness data as close as possible to its production location. To this end, they refer that the GAIA-X, a project initiative launched by the European Union to develop a data infrastructure and data-related service providers for Europe, which intends to tackle this challenge by meeting the highest standards in terms of digital sovereignty and aiming to foster innovation. Data and services are envisioned to be available, grouped and shared in a trusted environment. This paper also refers to the IDS initiative, created by the International Data Spaces Association (IDSA), which consists of a global reference architecture standard, to create and operate virtual data spaces. This architecture is based

on commonly recognized data governance models that facilitate the secure exchange and easy linkage of data within business ecosystems. IDS pretends to respond to GAIA-X challenges and, in this article, the functioning of its architecture and interconnections are explained. In Ref. [21], the authors also focus their research work around IDS described as a virtual data space that uses common standards and governance models to facilitate the secure exchange and easy linkage of data across business ecosystems. It provides a foundation for the creation and use of intelligent services and innovative business processes, while ensuring the digital sovereignty of data owners.

Given all the results regarding the General Review, the research questions formulated can be answered as follows:

- RQ1 — What is the progress of the cybersecurity area for Industry 4.0, in number of papers, relative to vulnerabilities, defense and attacks topics?

  Answer — The results obtained show that the number of papers for the three topics (Vulnerabilities, Attacks and Defenses) have increase from 2014 to 2020. In the current year of 2021, the projection is that the number will be greater for Attacks and Vulnerabilities topics, and the projection for the Defense topic is to be similar to the last year.
- RQ2 — What is the progress, in number of papers for the intersections of the topics of vulnerabilities, attacks and defense mechanisms for Industry 4.0?

  Answer — Regarding the intersection topics, a strong increase of papers was verified regarding V&A, followed by D&A, and, with a slight increase, the V&D.
- RQ3 — What is the progress of the number of papers for challenges and trends related to data sovereignty, digital sovereignty and cyber sovereignty areas for Industry 4.0?

  Answer — With the results obtained, it is concluded that digital, cyber and data sovereignty are relatively recent topics that presumably will grow over the years, particularly data sovereignty. Additionally, GAIA-X and IDS are initiatives taking shape and intend to tackle the data sovereignty-related challenges.

4. Review of Abstracts

In this section, a review of the abstracts is presented. The papers with a score greater than or equal to 100 were selected and examined.

Figure 5 presents the number of papers per year, out of 109, regarding security vulnerabilities, attacks and defense keywords.

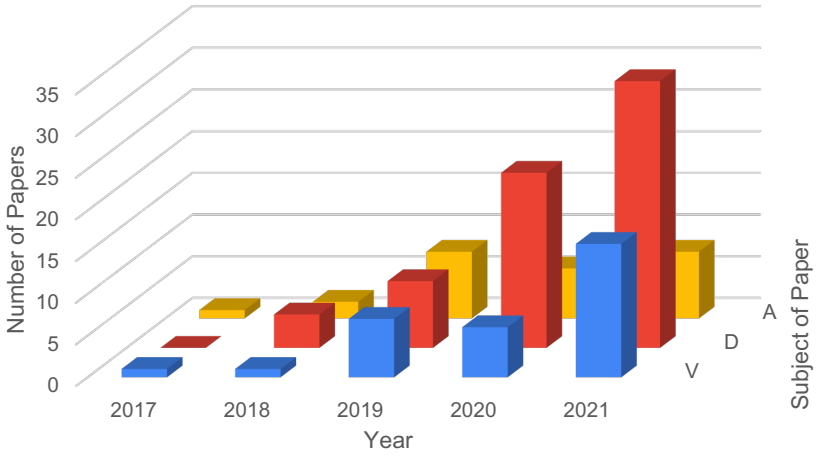

Figure 5. Review of Abstracts—number of papers focusing on vulnerabilities, attacks and defenses.

Figure 6 shows the number of papers found per year, with a score equal to or greater than 100, on vulnerabilities and defenses, attacks and on the intersection of these three main topics, Vulnerabilities and Defenses (V&D), Defenses and Attacks (D&A) and Vulnerabilities and Attacks (V&A). From the results, it can be verified that:

- the number of papers referring to defense mechanisms has grown in recent years, and reaches 24 for 2021 (forecast).
- there are no papers matching V&D in any of the years in review.
- between 2014 and 2016, no papers were found.
- between 2017 and 2021, the number of papers increases for all topics, with the exception of V&D, which remains null.

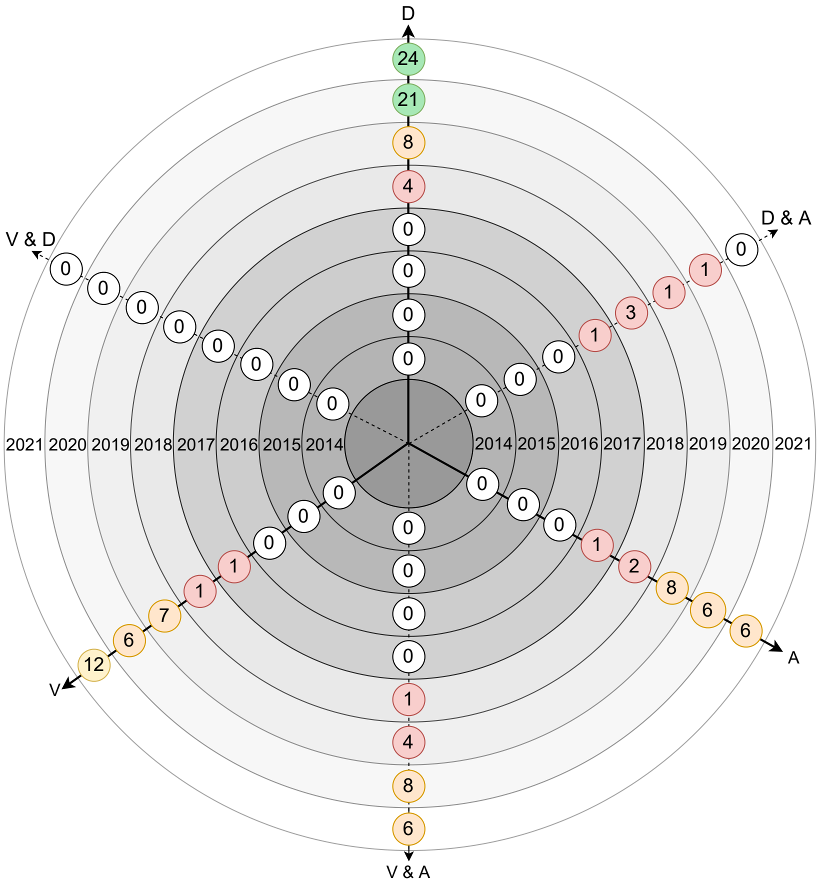

Figure 6. Number of attacks, vulnerabilities and defenses-related papers on multiple axis per year.

In Table 3 papers are categorized according to their score and regarding the occurrence of the Attacks, Defenses, Vulnerabilities keywords. From the results, it can be verified that:

- there are no papers that address vulnerabilities and defenses simultaneously
- the largest group of papers have scores from 100 to 130
- the highest-scoring papers match the three topics: attacks, defenses and vulnerabilities and addresses a risk-assessment of cyber-attacks and defense strategies for Industry 4.0. This paper also reviews the most common cybersecurity vulnerabilities and defense strategies regarding Industry 4.0, in corporate and end-user dimensions.

Table 3. Paper Score and Categorization for the Review of Abstracts.

Score	Papers	Attacks	Defenses	Vulnerabilities
100–130	[22–35]			•
	[36–57]		•	
	[58–68]	•		
	[69–78]	•		•
	[79–83]	•	•	
	[83–88]	•	•	•
131–160	[89,90]			•
	[89–98]		•	
	[99–102]	•		
	[69,103–107]	•		•
	[108]	•	•	•
161–190	[109]			•
	[93,93,110–115]		•	
	[103,116,117]	•		
	[118,119]	•	•	
	[120]	•	•	•
191–220	[121,122]			•
	[123]	•		
	[124]	•		•
221–250	[125–128]		•	
251–260	[129]	•	•	•

5. Review of Selected Studies

In this section, a more specific analysis is performed regarding the 22 papers selected after the full text analysis step of the systematic review. In Figure 7 the number of papers for each year regarding the three main topics is presented: vulnerabilities, attacks and defenses. The results for 2021 are projected based on the numbers to date.

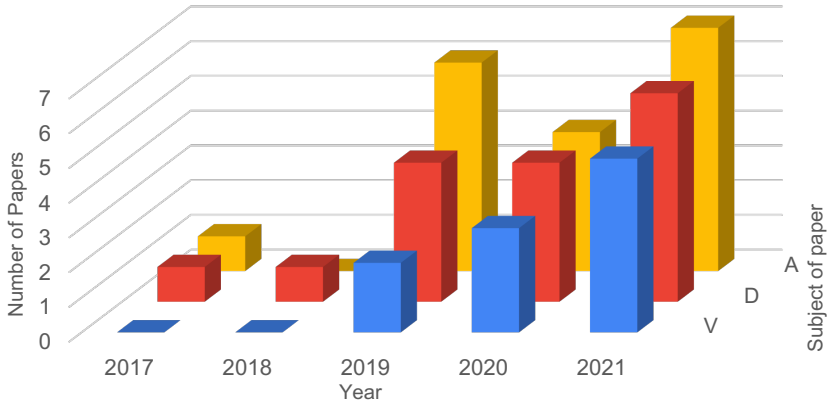

Figure 7. Review of Selected studies—number of papers focusing on vulnerabilities, attacks and defenses.

A finer analysis regarding the three main topics was performed and, following a similar approach of the previous works in [63,72], a set of categories were defined to fit the results for the selected studies as follows.

5.1. Attacks

In this section, 14 relevant papers were found. As shown in Table 4, the attacks studied were grouped in 6 categories: Network, Web Application, System, Devices, Malware, and Social Engineering attacks.

Table 4. Attacks.

Attack Type	Description	Paper
Network	An attack intended to access or map a network to cripple its performance or obtain sensitive information.	[31,62,64,76,103,105] [63,75,85,107,129]
Malware	Malicious software created to attack and exploit systems.	[63,76,85,103,107,108,129]
Web Application	Attacks on web services and applications in order to access sensitive data.	[25,76,85]
System	Attacks on control systems and other manufacturing control related devices.	[31,63,72,75]
Devices	Attacks exploiting software and/or firmware of IoT devices.	[25,63,75]
Social Engineering	Physiological manipulation of a victim with the intent of obtaining sensitive information.	[31,107,129]

- **Network**
  Network attacks are commonly designed to impact a network's performance. To impact the performance, a malicious actor can perform a DoS [31,63,64,76] attack. This attack consists of generating huge amounts of bogus traffic towards a network with the intent of denying the service to the real users. Distributed Denial of Service (DDoS) is a variation of the previous attack, and is the use of a Botnet, also called zombies, which are computers under control of the hacker (e.g., Mirai IoT Botnet [76]) to augment the attack efficiency, using the zombies to generate bigger amounts of traffic directed towards the target, with higher possibilities of rendering it ineffective [62,75,85,103,105,107,129]. Jamming [75] is an attack intended to disrupt network availability. MITM [64,75,85], replay attack [75,108], selective forwarding attack [75], and sybil attack [63,75,85] are all attacks performed on networks, the first, MITM, is the interception of communications by an unintended user. The intercepted traffic can be used to perform other attacks or can be used for gathering sensitive data. Replay attack, also known as playback attack, is an attack in which the traffic gathered by the hacker is repeated maliciously. A Sybil attack consists of multiple fake identities being used to generate additional node identities capable of receiving and forwarding data from and to the victim.
- **Malware**
  Malware is intended to cause damage, steal or modify information in a target computer. This type of attack can be presented in many shapes or forms, such as a virus [103,129], which is a stealth piece of code made to be executed on a victim computer, replicate

and propagate into other victims. Worms [63,75,103,129] are also malicious code made to propagate in a network or through emails with the intent of gaining access to the victim computer. Trojan horses [103,129] are another type of malware, designed not to be suspicious when executing, generally disguised as legitimate software. One type of malware that distinguishes itself from the others is ransomware [63,76,107,129]. Ransomware is made to hijack the victim computer, encrypting all the data on the hard drive and requesting a ransom for the decryption of the computer data.

- **Web Application**
  To access sensitive data, web application attacks can lead to compromises in a company's network. Metadata spoofing and Structured Query Language (SQL) Injection are types of attacks that threaten security in IIoT. Metadata spoofing is when an attacker modifies a database and causes its integrity to be compromised [76]. When the attackers use SQL commands to steal contents within a database, taking advantage of SQL injection vulnerabilities, some attacks may occur, such as remote command execution, information disclosure, and authentication bypass [76].
- **System**
  Attacks targeting the Industrial Control Systems (ICSs) have increased by 110% since 2016 [75]. For Industry 4.0 systems, the Stuxnet virus [63,75] was detected as a more visible security incident that exploited vulnerabilities in Supervisory Control and Data Acquisitions (SCADAs) [31,72]. Other attacks such as false logic, zero-day and deception attack can target the ICS. False logic attack is one attack that could affect SCADA systems to disrupt control [75]. Zero-day attacks are when a vulnerability is discovered by a hacker and not publicly disclosed, and this type of attack can sabotage SCADA and power transmission systems [75]. Deception attacks affecting SCADA and Distributed Control System (DCS) are where the hacker makes the worker accept as true an incorrect scenario to degrade system performance [75].
- **Devices**
  Devices for Industry 4.0, such as sensors, robots and industrial machines, can be attacked by various types of attacks. Physics, measurement injection, side channel and time delay are the most common attacks. Physical attack is when an untrusted worker gains physical access and makes unwanted modifications to devices. Measurement injection is when false data are injected into the sensors. In a side-channel attack, the attacker can gather sensitive information from the device by measuring side-channel information. A time delay attack can disturb the stability of all the industrial control system, by adding extra time delays into measurements and control commands [75].
- **Social Engineering**
  An attacker using social engineering often uses his abilities to convince the user [72,129]. In Ref. [107], the German Steel Mill Cyberattack is detailed. The attackers used a spear-phishing attack which consisted of sending a targeted email from an apparently trusted source to prompt the target to open an illicit attachment or visit a malicious website, where malware is downloaded to their computer to access the corporate network. Another type of social engineering is the phishing attack, different from spear-phishing attack by not having a specific target but a group of targets. The phishing method spoofs the sites of publicly known and trusted organizations and institutions, and allows users to log into these fake websites [129], stealing their credentials.

5.2. Vulnerabilities

Regarding vulnerabilities, seven (7) relevant papers were found. The vulnerabilities studied were divided into 4 categories Web Application, Devices, Network, and Authentication, as presented in Table 5.

Table 5. Vulnerabilities.

Vulnerability Type	Description	Paper
Web Application	Flaws in web services and applications that can compromise sensitive data and service availability	[25,85,104,105]
Devices	Flaws in source code, capable of allowing unwanted access	[62,85,105]
Network	Flaws capable of enabling network attacks or leaks of sensitive information.	[63,75]
Authentication	Incorrect validation of user credentials	[25]

- **Web Application**
  Vulnerabilities related to web services and applications are usually associated with coding errors that enable destructive or non-destructive attacks. Vulnerabilities that allow malicious users to execute unwanted scripts [25], such as Insecure Deserialization, XML External Entities (XXE), Cross-site Request Forgery (CSRF), Cross-site Scripting (XSS) and SQL Injection in a web application are the most common. Insecure Deserialization occurs when user-controllable data are deserialized by a website, allowing attackers to manipulate serialized objects to pass harmful data to the application code. XXE is a vulnerability that allows an attacker to interfere with an application's XML data processing, enabling him to view files on the application server's file system and interact with any back-end or external systems that the application itself can access. CSRF is a web security vulnerability that allows an attacker to trick users into taking actions they do not intend to take. XSS is a vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application, in which malicious scripts are injected into sites that are not marked as trusted. SQL Injection is a vulnerability that allows an attacker to interfere with the queries an application makes to your database.
- **Devices**
  With regards to IIoT devices, such as Programmable Logic Controller (PLC), cameras, smart-routers, smart-meters from various vendors, vulnerabilities were found in the software and firmware of the devices. These are Buffer Overflow, Infinite Loop, Use After Free (UAF), Heap Overflow and DDoS vulnerabilities [105]. Buffer overflow happens when a program or process attempts to write more data to a fixed-length block of memory, or buffer, than the buffer is designed to hold. Infinite Loop happens when an iteration or loop implemented in the program cannot reach the exit condition. If an attacker can manipulate the loop, it could allow him to force the device to consume excessive resources, e.g., CPU and RAM. UAF vulnerability is related to incorrect use of the dynamic memory, the program does not clear the pointer to the freed memory location, enabling the attacker to cause an error on the program. Heap Overflow is a type of buffer overflow vulnerability, but this one happens on the heap data area. Vulnerabilities such as password leakage and password hash cracking are also vulnerabilities that attack IIoT devices [76]. Backdoors are also found on these devices, in which they are classified as a special vulnerable point in software or firmware analysis, which is different from traditional vulnerabilities or bugs in control-flow types [105].
- **Network**
  Network vulnerabilities are directly related to attacks to devices and services [72]. According to the authors in [71], Industry 4.0 has created new scenarios of cyber-threats designed for classic IT. To cope with this problem the authors address the

security issues related to covert channels applied to industrial networks, identifying vulnerability points when classic IT converges with operational technologies such as edge computing infrastructures. The authors define the strategy of attack starting by exploiting the Transmission Control Protocol (TCP) protocol to set up a covert channel and then proceeding to more active and offensive methods to exploit a real industrial IoT test bed.

- **Authentication**
  According to [25] improper authentication allows malicious users to access sensitive data through dictionary, birthday and brute force attacks focused on in [75,76]. Dictionary attacks are only possible due to the improper setup of authentication, allowing attackers to perform countless login tries with every word from a word list. Birthday attack comes from the birthday paradox, where it was used to create password hash collision. Brute force is an attack of trial and error, where attacker use every available resource to guess login credentials and encryption keys, among others.

5.3. Defenses

Regarding defense mechanisms, 8 relevant papers were found. The defense mechanisms studied were divided into the following 6 categories, Application, Devices, Network, Social Engineering, Policy, and System, as shown in Table 6.

Table 6. Defenses.

Defense	Description	Paper
Application	Mechanisms that enable secure processing in applications.	[38,62–64,103,119]
Devices	Mechanisms that enable device security.	[62,86,105,130]
Network	Strategies or software designed to maintain network security and efficiency	[62,64,108]
Social Engineering	Promote training and awareness	[62,129]
Policy	Established rules used in a procedure, protocol or standard	[31,63]
System	Technologies used in order to ensure security in systems	[63,103]

- **Application**—Application defense can be seen as developing custom defense mechanisms to improve overall safety of a product. Various methods can be selected to achieve a certain desired result. The authors in [83] propose a defense mechanism against timing-based side-channel attacks to response time on the Internet of Things. This mechanism follows two modules, vulnerability testing and privacy protection. The result of this proposal, in an experimental scenario, shows that the mechanism created is capable of precisely identify the side-channel leakages related to response time and efficiently mask them. In [119] the authors propose a Mixture-Hidden Markov Mechanism (MHMM) for designing threat intelligence that is capable of monitoring and recognizing cyber-attacks for Industry 4.0 systems. The mechanism developed showed the capability of completely discovering physical and network attacks using physical power systems and UNSW-NB15 datasets [131]. In terms of performance, the mechanism outnumbered five different peer techniques in terms of detection rates, false positives and processing times. This paper presents a useful mechanism to be deployed in any Industry 4.0 scenario to assess cybersecurity threats. In study [38], a framework is proposed, which consists of a Blockchain-based model distributed

through an SDN-IoT-enabled architecture to ensure adequate security, which is the main concern in Industry 4.0. With Blockchain integration, the authors ensure that all data are safe for Industry 4.0 applications.

- **Devices**—All devices and software used in organizations should be configured safely, and controlled changes should be ensured [62]. In Ref. [105], the authors present a framework for analyzing and discovering vulnerabilities in IoT and Industry 4.0, called *VulHunter*, which aims to discover unknown vulnerabilities in the analysis based on the patch of known vulnerabilities. To secure network devices, the authors in [62] address systems that perform identity checks and data packets, which can be used against attacks on routing tables. In Ref. [86] the authors present the framework IIoT-SIDefender, to measure security of sensitive information leakage and leverage in every layer of IIoT devices. The results of the framework demonstrate that the leakage points of sensitive information can be detected, and attacks can also be defended with real-time hot fixes generated to prevent such attacks. In Ref. [130] AI is seen as a means of threat detection in devices and the combination of attack surface reduction, secure development life cycle, data protection, secure and hardened device hardware and firmware, and machine learning may be critical in moving forward with a secure, vigilant and resilient Industry 4.0-enabled devices.
- **Network**—Traffic between networks with different security levels should be restricted and monitored [62]. With the aim of ensuring communications between industry 4.0 supply chain partners, the authors in [64] propose an efficient Transport Layer Security (TLS)-based authentication mechanism that is resistant to MITM attacks for web applications that use the TLS protocol to protect HTTP communications. The proposed mechanism prevents the attacker from impersonating the legitimate server for the user to guarantee confidentiality. The authors in [87] aim to identify and map potential vulnerable endpoints in an industrial paradigm and propose a robust way of securing a wireless sensor network, ensuring the integrity and authenticity of data acquisitions. During the case study, the authors identify technologies used in the Industry 4.0, and their respective security mechanisms, possible attacks, solutions and vulnerable points, one being on Data Acquisition (DAQ) devices, and on the Communication Layer between DAQ and the cloud. In Ref. [108], the authors propose a defense framework based on Software Defined Network (SDN) that consists of a model for traffic management and anomaly detection. Based on this framework, the authors studied the use of this methodology for IoT networks and for SCADA systems [84], in which it allowed the extraction of traffic patterns to detect and prevent various network attacks such as Address Resolution Protocol (ARP) spoofing, replay attacks and detect malicious command forwarding behaviors.
- **Social Engineering**—Defense strategies for social engineering can include collaborators training to recognize sensitive information requests (phone numbers, emails, etc.) or a redirection to false web sites that intend to capture this data outside the scope of the corporation. For the authors in [129], the use of *Truecaller* or *Dialer* Software is seen as a method of defense against phishing attacks. According to [62], emails, attachments, and links that appear suspicious should be used with caution or avoided; these links should be double-checked and/or typed directly into the browser, to reduce the risk of attack.
- **Policy**—In Ref. [129], authors state that institutions that intend to implement Industry 4.0 architectures must determine first the information security policies, taking advantage of the ISO/IEC 27001 [132] and ISO/IEC 27002 [133] standards. Privacy, integrity and accessibility topics, such as access controls, backups, use of cryptographic controls, human resources security and software installation restrictions should also be included, and inventory of hardware and software assets and security vulnerability management [62,129] must also be taken into account.
- **System**—According to [63], Blockchain technology that uses hash and cryptography algorithms can also be used as a solution against various attacks on IIoT systems, such

as injection attacks and malware attacks, guaranteeing confidentiality and integrity for databases and Blockchain. In Ref. [103], the authors also use Blockchain, taking into account that it is decentralized and resistant to cyber hacks and can also be incorporated with the smart contract system to increase operational security in the battery's energy storage systems against cyber-attacks.

6. Discussion and Future Challenges

As a result of the systematic review, it is possible to identify the most common types of attacks, vulnerabilities and defense mechanisms for Industry 4.0, and check their progress in recent years. The main highlights that can be drawn from the results are that:

- Regarding attacks: the number of papers was constant until 2015, and has been growing significantly since. Papers addressing attacks are the highest in number, followed by the number of papers including defense mechanisms;
- Regarding defenses: the number of papers had the highest increase in number, per year, from all subjects analyzed, but the forecast for 2021 is to maintain, approximately, the previous year's number.
- Regarding vulnerabilities: the number of papers addressing vulnerabilities, despite growing over the years, has reduced compared to attack and defenses topics.
- Regarding the correlation between topics (attacks, defenses and vulnerabilities), between 2017 and 2021 it is possible to identify that for all topics, the number of papers had a strong increase, except for the topic of V&D, which had a small increase.

Regarding selected studies on attacks categorized in Table 4, it can be concluded that the largest number of attacks for Industry 4.0 can occur as network attacks, in which it can be identified that DoS, DDoS and MITM are the most common attacks to be taken into account. It is also identified that attacks have been increasing over the years since 2017.

Regarding selected studies on vulnerabilities categorized in Table 5, it is possible to conclude that with the advancement of technology, the number of threats has increased. The most relevant vulnerabilities were identified in the *Device* categories and in the *Networks* category. Buffer overflows, DDoS vulnerabilities and backdoors are the most common vulnerabilities found in devices, and network vulnerabilities are directly related to attacks on devices and services.

Regarding selected studies on defenses categorized in Table 6, it can be concluded that defense mechanisms tend to evolve in the face of attacks that respond to them. Blockchain was one of the most relevant technologies studied, to guarantee the security of some attacks. Cryptography mechanisms were also addressed in this study as being an effective method, e.g., for MITM attacks.

From the results obtained regarding data sovereignty, digital sovereignty and cyber sovereignty, it can be concluded that these areas are very recent. The terms "digital sovereignty" and "cyber sovereignty" were less recurrent and, on the other hand, the term "data sovereignty" seems to be a trend for cybersecurity in the context of Industry 4.0. These concepts, focused on secure sharing and owning data, are being addressed and the research work in this area seems to be growing (by the progress of the published papers), while recent initiatives such as IDS and GAIA-X are also being promoted. Thus, the following set of future challenges for corporations and industries can be depicted:

- Enable intra-exchange and inter-exchange of industrial data, taking into account the full value of exchanged data;
- Enable secure data exchange within particular corporation scopes and time frames, while maintaining the control on the data providers;
- Exercise control of data over devices and the Internet, taking into account industrial spaces and borders;
- Massive data sharing within sectors or groups of companies;
- Allow secure data ownership transfer between sectors or groups of companies;
- Perform real-time analysis of massively generated data;
- Enforce personal data privacy mechanisms when sharing data between companies;

- Enable sharing of secure and trusted data based on standards;
- Share information in an environment of trust between producers and consumers;
- Allow interoperability for business ecosystems;
- Enable data sharing between companies to enhance corporation sustainability;
- Enforce self-determined control of data use (data sovereignty) while offering new "smart services" and innovative business processes across companies and industries.

7. Conclusions

Security incidents may impact industries that are progressing and deploying Industry 4.0 concepts and, since recent technologies such as AI or IoT are being included in Industry 4.0, the progress of these implementations requires constant surveillance regarding cybersecurity. At the same time, it is also important to forecast cybersecurity-related challenges and trends to better build and adapt these implementations to possible future attacks and their impacts.

This paper reviews recent research efforts on attacks, vulnerabilities, and defenses in Industry 4.0 implementations, and highlights security-related topics and challenges that seem to be surging in this area. The contributions of this paper can be divided in the following: (1) it presents a systematic survey based on a general and abstract analysis, (2) it analyzes in detail and categorizes selected studies on attacks, vulnerabilities and defenses mechanisms, and (3) it provides a discussion on recent challenges and trends regarding these areas on Industry 4.0.

From the systematic review results we concluded that attacks, defenses and vulnerabilities in Industry 4.0 implementations are increasing and capturing researcher attention. When categorizing selected studies, we concluded that the greatest number of attacks are network-based attacks, such as DoS and MITM attacks, exploiting vulnerabilities in Industry 4.0 networks and devices. Additionally, it is highlighted that topics related to digital sovereignty and mainly data sovereignty appear to be a trend in this area, and IDS and GAIA-X are recent initiatives intended to face the challenges related to the data sovereignty topic.

Author Contributions: Investigation, V.P., D.B. and P.P.; Formal analysis, V.P.; Methodology, P.P.; Writing—original draft, V.P. and D.B.; Writing—review & editing, V.P., D.B. and P.P.; Supervision, P.P.; Project Administration, P.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by European Regional Development Fund (ERDF) through the COMPETE2020 Programme, within the STVgoDigital project (POCI-01-0247-FEDER-046086).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. De Melo, P.F.S.; Godoy, E.P. Controller Interface for Industry 4.0 based on RAMI 4.0 and OPC UA. In Proceedings of the 2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0 IoT), Naples, Italy, 4–6 June 2019; pp. 229–234. [CrossRef]
2. D'Aloia, M.; Longo, A.; Guadagno, G.; Pulpito, M.; Fornarelli, P.; Laera, P.N.; Manni, D.; Rizzi, M. Low Cost IoT Sensor System for Real-time Remote Monitoring. In Proceedings of the 2020 IEEE International Workshop on Metrology for Industry 4.0 IoT, Rome, Italy, 3–5 June 2020; pp. 576–580. [CrossRef]
3. Pan, J.; Yang, Z. Cybersecurity Challenges and Opportunities in the New "Edge Computing + IoT" World. In Proceedings of the SDN-NFV Sec'18: 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, Tempe, AZ, USA, 21 March 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 29–32. [CrossRef]
4. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
5. Schütze, A.; Helwig, N.; Schneider, T. Sensors 4.0—Smart sensors and measurement technology enable Industry 4.0. *J. Sens. Sens. Syst.* **2018**, *7*, 359–371. [CrossRef]

6. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–4. [CrossRef]
7. Radanliev, P.; De Roure, D.; Cannady, S.; Montalvo, R.M.; Nicolescu, R.; Huth, M. Economic impact of IoT cyber risk—Analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT-2018, London, UK, 28–29 March 2018; pp. 1–9. [CrossRef]
8. Langner, R. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51. [CrossRef]
9. BlackEnergy APT Attacks | What is BlackEnergy? | Threat Definition | Kaspersky. Available online: https://www.kaspersky.com/resource-center/threats/blackenergy (accessed on 22 June 2021).
10. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A.; Invernizzi, L.; Kallitsis, M.; et al. Understanding the Mirai Botnet. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 16–18 August 2017; USENIX Association: Vancouver, BC, Canada, 2017; pp. 1093–1110.
11. Mohurle, S.; Patil, M. A brief study of wannacry threat: Ransomware attack 2017. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 1938–1940.
12. Leppänen, S.; Ahmed, S.; Granqvist, R. *Cyber Security Incident Report—Norsk Hydro*; Elsevier: Amsterdam, The Netherlands, 2019.
13. Usmonov, B.; Evsutin, O.; Iskhakov, A.; Shelupanov, A.; Iskhakova, A.; Meshcheryakov, R. The cybersecurity in development of IoT embedded technologies. In Proceedings of the 2017 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2–4 November 2017; pp. 1–4. [CrossRef]
14. Cybersecurity is a Key Enabler for Industry 4.0 Adoption—ENISA. Available online: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-is-a-key-enabler-for-industry-4-0-adoption (accessed on 22 June 2021).
15. International Data Spaces | The Future of the Data Economy is Here. Available online: https://internationaldataspaces.org/ (accessed on 22 June 2021).
16. GAIA-X—Home. Available online: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html (accessed on 22 June 2021).
17. Guidelines for Performing Systematic Literature Reviews in Software Engineering. EBSE Technical Report, Number EBSE-2007-01. Available online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.471 (accessed on 22 June 2021)
18. Pedreira, V.; Barros, D.; Pinto, P. A Review on Security Vulnerabilities, Attacks and Defense Strategies in Industry 4.0 Scenarios. 2021. Available online: https://zenodo.org/record/4968365#.YQewgI4zaMo (accessed on 22 June 2021).
19. Fabbri, S.; Silva, C.; Hernandes, E.; Octaviano, F.; Di Thommazo, A.; Belgamo, A. Improvements in the StArt Tool to Better Support the Systematic Review Process. In Proceedings of the EASE '16: 20th International Conference on Evaluation and Assessment in Software Engineering, Limerick, Ireland, 1–3 June 2016.
20. Braud, A.; Fromentoux, G.; Radier, B.; Le Grand, O. The Road to European Digital Sovereignty with Gaia-X and IDSA. *IEEE Netw.* **2021**, *35*, 4–5.
21. Sang, G.; Xu, L.; De Vrieze, P.; Bai, Y.; Pan, F. Predictive Maintenance in Industry 4.0. Available online: https://dl.acm.org/doi/abs/10.1145/3447568.3448537?casa_token=N10tGNVO1pEAAAAA:6qQA8bru1RbBbdQBsviunG0FgeLKJaHo84dxQT78TL39RJ01Y-UrL7FM_iHLdiX9e-3bEOjp3N8 (accessed on 22 June 2021).
22. Sawik, T. A linear model for optimal cybersecurity investment in Industry 4.0 supply chains. *Int. J. Prod. Res.* **2020**, 1–18. [CrossRef]
23. Mora Sanchez, D.O. Corporate Social Responsibility Challenges and Risks of Industry 4.0 technologies: A review. In Proceedings of the Smart SysTech 2019, European Conference on Smart Objects, Systems and Technologies, Magdeburg, Germany, 4–5 June 2019; pp. 1–8.
24. Brocal, F.; González, C.; Komljenovic, D.; Katina, P.F.; Sebastián, M.A. Emerging risk management in industry 4.0: An approach to improve organizational and human performance in the complex systems. *Complexity* **2019**, *2019*, 2089763. [CrossRef]
25. Sołtysik-Piorunkiewicz, A.; Krysiak, M. The Cyber Threats Analysis for Web Applications Security in Industry 4.0. In *Studies in Computational Intelligence*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 887, pp. 127–141. [CrossRef]
26. An, H.; Ha, D.S.; Yi, Y. Powering next-generation industry 4.0 by a self-learning and low-power neuromorphic system. In Proceedings of the 7th ACM International Conference on Nanoscale Computing and Communication, Online, 23–25 September 2020; pp. 1–6.
27. Kumar, P.; Singh, R.K. Application of Industry 4.0 technologies for effective coordination in humanitarian supply chains: A strategic approach. *Ann. Oper. Res.* **2021**. [CrossRef]
28. Rajput, S.; Singh, S.P. Connecting circular economy and industry 4.0. *Int. J. Inf. Manag.* **2019**, *49*, 98–113. [CrossRef]
29. Türkeș, M.C.; Oncioiu, I.; Aslam, H.D.; Marin-Pantelescu, A.; Topor, D.I.; Căpușneanu, S. Drivers and barriers in using industry 4.0: A perspective of SMEs in Romania. *Processes* **2019**, *7*, 153. [CrossRef]
30. Majumdar, A.; Garg, H.; Jain, R. Managing the barriers of Industry 4.0 adoption and implementation in textile and clothing industry: Interpretive structural model and triple helix framework. *Comput. Ind.* **2021**, *125*, 103372. [CrossRef]
31. Pereira, T.; Barreto, L.; Amaral, A. Network and information security challenges within Industry 4.0 paradigm. *Procedia Manuf.* **2017**, *13*, 1253–1260. [CrossRef]
32. Koch, S.; Wunderlich, T.; Hansert, J.; Heinrich, R.; Schlegel, T. Tackling Problems on Maintenance and Evolution in Industry 4.0 Scenarios Using a Distributed Architecture. Software Engineering (Satellite Events). 2021. Available online: http://ceur-ws.org/Vol-2814/short-A5-4.pdf (accessed on 22 June 2021).

33. Marcucci, G.; Antomarioni, S.; Ciarapica, F.E.; Bevilacqua, M. The impact of Operations and IT-related Industry 4.0 key technologies on organizational resilience. *Prod. Plan. Control* **2021**, 1–15. [CrossRef]
34. Oliveira, M.; Afonso, D. Industry Focused in Data Collection: How Industry 4.0 is Handled by Big Data. In Proceedings of the DSIT 2019: 2nd International Conference on Data Science and Information Technology, Seoul, Korea, 19–21 July 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 12–18. [CrossRef]
35. Sanchez, D.O.M. Sustainable Development Challenges and Risks of Industry 4.0: A literature review. In Proceedings of the 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17–21 June 2019; pp. 1–6.
36. Sevinc, A.; Gür, Ş.; Eren, T. Analysis of the difficulties of SMEs in industry 4.0 applications by analytical hierarchy process and analytical network process. *Processes* **2018**, *6*, 264. [CrossRef]
37. Rane, S.B.; Potdar, P.R.; Rane, S. Development of Project Risk Management framework based on Industry 4.0 technologies. *Benchmarking Int. J.* **2019**. [CrossRef]
38. Rahman, A.; Sara, U.; Kundu, D.; Islam, S.; Islam, M.J.; Hasan, M.; Rahman, Z.; Nasir, M.K. DistB-SDoIndustry: Enhancing Security in Industry 4.0 Services based on Distributed Blockchain through Software Defined Networking-IoT Enabled Architecture. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*. [CrossRef]
39. Munim, K.M.; Islam, I.; Rahman, M.M.; Nazrul Islam, M. Adopting HCI and Usability for Developing Industry 4.0 Applications: A case study. In Proceedings of the 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 19–20 December 2020; pp. 1–6. [CrossRef]
40. Gashenko, I.V.; Khakhonova, N.N.; Orobinskaya, I.V.; Zima, Y.S. Competition between human and artificial intellectual capital in production and distribution in Industry 4.0. *J. Intellect. Cap.* **2020**. [CrossRef]
41. Firmino, A.S.; Perles, G.X.; Mendes, J.V.; da Silva, J.E.A.R.; Silva, D.A.L. Towards Industry 4.0: A SWOT-based analysis for companies located in the Sorocaba Metropolitan Region (São Paulo State, Brazil). *Gest ao Produç ao* **2020**, *27*. [CrossRef]
42. Emir, O.; Gergin, Z.; Üney-Yüksektepe, F.; Dündar, U.; Gençyılmaz, G.M.; Çavdarlı, A.İ. A Comparative Sectoral Analysis of Industry 4.0 Readiness Levels of Turkish SMEs. In Proceedings of the International Symposium for Production Research, Antalya, Turkey, 24–26 September 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 251–263.
43. Brezeanu, T.M.; Lazarou, E. Alignment between engineering curriculum and skills development for industry 4.0. In Proceedings of the The International Scientific Conference eLearning and Software for Education, "Carol I" National Defence University, Bucharest, Romania, 30 April–1 May 2020; Volume 2, pp. 328–334.
44. Vrchota, J.; Řehoř, P.; Maříková, M.; Pech, M. Critical Success Factors of the Project Management in Relation to Industry 4.0 for Sustainability of Projects. *Sustainability* **2021**, *13*, 281.
45. Shin, H.J.; Cho, K.W.; Oh, C.H. SVM-based dynamic reconfiguration CPS for manufacturing system in Industry 4.0. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 5795037. [CrossRef]
46. Mariani, M.; Borghi, M. Industry 4.0: A bibliometric review of its managerial intellectual structure and potential evolution in the service industries. *Technol. Forecast. Soc. Chang.* **2019**, *149*, 119752. [CrossRef]
47. Kumar, P.; Bhamu, J.; Sangwan, K.S. Analysis of Barriers to Industry 4.0 adoption in Manufacturing Organizations: An ISM Approach. *Procedia CIRP* **2021**, *98*, 85–90. [CrossRef]
48. Kipper, L.M.; Furstenau, L.B.; Hoppe, D.; Frozza, R.; Iepsen, S. Scopus scientific mapping production in industry 4.0 (2011–2018): a bibliometric analysis. *Int. J. Prod. Res.* **2020**, *58*, 1605–1627. [CrossRef]
49. Kalsoom, T.; Ramzan, N.; Ahmed, S.; Ur-Rehman, M. Advances in Sensor Technologies in the Era of Smart Factory and Industry 4.0. *Sensors* **2020**, *20*, 6783. [CrossRef]
50. Iqbal, A.; Zhao, G.; Suhaimi, H.; He, N.; Hussain, G.; Zhao, W. Readiness of subtractive and additive manufacturing and their sustainable amalgamation from the perspective of Industry 4.0: A comprehensive review. *Int. J. Adv. Manuf. Technol.* **2020**, *111*, 2475–2498. [CrossRef]
51. Glogovac, M.; Ruso, J.; Maricic, M. ISO 9004 maturity model for quality in industry 4.0. *Total Qual. Manag. Bus. Excell.* **2020**, 1–19. [CrossRef]
52. Elibal, K.; Özceylan, E. A systematic literature review for industry 4.0 maturity modeling: State-of-the-art and future challenges. *Kybernetes* **2020**. [CrossRef]
53. Chiarini, A.; Kumar, M. Lean Six Sigma and Industry 4.0 integration for Operational Excellence: Evidence from Italian manufacturing companies. *Prod. Plan. Control* **2020**, 1–18. [CrossRef]
54. Arromba, I.F.; Martin, P.S.; Cooper Ordoñez, R.; Anholon, R.; Rampasso, I.S.; Santa-Eulalia, L.A.; Martins, V.W.B.; Quelhas, O.L.G. Industry 4.0 in the product development process: Benefits, difficulties and its impact in marketing strategies and operations. *J. Bus. Ind. Mark.* **2021**, *36*, 522–534. [CrossRef]
55. Robson, P.; Costa, M. Princípios e Cenários da Indústria 4.0: Uma Revisão de Literatura; Available online: http://aprepro.org.br/conbrepro/2019/anais/arquivos/10192019_121035_5dab32ab50f71.pdf (accessed on 22 June 2021).
56. Pacaux-Lemoine, M.P.; Berdal, Q.; Guérin, C.; Rauffet, P.; Chauvin, C.; Trentesaux, D. Designing human–system cooperation in industry 4.0 with cognitive work analysis: A first evaluation. *Cogn. Technol. Work.* **2021**. [CrossRef]
57. Imran, F.; Kantola, J. Review of Industry 4.0 in the Light of Sociotechnical System Theory and Competence-Based View: A Future Research Agenda for the Evolute Approach. In *Advances in Human Factors, Business Management and Society*; Kantola, J.I., Nazir, S., Barath, T., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 118–128.
58. Xu, L.D.; Duan, L. Big data for cyber physical systems in industry 4.0: A survey. *Enterp. Inf. Syst.* **2019**, *13*, 148–169. [CrossRef]

59. Zivic, N. Distributed Ledger Technologies for Car Industry 4.0. In Proceedings of the 2020 International Conference on Computer Communication and Information Systems, Ho Chi Minh, Vietnam, 1–3 August 2020; pp. 45–51.
60. Luco, J.; Mestre, S.; Henry, L.; Tamayo, S.; Fontane, F. Industry 4.0 in SMEs: A sectorial analysis. In Proceedings of the IFIP International Conference on Advances in Production Management Systems, Austin, TX, USA, 1–5 September 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 357–365.
61. Rajput, S.; Singh, S.P. Industry 4.0 model for circular economy and cleaner production. *J. Clean. Prod.* **2020**, *277*, 123853. [CrossRef]
62. Ilhan, I.; Karakose, M. Requirement Analysis for Cybersecurity Solutions in Industry 4.0 Platforms. In Proceedings of the 2019 International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, Turkey, 21–22 September 2019; pp. 1–7. [CrossRef]
63. Elmamy, S.B.; Mrabet, H.; Gharbi, H.; Jemai, A.; Trentesaux, D. A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0. *Sustainability* **2020**, *12*, 9179. [CrossRef]
64. Esfahani, A.; Mantas, G.; Ribeiro, J.; Bastos, J.; Mumtaz, S.; Violas, M.A.; De Oliveira Duarte, A.M.; Rodriguez, J. An Efficient Web Authentication Mechanism Preventing Man-In-The-Middle Attacks in Industry 4.0 Supply Chain. *IEEE Access* **2019**, *7*, 58981–58989. [CrossRef]
65. Jaradat, O.; Sljivo, I.; Habli, I.; Hawkins, R. Challenges of safety assurance for industry 4.0. In Proceedings of the 2017 13th European Dependable Computing Conference (EDCC), Geneva, Switzerland, 4–8 September 2017; pp. 103–106.
66. Bertoncel, T.; Meško, M. Early Warning Systems in Industry 4.0: A Bibliometric and Topic Analysis. *Int. J. E Serv. Mob. Appl. (IJESMA)* **2019**, *11*, 56–70. [CrossRef]
67. Raza, S.; Faheem, M.; Guenes, M. Industrial wireless sensor and actuator networks in industry 4.0: Exploring requirements, protocols, and challenges—A MAC survey. *Int. J. Commun. Syst.* **2019**, *32*, e4074. [CrossRef]
68. Derigent, W.; Cardin, O.; Trentesaux, D. Industry 4.0: Contributions of holonic manufacturing control architectures and future challenges. *J. Intell. Manuf.* **2020**, 1–22. [CrossRef]
69. EFE, A.; Isık, A. A General View of Industry 4.0 Revolution From Cybersecurity Perspective. *Int. J. Intell. Syst. Appl. Eng.* **2020**, *8*, 11–20. [CrossRef]
70. Alladi, T.; Chamola, V.; Parizi, R.M.; Choo, K.K.R. Blockchain applications for industry 4.0 and industrial IoT: A review. *IEEE Access* **2019**, *7*, 176935–176951. [CrossRef]
71. Alcaraz, C.; Bernieri, G.; Pascucci, F.; Lopez, J.; Setola, R. Covert Channels-Based Stealth Attacks in Industry 4.0. *IEEE Syst. J.* **2019**, *13*, 3980–3988. [CrossRef]
72. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]
73. Butt, J. Exploring the interrelationship between additive manufacturing and Industry 4.0. *Designs* **2020**, *4*, 13. [CrossRef]
74. Yadav, G.; Paul, K. PatchRank: Ordering updates for SCADA systems. In Proceedings of the 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Zaragoza, Spain, 10–13 September 2019; pp. 110–117. [CrossRef]
75. Jamai, I.; Ben Azzouz, L.; Saïdane, L.A. Security issues in Industry 4.0. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 481–488. [CrossRef]
76. Borra, V.; Venkateswarlu, S. Security threats and concerns, firmware vulnerability analysis in industrial internet of things. *Int. J. Emerg. Trends Eng. Res.* **2020**, *8*, 5255–5258. [CrossRef]
77. Terziyan, V.; Gryshko, S.; Golovianko, M. Taxonomy of generative adversarial networks for digital immunity of Industry 4.0 systems. *Procedia Comput. Sci.* **2021**, *180*, 676–685. [CrossRef]
78. Fernandez-Carames, T.M.; Fraga-Lamas, P. Use Case Based Blended Teaching of IIoT Cybersecurity in the Industry 4.0 Era. *Appl. Sci.* **2020**, *10*, 5607. [CrossRef]
79. Fernandez-Carames, T.M.; Fraga-Lamas, P. A review on human-centered IoT-connected smart labels for the industry 4.0. *IEEE Access* **2018**, *6*, 25939–25957. [CrossRef]
80. Fernandez-Carames, T.M.; Fraga-Lamas, P. A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *IEEE Access* **2019**, *7*, 45201–45218. [CrossRef]
81. Bordel, B.; Alcarria, R.; Sánchez-de Rivera, D.; Robles, T. Protecting industry 4.0 systems against the malicious effects of cyber-physical attacks. In Proceedings of the International Conference on Ubiquitous Computing and Ambient Intelligence, Philadelphia, PA, USA, 7–10 November 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 161–171.
82. Faheem, M.; Shah, S.B.H.; Butt, R.A.; Raza, B.; Anwar, M.; Ashraf, M.W.; Ngadi, M.A.; Gungor, V.C. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Comput. Sci. Rev.* **2018**, *30*, 1–30. [CrossRef]
83. Prates, N.; Vergütz, A.; Macedo, R.T.; Santos, A.; Nogueira, M. A Defense Mechanism for Timing-based Side-Channel Attacks on IoT Traffic. In Proceedings of the GLOBECOM 2020–2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
84. Mullet, V.; Sondi, P.; Ramat, E. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access* **2021**, *9*, 23235–23263. [CrossRef]
85. Aydos, M.; Vural, Y.; Tekerek, A. Assessing risks and threats with layered approach to Internet of Things security. *Meas. Control* **2019**, *52*, 338–353. [CrossRef]

86. Sha, L.; Xiao, F.; Chen, W.; Sun, J. IIoT-SIDefender: Detecting and defense against the sensitive information leakage in industry IoT. *World Wide Web* **2018**, *21*, 59–88. [CrossRef]
87. Mourtzis, D.; Angelopoulos, K.; Zogopoulos, V. Mapping Vulnerabilities in the Industrial Internet of Things Landscape. *Procedia CIRP* **2019**, *84*, 265–270. [CrossRef]
88. Von Solms, S.; Marnewick, A. Towards Educational Guidelines for the Security Systems Engineer. In *Information Security Education—Towards a Cybersecure Society*; Drevin, L., Theocharidou, M., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 57–68.
89. Özdemir, V.; Hekim, N. Birth of Industry 5.0: Making Sense of Big Data with Artificial Intelligence, "The Internet of Things" and Next-Generation Technology Policy. *OMICS J. Integr. Biol.* **2018**, *22*, 65–76. [CrossRef]
90. Hoyer, C.; Gunawan, I.; Reaiche, C.H. The Implementation of Industry 4.0—A Systematic Literature Review of the Key Factors. *Syst. Res. Behav. Sci.* **2020**, *37*, 557–578. [CrossRef]
91. Bibby, L.; Dehe, B. Defining and assessing industry 4.0 maturity levels—case of the defence sector. *Prod. Plan. Control* **2018**, *29*, 1030–1043. [CrossRef]
92. Kalsoom, T.; Ramzan, N.; Ahmed, S. Societal Impact of IoT-Lead Smart Factory in the Context of Industry 4.0. In Proceedings of the 2020 International Conference on UK-China Emerging Technologies (UCET), Glasgow, UK, 20–21 August 2020; pp. 1–5. [CrossRef]
93. Hizam-Hanafiah, M.; Soomro, M.A.; Abdullah, N.L. Industry 4.0 Readiness Models: A Systematic Literature Review of Model Dimensions. *Information* **2020**, *11*, 364. [CrossRef]
94. Hizam-Hanafiah, M.; Soomro, M.A. The Situation of Technology Companies in Industry 4.0 and the Open Innovation. *J. Open Innov. Technol. Mark. Complex.* **2021**, *7*, 34. [CrossRef]
95. Garay-Rondero, C.L.; Martinez-Flores, J.L.; Smith, N.R.; Caballero Morales, S.O.; Aldrette-Malacara, A. Digital supply chain model in Industry 4.0. *J. Manuf. Technol. Manag.* **2020**, *31*, 887–933. [CrossRef]
96. Bonamigo, A.; Frech, C.G. Industry 4.0 in Services: Challenges and Opportunities for Value Co-Creation. 2020. Available online: https://www.emerald.com/insight/content/doi/10.1108/JSM-02-2020-0073/full/html (accessed on 22 June 2021). [CrossRef]
97. Büchi, G.; Cugno, M.; Castagnoli, R. Smart factory performance and Industry 4.0. *Technol. Forecast. Soc. Chang.* **2020**, *150*, 119790. [CrossRef]
98. Aydin, S.; Kutlu Gundougdu, F. Interval-Valued Spherical Fuzzy MULTIMOORA Method and Its Application to Industry 4.0. In *Decision Making with Spherical Fuzzy Sets: Theory and Applications*; Kahraman, C., Gündoğdu, F.K., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 295–322. [CrossRef]
99. Zia, N.U.; Owusu, V.K. A Viewpoint on Management Practices for Cybersecurity in Industry 4.0 Environment. Available online: https://www.proquest.com/openview/c2aec316cc585ff98a5381baa1cd126a/1?pq-origsite=gscholar&cbl=396497 (accessed on 22 June 2021). [CrossRef]
100. Xu, L.D.; Xu, E.L.; Li, L. Industry 4.0: State of the art and future trends. *Int. J. Prod. Res.* **2018**, *56*, 2941–2962. [CrossRef]
101. Bag, S.; Yadav, G.; Dhamija, P.; Kataria, K.K. Key resources for industry 4.0 adoption and its effect on sustainable production and circular economy: An empirical study. *J. Clean. Prod.* **2021**, *281*, 125233. [CrossRef]
102. Prinsloo, J.; Vosloo, J.C.; Mathews, E.H. Towards Industry 4.0: A Roadmap for the South African Heavy Industry Sector. *S. Afr. J. Ind. Eng.* **2019**, *30*, 174–186. [CrossRef]
103. Lim, C.H.; Lim, S.; How, B.S.; Ng, W.P.Q.; Ngan, S.L.; Leong, W.D.; Lam, H.L. A review of industry 4.0 revolution potential in a sustainable and renewable palm oil industry: HAZOP approach. *Renew. Sustain. Energy Rev.* **2021**, *135*, 110223. [CrossRef]
104. Riegler, M.; Sametinger, J. Multi-mode Systems for Resilient Security in Industry 4.0. *Procedia Comput. Sci.* **2021**, *180*, 301–307. [CrossRef]
105. Xiao, F.; Sha, L.T.; Yuan, Z.P.; Wang, R.C. VulHunter: A Discovery for Unknown Bugs Based on Analysis for Known Patches in Industry Internet of Things. *IEEE Trans. Emerg. Top. Comput.* **2020**, *8*, 267–279. [CrossRef]
106. Butt, J. A Strategic Roadmap for the Manufacturing Industry to Implement Industry 4.0. *Designs* **2020**, *4*, 11. [CrossRef]
107. Oueslati, N.E.; Mrabet, H.; Jemai, A.; Alhomoud, A. Comparative Study of the Common Cyber-physical Attacks in Industry 4.0. In Proceedings of the 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Gammarth, Tunisia, 20–22 December 2019; pp. 1–7. [CrossRef]
108. Najeem, J.S.; Krishnan, P. Advanced defence mechanisms for future network security using SDN. *Int. J. Recent Technol. Eng.* **2019**, *7*, 686–690.
109. Vrchota, J.; Pech, M. Readiness of Enterprises in Czech Republic to Implement Industry 4.0: Index of Industry 4.0. *Appl. Sci.* **2019**, *9*, 5405. [CrossRef]
110. Gonzalez-Prida, V.; Zamora, J.; Crespo Márquez, A.; Villar-Fidalgo, L.; De la Fuente, A.; Martínez-Galán, P.; Guillén, A. An overview on the obsolescence of physical assets for the defence facing the challenges of industry 4.0 and the new operating environments. In *Safety and Reliability—Safe Societies in a Changing World—Proceedings of the 28th International European Safety and Reliability Conference, ESREL 2018*; CRC Press/Balkema: Boca Raton, FL, USA, 2018; pp. 2959–2964. [CrossRef]
111. Yi, J.S.; Moon, S.Y. Trade Facilitation for the Products of the Industry 4.0: The case of Customs Classification of Drone. *J. Korea Trade* **2019**, *23*, 110–131. [CrossRef]
112. Sony, M.; Naik, S. Critical factors for the successful implementation of Industry 4.0: A review and future research direction. *Prod. Plan. Control* **2020**, *31*, 799–815. [CrossRef]

113. Menanno, M.; Savino, M.M.; Palmieri, A. Analysing the Determinants of Industry 4.0 Technologies in Southern Italian Industries through Structural Equation Modeling. Available online: http://www.summerschool-aidi.it/edition-2019/cms/extra/papers/531.pdf (accessed on 22 June 2021).
114. James, S.; Cervantes, A. Study of Industry 4.0 and its Impact on Lean Transformation in Aerospace Manufacturing. In Proceedings of the 15th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications, Anaheim, CA, USA, 18–21 August 2019. [CrossRef]
115. Felsberger, A.; Qaiser, F.H.; Choudhary, A.; Reiner, G. The impact of Industry 4.0 on the reconciliation of dynamic capabilities: Evidence from the European manufacturing industries. *Prod. Plan. Control* **2020**, 1–24. [CrossRef]
116. Vasin, S.; Gamidullaeva, L.; Shkarupeta, E.; Palatkin, I.; Vasina, T. Emerging Trends and Opportunities for Industry 4.0 Development in Russia. *Eur. Res. Stud. J.* **2018**, 63–76. [CrossRef]
117. Bongomin, O.; Gilibrays Ocen, G.; Oyondi Nganyi, E.; Musinguzi, A.; Omara, T. Exponential Disruptive Technologies and the Required Skills of Industry 4.0. *J. Eng.* **2020**, *2020*, 4280156. [CrossRef]
118. Petrenko, S. 1 Cyber Immunity Concept of the Industry 4.0. In *Developing a Cybersecurity Immune System for Industry 4.0*; River Publishers: Gistrup, Denmark, 2020; pp. 5–66.
119. Moustafa, N.; Adi, E.; Turnbull, B.; Hu, J. A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems. *IEEE Access* **2018**, *6*, 32910–32924. [CrossRef]
120. Mosteiro-Sanchez, A.; Barcelo, M.; Astorga, J.; Urbieta, A. Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0. *J. Manuf. Syst.* **2020**, *57*, 367–378. [CrossRef]
121. Gajdzik, B.; Grabowska, S.; Saniuk, S.; Wieczorek, T. Sustainable Development and Industry 4.0: A Bibliometric Analysis Identifying Key Scientific Problems of the Sustainable Industry 4.0. *Energies* **2020**, *13*, 4254. [CrossRef]
122. Newman, C.; Edwards, D.; Martek, I.; Lai, J.; Thwala, W.D.; Rillie, I. Industry 4.0 deployment in the construction industry: A bibliometric literature review and UK-based case study. *Smart Sustain. Built Environ.* **2020**. [CrossRef]
123. Sony, M.; Naik, S. Key ingredients for evaluating Industry 4.0 readiness for organizations: A literature review. *Benchmarking Int. J.* **2019**. [CrossRef]
124. Oztemel, E.; Gursev, S. Literature Review of Industry 4.0 and Related Technologies. 2020. Available online: https://link.springer.com/article/10.1007/s10845-018-1433-8 (accessed on 22 June 2021). [CrossRef]
125. Wibowo, E.B.; Legionosuko, T.; Mahroza, J.; Chandra Jaya, Y. Industry 4.0: Challenges and Opportunities in Competency Development for Defense Apparatus' Human Resources. *Int. J. Adv. Sci. Technol.* **2020**, *29*, 45–60.
126. Stentoft, J.; Wickstrøm, K.A.; Philipsen, K.; Haug, A. Drivers and barriers for Industry 4.0 readiness and practice: Empirical evidence from small and medium-sized manufacturers. *Prod. Plan. Control* **2021**, *32*, 811–828. [CrossRef]
127. Lin, B.; Wu, W.; Song, M. Industry 4.0: Driving factors and impacts on firm's performance: An empirical study on China's manufacturing industry. *Ann. Oper. Res.* **2019**, 1–21. [CrossRef]
128. Kumar, V.; Vrat, P.; Shankar, R. Prioritization of strategies to overcome the barriers in Industry 4.0: A hybrid MCDM approach. *Opsearch* **2021**. [CrossRef]
129. Süzen, A.A. A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. *Int. J. Comput. Netw. Inf. Secur.* **2020**, *12*, 1–12. [CrossRef]
130. Deloitte. Industry 4.0 and cybersecurity: Managing risk in an age of connected production. *Deloitte Univ. Press* **2017**, *1*, 1–22.
131. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; pp. 1–6. [CrossRef]
132. ISO—ISO/IEC 27001 — Information Security Management. Available online: https://www.iso.org/isoiec-27001-information-security.html (accessed on 22 June 2021).
133. ISO—ISO/IEC 27002:2013—Information Technology—Security Techniques—Code of Practice for Information Security Controls. Available online: https://www.iso.org/standard/54533.html (accessed on 22 June 2021).