energies

MDPI

Review

Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities—A Review

Krzysztof Wójcicki [1,*], Marta Biegańska [1], Beata Paliwoda [2] and Justyna Górna [2]

[1] Institute of Quality Science, Poznań University of Economics and Business, Al. Niepodległości 10, 61-875 Poznań, Poland; marta.bieganska@ue.poznan.pl
[2] Institute of Management, Poznań University of Economics and Business, Al. Niepodległości 10, 61-875 Poznań, Poland; beata.paliwoda@ue.poznan.pl (B.P.); justyna.gorna@ue.poznan.pl (J.G.)
* Correspondence: krzysztof.wojcicki@ue.poznan.pl

Abstract: The fourth industrial revolution taking place in the industrial sector is related to the increasing digitization and linkage of goods, products, value chains and business models. Industry 4.0 is based on the global connection of people, things and machines. By connecting devices and sensors to the internet, we are entering a new era of data analysis, connectivity and automation. This gives great opportunities for innovation and progress, previously unattainable in such a dimension. The term Internet of Things (IoT) has spread along with the vision of a world instrumented with intelligent inputs and outputs able to communicate with each other through internet data and technologies. IoT is being implemented in various areas of the modern economy, for example, healthcare, quality control, logistics, energy, agriculture and production. The Industrial Internet of Things (IIoT) blazes the trail to a better understanding of the manufacturing process, thus enabling efficient and sustainable production. The paper explains the concepts of IoT, IIoT and Industry 4.0. It highlights the accompanying opportunities, threats and challenges related to their implementation. Additionally, it presents an outline of computing architecture in IoT and related energy consumption issues. Moreover, it provides examples of application and IIoT research profiling.

Keywords: Industry 4.0; Internet of Things (IoT); IIoT; smart grid; Cloud computing; Fog computing; Edge computing; Blockchain

Citation: Wójcicki, K.; Biegańska, M.; Paliwoda, B.; Górna, J. Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities—A Review. *Energies* **2022**, *15*, 1806. https://doi.org/10.3390/en15051806

Academic Editors: Igor Kotenko and Jaume Segura-Garcia

Received: 15 December 2021
Accepted: 25 February 2022
Published: 28 February 2022

1. Introduction

One of the fundamental elements facilitating societal development and economic growth is energy. In recent years, among other things, due to development and dissemination of the Internet of Things, increasing energy consumption can be observed [1]. Technology advancements and their growing abundance lead to unavoidable energy consumption. The increasing demand for energy from industry, commercial and individual customers impacts the energy security of countries on every continent. Additionally, the implementation of United Nations Sustainable Development Goals creates possibilities for wider IoT applications and environmentally friendly solutions in the energy sector.

Deloitte Report [2] reveals that, "across the world, spending on software and hardware related to IoT is projected to grow rapidly, from USD 726 billion in 2019 to USD 1.1 trillion in 2023". According to a recent IoT industry spending report, "Asia/Pacific accounted for most of the spending on IoT in 2019, with India spending USD 20.6 billion" [2]. Furthermore, Cisco [3] predicted that "there will be 500 billion devices connected with the Internet of Things (IoT) by 2030". According to Microsoft Report [3], the growing application of IoT is being observed. In 2019, 85% of surveyed companies used IoT technology; in 2020, the rate increased to 91%, while in 2021, it was 90%. In total, 90% of these organizations lead one or more projects that have already reached the "use" stage. In 2020, it was 83%, while in 2019, it was only 74%. The highest percentage of IoT adopters was observed in Australia

(96%), Italy (95%) and US (94%). The US is leading when it comes to the percentage of projects which are in the "use" phase. It was 27% last year. The Italians are next with 26% [4]. The applications of next-generation IoT were presented by Zikria et al. [5] in their work. Authors found that IoT technology could be applied in: smart healthcare, smart cities, smart transportation, smart grid, smart industries and smart households.

Figure 1 presents the autocomplete data from search engines such as Google that contained all the useful phrases and questions people were looking for around the keyword "IoT". Analysis was carried out using "Answer the Public" search engine. Figure 1 shows the 56 most frequently asked questions related to IoT in the United States. Analysis was carried out on 30 November 2021.

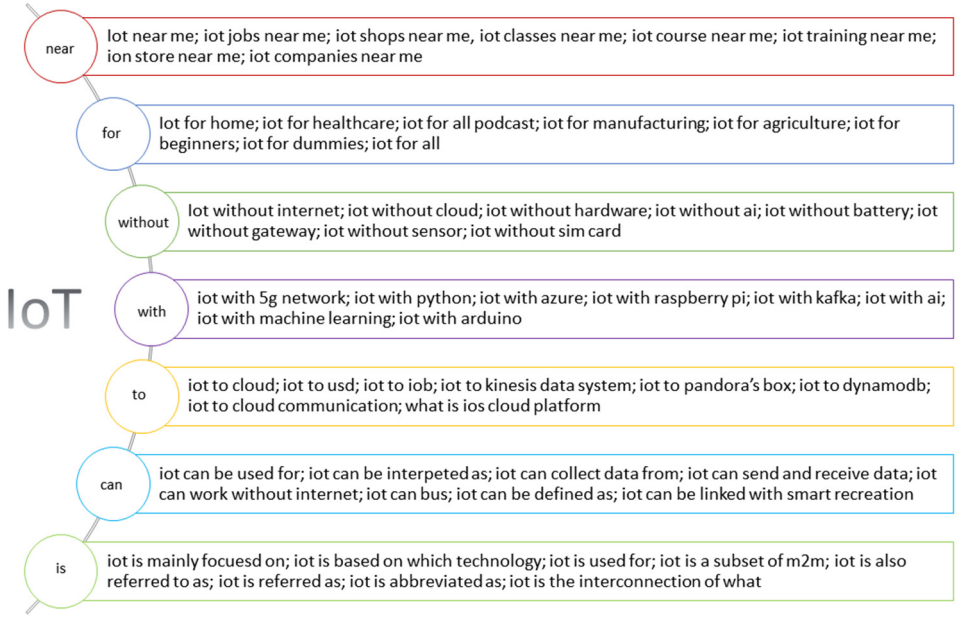

Figure 1. The 56 most frequently asked questions within the IoT in the United States, based on "Answer the Public" search engine.

For businesses around the globe, IoT has already passed the stage of being seen only as an exploratory technology [2]. The IoT provides industries with multiple opportunities, allowing initiation of unique strategies and projects to implement their concepts. Moreover, such industrial opportunities lead to "creative and effective examination possibilities for researchers and specialists in multi-disciplinary research areas, thus combining research studies, engineering abilities, sciences and humanities" [5]. The IoT transforms the world into a digital, modern and smart world where everything is readily available at hand. To catch up with the trend, industries will need to participate in ventures and invest in the IoT technologies [5]. "These new technological advancements are making it conceivable to embrace this technology worldwide, while the user's Quality of Experience (QoE) and applications' Quality of Service (QoS) prerequisites are expanding radically" [5].

The future of global manufacturing has permanently changed as a result of improvement of smart industries. The transformation has increased digitization and influenced manufacturing and distribution processes in companies. Adopting IoT appliances in factories not only influences productivity, but also has an impact on safety and quality and makes complex advancements more efficient and effective. IoT, Artificial Intelligence (AI), Cloud and Big Data Analytics (BDA) are known as "big four technologies", enabling the following: connecting organizations, generating data, implementing automation and making intelligent decisions based on facts, figures and data. IoT provides tools enabling automated data accumulation and generating insights by using sensors, networks and analytics. It is the most significant element in the "digital stack".

2. Industry 4.0

The Industry 4.0 definition refers to the fourth industrial revolution, Figure 2. Previous industrial revolutions led to increases in productivity and were driven by mechanization (first industrial revolution or industry 1.0), electricity (second industrial revolution or industry 2.0) and information technology (third industrial revolution or industry 3.0) [6,7]. Industry 4.0 refers to digital transformation [8]. It describes changes in manufacturing systems and transformation from "machine manufacturing" to "digital manufacturing", driven mainly by information technology [9].

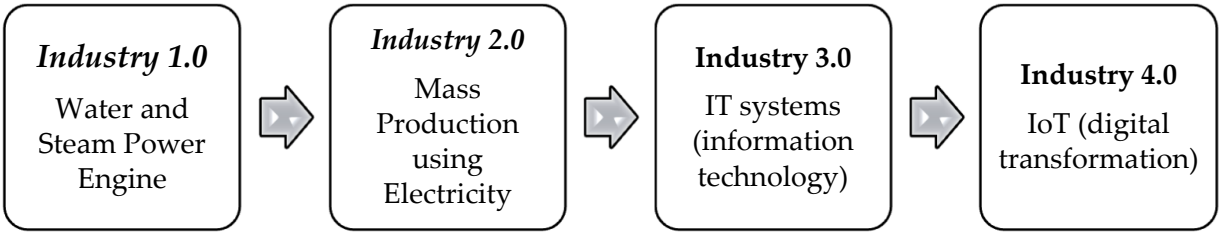

Figure 2. Four industrial revolutions.

Simultaneously with the transformation of manufacturing models, there was a transformation of the society from "Hunting society, through Agricultural society, Industrial society, Information society to Super smart society" [10], Figure 3.

Figure 3. Transformation of society.

According to Lasi et al. [9], the transformation to Industry 4.0 is driven by an enormous emphasis on applications, resulting in a tremendous need for change due to changing operational conditions and huge technological impulses (application-pull and technology-push). According to Zheng [7] the transformation to Industry 4.0 is driven by the demand for faster delivery, more effective and automated processes, better quality and customized products.

Key technologies of Industry 4.0 consist of cyber physical systems (CPS), IoT, smart factory, embedded systems, sensors, BDA, Cloud manufacturing and computing, radio frequency identification (RFID), automation, autonomous robots, additive manufacturing, virtual reality (VR), augmented reality, data mining, advanced/smart materials, AI, machine learning (ML) and cyber security [11,12].

Industry 4.0 introduces those technology pillars into core manufacturing processes, taking a significant step forward from information technology, including computerization or automation of processes that were characteristic of the third industrial revolution [13]. Although digital transformation has changed both (the software and the hardware side of organizations), not all organizations are digitally mature enough to be able to take advantage of the Industry 4.0 technologies [14,15].

The task of the fourth industrial revolution is to transform the traditional machines and equipment into smart and self-learning devices to boost their efficiency and maintenance [16]. The main goal of Industry 4.0 is the creation of collaborative, smart manufacturing platforms enabling the implementation of networked information systems [17]. "Real time data monitoring, tracking the status and positions of product as well as to hold the instructions to control production processes" are the objectives of Industry 4.0 [18,19].

3. Internet of Things (IoT)

The concept of the IoT appeared at the end of the 20th century and is gaining more and more supporters. It originated from radiofrequency technology (Massachusetts Institute of Technology, Cambridge, MA, USA, 1999) [20]. By design, IoT is to be universal and easy to use on a massive scale. As a rule (simplified to a great extent), IoT is a variety of devices with embedded systems connected to the telecommunications network—the internet. They have the ability to generate and automatically send information without direct human intervention. Their potential is almost unlimited and they are used, among others, in economy, medicine and households. IoT mainly consists of Machine-To-Machine (M2M) networks, in which intelligent devices can communicate with each other and, on the basis of generated and transmitted information, are able to make independent decisions [21–24]. These include, for example, commonly used smartphones, intelligent household appliances and electronics, heating and lighting systems that can be operated remotely using appropriate applications, but also a machine park whose devices connected to the network allow it to be managed from anywhere in the plant and/or outside of it [25–27]. There are 5 billion IoT devices worldwide and forecasts show that this will reach 29 billion by 2022 [24] or 9.27 billion according to Matsumoto et al. [28].

Different smart technologies such as sensors, actuators and intelligent systems can be integrated and enable digitalization of organizations and even industries, providing a novel paradigm in business operations. This is supported by development of information systems such as Cloud computing technologies that provide borderless sharing and access to information. The amount of data generated from IoT is enormous and allows organizations to conduct efficient analysis [23,29,30]. It plays a significant role not only in a digitalized and connected society, but also in industry, healthcare, transportation, etc., and the economy as a whole [31]. From small companies to enterprises, all seek huge data storage capacity with efficient scalability. This can be achieved by switching to Cloud, Fog and Edge paradigms [32]. Computing architecture of these paradigms is presented in Figure 4.

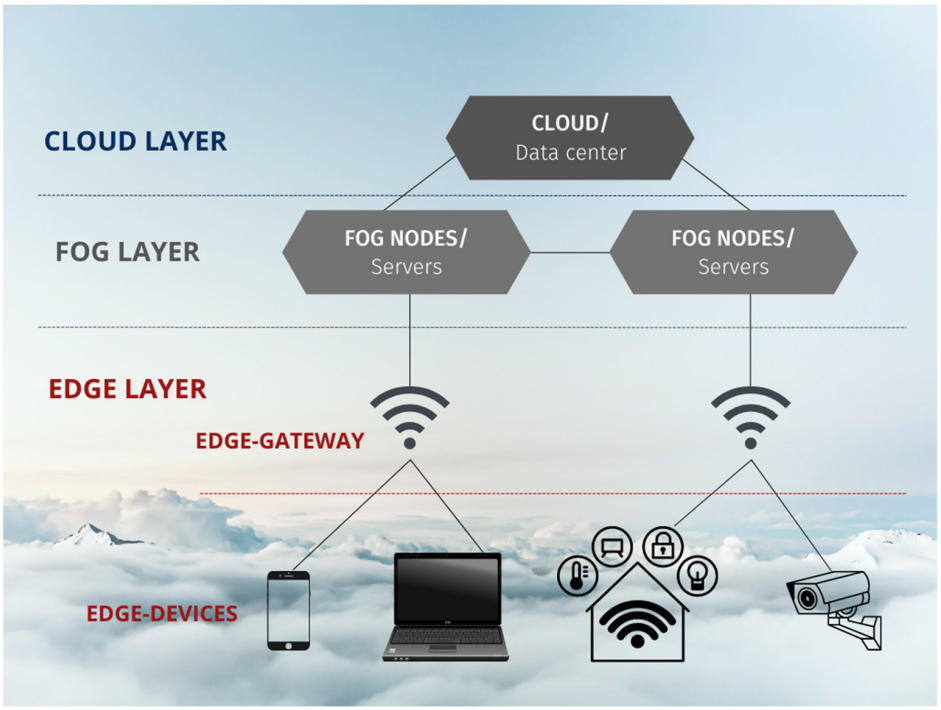

Figure 4. Computing architecture.

Internet of Things through the application of different sensors and actuators generates petabytes (PB) of data streamed to the Cloud service for maintaining and computing [33]. As shown in the above figure, Cloud is a data center or server that can be accessed from

anywhere in the world via the internet such as Microsoft Azure, Google Cloud Platform, Amazon Web Services, IBM Watson Cloud or ORACLE Cloud. The Cloud provides low-cost, scalable storage and processing capabilities. The term Cloud computing, defined by the National Institute of Standards and Technology (NIST), describes it as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [34]. However, this paradigm has its limitations as the data within the Cloud infrastructure needs to be provided to the servers for processing and then must be sent back to the device. This in turn drastically increases latency [35]. Moreover, Cloud computing offers a centralized architecture that results in bandwidth limitations [33,36,37].

The second tier of computing architecture is the Fog computing. It is as an extension of a Cloud. It employs nodes (e.g., base stations, access points, switches, routers, gateways) located between the Cloud and Edge tiers [35,36,38]. Thus, it performs low-latency computation on the IoT data, routing it to the Cloud for extensive data aggregation [39]. The OpenFog defines Fog as a "horizontal, system-level architecture that distributes computing, storage, control, and networking functions closer to the users along a Cloud-to-thing continuum" [32,40]. The Fog typically is located close to the nodes on the local network and offers decentralized architecture in Cloud computing. It serves the same purposes as the Cloud, but allows for transferring to it only the data for permanent storage, thus reducing the bandwidth [33].

The third and bottom layer of the described architecture is Edge computing. Like Fog computing, it offers distributed architecture, low latency and bandwidth, but high scalability. It uses shared computing and processes information at the Edge gateway to the device level, in turn enabling the reduction of the amount of data required to be moved to the Cloud. In other words, Edge computing uses Edge devices as tools for moving the computing power and intelligence of an Edge gateway. Its aim is to offload computational capabilities from the Cloud to the Edge [35].

Both Fog and Edge computing can operate together with the Cloud, providing better latency, data reliability and security and better response times. Stream data processing can successfully be performed by distributed Fog and Edge nodes. Whereas, big data (batch data) would typically be processed in the Cloud.

Edge and Cloud systems can be integrated together as the IoT-to-cloud continuum. The communication within the described architecture should use standard communication protocols such as Open Platform Communications United Architecture (OPC UA). It is used for industrial automation in machine-to-machine (M2M) communication [41]. Other connectivity standards are, for example, Highway Addressable Remote Transducer Protocol (HART), WirelessHart and Data-Distribution Service (DSS) [37]. Cabrini et al. [42] investigated a Helix Multilayered platform offering an Industrial IoT service platform extending the horizontal digital continuum towards Fog and Edge layer based on open standards. They were able to route "context information through the near edge and the city's cloud datacenter".

The vast amount of data generated in IoT and transferred to the Cloud requires data management solutions such as Big Data Analytics (BDA). BDA processing tools can support or in some cases enable real-time problem solving and enhance decision making, thus creating a competitive advantage for organizations in constantly changing business environments [23,29,30]. On the other hand, IoT solutions require specific databases to support data management; NoSQL is an example of such a database. For instance, Google has developed the Google IoT framework services, allowing for easy and secure data management from devices located globally in real time. Whereas a General Electric framework PREDIX aids in functioning (operation, deployment, development) of industrial applications in the Cloud and at the Edge [30].

One potential concern in wide implementation of IoT is security of information. Blockchain technology combined with IoT can overcome this issue. Such a combination

of technologies can enable a wide range of applications that would increase value chain transparency and support Business-To-Business (B2B) trust. A Blockchain is a digital, decentralized and distributed data structure (also known as ledger) where data/transactions are logged and added chronologically, and shared in a Peer-To-Peer (P2P) network providing permanent and tamperproof records [24,30,43]. Blockchain allows for vast amounts of IoT-generated data to be aggregated in a centralized or decentralized manner. This influences the scalability of IoT solutions.

Decentralized Blockchain consists of multiple users sharing decision making, whereas the centralized one has one central entity as the primary decision-maker. This technology was first introduced by Bitcoin cryptocurrency applications, but it can well be employed in different industries. Each transaction, file or data (block) has a cryptographic hash and is linked to a previous block. Once a block is verified by a certain number of network members (nodes), it is then added to previous blocks and forms a Blockchain. It usually comprises a shared ledger, permissioning, smart contracts and consensus [30]. This technology increases the transparency, security, authenticity and auditability of data shared [44,45]. Blockchain technology provides privacy protection by encrypting and verifying the data. To overcome block creation time shortfall of Blockchain, Ethereum became useful. It is slightly different from Bitcoin; however, it enables developers to write smart contracts for Blockchain platforms. Due to which, it is possible to customize Blockchain towards desired applications. In other words, Ethereum makes possible the configuration of IoT devices and authentication of operations management in public key infrastructure. Today, Blockchain technology is slowly entering non-currency domain usage [25].

4. Industrial Internet of Things (IIoT)

4.1. Research Profiling

The purpose of a systematic literature review is to gain an understanding of the existing research and share the results of other studies relevant to a particular topic or area of study. The most universal method for finding the relevant literature is keyword searches. A graphic visualization using VOSviewer software (Leiden University, Leiden, The Netherlands) showing co-occurrence networks is presented in Figure 5.

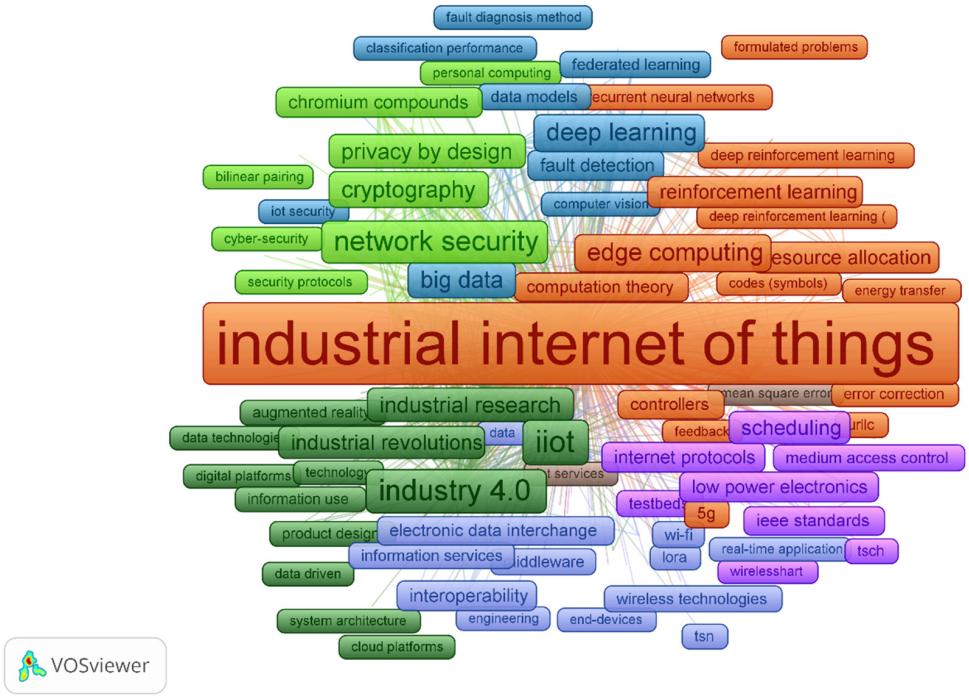

Figure 5. Network resulting from the Scopus bibliometric data analysis. Source: own work based on obtained Scopus metadata [46].

The research profiling was conducted in Scopus database (www.scopus.com; accessed on 16 October 2021) according to "Article title, Abstract, Keywords" in October 2021. No temporal restriction was chosen [47]. The choice of Scopus was based on the knowledge that it is more comprehensive than Web of Science, which encloses only International Scientific Indexing (ISI) journals [48]. The selected keyword, which was "IIoT" allowed us to find 3815 papers from 2010 to 2021, as seen in Figure 5. The metadata of the papers were then exported in a CSV format to gather necessary data for further analysis. VOSviewer software was used for bibliometric analysis at the macro-level [49]. As shown in Figure 5, it enabled structuring and visualization of the co-occurrence networks based on the most important terms extracted from the metadata. In our analysis, we have set a threshold of minimum number of occurrences of the IIoT keyword to 5. This allowed the retrieving of 1053 keywords meeting this threshold of the total 14,444 keywords. Then, for each of the 1053 keywords, the total strength of the co-occurrence links with other keywords was calculated. The keywords with the greatest total link strength were selected. The obtained results from the sample with the keyword Industrial Internet of Things (IIoT) had 1811 occurrences and IIoT had 295 and Industrial Internet of things had 277. Their total link strength was 15,350, 2586 and 2946, respectively. With the least occurrences equal to 5 were such keywords as: public works, process industries, power plants, practical swarm optimization and diverse applications. These also had the lowest total link strength, amounting to 41.

With the help of VOSviewer software, a two-dimensional map was created (Figure 5). In this co-occurrence network, keywords with high relevance are automatically grouped together into clusters with different colors and sizes of nodes for better data visualization. The relationships between each node are shown as curved lines [50]. Analysis of the terms in each of the eight obtained clusters allowed for subject area recognition as shown in Table 1. In some clusters, more than one subject area was referred to.

Table 1. Cluster analysis based on Scopus bibliometric analysis [46].

Cluster No.	Color	Item No.	Proposed Subject Area
1	Brick red	222	Software engineering, System engineering
2	Green	211	Industry 4.0
3	Turquoise	168	Deep Learning, Data Mining
4	Lime green	128	Data management
5	Lilac	104	Internet of Things
6	Blue	93	Sensors, Automation, Process management
7	Orange	68	Computing
8	Brown	59	Traceability, Inventory control, Inventory management

Source: own work based on obtained Scopus metadata by VOSviewer software.

The IIoT presented as the largest red node was linked to terms such as: Industry 4.0, network security, edge computing, cryptography, deep learning, reinforced learning, interoperability, resource allocation scheduling, IEEE standards or blockchain and many more. This shows how vast and broad are the correlations related to IIoT keyword.

The year 2011 was the first time the "IIoT" keyword was used by Chen et al. [51]. After ten years, the number of publications with IIoT keyword has rapidly increased. In 2020, there were 1248 documents while in 2021 (until October 2021), there were 1134. This suggests that the IIoT topic is gaining interest today, as seen in Figure 6.

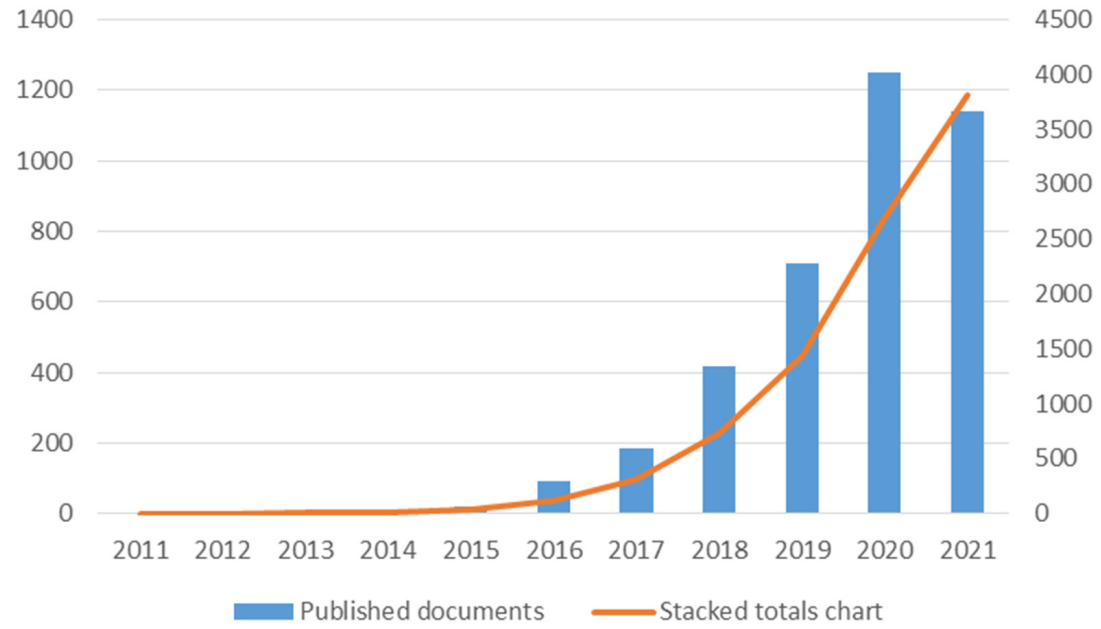

Figure 6. Publishing trend of the sample based on Scopus bibliometric analysis [46]. Keyword "IIoT".

The next step was to compare the document counts for five sources with the largest number of published articles. The results are presented in Figure 7. The largest number of published documents (with IIoT keyword) is in IEE Transactions on Industrial Informatics journal, with 255 papers. In 2018, they had 35 published documents while in 2021, it was 147. The IEEE Internet of Things Journal is also very popular, with 179 published documents. The first two documents were published in 2017. In 2021, they had 105 published documents. The first publication about IIoT was published in 2016 in Lecture Notes in Computer Science. Until October 2021, 124 documents were published in that journal (41 documents in 2021). The IEEE Access has 119 published documents. In 2018, they had 17 documents, while in 2021, it was 39. The last journal is Sensors; until October 2021, they had 76 published documents.

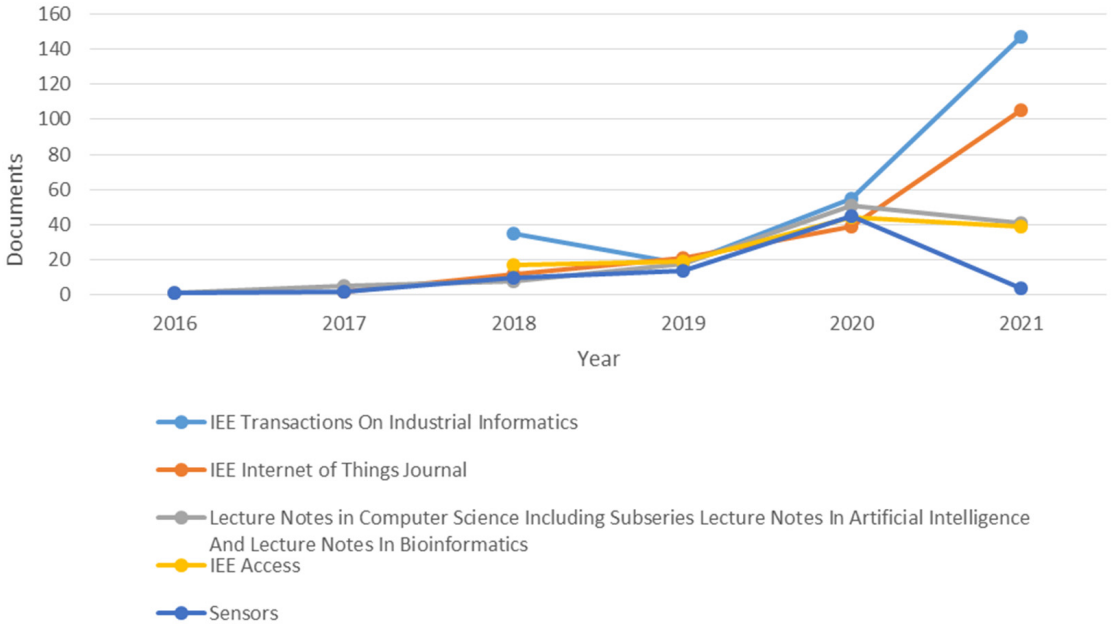

Figure 7. Top five sources based on Scopus bibliometric analysis [46]. Keyword "IIoT".

Next, we compared authors and co-authors of IIoT-related publications, as seen in Figure 8. Gidlund M. (Sweden) published the largest number of documents with IIoT keyword. It was 21 documents in Scopus (first in 2018). Kumar N. (India) is in the second place with 18 documents in Scopus. The top 10 authors altogether published 155 documents in Scopus.

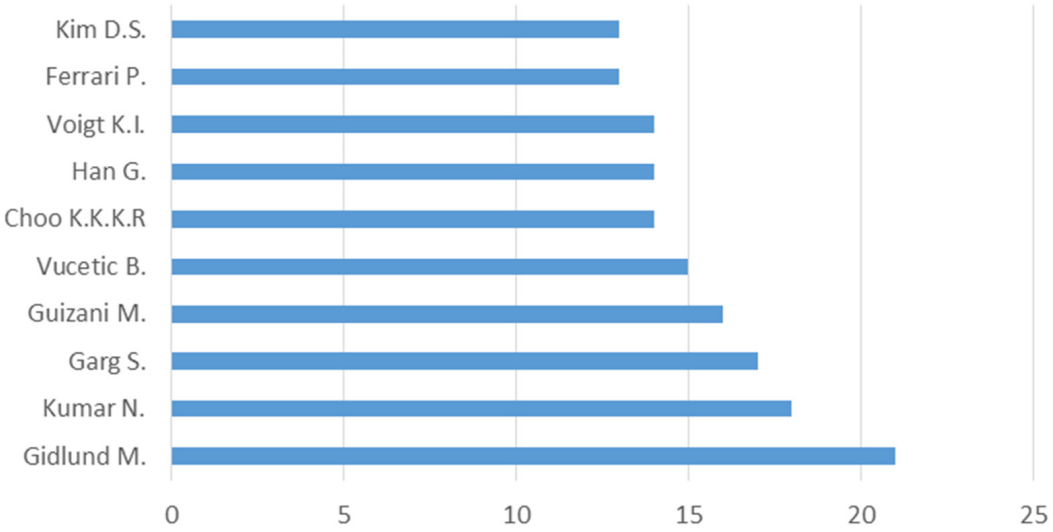

Figure 8. Number of published documents sorted by authors based on Scopus bibliometric analysis [46]. Keyword "IIoT".

Conducting a comparison of the published documents by type of document enabled us to spot that nearly half (49.4%) of the published documents were conference papers. Articles and book chapters accounted for 45.7%. There were 1647 published articles (43.3%) and 86 book chapters (2.3%). Review (82 documents) and conference review (40 documents) consisted of a total of 122 publications (3.3%). List of all published documents sorted by type is presented in Figure 9.

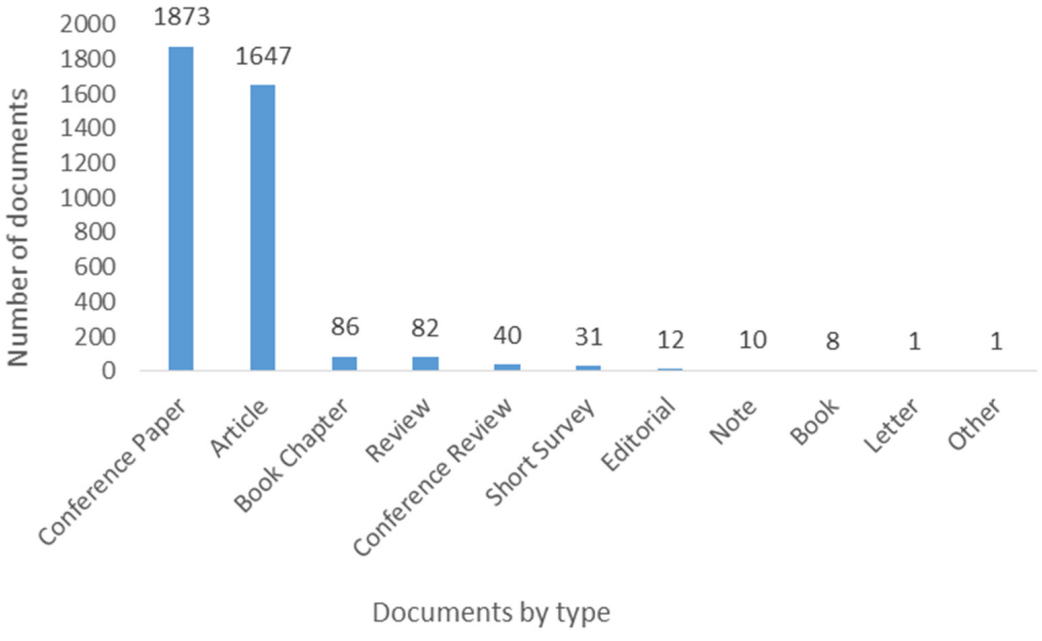

Figure 9. Documents type trend of the sample based on Scopus bibliometric analysis [46]. Keyword "IIoT".

The comparison of documents by country or territory is presented in Figure 10, which shows that 825 published documents were from China. The United States are in second place with 526 documents. Germany has 365 published documents, while India has 341.

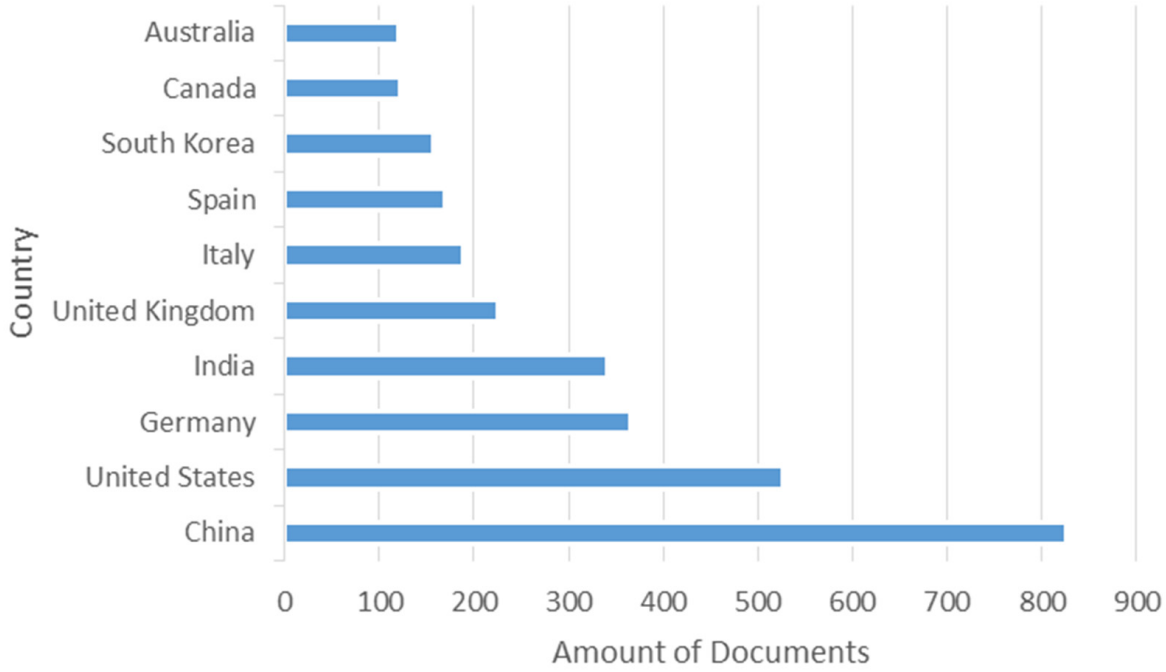

Figure 10. Top 10 countries of the sample with the largest number of publications based on Scopus bibliometric analysis [46]. Keyword "IIoT".

4.2. Application of IoT in Industry

IoT application in industry leads to the creation of Smart Factories where almost all objects such as machinery, devices and products are equipped with sensors connecting each to each and to the Internet [52]. Industrial IoT is one of the most demanding applications [42]. This in turn provides advanced visibility into operations through real-time access to information. In this novel environment, manufacturing equipment and other devices can communicate their real-time performance and improve productivity, efficiency and quality by providing a high level of responsiveness and flexibility at the process level [23]. In 2017, the global IIoT market was valued at USD 312.79 billion with the prediction to reach USD 700.38 billion by 2023 [53]. Typically, unlicensed bands of 2.4 GHz are used in IoT where several technologies compete for spectrum access. However, there is no inter-technology coordination mechanism due to which there is mutual interference, which in turn discourages implementation of industrial monitoring and control. The above-mentioned 2.4 GHz unlicensed band offers a free 85 MHz wide spectrum worldwide. This has led to increased usage of wireless standards such as Bluetooth Low Energy (BLE), IEEE 802.11 and IEEE 802.15.1 on an enormous scale. Process automation domain in IIoT uses the IEEE 802.15.4 physical layer on which WirelessHART and ISA 100.11a leading wireless standards are based [54–57].

IoT at the industrial level leads to the creation of fully automated production systems, together with Cloud systems and BDA enabling improved analysis of market demand patterns, thus significantly improving planning and production control. This in turn contributes to the rapid customization of products at the individual or local level [23]. Selected industry sector categories with the potential for IIoT implementation are presented in Figure 11.

Figure 11. Selected industry sector categories [21].

As the manufacturing environment has changed over the past decades, along with it new business models have developed Industrial Product-Service Systems (IPSS). They shift business from simply selling products, thus generating profits, to selling functionalities. In the IPSS model, industrial products and services are delivered consistently, which in many cases requires BDA coming from different sources such as the IoT devices. The IIoT solutions take into account both technical details of product production and the stakeholders being part of the IPSS business model. In that sense, they allow for dynamic adoption to constantly changing consumer demand and manufacturing abilities [29].

Industrial internet concept originated in the United States and was first mentioned by General Electric, whereas the concept of Industry 4.0 itself originated in Germany. The two concepts are not identical, but indeed they overlap. "Industrial Internet of Things: A system comprising networked smart objects, cyber-physical assets, associated generic information technologies and optional cloud or edge computing platforms, which enable real-time, intelligent, and autonomous access, collection, analysis, communications, and exchange of process, product and/or service information, within the industrial environment, so as to optimize overall production value." [21]. IIoT is an extension of IoT technology, providing industry with a set of tools used in creating its competitive advantage. It serves the industry and therefore has to meet much stricter requirements than in the case of consumer domain. Usually, an IIoT architecture model (Figure 12) consists of several layers with different sets of networks [58]. IIoT through the use of sensors and actuators within an organization, through data collection, analysis and exchange, enables machines (embedded with sensors) to change their own mode of action or to indicate other devices to do so without the need for human action. Moreover, it can support human decision making based on collected data in real time, but also by the ability to store that data, to use them for periodic assessment and/or maintenance prediction.

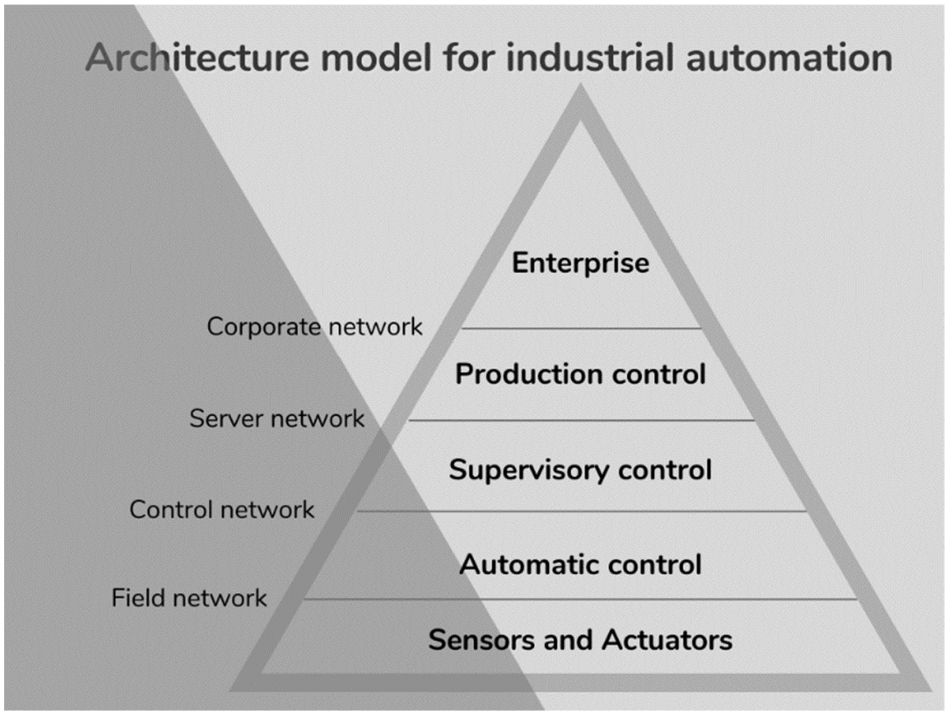

Figure 12. IIoT architecture model [58].

Despite many possibilities of use, the IIoT faces barriers (e.g., security issues, non-scalable systems and interoperability challenges) that can be addressed by IIoT reference architectures. We mention only three: Reference Architecture Model Industrie 4.0 (RAMI 4.0), Industrial Internet Reference Architecture (IIRA) and Internet of Things Architecture (IoT-A).

Sensors and actuators (e.g., position, motion, biosensor, mass/volume measurement and environment) connected to different devices and to the internet are an essential source of ubiquitous production data in IIoT [29]. Such sensors, together with energy balance sheets and smart embedded devices, can support energy monitoring in order to aid manufacturing decision making using real-time online data [59]. One of IoT and IIoT technological solutions is RFID tags and sensors. RFID technology is based on data collection and automatic object identification via radio waves, where a tag transmits its identity to the tag reader. The tag can be either attached or embedded to a device or product and is equipped with a microcircuit with a unique code and/or a set of information. The tag reader has an antenna emitting radio waves and the tag sends back its data to the reader. Collected data are sent and grouped in an information management system including a server connected with a database and software that can be connected with Enterprise Resource Planning (ERP) programs [60,61]. The use of RFID tags can enhance transparency in the supply chain by providing tools and products for real-time tracking system. Those tags can also be used for real-time traceability of resources, thus improving inventory management, but also for the machines at production lines to detect variations in production or assembly performance [23,24]. Such innovations are already being implemented in industry where machines monitor and control assembly parts' speed and status, and send information to the next operators with specific instructions on how and when to put elements together via digital displays [20,62]. Other RFID applications in manufacturing and supply chain management are presented in Figure 13. Examples of industry branches that already exploit RFID technology include automotive, car parts, machine, heavy industry, electronic, food industry, pharmaceutical industry and many others [60]. Utilization of RFID also assists in anti-counterfeit approaches through product traceability, ensuring high supply chain visibility and product authentication. In addition, RFID tags become part of the product moving through the supply chain to the point of sale. However, although RFID

technology is well known and low cost, it is not the only tool building up Industrial IoT. Other components with the ability to link real world with the digital one are Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) [61].

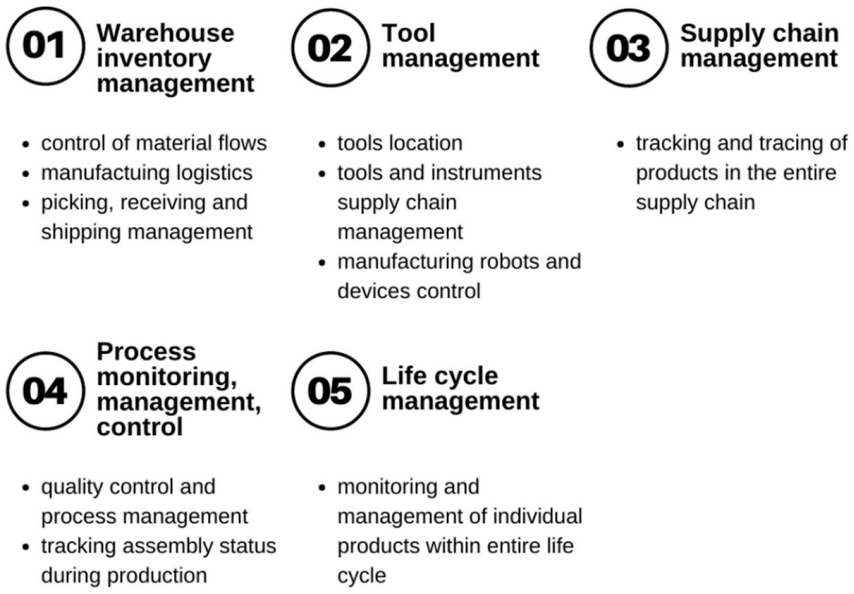

Figure 13. RFID applications in manufacturing and supply chain management [60].

RFID tags and ML algorithms were investigated by Sharif et al. [63] for food contamination detection. The study was conducted using sticker-type inkjet printing UHF RFID tags. The obtained backscattered power from food samples and contaminated food samples was compared and used as input data to the machine learning algorithm. At first, samples of water contaminated with known amounts of salt and sugar ranging from 2 to 10 g per 500 mL PET bottle were prepared and UHT RFID tags were attached. Received Signal Strength Indicator (RSSI) of samples was measured. The RSSI values (dBm) increased with increasing salt or sugar concentrations in the samples. The next step was to prepare spring water samples with added known amounts of sugar/salt. The contamination was sensed with 90% accuracy. The obtained RSSI data were used as input for ML XGBoost algorithm to improve sensing accuracy. The authors used a commercial handheld UHF RFID reader-based setup that was connected via BLE with a smartphone provided with a preinstalled Android application, for water contamination sensing.

The implementation of IIoT reduces human errors, time and maintenance costs, among others, as it allows for collecting, analyzing and storing data consistently to avoid machinery faults, maintenance prediction and customization [24,29]. Moreover, Industrial IoT solutions reduce manufacturing costs through optimized assets and inventory management, also reducing machine downtime and contributing to the monitoring and controlling of workplace environment. In manufacturing, this is a shift from reactive to proactive maintenance of equipment that relies on collected and analyzed data allowing for prognostics rather than diagnostics after the device's failure [26]. Additionally, use of IoT (e.g., RFID tags, barcodes, Quick Response (QR) codes, NFC) can facilitate warehouse inventory management. When a product or product packaging equipped with an RFID tag moves through an RFID reader installed on the warehouse gate and/or racks, etc., the data of the inbound and outbound item are collected and stored and the warehouse inventory database is updated. Whenever the item moves within or outside the warehouse, it is easy to track and trace it automatically [57]. Moreover, some warehouse operations, thanks to IIoT, can be performed without human intervention by means of Automated Guided Vehicles (AGVs) [22].

Thames Water (the largest provider of drinking water and wastewater service in the UK) installed over 100,000 sensors in London for real-time data gathering and analytics. The aim is to cover all customers in London by 2030 [27]. This IIoT solution allows for anticipating equipment failures and enables fast response in crisis situations. IIoT devices have been installed as well at the Mitsubishi plant in Kashima (Japan), producing chemicals for real-time process management. This allowed for increase of production performance. Furthermore, mining industries also benefit from implementing IIoT solutions. Different sensor and real-time data collection and analysis make mining in difficult locations more economical and productive, but also support decrease of safety incidents [27].

IoT technology also has applications in the food sector, where it helps in improving process control and optimizing the decision-making process. The so-called Agriculture 3.0 implements IoT for precision agriculture that, among others, includes the utilization of sensors for nutrients control and monitoring, growth patterns and disease as well as pesticide or fertilizer application control. The development of novel information technologies has led to Agriculture 4.0 which uses satellite data to precisely control field operations, sensors and computers to optimize the production process in glasshouses, introduces robotic milking and improves traceability. Smart irrigation systems include the monitoring of soil moisture and humidity sensors connected with a microcontroller that obtain weather reports from the internet and are able to measure the probable time of the next irrigation. Modern, digitized farms are equipped with sensors monitoring various soil parameters (e.g., moisture content, pH, humidity), which support process control and decision making. Passive infrared (PIR) sensors are used in intruder detection systems, allowing for repelling of birds and rodents in the fields [63,64]. Wireless Sensor Networks (WSN) are cost efficient as they eliminate the necessity of using cables. To overcome the access to the internet infrastructure, power grid solar panels can be utilized [65,66]. Companies such as AT & T, Microsoft, Climate Corp. or Monsanto are promoting IoT in agriculture which provides additional support for the development of this technology [27].

Combining Industrial IoT with Blockchain gives additional benefits as it provides greater transaction transparency and supports product traceability in the case of recall or counterfeit products. This is extremely important, i.e., in counterfeiting of electronic parts that can cause potential safety risk and loss of company profits and also damages the reputation of manufacturers [45]. Maersk and IBM cooperated to implement Blockchain in solving cross-border supply chain problems. This increased information transparency and information sharing between partners was carried out [43]. Esmaeilian et al. [30] give examples of Blockchain application in the food sector, such as an IBM and Brooklyn Roasting Company project that enabled consumers to follow the product's journey through the entire supply chain. Another one mentioned is the BeefChain platform simplifying the tracking of beef in Wyoming (USA) being raised in open range conditions [30]. Rising consumer demand forces manufacturers to provide more and more information, including information related to allergens, ingredients, provenance, traceability or processing method. The Blockchain technology supports access to relevant and authentic (tamperproof) data that can be coded in the form of a barcode or QR code placed on the primary packaging. Consumers can scan such a code with their smartphone to access information. It is also worth mentioning that these solutions are also implemented in containers for refrigerated biopharmaceuticals to monitor temperature, humidity and location [24]. Smart devices connected to the internet through smart equipment such as smartphones and tablets can communicate with the controller and send alarms each time a deviation from variables' acceptable limits occurs. This allows for taking quick actions regarding process control and supports maintenance of the product quality. Perishable food products are usually transported in a specific temperature regime and when temperature monitoring sensors are used for such transport they have the ability to monitor and even regulate the temperature if it deviates from acceptable limits. They can also inform food suppliers in case of failure, thus preventing quality deterioration, spoilage and food and economic losses [60]. The pos-

sibilities of the IIoT are endless, and it is only a matter of time before they are implemented on a massive scale.

4.3. Challenges of Internet of Things in Industry

During the global financial crisis caused by the pandemic situation (COVID-19), more and more industrial companies are transferring to the IIoT. These companies want to be able to remotely monitor their systems and prevent unplanned downtime. A survey by Microsoft [4] found that 44% of organizations will invest more in IoT while in 2020 it was 31%. Moreover "82% of surveyed companies have at least one IoT project in the use stage". IoT is changing the future of manufacturing, but it does carry major challenges that companies will have to face in order to be able to implement the new solutions, which will accelerate their digital transformation. Below we listed some main challenges that companies have to face in their implementing phase of Internet of Things.

a. Technical and technological challenges

The complexity and technical challenges are the biggest barriers for companies that want to exploit the IoT. For these reasons, 30% of surveyed organizations decide against adopting IoT [4] in favor of using current solutions.

Connecting together so many devices is a serious challenge of the IoT/IIoT. Today, we rely on the centralized, server/client paradigm to authorize, authenticate and connect different nodes in a network. For an interconnected system, devices should work together to function properly, even if these devices work in different fields. A lack of common connectivity, standard data formats and common software interfaces complicates implementation of IoT. Another challenge is costly retrofitting or replacement of the traditional devices to work with the latest technologies [67]. Most of the IoT devices are powered by batteries, so IoT must also deal with high energy consumption. Expenses related to servicing and/or replacement of such devices are a serious concern due to the fact that in the future a huge number of sensors will be used. Without appropriate maintenance and life cycle assessment consideration, sooner or later they may become electro-rubbish. Even today, the number of devices connected to the internet outnumbers the human population. Another challenge is to develop high-energy-efficient and long-life sensor batteries which will operate over the lifetime of a sensor [68,69], and define responsible methods of their reprocessing at the end of their life.

The high amount of data produced via the IoT has a crucial role in the big data landscape. Millions of devices are equipped with sensors connected together, communicating, collecting and exchanging data. These devices collect a huge amount of data which is known as Big Data. The significant challenge will be ensuring appropriate handling of these various types of data, in particular in time, resources and processing capability shortages. According to Said and Masud [70], the biggest concern is related to the growing amount of information which is generated through RFID. Each object in the IoT produces information about itself. This information (in a massive quantity) must be collected and then processed, which can cause problems in transmission and storage of data that accelerate every day. As mentioned in [71], "80,000 petabytes of data were stored across the world in 2000, and this is predicted to rise to 35 zettabytes by 2020". The different types of data such as structured data, semi-structured data and unstructured data which come from sensors are collected and analyzed by Big Data and stored in a data warehouse. Only 20% of that data is processed while 80% cannot be used by traditional methods. Most of these data are useless for decision-making processes [43]. Layers of intelligence are required to transform that tremendous amount of data collected by devices connected to the internet into wisdom [69]. Another challenge is to "adjust structures in semi-structured and unstructured data before integrating and analyzing these types of data" [72].

b. Lack of budget and knowledge

When building the IIoT, it is necessary to bear in mind its future updates and maintenance. IIoT, which is a tangled network of interconnected devices, poses a considerable

challenge to system operators. They will not only have to manage the original system, but also administer all new systems. Training engineers takes a long time, especially since most user interface management systems (UIMSs) are not dedicated to industrial automation. Management tasks are very different and require different tools. Manually configuring the network can add to human error and add hours of work. Moreover, it involves additional costs for the company through hiring digital transformation specialists and engineers and training them in the use of systems (to improve the speed of response to errors).

According to Microsoft's IoT Signals Report [4], 26% of organizations reported that a lack of budget and staff were at the top of the reasons for holding off on IoT adoption. Companies complain that it is hard to find the right skilled and experienced employees. In total, 26% of companies that have already adopted IoT said that they still do not have enough skilled workers, and 24% of organizations reported lack of technical knowledge.

c. Information security and data protection challenges

One of the IoT adoption barriers is corporate concerns about information security and privacy. Almost a third (29%) of organizations believe that security risks prevail over benefits of implementing the IoT [3]. Basically, billions of interconnections between devices and people and data exchange cause huge risk of data leakage. Due to the ubiquity and pervasiveness of IoT systems, inevitable problems with privacy and security in the network will arise. From the point of view of the development and expansion of the IoT, it is crucial to ensure data protection and information security in various activities, such as transport services, personal activities, processes or information protection. This is a significant matter; a lot of research has been done, but there are also services related to current trends in the IoT security system [61]. Various services have presented some of the challenges, as they are not designed with security in mind, and can potentially become attack vectors to various IoT devices and device guards [73].

According to Siby et al. [74], today it is hard to manage the security of IoT organization and businesses while various privacy threats emerge, which can penetrate IoT and its network. Organizations need to develop scanning and monitoring systems for all types of IoT devices that could be at risk of information privacy and security breach. Analyzers and traffic interceptors help identify and investigate various cyber threats. One of the major types of cyber-attacks is called the "False Data Injection" (FDI) attack. An FDI attack corrupts sensor measurements; as a result, the device mislead the industrial platform [75].

In order to prevent outside malicious attacks, the following security systems can be used: encryption to ensure data confidentiality and message authentication codes to ensure data integrity and authenticity [76]. However, the encryption does not protect against "insider attacks". Such attacks pose a serious threat for wireless sensor networks. Different IoT wireless network attacks and detection possibilities were presented by Pamarthi and Narmadha [77] and Balogh et al. [78].

Security in the cloud is the next significant area of research which will need more consideration. This is due to the fact that businesses will use hybrid clouds which contain private as well as public clouds. For this reason, security and protection become very important to prevent cyber-attacks [79].

Abomhara and Koien [80] proposed a series of security components contributing to the improvement of IoT security. The authors mentioned also that there are many security and privacy challenges, such as the following:

- "user privacy and data protection,
- authentication and identity management,
- trust management and policy integration,
- authorization and access control,
- end-to-end security,
- attack resistant security solutions".

The above-mentioned issues are significant for IoT development. To overcome those challenges, several solutions have been developed, such as the anonymous orthogonal

code-based privacy preserving scheme for cyber-physical systems. It uses, among others, orthogonal bit codes for user privacy, authentication and anonymity while at the same time it provides low communication and computation overheads [81].

Tawalbeh et al. [82] said that implementation of existing information security concepts in IIoT systems is not so easy. The authors proposed to implement security in multiple layers, starting from the device level to the system level. To ensure that real-time communication and control processes (10–100 ms cycle duration) are not disrupted, security countermeasures are required in IoT. However, solutions used in IT systems such as malware detection software are insufficient [28]. In typical IIoT, symmetric-key cryptography can provide a lightweight solution [83]. This, however, can be insufficient when low-capacity devices are used. Ali et al. [84] proposed a symmetric encryption scheme to tackle this problem. This solution allowed one to obtain user privacy and integrity while using lower computing resources and communication overhead. Another security solution is Elliptic-Curve Cryptography (ECC) which provides smaller key size, thus reducing storage and transmission requirements [27].

Another solution for securing data within IoT is steganography. According to Djebbar [85], such systems "manipulate the characteristics of digital media files to use them as carriers or covers" (e.g., images, audio, video, text, protocols or storage devices) in order to hide secret information (payload). The payload itself is hidden in any type of digital cover. It uses a key for securing data and produces a stego file (blind steganalysis).

As different control systems used in IoT need to operate 24 h a day, all year round, and have a service life of 5–10 years, security updates become a challenge. They cannot cause system malfunctions, and unlike in IT systems, updates cannot result in the system being stopped and restarted [28].

d. Scalability

As mentioned before, the IoT and IIoT are composed of an enormous number of devices. Those devices are usually connected one to another in hierarchical subdomains rather than in a mesh. This in turn results in the number of connected objects being significantly greater than the current internet. The complexity of such architecture is an obstacle for scalability. To overcome this challenge, retaining technologies very simply in the network and dealing with complexity at the end point should be implemented [56,86]. This could be achieved with a scheme that identifies, addresses and names a large number of devices and that will support and scale with them [58].

e. Interoperability of the IIoT environment

Key to the IIoT interoperability is the standardization and adoption of protocols that define the details of communication between devices. Interoperability means that any device is able to connect to another device or system and exchange information. However, it is not always possible for all production aspects, required or wanted. In some cases, within the IIoT, it is necessary in order to achieve interchangeability between devices from different vendors. However, when interoperability is thought of as using the IP protocol, it does not ensure that devices from vendor A and vendor B can be interoperable [58].

f. Standardization issues

Standardization issues play a key role in the development and dissemination of the IoT and IIoT. There are still overlapping activities and fragmented efforts of different providers around the world. Standardization would lower entry barriers and allow for better performance of products/services. Standardization of, e.g., functionalities or requirements should be carried out at an international level in order to enable easier integration of various services [27,56,58]. The aforementioned fragmentation was brought about by the European Telecommunications Standards Institute (ETSI) technical report ETSI TR 103375. This report aimed at providing roadmaps of IoT standards. Moreover, International Electrotechnical Commission (IEC) set up study groups and technical committees on IoT standardization and also published several white papers on IIoT [27]. An IEC 62657-2:2017+AMD1:2019

standard specifies the fundamental assumptions, concepts, parameters and procedures for wireless communication coexistence, as well as its availability and performance in an industrial automation plant. It also provides a common point of reference [87].

g. Legal and regulatory security

Legal and regulatory security is understood as compliance by IoT devices with legal standards regarding, for example, the admissibility of processing specific information and compliance with the regulations of the EU and other countries. For example, there are no separate and detailed regulations for IoT technology in the Polish legal system. IoT regulations are scattered throughout many legal acts (including General Data Protection Regulation (GDPR), telecommunications law and sector secrets, but also Network and Information Security directive (NIS directive)), which often grant administrative or supervisory authorities the power to impose severe financial penalties. Although an EU Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (text with EEA relevance) has been adopted, it does not respond to the challenges of using anonymous data in IoT [88].

4.4. Opportunities of Internet of Things in Industry

Quality assurance (43%) and cloud security (42%) are major motivators that cause companies to implement IoT [4]. Other factors for IoT adopters are issues related to device security (40%) and operations optimization (40%). Over one third of enterprises also adopt IoT to improve products and services for customers [4].

There are many benefits for organizations which adopt IoT. Based on the Microsoft [4] report, the most important are: "increased efficiency of operations (55%), improved safety conditions (51%) and increased employee productivity (50%)". Enterprises also noticed that IoT implementation gave a return on investment through better productivity, increasing production capacity, reducing human mistakes and reducing expenses. IoT can also boost customer satisfaction and increase opportunities for organizations based on more informed and better decisions. Below, we list some main opportunities for implementing IoT in industry.

a. Software development

The proper software for the collection of data by IoT devices, and then their analysis, could improve efficiency and reliability [89].

b. Energy Consumption

Industrial IoT can become a major player in controlling energy consumption. It can contribute to minimizing energy consumption and optimizing its production. A lot of energy is consumed to produce the final product and to ensure its good quality in traditional factories. Moreover, human resources are needed for controlling every single process and operation of production. For this reason, actions should be taken to avoid wasteful energy consumption in production processes [36]. Various technological solutions such as Green IoT are proposed by Xu et al. [90].

Cloud platforms, gateway devices, web servers and IoT hub networks, which are accessible with smart mobile devices, could be used as monitoring equipment. Wired and wireless communications (Bluetooth, WiFi, ZigBee, etc.) can be used to connect together different devices. Moreover, the smart sensors may be installed on each device in the smart factory, which will detect higher energy consumption of the components, exceeding set limits [36].

Another opportunity will be the development of low-power sensing units. The new compact and efficient batteries, energy-generation devices and fuel cells will be the key factor for the implementation of autonomous wireless smart systems. [91]. The concept of green Sensors On a Chip (SoC) could be used to reduce energy consumption of the entire infrastructure (traffic, e-waste, carbon footprint) [92,93].

Another example which enables the reduction of energy consumption by adjusting power transmission to minimum level and using more efficient communication protocols is green M2M [36]. In contrast to the Low Power Wide Area Networks (LPWANs), they are developed to be low cost, with low energy consumption and operating over a wide transmission range. They rely on limited energy sources that need to be either replaced or recharged. Peruzzi and Pozzebon described energy harvesting techniques for Wireless Sensor Networks (WSN) [94], whereas Elahi et al. [95] presented different energy harvesting methods (e.g., mechanical energy harvesting, aeroelastic energy harvesting and others).

The application of blockchain in the energy sector will improve IoT efficiency by providing a decentralized platform for distributed power generation and storage system, which will enhance energy efficiency and security. Blockchain also enables energy distribution between devices and remotely controls energy flow to the particular area. People will have direct access to energy information with no involvement of third parties [96].

Smart Grid (SG), Electricity System Network (ESN), and IoT nodes may be potential solutions to the upcoming global energy crisis [97]. The SG framework, combined with IoT and Energy Internet, can be used in various applications related to energy. Smart grid is a bidirectional grid which allows for power and information flow. The recent era has brought growing energy consumption worldwide and, as a result, increased fossil fuel burning. Environment concerns led to introduction and development of Renewable Energy Sources (RES). Making these solutions more abundant and available to consumers has changed their role on the energy market to prosumers. Now, consumers not only consume energy, but are also producers of energy to the grid. In addition, individual consumers are not only consuming energy provided by the energy sector, but also contribute to the energy production which is made available commercially and for industrial purposes. Implementing IoT in the smart grid environment aids monitoring and control of the power system in real time. Tightiz and Yang [98] describe different communication protocols in the smart grid such as Common Object Request Broker Architecture (COBRA), Advanced Message Queuing Protocol (AMQP), Open Platform Communications United Architecture (OPC UA), Data Distribution Services (DDS), Message Queue Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP).

Energy harvesting is a major player when it comes to the increase of the efficiency and lifetime of IoT devices [95]. To minimize the power draining of the batteries, a crucial role is played by power management integrated circuits, which help increase the system's life span. The concept of Internet Nano-Things (IoNT) discussed by Elahi et al. [95], shows that in the future IoT devices might be the self-powering sources which will make high-performance nanosystems.

c. Connectivity

Sensor technology will continue to become more efficient, cheaper and widely available, which will lead to the application of sensors on a large scale for monitoring and detection. Moreover, many wireless standards, which are used today, are optimized for human-to-human applications, so another opportunity will be making clusters of the machines [69].

5. Conclusions

The revolution of the IoT keeps going forward; this means that we are at the beginning of a new age of data. This revolution will have a significant impact on the day to day life and behaviors of users, both private and corporate. IoT applications will expand in various industries, improving them and bringing tangible benefits. The opportunities offered by IoT implementation will mean that all affected sectors can now access functionality that did not exist a few years earlier. IoT applications can affect, among others: automation of industrial production, logistics, management of individual processes and enterprise management, as well as transport through the development of an intelligent system for transporting people and goods. Industrial Internet of Things, as confirmed by the profiling research, enjoys constant interest. It is also important that these solutions enable unmanned

work and limit human work, especially in places where manpower could be exposed to dangerous factors (work in a mine, at heights, underwater at great depths, etc.). IoT is in the early stage of development, and despite the many benefits and opportunities it brings, it faces challenges, barriers and risks. The concerns related to the implementation of IoT are not unfounded. Each organization must ask itself whether the benefits of implementing IoT outweigh the challenges associated with it. Moreover, as with most new technologies it is subject to certain rules; in particular, the technology adoption life cycle. As IoT is in the diffusion growth phase, innovators and early adopters have already paved the way for other organizations which need complete and reliable solutions to implement IoT. From our analysis, the image of IoT diffusion is shaped in a way in which the benefits and opportunities for companies resulting from the implementation of this technology are recognized. At the same time, participants of the so-called early market experienced problems with the implementation and operation of IoT. These limitations and barriers currently stand in the way of faster diffusion of IoT, but on the other hand, there are more and more research studies and solutions that tackle these issues. It will take time to overcome these problems, and mistakes and failures will occur along the way. However, all of us will benefit from IoT to a greater or lesser extent. It will have impacts on our everyday life and lifestyle and reduce human errors in many activities.

Author Contributions: K.W. was involved in project administration and supervision. K.W., M.B., B.P. and J.G. were involved in funding acquisition, conceptualization, writing the initial draft of the paper, and revisions. K.W., M.B. and B.P. contributed to data collection and revisions. K.W. and M.B. were involved in writing the paper, editing, designing the figures and the layout of the paper. B.P. and J.G. were involved in commenting on the content and its relevance to the scope of the journal. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the project Economics in the face of the New Economy financed within the Regional Initiative for Excellence programme of the Minister of Science and Higher Education of Poland, years 2019–2022, grant no. 004/RID/2018/19, financing 3,000,000 PLN.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

Alphabetical list of abbreviations used within the text:

AGVs	Automated Guided Vehicles
AI	Artificial Intelligence
B2B	Business-to-Business
BDA	Big Data Analytics
BLE	Bluetooth Low Energy
CPS	Cyber Physical Systems
ECC	Elliptic-Curve Cryptography
ERP	Enterprise Resource Planning
FDI	False Data Injection
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoT	Internet of Things
IoT-A	Internet of Things Architecture
IIRA	Industrial Internet Reference Architecture
IPSS	Industrial Product-Service Systems
M2M	Machine-To-Machine
ML	Machine Learning

NFC	Near Field Communications
P2P	Peer-To-Peer
PIR	Passive infrared
QoE	Quality of Experience
QoS	Quality of Service
QR	Quick Response
RAMI	Reference Architecture Model Industrie
RFID	Radio Frequency Identification
RSSI	Received Signal Strength Indicator
SG	Smart Grid
SVM	Support Vector Machine
WSAN	Wireless Sensor and Actuator Networks
WSN	Wireless Sensor Networks

References

1. Fan, Y.V.; Pintarič, Z.N.; Klemeš, J.J. Emerging Tools for Energy System Design Increasing Economic and Environmental Sustainability. *Energies* **2020**, *13*, 4062. [CrossRef]
2. Deloitte. Internet of Things (Iot)—The Rise of the Connected World. Available online: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-IoT_Theriseoftheconnectedworld-28aug-noexp.pdf (accessed on 12 January 2021).
3. Cisco. Internet of Things. Available online: https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf (accessed on 12 January 2021).
4. Microsoft. *IoT Signals*, 3rd ed.; Available online: www.azure.microsoft.com (accessed on 16 October 2021).
5. Zikria, Y.B.; Ali, R.; Afzal, M.K.; Kim, S.W. Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions. *Sensors* **2021**, *21*, 1174. [CrossRef] [PubMed]
6. Liao, Y.; Deschamps, F.; Loures, E.D.; Ramos, L.F. Past, present and future of Industry 4.0—A systematic literature review and research agenda proposal. *Int. J. Prod. Res.* **2017**, *55*, 3609–3629. [CrossRef]
7. Zheng, T.; Ardolino, M.; Bacchetti, A.; Perona, M. The applications of Industry 4.0 technologies in manufacturing context: A systematic literature review. *Int. J. Prod. Res.* **2021**, *59*, 1922–1954. [CrossRef]
8. Oztemel, E.; Gursev, S. Literature review of Industry 4.0 and related technologies. *J. Intell. Manuf.* **2020**, *31*, 127–182. [CrossRef]
9. Lasi, H.; Fettke, P.; Kemper, H.-G.; Feld, T.; Hoffmann, M. Industry 4.0. *Bus. Inf. Syst. Eng.* **2014**, *6*, 239–242. [CrossRef]
10. Yikilmaz, İ. New era: The transformation from the information society to super smart society (society 5.0). In *Data, Information and Knowledge Management*; Nobel Bilimsel Eserler: Ankara, Turkey, 2020; pp. 85–112.
11. Wichmann, R.; Eisenbart, B.; Gericke, K. *The Direction of Industry: A Literature Review on Industry 4.0*; Cambridge University Press: Cambridge, UK, 2019; Volume 1, pp. 2129–2138. [CrossRef]
12. Silvestri, L.; Forcina, A.; Introna, V.; Santolamazza, A.; Cesarotti, V. Maintenance transformation through Industry 4.0 technologies: A systematic literature review. *Comput. Ind.* **2020**, *123*, 103335. [CrossRef]
13. Alqahtani, A.Y.; Gupta, S.M.; Nakashima, K. Warranty and maintenance analysis of sensor embedded products using internet of things in industry 4.0. *Int. J. Prod. Econ.* **2019**, *208*, 483–499. [CrossRef]
14. 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]
15. Stentoft, J.; Adsbøll Wickstrøm, K.; 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]
16. Lee, J.; Kao, H.-A.; Yang, S. Service Innovation and Smart Analytics for Industry 4.0 and Big Data Environment. *Procedia CIRP* **2014**, *16*, 3–8. [CrossRef]
17. Bahrin, M.; Othman, F.; Azli, N.; Talib, M. Industry 4.0: A review on industrial automation and robotic. *J. Teknol.* **2016**, *78*, 6–13. [CrossRef]
18. Almada-Lobo, F. The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES). *J. Innov. Manag.* **2016**, *3*, 16–21. [CrossRef]
19. Vaidya, S.; Ambad, P.; Bhosle, S. Industry 4.0—A Glimpse. *Procedia Manuf.* **2018**, *20*, 233–238. [CrossRef]
20. Malik, P.K.; Sharma, R.; Singh, R.; Gehlot, A.; Satapathy, S.C.; Alnumay, W.S.; Pelusi, D.; Ghosh, U.; Nayak, J. Industrial Internet of Things and its Applications in Industry 4.0: State of the Art. *Comput. Commun.* **2021**, *166*, 125–139. [CrossRef]
21. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
22. Dlodlo, N.; Foko, T.; Mvelase, P.; Mathaba, S. The State of Affairs in Internet of Things Research. *Electron. J. Inf. Syst. Eval.* **2012**, *3*, 244–258.
23. Fatorachian, H.; Kazemi, H. Impact of Industry 4.0 on supply chain performance. *Prod. Plan. Control* **2021**, *32*, 63–81. [CrossRef]

24. Rejeb, A.; Keogh, J.G.; Treiblmaier, H. Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management. *Future Internet* **2019**, *11*, 161. [CrossRef]
25. Alfa, A.A.; Alhassan, J.K.; Olaniyi, O.M.; Olalere, M. Blockchain technology in IoT systems: Current trends, methodology, problems, applications, and future directions. *J. Reliab. Intell. Environ.* **2021**, *7*, 115–143. [CrossRef]
26. Garg, K.; Goswami, C.; Chhatrawat, R.S.; Kumar Dhakar, S.; Kumar, G. Internet of things in manufacturing: A review. *Mater. Today Proc.* **2022**, *51*, 286–288. [CrossRef]
27. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
28. Matsumoto, N.; Fujita, J.; Endoh, H.; Yamada, T.; Sawada, K.; Kaneko, O. Asset Management Method of Industrial IoT Systems for Cyber-Security Countermeasures. *Information* **2021**, *12*, 460. [CrossRef]
29. Alexopoulos, K.; Koukas, S.; Boli, N.; Mourtzis, D. Architecture and development of an Industrial Internet of Things framework for realizing services in Industrial Product Service Systems. *Procedia CIRP* **2018**, *72*, 880–885. [CrossRef]
30. Esmaeilian, B.; Sarkis, J.; Lewis, K.; Behdad, S. Blockchain for the future of sustainable supply chain management in Industry 4.0. *Resour. Conserv. Recycl.* **2020**, *163*, 105064. [CrossRef]
31. Forsstrom, S.; Butun, I.; Eldefrawy, M.; Jennehag, U.; Gidlund, M. Challenges of Securing the Industrial Internet of Things Value Chain. In Proceedings of the 2018 Workshop on Metrology for Industry 4.0 and IoT, Brescia, Italy, 16–18 April 2018; pp. 218–223. [CrossRef]
32. Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A Survey of Security in Cloud, Edge, and Fog Computing. *Sensors* **2022**, *22*, 927. [CrossRef]
33. Karakaya, A.; Akleylek, S. A novel IoT-based health and tactical analysis model with fog computing. *PeerJ Comput. Sci.* **2021**, *7*, e342. [CrossRef]
34. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing*; National Institute of Standards & Technology: Gaithersburg, MA, USA, 2011; p. 2.
35. Mijuskovic, A.; Chiumento, A.; Bemthuis, R.; Aldea, A.; Havinga, P. Resource Management Techniques for Cloud/Fog and Edge Computing: An Evaluation Framework and Classification. *Sensors* **2021**, *21*, 1832. [CrossRef]
36. Motlagh, N.H.; Mohammadrezaei, M.; Hunt, J.; Zakeri, B. Internet of Things (IoT) and the Energy Sector. *Energies* **2020**, *13*, 494. [CrossRef]
37. Wang, G.; Nixon, M.; Boudreaux, M. Toward Cloud-Assisted Industrial IoT Platform for Large-Scale Continuous Condition Monitoring. *Proc. IEEE* **2019**, *107*, 1193–1205. [CrossRef]
38. Pinto, D.; Dias, J.P.; Ferreira, H.S. Dynamic Allocation of Serverless Functions in IoT Environments. In Proceedings of the 2018 IEEE 16th International Conference on Embedded and Ubiquitous Computing (EUC), Bucharest, Romania, 29–31 October 2018; pp. 1–8.
39. Mohan, N.; Kangasharju, J. Edge-Fog cloud: A distributed cloud for Internet of Things computations. In Proceedings of the 2016 Cloudification of the Internet of Things (CIoT), Paris, France, 23–25 November 2016. [CrossRef]
40. OpenFogConsortium. *OpenFog Reference Architecture for Fog Computing*; OPFRA001.020817; OpenFogConsortium: Fremont, CA, USA, 2017.
41. Vaclavova, A.; Strelec, P.; Horak, T.; Kebisek, M.; Tanuska, P.; Huraj, L. Proposal for an IIoT Device Solution According to Industry 4.0 Concept. *Sensors* **2022**, *22*, 325. [CrossRef]
42. Cabrini, F.H.; Filho, F.V.; Rito, P.; Filho, A.B.; Sargento, S.; Neto, A.V.; Kofuji, S.T. Enabling the Industrial Internet of Things to Cloud Continuum in a Real City Environment. *Sensors* **2021**, *21*, 7707. [CrossRef]
43. Lim, M.K.; Li, Y.; Wang, C.; Tseng, M.-L. A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. *Comput. Ind. Eng.* **2021**, *154*, 107133. [CrossRef]
44. Benzidia, S.; Makaoui, N.; Subramanian, N. Impact of ambidexterity of blockchain technology and social factors on new product development: A supply chain and Industry 4.0 perspective. *Technol. Forecast. Soc. Chang.* **2021**, *169*, 120819. [CrossRef]
45. Dietrich, F.; Ge, Y.; Turgut, A.; Louw, L.; Palm, D. Review and analysis of blockchain projects in supply chain management. *Procedia Comput. Sci.* **2021**, *180*, 724–733. [CrossRef]
46. Scopus. Abstract and Citation Database. 2021. Available online: https://www.scopus.com (accessed on 16 October 2021).
47. Katoch, R. IoT research in supply chain management and logistics: A bibliometric analysis using vosviewer software. *Mater. Today Proc.* **2021**, *in press*. [CrossRef]
48. Singh, V.K.; Singh, P.; Karmakar, M.; Leta, J.; Mayr, P. The journal coverage of Web of Science, Scopus and Dimensions: A comparative analysis. *Scientometrics* **2021**, *126*, 5113–5142. [CrossRef]
49. Donthu, N.; Kumar, S.; Mukherjee, D.; Pandey, N.; Lim, W.M. How to conduct a bibliometric analysis: An overview and guidelines. *J. Bus. Res.* **2021**, *133*, 285–296. [CrossRef]
50. Xie, L.; Chen, Z.; Wang, H.; Zheng, C.; Jiang, J. Bibliometric and Visualized Analysis of Scientific Publications on Atlantoaxial Spine Surgery Based on Web of Science and VOSviewer. *World Neurosurg.* **2020**, *137*, 435–442.e434. [CrossRef]
51. Chen, Y.; Guo, G.; Hu, Y.; Ning, B.; Wang, W. Spindle and workpiece information collecting for industrial internet of things. *ICIC Express Lett.* **2011**, *5*, 455–459.
52. Gebremichael, T.; Ledwaba, L.P.I.; Eldefrawy, M.H.; Hancke, G.P.; Pereira, N.; Gidlund, M.; Akerberg, J. Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. *IEEE Access* **2020**, *8*, 152351–152366. [CrossRef]

53. Gidlund, M.; Han, S.; Sisinni, E.; Saifullah, A.; Jennehag, U. Guest Editorial From Industrial Wireless Sensor Networks to Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2194–2198. [CrossRef]
54. Grimaldi, S.; Mahmood, A.; Hassan, S.A.; Gidlund, M.; Hancke, G.P. Autonomous Interference Mapping for Industrial Internet of Things Networks Over Unlicensed Bands: Identifying Cross-Technology Interference. *IEEE Ind. Electron. Mag.* **2021**, *15*, 67–78. [CrossRef]
55. Åkerberg, J.; Gidlund, M.; Lennvall, T.; Neander, J.; Björkman, M. Efficient integration of secure and safety critical industrial wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.* **2011**, *2011*, 100. [CrossRef]
56. Basir, R.; Qaisar, S.; Ali, M.; Aldwairi, M.; Ashraf, M.I.; Mahmood, A.; Gidlund, M. Fog Computing Enabling Industrial Internet of Things: State-of-the-Art and Research Challenges. *Sensors* **2019**, *19*, 4807. [CrossRef] [PubMed]
57. Grimaldi, S.; Martenvormfelde, L.; Mahmood, A.; Gidlund, M. Onboard Spectral Analysis for Low-Complexity IoT Devices. *IEEE Access* **2020**, *8*, 43027–43045. [CrossRef]
58. Lennvall, T.; Gidlund, M.; Akerberg, J. Challenges when bringing IoT into industrial automation. In Proceedings of the 2017 IEEE AFRICON, Cape Town, South Africa, 18–20 September 2017; pp. 905–910. [CrossRef]
59. Peng, C.; Peng, T.; Liu, Y.; Geissdoerfer, M.; Evans, S.; Tang, R. Industrial Internet of Things enabled supply-side energy modelling for refined energy management in aluminium extrusions manufacturing. *J. Clean. Prod.* **2021**, *301*, 126882. [CrossRef]
60. Liukkonen, M. RFID technology in manufacturing and supply chain. *Int. J. Comput. Integr. Manuf.* **2015**, *28*, 861–880. [CrossRef]
61. Arulogun, O.T.; Falohun, A.S.; Akande, N.O. Radio Frequency Identification and Internet of Things: A Fruitful Synergy. *Br. J. Appl. Sci. Technol.* **2016**, *18*, 1–16. [CrossRef]
62. Maśniak, L.; Marcisz, K.; Płodzich, J.; Świętochowska, E.; Tomala, A.; Zaboklicki, J. *IOT W Polskiej Gospodarce*; Ministerstwo Cyfryzacji: Warsaw, Poland, 2019.
63. Sharif, A.; Abbasi, Q.H.; Arshad, K.; Ansari, S.; Ali, M.Z.; Kaur, J.; Abbas, H.T.; Imran, M.A. Machine Learning Enabled Food Contamination Detection Using RFID and Internet of Things System. *J. Sens. Actuator Netw.* **2021**, *10*, 63. [CrossRef]
64. Kodan, R.; Parmar, P.; Pathania, S. Internet of Things for Food Sector: Status Quo and Projected Potential. *Food Rev. Int.* **2020**, *36*, 584–600. [CrossRef]
65. Lloret, J.; Sendra, S.; Garcia, L.; Jimenez, J.M. A Wireless Sensor Network Deployment for Soil Moisture Monitoring in Precision Agriculture. *Sensors* **2021**, *21*, 7243. [CrossRef]
66. Abdollahi, A.; Rejeb, K.; Rejeb, A.; Mostafa, M.M.; Zailani, S. Wireless Sensor Networks in Agriculture: Insights from Bibliometric Analysis. *Sustainability* **2021**, *13*, 12011. [CrossRef]
67. Petrut, I.; Otesteanu, M. The IoT Connectivity Challenges. In Proceedings of the 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 17–19 May 2018; pp. 000385–000388.
68. Farhan, L.; Shukur, S.T.; Alissa, A.E.; Alrweg, M.; Raza, U.; Kharel, R. A survey on the challenges and opportunities of the Internet of Things (IoT). In Proceedings of the 2017 Eleventh International Conference on Sensing Technology (ICST), Sydney, Australia, 4–6 December 2017; pp. 1–5.
69. Chen, Y. Challenges and opportunities of internet of things. In Proceedings of the 17th Asia and South Pacific Design Automation Conference, Sydney, Australia, 30 January–2 February 2012; pp. 383–388.
70. Said, O.; Masud, M. Towards Internet of Things: Survey and Future Vision. *Int. J. Comput. Netw.* **2013**, *5*, 1–17.
71. Thabet, N.; Soomro, T. Big Data Challenges. *Comput. Eng. Inf. Technol.* **2015**, *4*, 31–40. [CrossRef]
72. Baars, H.; Kemper, H.-G. Management Support with Structured and Unstructured Data—An Integrated Business Intelligence Framework. *Inf. Syst. Manag.* **2008**, *25*, 132–148. [CrossRef]
73. Noor, M.B.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]
74. Siby, S.; Maiti, R.R.; Tippenhauer, N.O. IoTScanner: Detecting Privacy Threats in IoT Neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi, United Arab Emirates, 2 April 2017; pp. 23–30.
75. Aboelwafa, M.M.N.; Seddik, K.G.; Eldefrawy, M.H.; Gadallah, Y.; Gidlund, M. A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. *IEEE Internet Things J.* **2020**, *7*, 8462–8471. [CrossRef]
76. Neill, D.B. Fast Bayesian scan statistics for multivariate event detection and visualization. *Stat. Med.* **2011**, *30*, 455–469. [CrossRef]
77. Pamarthi, S.; Narmadha, R. Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: Network attacks and detection mechanisms. *Int. J. Intell. Unmanned Syst.* **2021**. *ahead-of-print*. [CrossRef]
78. Balogh, S.; Gallo, O.; Ploszek, R.; Špaček, P.; Zajac, P. IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques. *Electronics* **2021**, *10*, 2647. [CrossRef]
79. Kaufman, L.M. Data Security in the World of Cloud Computing. *IEEE Secur. Priv.* **2009**, *7*, 61–64. [CrossRef]
80. Abomhara, M.; Køien, G.M. Security and privacy in the Internet of Things: Current status and open issues. In Proceedings of the 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, 11–14 May 2014; pp. 1–8.
81. Ali, W.; Din, I.U.; Almogren, A.; Kumar, N. ALPHA: An Anonymous Orthogonal Code-Based Privacy Preserving Scheme for Industrial Cyber–Physical Systems. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7716–7724. [CrossRef]
82. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
83. Vinoth, R.; Deborah, L.J.; Vijayakumar, P.; Kumar, N. Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT. *IEEE Internet Things J.* **2021**, *8*, 3801–3811. [CrossRef]

84. Ali, W.; Din, I.U.; Almogren, A.; Guizani, M.; Zuair, M. A Lightweight Privacy-Aware IoT-Based Metering Scheme for Smart Industrial Ecosystems. *IEEE Trans. Ind. Inform.* **2021**, *17*, 6134–6143. [CrossRef]
85. Djebbar, F. Securing IoT Data Using Steganography: A Practical Implementation Approach. *Electronics* **2021**, *10*, 2707. [CrossRef]
86. Van Kranenburg, R.; Bassi, A. IoT Challenges. *Commun. Mob. Comput.* **2012**, *1*, 9. [CrossRef]
87. IEC+AMD. Industrial communication networks—Wireless communication networks—Part 2: Coexistence management. In *IEC 62657-2:2017+AMD1:2019 CSV*; IEC: Geneva, Switzerland, 2019.
88. Iot and the Polish Economy, Report of the Working Group for the Internet of Things at the Ministry of Digital Affairs. Available online: https://www.gov.pl/attachment/f79e07cc-9f3e-491b-a205-30b4a67855a7 (accessed on 12 January 2021).
89. Nižetić, S.; Šolić, P.; González-De-Artaza, D.L.-D.; Patrono, L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *J. Clean. Prod.* **2020**, *274*, 122877. [CrossRef]
90. Xu, L.; He, W.; Li, S. Internet of Things in Industries: A Survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]
91. Chen, S.; Xu, H.; Liu, D.; Hu, B.; Wang, H. A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective. *IEEE Internet Things J.* **2014**, *1*, 349–359. [CrossRef]
92. Arshad, R.; Zahoor, S.; Shah, M.A.; Wahid, A.; Yu, H. Green IoT: An Investigation on Energy Saving Practices for 2020 and beyond. *IEEE Access* **2017**, *5*, 15667–15681. [CrossRef]
93. Bol, D.; Vos, J.D.; Botman, F.; Streel, G.d.; Bernard, S.; Flandre, D.; Legat, J. Green SoCs for a sustainable Internet-of-Things. In Proceedings of the 2013 IEEE Faible Tension Faible Consommation, Paris, France, 20–21 June 2013; pp. 1–4.
94. Peruzzi, G.; Pozzebon, A. A Review of Energy Harvesting Techniques for Low Power Wide Area Networks (LPWANs). *Energies* **2020**, *13*, 3433. [CrossRef]
95. Elahi, H.; Munir, K.; Eugeni, M.; Atek, S.; Gaudenzi, P. Energy Harvesting towards Self-Powered IoT Devices. *Energies* **2020**, *13*, 5528. [CrossRef]
96. Alladi, T.; Chamola, V.; Rodrigues, J.J.P.C.; Kozlov, S.A. Blockchain in Smart Grids: A Review on Different Use Cases. *Sensors* **2019**, *19*, 4862. [CrossRef] [PubMed]
97. Kumar, N.M.; Chand, A.A.; Malvoni, M.; Prasad, K.A.; Mamun, K.A.; Islam, F.; Chopra, S.S. Distributed energy resources and the application of AI, IoT, and blockchain in smart grids. *Energies* **2020**, *13*, 5739. [CrossRef]
98. Tightiz, L.; Yang, H. A Comprehensive Review on IoT Protocols' Features in Smart Grid Communication. *Energies* **2020**, *13*, 2762. [CrossRef]