applied sciences

MDPI

Review

Production Plant and Warehouse Automation with IoT and Industry 5.0

Zainab Fatima [1], Muhammad Hassan Tanveer [2,*], Waseemullah [1], Shehnila Zardari [1], Laviza Falak Naz [1], Hina Khadim [1], Noorah Ahmed [1] and Midha Tahir [1]

[1] Department of Software Engineering, NED University of Engineering and Technology, Karachi 75270, Pakistan; zainab.ned@cloud.neduet.edu.pk (Z.F.); waseemu@cloud.neduet.edu.pk (W.); shehnilaz@cloud.neduet.edu.pk (S.Z.); naz4108845@cloud.neduet.edu.pk (L.F.N.); khadim4100626@cloud.neduet.edu.pk (H.K.); ahmed4130187@cloud.neduet.edu.pk (N.A.); tahir4100834@cloud.neduet.edu.pk (M.T.)

[2] Department of Robotics and Mechatronics Engineering, Kennesaw State University, Marietta, GA 30067, USA

* Correspondence: mtanveer@kennesaw.edu

Abstract: The Internet of Things (IoT) has been implemented by multiple manufacturing companies into their production chain as this technology is the main source of digitalization in a production plant. It improves the data assembling, productivity of the operation, communication efficiency, and overall manufacturing performance. IoT is also serves to be a good means for improved and efficient warehouse automation. It makes the delivery of products more efficient by calculating the least routes and also reduces the time that is consumed during the management of inventory. The basic objective of Industry 4.0 is to lessen the participation of human operators and to emphasize the automation systems. However, this objective has changed in Industry 5.0, which aims to achieve the maximum benefits through the human–machine interaction by maintaining a balance. Industry 5.0 aims to strengthen the interaction between ever-increasing powerful machinery and the productive abilities of human beings. This paper introduces a detailed overview of IoT in enabling digital transformations and Industry 4.0. The authors have discussed the application of IoT in different industrial sectors, and how the concept of IIoT has evolved. In addition to this, the present paper highlights several research studies that enable the authors to elicit the major challenges, implementation analysis, and future scope of IIoT.

Keywords: IoT; Industry 4.0; Industry 5.0; automation; Industrial IoT (IIoT)

check for updates

Citation: Fatima, Z.; Tanveer, M.H.; Waseemullah; Zardari, S.; Naz, L.F.; Khadim, H.; Ahmed, N.; Tahir, M. Production Plant and Warehouse Automation with IoT and Industry 5.0. *Appl. Sci.* **2022**, *12*, 2053. https://doi.org/10.3390/app12042053

Academic Editor: Luis Javier Garcia Villalba

Received: 29 November 2021
Accepted: 10 January 2022
Published: 16 February 2022

1. Introduction

The innovation in technologies make the world stand on the 4th Industrial Revolution named Industry 4.0. The technologies of design and production cardinally changed due to the implementation of Industry 4.0 [1]. The role of computers in automating industries and production plants is also varying, which uses sensors and the automation of technological processes to integrate and visualize data that affects the decision-making capability of users. In 2011, Industry 4.0 was publicly defined as a means to achieve the competitiveness of industries and factories through the implementation of cyber-physical systems. Industry 4.0 is a concept that describes the technological advancements that increase the level of digitization of production plants and warehouse automations [2]. Four major domains of the internet 4.0 are named as [3]:

- Cyber-Physical Systems (CPS);
- Internet of Things (IoT);
- Internet of Services (IoS);
- Smart factories

The main objective of every industrial revolution is to use the emerging technologies that maximize productivity and achieve mass production. The Fourth Industrial Revolution is centered around the concept of the implementation of technology. Man is not at the center lies behind in the context of its ideology [2]. The 4th Industrial Revolution will present its expected results no earlier than 2020–2025, and now a new paradigm is being observed that is called the 5th Industrial Revolution, of which the purpose is to enhance man's capacity and to benefit society and people by the use of technology [4]. It involves the use of artificial intelligence in man's common life, to return man to the "Center of Universe" [3]. The fifth Industrial Revolution contains advanced IT technologies, IoT, robots, augmented reality, and artificial intelligence, which not only will be used in every man's common life, but also in industry, healthcare, and other fields to provide benefits and convenience to man [5].

Industry 5.0 is the future stage of evolution, in which human creativity will collaborate with smart systems, such as robots and machines, especially in the production plants and warehouse systems. Due to this, humans can use their creativity for more responsible tasks and machines will take over the repetitive and monotonous tasks that will help in elevating the quality of production [6]. The second vision of Industry 5.0 is to make production plants and industries faster, efficient, and more scalable. It will increase the human–machine interaction by good interfaces, and improve the automation of robots programmed by the creativity of human beings, which will increase productivity multiple times [7].

The world will be transformed into virtual replicas as a result of Industry 5.0. The debate over the effects of high automation was triggered by an automated machine that was not supervised by a human. Wireless connectivity, sensors, and big data are the foundations of the IoT. Extreme automation, to the point that "everything is connected to everything else", creates weaknesses that lead to systematic dangers [2]. To overcome the absence of symmetry in Industry 4.0, Industry 5.0 introduces new symmetrical innovation concepts. It uses innovation brakes, next-generation technologies, society research, and orthogonal safe exits to address the difficulties related to Industry 4.0 innovations, automating manufacturing, and production [8].

Industry 5.0 has remained a theoretical perspective since 2018, emphasizing the development of intelligent IoT for industrial and commercial operations. It supports various concepts of Edge AI, blockchain over IoT, and various other domains, that we will discuss later in this paper. This field has opened a vast research ground for the researchers We analyzed the Google trends that we used to see the trends in Industry 5.0. The last past five trends have been shown in Figure 1, which indicate the increasing intent of researchers towards this domain [6,8].

It is evident, from the picture above, that a lot of centric research is being conducted for the development of better perspectives under the domain of Industry 5.0. A total of 416 research papers have been published since the foundation paper was published in 2018. It, therefore, opens ground for innovative networking and automation technologies. The perspective has majorly evolved for the automation of industrial and production processes, which is the major intent behind the work of this research. These authors have found this topic to be a progressive domain for which to conduct research and propose solutions.

The rest of the paper is organized as follows: Section 1 defines a brief introduction of the paper that includes the motivation for this article and Industry 4.0. Section 2 contains the introduction to IoT. Section 3 illustrates the findings from different research papers. Section 4 presents the observations and derivations for the major challenges, key findings, and the implementation of the analysis of IoT in different industrial sectors. In Section 5, the concept of Smart World is discussed and how it can be achieved by the amalgamation of various cutting-edge technologies with IoT. Section 6 describes the contribution of IoT in performance indication. In Section 7, the various challenges of IoT related to platform shift are elaborated. Section 8 points out the industrial achievement of IIoT. The future scope is covered in Section 9. Section 10 ends the paper with a detailed conclusion of the study.

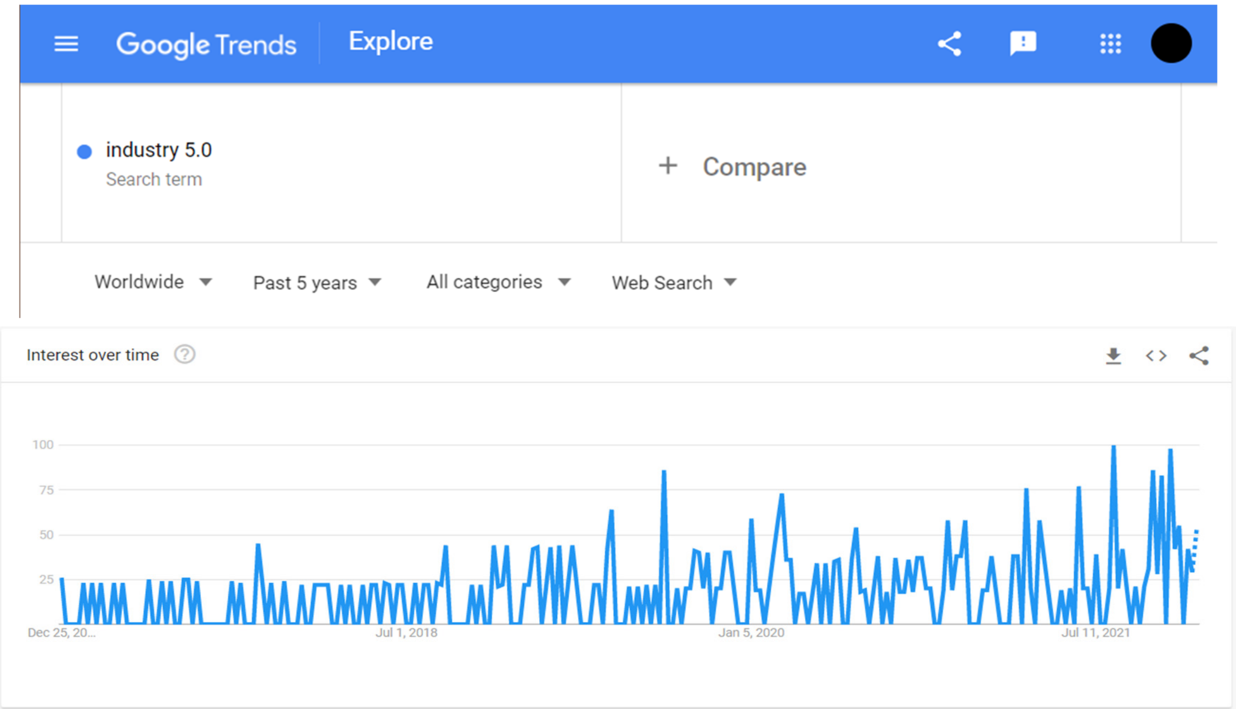

Figure 1. Research publications related to Industry 5.0 over the last 5 years.

1.1. Motivation for the Article

Industry 4.0 has transformed the warehousing and manufacturing sectors by incorporating new technologies domains, including data mining, machine learning, and IoT. The main purpose of the Fourth(4th) Industrial Revolution is to make industries smart through the use of machines that can control each other forever [9]. Industry 4.0 focuses on industrial automation, improving mass productivity and performance through the use of intelligent machines by reducing human intervention. Researchers and scientists are always motivated to find solutions to benefit society by making constant advancements and innovations in technology [2].

Industry 5.0 introduces the leverages that are the unique creations of human beings, along with the collaboration of machines. It will increase manufacturing efficiency and constantly monitor machines under the supervision of human beings to enhance the quality of production. The Fifth Industrial Revolution also promotes more skilled jobs, as intellectual and creative minds work with machines to enhance customer satisfaction [10]. Industry 5.0 also protects the natural environment through more accurate decision-making, using predictive analytics and operating intelligence. Hence, the authors identified the importance of writing a descriptive research review on industrial automation using IoT and Industry 5.0. Studying the challenging prospects of Industry 4.0 and the solutions in the production of plants and warehouse automation using IoT and Industry 5.0, is presented in this study [11].

1.2. Industry 4.0

Industry 4.0 is often named as the Fourth Industrial Revolution in research papers, i.e., 4IR, as it shows the changes or the revolutions that occur in the production or manufacturing methods followed in traditional industries [3]. These changes have been achieved by enhancing Industry 3.0, which occurred with the usage of computers in industries. These computers are used more efficiently in Industry 4.0 when IoT was introduced in operational and digital domains, machine learning, and other technologies, to make machines smart, autonomous, or less human-dependent [12]. Since 4IR machines are smart enough to analyze or diagnose the issues, it has made communication between the product and production tools for improved monitoring and tracking possible [4].

1.2.1. Evolution of the Internet to IIoT

In industries, we have implemented IoT to reduce labor waste and to monitor and inform the competent decent owner regarding the relevant measures. However, it will not fulfil all of our requirements as it can be prolonged, and danger can sometimes result in both assets and human lives being harmed [13,14]. The IIoT is a new addition to the world of technology that is altering the great industries of transportation, manufacturing, energy consumption, extraction, and mining [15]. For the future, producers are trying to enhance the commercial automation system by combining IoT and artificial intelligence. AI with IoT are nowadays being used like robots, but they are not very efficient as they have limited intelligence, and the proper integration of artificial intelligence with IoT in industries can be more beneficial to the owner of the company to maximize profits as there will be no need for human labor resources [16]. It covers the goal of intelligently connecting resources that can work together as a system, eventually leading to smart manufacturing sectors [17]. Now, after discussing the evolution of the network, the authors ask the following question: what evolution has IoT brought to the different industry sectors? IoT works in connection with various techniques and technologies, such as advanced ML algorithms and protocols, to provide every sector with a better reach, higher quality, and an interactive environment [17].

1.2.2. Technologies for Communication and Security

The benefit from deploying IoT technology to boost efficiency and productivity, runs counter to the cyber security goals of keeping out attackers. The IIoT makes use of IP-based communications and network standards, and this can lead to cyber-attacks [18]. With more access points, attackers will have more opportunities to obtain access. The ability to take control of remote control increases as the number of remote controls increases. In the industry, the hazards of inadvertent breaches, industrial espionage, and state-sponsored attacks on production settings have considerably increased [19].

We were assigned the bulk of the technological solutions used in the industrial sector by proprietary technology companies, which make the communication between equipment extremely challenging. In most situations, these interoperability issues have resulted in technological reliance. As a result, until interfaces, protocols, and applications are standardized, the connectivity necessary for Industry 4.0 deployment will potentially be costly, inefficient, and perhaps dangerous. As a result, the ongoing innovation in open hardware and software is critical to accelerate the improvements in the fields of manufacturing plant monitoring, industrial control, and interoperability while maintaining cheap costs for small and medium-sized businesses [20].

The existing industrial companies are currently being converted by Industrial Revolution (IR) 4.0 standards, to optimize the production rates and monetary profits, thanks to the introduction of contemporary communication and control systems. Traditional resources are repurposed as sentient entities that can detect, act, and react in a smart environment. The application of IR 4.0 in the industrial sector is projected to result in increased production flexibility, mass customization, greater quality, and increased efficiency [21].

New technologies, such as IoT, IoS (Internet of Service), and service oriented architecture (SOA), are projected to fulfill the needs of rapidly changing market demands in the industrial systems; these new paradigms introduced the physical operational technologies (OT) and cyber information technologies (IT). Both of these complementary domains are dissimilar. In relation to the convergence of these two domains, structural connectivity and functional interoperability are required for the components of the system. An interoperability layer that maps the field device data to the ISA95-based information model is proposed to migrate the legacy industrial systems to the IT–OT levels of technologies in a cost-effective manner, and requires no changes to the legacy devices [22].

The effective communication between advanced cutting-edge technologies, such as IoT, CPS, Industry 4.0 and 5.0, becomes a great challenge. To achieve a seamless connection, secure interoperability, and functionality between the distributed systems, different protocols, architectures, and systems are presented with the heterogeneity of hardware and software. In this context, open platform communication (OPC) and unified architecture (UA) combine to support the connections for the automation, intelligent systems, and large infrastructures by their powerful methods [23].

The automated production systems (APS), with the combination of production systems, require high flexibility, scalability, and interconnectivity. The research activities and current existing systems focused on the development of standard architectures, but all these system architectures lack general use cases and realization techniques. This paper collates the requirements from three research projects and presents a general system architecture that overcomes the limitations of specific system architectures [24].

For security, advanced tools are used, such as the Next-Generation Firewall (NGFW), IDS and IPS, and Sandbox. These tools are used by organizations as well as by individuals, as any network's first line of protection is its firewall. A firewall is a hardware or software device that is often positioned at the top of the network, to operate as a guard to monitor both the ingoing and outgoing traffic [20]. Intrusion detection and prevention systems, or IDS and IPS, are mature network-level defenses used in hundreds of computer networks around the world. Intrusion detection systems (IDS) are devices or software applications that analyze the network and/or network activity for illicit behavior or policy changes [21]. Intrusion prevention systems (IPS) perform the same analysis as IDS, but they are installed in-line, between other network components, and they detect harmful activity, log information about it, seek to block it, and report it. The simple network management protocol (SNMP) is also commonly used to simplify network device management from a central location. SNMP is a protocol that allows network managers to collect information about and identify devices on a network, such as hubs, bridges, routers, and switches [6].

1.2.3. IoT-Based Architecture in Industrial Automation

The architecture followed by industrial automation systems, based on IoT, generally follows architecture that has 3 layers [22], which are:

- Detection/sensors layer;
- Communications layer;
- Application layer.

The smart sensors, remote I/O, smart camera, radio frequency identification (RFID) tag, and switches are held in the sensing layer to collect information. The network or communication layer contains the communication technology, fiber optic, 2G/3G mobile communication network, Wi-Fi technology. The data will be transferred from this, i.e., the network layer, to the application layer. There are several protocols of communication in the network layer, according to the different requirements, such as security [6]. Every protocol has its pros and cons, but MQTT is mostly used as it can handle high latency networks. The IIoT application layer is the industrial control center. This layer contains the display units, final controlling elements, auto-contractors, and resource planning, safety, and security management; furthermore, users can integrate data analysis to obtain some intelligent decisions of the control and services. All the technologies in the architecture are effectively employed together to provide the automation of the process, communication, and calibration [23].

1.2.4. Research Methodology and Selection Criteria

The major intention behind this research is to discuss the automation of production plants and warehouses using IoT. The 4IR has brought about tremendous change towards smart industries using IoT [3]. In this paper, the authors analyze the methods and technologies proposed by other researchers to better understand how autonomous machines can be efficiently used in Industry 5.0, which further minimizes human intervention by introducing robots in the industries.

For this review paper, the authors have performed a thorough examination of research that has already been performed. For the enhanced understanding of the effective usage of Industry 5.0, the authors have performed a broad analysis of the available material [23]. The authors have briefly discussed Industry 4.0 and IoT to set a strong base for our paper. Then, the authors have discussed the main pros and cons of the different technologies, frameworks, and approaches suggested or discussed in the papers under review.

Comprehensive research is performed regarding all the selected material by reviewing different journals, websites, and conferences. These materials have been gathered from Google Scholar by entering keywords, such as "IoT in the industry", "smart industry and IoT", "industrial 5.0", and "industrial automation and robots". Table 1 shows the resources accessed for an in-depth knowledge about industrial automation, IoT, Industry 4.0, and 5.0.

Table 1. Research resources.

Keywords	Springer	IEEE Xplore	Science Direct	ACM
IoT in industry	77	67	182	15
Smart industry and IoT	77	73	40	20
Industrial automation and robots	2	251	43	18
Industrial 5.0	35	155	114	18
Industrial 4.0	33	53	20	19
Blockchain for IoT	66	21	16	20
Industrial automation using IoT	34	29	106	10

"Internet-oriented" refers to the technologies and protocols implemented to ensure the improvised networking of the physical devices and their connectivity on the internet. "Things-oriented" refers to the electronic devices (for instance, sensors, actuators, RFID, LTE, Z-WAVE, NFC, UWB, and M2M) connected to the internet. The semantic-oriented type deals with the challenges of data management, which occurs due to the immense information shared by the smart devices. Due to the improvements to wireless technologies, the IoT has gained significant popularity and has garnered the attention of the SCM community [24]. IoT has greatly contributed to industrial automation and allowed the incorporation of industrial sensor networks for various SCM functions. The term "Industry 4.0" has also been coined by the German economic development agency (GTAI), to indicate the 4th Industrial Revolution, which is conceptually described as assimilating the IoT technology to automate the industrial manufactories process and enhance the intercommunication of the machines. This concept has proven to be a vital success criterion for providing various business benefits, such as the optimization of business operations and value chain activities. Therefore, the IoT will continue to enable various functions and operations in various industries, to make them as efficient and effective as possible [25,26].

1.3. Supply Chain, IoT, and Big Data

IoT devices, such as cameras, GPS, laser tags, and battery-assisted passive (BAP) tags, can be used for effective project management in the SCM. The constant availability of real-time information is far more beneficial than manually updating it every few hours, and some of the most important areas of big data and IoT include the real-time reaction, which is the ability to meet demands of the client. Cloud computing, along with digital devices, helps to reduce the time gap between the order and shipment of the product [27]. IoT also enables these technicians to operate this machinery from a distance and this avoids the extra time and hazardous locations and conditions. The traceability of construction manpower directly impacts the cycle and has a critical risk factor. With GPS, the users can keep count of the number, strength, and location of the active hours on the site.

1.4. Existing Survey Deficiencies

So far, the literature review on IoT has remained theoretical, with a focus on IoT's applications but not on its functioning procedures and benefits. Its operational quality has rarely been analyzed. Recent research has provided a comprehensive analysis of IoT's utilization in transportation, but it did not confer its significance across its use in the supply chain [14]. Another study also provided an optimistic link between IoT-enabled supply chain integration (SCI) on the supply chain, but it did not provide evidence for the implementation of the use cases in the real world or industries. An analysis of the operational procedures is required to find how each technology will work and to what extent they will be efficient in each step of the process [26]. The technology's sustainability research is required to find any problems or risks in its use case, so that any insufficient/deficient process can be refined in the future.

Therefore, in this review, the authors will explore the following research questions:

- How can digitalization and IoT improve the industrial sectors, mainly the supply chain management cycle?
- How does IoT implementation affect the internal and external cross-communication of the organizational stakeholders in content to the SC performance?
- How much impact does IoT's implementation have on the performance of the supply chain of an organization as well as on its sustainability?
- How can various IoT devices impact the flexibility, traceability, quality, cost, and monitoring in SCM?
- Is IoT and modernization always beneficial, rather than a manual supply chain?
- What future enhancements can be applied to this sector that can simplify and improve workload and tracking in the future?

As of now, there are various theoretical models for Industry 4.0—one of the ways being the formation of smart factories that can keep track of all the information being exchanged within and around them using blockchain. Even though these are excellent innovations for the future, there is a dire need for the developers to come up with standardized testing practices that are widely agreeable to evaluate the near-accurate measurement of stability, performance, efficiency, and security of these systems [27]. Only then will consumers choose such technologies, and authors can deduce that IIoT has been truly successful in taking the world a step nearer to becoming a smart hub.

2. Introduction to IoT

The concept of IoT emerged in the summer of 2010. Data has revealed that Google's Street View service not only creates 360-degree images, but also stores a vast amount of data on human Wi-Fi networks. Whether this was the beginning of Google's new strategy for not only targeting the internet, but also the world, it became a hot topic [28]. The IoT is a system of interconnected computing devices that are equipped with unique identifiers and the ability to transport data within a network without the need for human-to-human or human-to-computer interaction, according to the technical definition. The devices can either be mechanical or digital. The basic idea of IoT is to take all physical devices around the world and connect them with the internet [29,30].

2.1. Applications of IoT

Since its invention, IoT has been implemented in various domains and fields, including agriculture, health, industry, home automation, automobiles, and energy engagement. In this article, the authors discuss one of the most popular applications of IoT in the field of industry [31,32].

2.1.1. IoT Application in the Business Area

When discussing different IoT applications, predictive monitoring and maintenance are better discussed as they involve several sensory data, such as temperature, density, vibration, temperature, voltage, and current, using machine learning models. These models are capable of making predictions related to failure [33]. The industrial sector wants to lessen the number of incidents and any accident, failure, and breakdown. Any machine having sensors can collect the data, and the data will be used for the training of the ML model, which will lead to the provision of accurate probability and prediction.

2.1.2. IoT in Process Automation

To increase the efficiencies and the reduce costs of the different processes in warehouses, plants, and factories, the world is moving towards automating the mundane and repetitive tasks to free humans, so they can think for high-level activities. Different industries use different ways to automate the process, such as robots, IoT, and software [11]. In industrial processes, IoT is used to track and monitor the analytics of different machines. In production plants, IoT monitors the temperature and pressure and switches different processes on and off, based on the conditions. It also monitors harmful gas leaks and rings alarms to inform the industrial managers about danger.

2.1.3. IoT in Production Testing

In production testing, IoT is used to test the quality of different products to reduce the time and cost of testing. To test the quality of the product, different sensors with IoT devices are used with the combination of machine learning models. ML models in IoT identify the object, then test its quality using sensor data and provide quality level feedback of the product to the managers. If the quality level of the product is low, then it separates that product from the high-quality products using cranes. In this way, manual work and costs are reduced by automating the whole flow using IoT.

2.1.4. IoT and the Supply Chain

The IoT (IoT) is a global platform of internet-connected smart devices that enhance supply chain ICT infrastructure for an improved internal and external connectivity with suppliers and customers. The observation of storage conditions throughout the supply chain, product tracking for traceability, payment processing based on the location or activity time in public transportation, and other benefits of incorporating IoT in supply chain management are just a few examples [34]. IoT can be used to direct customers in a store, based on a pre-determined list, to automate payment processes, such as automatic check-out with biometrics, to detect potential allergen products and to control the product rotation on shelves and warehouses to automate restocking procedures.

2.1.5. Temperature Monitoring/Controlling System

Mining, refining, extraction, transportation, and other operations in the industries increase the temperature levels. The temperature is monitored in the oil and gas industry to ensure the system's overall safety [31]. The temperature is monitored in the food industry to ensure food safety. The sensor communicates with the process station, which collects the temperature data and sends it to the cloud. Some algorithms are used to determine if it is within the required range or not. After that, if necessary, corrective actions are taken [35].

2.1.6. IoT and the Control Systems

Control systems are the main element in factory automation, as the integration of physical systems with the internet requires a collaboration with ICT experts; the sensors can be connected to the actuators through algorithms over the internet to obtain some level of performance, for example the flow, temperature, and pressure sensors can be used in a manufacturing process that involves chemical mixing [14]. To control the chemical process, the sensors take constant readings. Each sensor has an IP address, which allows the controller to determine the location from where the reading was taken. The controller and the sensors connect via Ethernet or Wi-Fi [6]. If the chemical used in the process heats to more than the required temperature, then the controller quickly takes control by controlling the power that is given to the heater. When the controller notices trends toward failure levels, he or she can take the necessary measures to mitigate the issues. When the technicians receive alarms from the controller, they can evaluate the problems in real-time and take corrective action, or they can analyze the problems later [7]. The data gathered, stored, and/or communicated in real-time by the controller, provides a complete picture of the process. By controlling the quality after evaluating the actual process, engineers can identify the process conditions and determine if there are any quality issues [15].

2.1.7. IoT and Energy Efficient Systems

An application of IoT lies in making an energy efficient system for the industry, which incorporates an IoT layer. This layer groups all the problem-causing sources, i.e., the loads with variations that decrease the power quality and increase the energy usage. It sends the statistics to the central processing server, which decides on whether to change from a traditional power store to node for the synchronous optimization of power [19]. The architecture of an energy efficient system using IoT is designed to use the concept of sensor area network, by observing the various loads linked to it in real-time. Therefore, the temporary behavior of the loads shows the changes linked to the quality of power owing to the direct (not inline) performance of the grid loads. The variations can be a drop or rise of the voltage, power components, and changes in the harmonics. A measurement sample is created and analyzed to inspect the subsystems for detecting any such issues [7]. With the results presented in the study, the suggested industrial energy consumption system utilizing IoT improves the power quality and can be applied for following ISO 50001, the latest guidelines [16].

2.1.8. IoT and the Intelligent/Smart Manufacturing System

Smart manufacturing is the foundation of Industry 4.0, and combining IoT technology with manufacturing science is the cornerstone of smart manufacturing. It integrates IoT technologies with current manufacturing processes to drive production and alter the traditional workshop management style [9]. The smart manufacturing approach employs the methods of Industrial IoT to track and monitor workshop goods and equipment, as well as intelligently control the production procedure. The smart control of the manufacturing procedure performs the self-activating decision-making process by utilizing a knowledge base for the decision making, and by storing, analyzing, and processing related manufacturing data [26]. Anti-interference, rapid deployment capabilities, convenient expansion, and security are the important performance factors for the systems that are used for production line data monitoring, to achieve intelligent manufacturing. The functional model of the system comprises of six modules that are the monitoring of the workshop, system login, DNC (Direct Numerical Control), warehouse management, statistical analysis, and product tracking. The client/server model is currently the most used computer model [27]. As the system involves a large volume of data exchange, multi-thread real-time data collection, as well as quick real-time interactive responsiveness and data security, is required. As a result, the traditional client/server architecture is used, and field-level end-devices and the workshop are linked via IoT.

2.2. Challenges of IoT

IoT has brought the world several advantages in almost every area of life, but it has also brought some major problems in terms of cyber security. It is very difficult to keep track of all the physical devices connected to the internet. Any vulnerability or cyber-attack can take down our entire IoT-based system [32]. In 2017, hackers used IoT thermostats to gain access to a casino's network and hack its data. Parents have also reported that some strangers on the internet tried to access their children's baby IoT monitor and tried to talk to them.

IoT has its own set of difficulties and implications that must be addressed before widespread adoption can occur [34]. Even while existing IoT enablement technologies have vastly advanced in recent years, there is still a slew of issues that need to be addressed.

Despite the significant advancements in monitoring and sensing technologies, sensors and actuators are typically required to continuously remain active to acquire instantaneous data—this aspect makes energy efficiency, particularly in terms of lifespan extension, difficult; thus, organizations must employ energy optimization techniques.

Another industrial challenge is the selection of appropriate communication technology; device communication protocols, which are the driving force behind the implementation of IoT applications, are the major support of data flow between sensors and physical objects or the outside world [33].

3. Literature Review

The following table (Table 2) outlines the findings obtained after a thorough study of field-related research papers. The key findings of this study contain the proposed technique, issues addressed, strengths, weaknesses (in Table 3), good and bad points of the proposed architecture, network security, technology, material devices, and the future scope of improvement. The technique proposed addresses the methodology used to solve the addressed issues in implementing IIoT. Then, the strengths and weaknesses of the proposed methodology are covered. The architecture, in terms of the advantages and disadvantages, is defined. After that, the network schemes applied to IIoT for security are mentioned. The communication technology and the devices used in the proposed architecture are mentioned. Finally, the future scope of the improvement of the corresponding proposed solution is presented.

Table 2. Current work analysis.

Paper Title	Technique/Proposed Methodology	The Issue Highlighted/Addressed	Proposed Architecture: Positive and Negative Points	Network Security Strong/Weak Also Named Security Schemes Applied	Technology	Material/ Devices Used
[35]	For large-scale industrial automation in Industry 4.0, narrowband IoT (NBIoT), a low power wide area (LPWA) technology, is proposed.	Industrial automation using IoT on a large scale consumes a large number of resources in terms of energy, bandwidth, and cost, which makes industrial automation a great issue.	No architecture is proposed. The paper highlights the benefits of using NBIoT in today's large-scale industries.	In this paper, no such network security scheme is proposed or used.	Wi-Fi	IoT devices, sensors, actuators.
[36]	The absolute innovation management (AIM) framework is proposed in this paper, after reviewing the literature on the already proposed models and frameworks, to efficiently manage innovations with the emergence of IoT and Industry 5.0.	In the age of IoT and Industry 5.0, as well as the rapid advancements in information technology, innovation management and integration with business processes have become a major challenge.	The positive point of the AIM a framework is that it makes the innovation process more human-centered and also helps in making the process fast. The negative point is that the framework is just a proposal and needs further work and experimentation to make it implementable.	In this paper, no such network security scheme is proposed or used.	N/A	N/A
[37]	Develop an industrial automation system using reusable artifacts and the domain repository.	The complex automation functions and the technical process that uses real-time requirements.	This approach reuses work products, such as models of the technical processes and automation solutions.	No specified network security is used in this proposed concept.	N/A	Sensors, actuators, PLC, bus system.
[38]	IConnector offers system-dependent interfaces for industrial automation as well as universal interfaces for IoT.	The interconnection between the existing industrial automation systems with IoT, even if a different protocol of communication is used for industrial automation.	This method allows existing systems to handle internet technologies and thus participate in Industry 4.0.	Different communication protocols are used in this approach.	Various communication protocols.	I4.0 connector.
[39]	The technique of virtualization is used to visualize the industrial environment before implementing physical constraints, so that the cost, storage, and efforts can be reduced.	The high-cost requirements and risks associated with industrial testing and warehouse challenges in bulk testing and phenomenal quality assurance.	The proposed architecture is based upon the selection of tools and their impacts that provide a detailed platform to test and conduct QA on the industrial systems. The positive point is that the system is based upon conventional desktop tools and does not require heavy technical investments for deployment; however, the negative point is that the lack of sufficient technical knowledge and higher hardware-based operation may not be included under the scope of this architecture.	The virtualization architecture does not include specific network deployment. It only focuses on the automation of industrial test processes by any means that can help to reduce the risks and costs associated with physical testing.	Does not include any specific network recommendation to analyze the communication constraints.	Industry literature and case studies of system failures due to physical testing approaches.

Table 2. *Cont.*

Paper Title	Technique/Proposed Methodology	The Issue Highlighted/Addressed	Proposed Architecture: Positive and Negative Points	Network Security Strong/Weak Also Named Security Schemes Applied	Technology	Material/ Devices Used
[40]	The theoretical basis for the project's analysis and construction was based on a survey on IoT and Industry 4.0. The quantitative analysis of the systematic review results provided an overview of the existing studies on IoT and Industry 4.0, as well as their significance.	The bibliographic research was carried out with two purposes: to gather knowledge about the concept of structured and unstructured data that compose the health area, and to find primary studies on the subject.	Does not include any specific network recommendation to analyze the architecture constraints.	Does not include any specific network recommendation to analyze the security constraints.	Does not include any specific network recommendation to analyze the communication constraints.	Web of Science and Semantics Scholar.
[41]	A secure wireless technique using wireless sensor networks.	This paper describes the implementation of one such WSN that can be used in industrial applications.	Does not include any specific network recommendation to analyze the architecture constraints.	Does not include any specific network recommendation to analyze the architecture constraints.	Wi-Fi and Bluetooth.	Sensors, IoT devices, actuators.
[42]	This study provides a detailed overview of virtualization in industrial automation for architecture sustainability.	This study highlights the issues faced in the different industries and recommends the solutions to automate industry techniques.	Does not include any specific network recommendation to analyze the architecture constraints.	Does not include any specific network recommendation to analyze the architecture constraints.	Wi-Fi	IoT devices, sensors, actuators.
[11]	The network's security and quality of service (QoS) are being enhanced at the moment.	This study focuses on the industry's inability to adapt to Industry 4.0, IoT, blockchain, and business analytics.	It does not propose any architecture to implement these technologies.	It does not include any recommendations to improve network security.	Wi-Fi	IoT devices, sensors, actuators.
[43]	This paper explores the various systems that can be developed by integrating IoT with blockchain to give rise to the fourth wave of IIoT, i.e., Industry 4.0. By utilizing the decentralized, distributed approach of blockchain, many systems can be made, including electric vehicle clouds and edge (EVCE), mobile commerce, trace food source, cloud storage, authentication and access management, big data, smart homes, and smart cities. This is because blockchain can record and sync the transactions and save information.	Security concerns of IIoT devices that inhibit the development of Industry 4.0 are scrutinized in this paper.	The discussion conducted by the authors is purely observational and theoretical; therefore, no architecture has been proposed to develop the mentioned applications. However, their research has emphasized how blockchain can advance all current systems in industry-based IoT.	The authors have highlighted blockchain to be the technology behind resolving network security issues for the mentioned IIoT systems. Anonymity, asymmetric encryption, and distributed control are the added benefits of using blockchain. However, some security issues persist, such as the culprits being able to form patterns from the publicly available information of the transactions and tracing roots of involved parties to dismantle the formed system.	Blockchain and a working Wi-Fi system are the main mediums of communication for all the applications.	The paper does not discuss the material/devices used to develop the systems.

Table 2. *Cont.*

Paper Title	Technique/Proposed Methodology	The Issue Highlighted/Addressed	Proposed Architecture: Positive and Negative Points	Network Security Strong/Weak Also Named Security Schemes Applied	Technology	Material/ Devices Used
[41]	The paper proposes a blockchain-based fair non-repudiation service provisioning scheme for IIoT scenarios, for which blockchain is used as an evidence recorder and service publisher.	There are several issues in the distrusted and distributed IIoT scenarios, due to malicious service providers or clients who can deny service provisions or usage for their interests. Traditional non-repudiation solutions are less effective in IIoT environments because of the demands of trusted third parties or unacceptable overheads.	• Low bloating rates; • Less transaction latency; • Less gas consumption.	Smart contracts.	Blockchain.	IoT clients and service providers.
[40]	This paper proposes the implementation of blockchain to support hierarchical storage for Industrial IoT architecture, and to provide immutable and verifiable services.	1. Most existing IIoT infrastructures work on a centralized architecture, which is easier for management purposes but cannot effectively support the immutable and verifiable services among multiple parties. 2. One of the most challenging problems when bringing blockchain technology into IoT applications is storage.	• Blockchain can prevent modification of data; • Blockchain can enable a trusty network; • The data is safe from tampering as it is decentralized; • Blockchain enables devices to be anonymous through smart contracts.	A blockchain connector is used to access control, manage permissions, verify and validate transactions.	Blockchain.	IoT storage, Data Engine, Gateway.
[44]	This paper proposes a technique to divide the architecture into two networks, namely the on-chain network and the off-chain network. The on-chain network will deal with the online transaction and digital signatures to ensure that the communication between our consumers and manufacturing resources is efficiently conducted and that smooth data transmission occurs. The off-chain network, on the other hand, will deal with the storage and load that checks correct code execution. In this way, network latency and load is made efficient.	Addresses the security, trust, and island connection problems in the process of Industrial IoT ecosystem construction, with blockchain techniques and smart contracts introduced into IoT.	Positive Points: 1. It uses mechanisms to enhance security; 2. It splits the network into the network to cater for blockchain issues, such as load and latency; 3. It resolves the trust problem between components with the help of a digital signature and access control mechanisms.	The network is highly secure as they have used secure multi-party computation and a secret sharing mechanism to guarantee data security and privacy.	Blockchain.	IoT Unit.

Table 2. *Cont.*

Paper Title	Technique/Proposed Methodology	The Issue Highlighted/Addressed	Proposed Architecture: Positive and Negative Points	Network Security Strong/Weak Also Named Security Schemes Applied	Technology	Material/ Devices Used
[43]	This paper proposes the implementation of blockchain to automate the conventional system used for the supply chain, so that data can be stored without possible errors and the thefts of goods.	The issues addressed in this paper are that the conventional systems do not usually offer the required amount of trust between the parties, they do not offer transparency of data, and they are usually prone to external attacks, such as theft and hiding information.	This paper only focuses on the benefits of automating the process in contrast to the conventional methods; hence, it does not possess explicit data regarding the said matter, except the strengths of the proposed technology. However, the data has greatly helped in setting the basis for carrying out the entire survey process.	Only provides a general overview and does not provide extensive research on how the said architecture is implemented.	Cryptographic keys, peer to peer communication.	Sensors were mainly used to keep track of the various products, to maintain the clean inventory records.
[45]	This paper proposes a mechanism that works on credit-based consensus for blockchain that enables the verified nodes to consume less power, whereas this makes it computationally difficult for the malicious nodes to penetrate the system while increasing the efficiency and throughput of the network.	The issue highlighted in this paper is that the chain structured blockchain-based systems cannot verify the continuous stream of data that is an integral part of the industrial sector; hence, the workflow of the system becomes slow and congestion starts occurring, resulting in the decreased performance of the network.	The positive point of the proposed architecture is that it greatly helps in enhancing the efficiency rate of the system and is extremely practical in various IIoT scenarios. The worst-case scenario is that it is still in its research phase; hence, it can only store a limited amount of data and is unable to have control over the quality of the sensory data.	The security of the network is extremely high as it is almost impossible to launch an attack on the network, because of the immense number of resources required to computationally solve complex mathematical problems to gain verification for carrying out illicit activities.	Raspberry Pi is used as the communication medium.	PC is used as the gateway, whereas Raspberry Pi Model 3B is used to serve the purpose of an IoT device.
[46]	This paper proposes to revolutionize IoT with the integration of blockchain and cryptocurrencies. It emphasizes the positive changes that will be seen when blockchain is used for data sharing throughout. It proposes a full node and lightweight node blockchain that enables IIoT architectures.	Many existing IIoT foundations depend on a centralized design, which is simpler for the board yet cannot effectively uphold the unchanging and unquestionable administrations among different gatherings.	The proposed architecture reduces redundancy, increases the security and privacy in data sharing, and makes the approach more efficient.	The network is highly secure, as data sharing through blockchain is safer than the conventional methods.	Blockchain.	IIoT service client, IIoT resource platform.
[47]	The lightweight blockchain platform for E-commerce transaction management, using the consensus mechanism called practical byzantine fault tolerance (PBFT)	The privacy and security concerns of IIoT devices that affect the development of Industry 4.0 are described to the point in this paper.	The industries of different sectors can benefit from the proposed architecture, a lot of examples of different sectors are given and reviewed in detail.	This 3-layered blockchain network is shown not only to be highly scalable and efficient but also to be secure against cyber-attacks.	Blockchain	PCs with sufficient computational powers are required.
[14]	The present study proposes several communication protocols and devices, the most effective of which are the LoRa protocol and ARM Cortex.	The study highlights the issue of the selection of the communication protocols and IoT devices in industries, and which technology is preferable for communication.	The architecture is based on the ARM Cortex and LoRa communication protocol.	The network security is strong. The LoRa protocol uses modern cryptography technology, which makes it very secure by design.	LoRa and Bluetooth protocols	ARM Cortex and Arduino.

Table 2. *Cont.*

Paper Title	Technique/Proposed Methodology	The Issue Highlighted/Addressed	Proposed Architecture: Positive and Negative Points	Network Security Strong/Weak Also Named Security Schemes Applied	Technology	Material/ Devices Used
[16]	This study focuses on the merits that Industrial IoT brings to the industries operating in different parts of the world, along with the challenges that arise due to IIoT.	This paper highlights the issues related to the lack of privacy in IIoT, and suggests a more thorough focus on the architecture of IIoT-based software to ensure that the interconnected devices are protected from any new attacks from communication channels. Additionally, the issues related to the lack of IIoT standards and cost for implementing IIoT are discussed.	Technology acceptance model to study the Fijian system—this model includes 8 major factors that show that the results of the test are: self-efficiency, risk cost, perceived usefulness and ease to use capability, actual use, compatibility, actual use, and behavioral intentions.	It analyzes the security of the present IIoT that, due to the lack of encryption techniques and absence of laws and regulation, can be attacked by unauthorized parties. This issue can be resolved if authors focus more on the encryption techniques for IIoT and the laws and regulation can control the unauthorized access.	Wi-Fi and Bluetooth	RFID tags, Wi-Fi, and sensors.
[17]	This study shows the overview of IoT in industrial automation, and discusses some of the advantages and disadvantages of automation and combined it with artificial intelligence to solve challenges.	Some challenges related to automation are highlighted.	Wireless communication and sensors, as well as RRFID-based architecture, are discussed, while it is further proposed to integrate IIoT with artificial intelligence to remove the disabilities present in commonly adopted architectures.	This paper shows the overview of IIoT that the network security of the present IIoT is not very good, but proposed that if AI is joined with IIoT so future security threats can be minimized,	Wireless sensor networks (WSNs).	RFIDs, CCTV, smart sensors.
[30]	The paper explains the usage of IoT in different domains, such as agriculture and industry, and also explains in detail all the research challenges that are faced in IoT.	The research challenges are highlighted, such as security, management of data, communication protocols, and interoperability. All these challenges are faced in IoT-based industrial solutions.	The paper proposes the fusion of blockchain and IoT, as blockchain is popular due to the security achieved by consensus algorithms.	for good network security, blockchain is used. The consensus algorithms used in blockchain will achieve the security of the network.	Wireless sensor networks (WSNs).	RFID tags, Wi-Fi, and sensors.
[28]	The paper explains the IoT-based architecture for industrial automation, and also explains the control systems used in industries that are based on IoT. it also explains the big data and cyber security view in IoT.	Some challenges are highlighted for security.	Proposed architecture: (IoT)-based architecture in industrial automation.	Good security, advanced network security, and monitoring tools, such as Generation Firewall (NGFW), IDS and IPS, Sandbox, anti-spam and antivirus, identity discovery, protocol analyzer, application control, and URL filtering.	Message queuing telemetry transport (MQTT), HTTP, and advanced message queuing protocol (AMQP).	IoT-based smart sensors; radio frequency identification (RFID) tag, remote input and output (I/O), and smart camera.

Table 2. *Cont.*

Paper Title	Technique/Proposed Methodology	The Issue Highlighted/Addressed	Proposed Architecture: Positive and Negative Points	Network Security Strong/Weak Also Named Security Schemes Applied	Technology	Material/ Devices Used
[7]	This article proposes an EMS based on the IoT (IoT) network that boosts the power quality for smart factories to establish an energy-efficient system. In addition, an architecture for improving the power quality in industries that follow ISO 50001 standards is suggested.	The electricity and fuel costs for industrial sectors has significantly increased in the past decade. Thus, factory owners needed to work on reducing the consumption of energy, by applying the factory energy management system.	Positive: architecture based on IoT will mitigate energy consumption and enhance the power quality of power electronic systems. This was verified through SIMULINK models, circumvents issues related to the reduction in power factors and the occurrence of harmonics. Negative: not applied to live-only in simulations, which means there are no unexpected situations. Can only figure out how well it works when applied to the actual world.	The paper does not mention any specific security safeguards.	M2M (machine-to-machine communications).	Simulink, MATLAB.
[21]	Presents an up-to-date review and evaluation of the IoT in the energy supply chain.	The traditional electricity supply chain is changing from uni-directional to bi-directional, but to further utilize the full efficacy, IoT would be needed to work with the existing smart grid and data analysis. IIoT challenges are faced.	No new architecture was proposed. Presents a review and evaluation of IoT in the electricity supply chain. IoT increases the utilization of smart grids, bi-directional electricity supply models.	The security of IIoT, in general, has a lot of room for improvement. No named security measures were mentioned. Thread (networking protocol) has some security measures in place. Utility companies have to keep in compliance with the privacy laws, such as the GDPR in Europe.	N/A	N/A
[46]	The purpose of this research is to examine the use of RFID (radio-frequency identification), IoT (IoT), and WSN (wireless sensor networks) in the industrial sector.	(1) Issues are related to the lack of a proper integration mechanism of RFID and WSN into the SOA (service-oriented architecture) in industrial applications.	(1) Proper analysis was performed and the proposed framework has a good presentation of data.	(1) HTTPS secured security moderate.	(1) Internet(ipv6), Wi-Fi, ZigBee, WiMAX, and 3G/4G mobile network.	(1) RFID, sensors, actuators, and WSN.
[4]	Service-oriented architecture (SOA)-based four-layer model.	This review paper addresses the IoT applications in manufacturing, sometimes referred to as the Industrial IoT IIoT. To that end, technologies related to the use of IoT in manufacturing to make it smart manufacturing.	SOA-based architecture aids in building effective IoT applications in manufacturing. whereas privacy, integrity, and technological barriers are major concerns.	This scheme has no official recognition of the security protocols, so it can endure the malfunction.	Cloud computing, WSNs, Bluetooth, and Wi-Fi.	Smart sensors.

Table 2. *Cont.*

Paper Title	Technique/Proposed Methodology	The Issue Highlighted/Addressed	Proposed Architecture: Positive and Negative Points	Network Security Strong/Weak Also Named Security Schemes Applied	Technology	Material/ Devices Used
[6]	Information technology system, IoT devices, and local shells.	Errors raise the production costs and offer quiet issues to emerge only under specific loads, posing a risk to safety and/or life.	Local shells and IoT devices are far best suited for these systems.	No such indication of security frameworks for this system; hence, the system can tolerate the fault	Information technology system	IoT devices and local shells.
[21]	It discusses the transfer of logistics on the internet and IoT, and enhances the operations by providing real-time updates while SAP works in parallel.	Improved the inventory management by using e-logistics to use real-time updated information through IoT with SAP, instead of updating it in the normalized system.	The architecture is only suited to those experts who have an understanding of both SAP and IoT. Through the real-time updating of the data stored in SAP, the costs can be reduced and the efficiency can be enhanced.	No specific security scheme is mentioned. The system is assumed to use the normal security associated with IoT so it can be moderate.	SAP enterprise software.	PC and IoT devices.
[22]	The benefits of IIoT and its challenges.	An overview of the latest advancements in the area of IoT-based manufacturing.	No architecture is proposed as it only discusses the benefits and challenges.	No specific security scheme is followed. The paper discusses various applications; hence, it is assumed that a mandatory level of security is maintained.	MODBUS, OPC, PROFIBUS, and MQTT.	IT system (ERP and CRM) with OT system (SCADA and MES).

Table 3. Recent literature evaluations and observations.

Paper Title	Strengths	Weaknesses	Future Scope for Improvement
[35]	NBIoT is very industrially friendly because of its low energy and resource consumption, cost-effectiveness, compatibility with cellular technologies, and simple connectivity. It provides long-term support and a sustainable production process.	This technology only supports low data rates and that is why a large amount or volume of data cannot be sent in a shorter interval of time, which makes this technology less effective as, in larger industries, a vast amount of plant information has to be transferred.	With further work on NBIoT, authors can make it feasible for larger data volume by increasing its bandwidth while keeping it cost-effective.
[36]	The AIM framework presents the innovations in such a way that they become more understandable, simple, clear, and implementable. This framework merges all the members of an organization in the innovations process, which makes the process quicker, makes the innovation process part of a routine activity, and adds more value to the innovations.	This framework is just a proposal after performing a thorough review of the existing options. The authors need to properly examine it to find out its cons. This framework is not a solution, but gives way to efficient innovation management in the era of IoT and Industry 5.0. The authors need to perform more tests to make it more authentic.	This framework is just an idea, not a complete solution or destination for organizations. The authors can make software based on this framework, so that production firms can adopt it to manage innovations.

Table 3. *Cont.*

Paper Title	Strengths	Weaknesses	Future Scope for Improvement
[37]	The reuse of work products, such as sensors, automation solutions, and auxiliary materials.	The artifacts, such as sensors, actuators, and PLCs, can be defective and not suitable for reuse.	Additional information of the domain repository and estimation using the case study can be planned.
[38]	Allows the existing systems to control the internet technologies that help to participate in Industry 4.0.	The research was limited to Industry 4.0.	The proposed concept can be helpful in the automation of industrial systems with minimum effort.
[39]	A good comparison of the software and hardware issues demonstrated alongside the benefits that can be achieved by the implementation of the virtual testing environment.	Does not include enough quantitative statistics to obtain the "extent" of success achieved during the test automation process.	Since all the industries have different work environments, it can be impossible to develop a single solution to assist in all the domains. However, the availability of common modules that can be customized and reused to optimize the process of deployment can be helpful to progress.
[40]	Based on the number of research papers produced, this graph depicts the industrialization trends and statistics. According to research, the industry themes 4.0 and IoT are relatively new, with only a few items addressing the two themes.	The article purely analyzes the flow of articles on the subject and does not have specific domain information on the matter. However, the research has helped in the selection of the papers for further studies.	With more papers developed in this domain and a greater number of architectures proposed, the research can then be modified to identify the architectures and propositions that are profitable, maintainable, reliable, and more secure among the developed systems.
[41]	The system is simple to set up and maintain. The WSN is unique in that it is a flexible, dependable, and low-cost system.	The network's security and quality of service (QoS) are currently being improved.	The WSN clusters can be used for the automation of various industries with the possibility of easy modification or expansion in the future.
[42]	This study suggests the strong and experimental methods that can be used in industrial automation to reach architecture sustainability.	N/A	Overall, it is clear that virtualization is a mature technology, which offers significant benefits in overcoming some architecture sustainability challenges.
[11]	This study discusses the applications of state-of-the-art researches and presents the different researches on the four mentioned technologies with their purposes. It also promotes these four technologies and identifies the forces driving them.	This study is limited to IoT, Industry 4.0, blockchain, and business analytics.	Further scope for improvement is to address Industry 5.0, robotics, and explore them in the agriculture and health field as well. Artificial intelligence algorithms can also be included, which is also the most important field to change the future of the industry.
[43]	The authors have rightly addressed the different applications or possible applications of blockchain-based IIoT, to innovate our current systems that can save resources and increase efficiency.	The authors have centered their work around the possibilities of blockchain-based IIoT and the advantages it will provide to improve current systems. Hence, no weaknesses have been highlighted.	The limitations of the powerful integration of blockchain and IIoT comprises of a relatively poor performance, increased complexity, some security concerns, and a lack of testing platforms and criteria that can be overcome in future works.

Table 3. *Cont.*

Paper Title	Strengths	Weaknesses	Future Scope for Improvement
[41]	The blockchain-based non-repudiation system offers significant performance with affordable additional overheads.	It assumes neither the client nor the service provider will perform any abnormal behaviors to damage their interests.	The authors intend to deploy our approach in a real network computing-enabled IIoT platform, for further practical evaluations. In addition, they would like to integrate more features, such as deposit and reputation mechanisms, to establish a more sophisticated and effective solution.
[40]	1. Blockchain technology provides many desired features for large-scale IIoT infrastructures, such as decentralization, trustworthiness, tractability, and immutability. 2. This paper focuses on solving the limited storage issue when introducing blockchain into the traditional cloud-based IoT architecture.	This work is the first of its kind to try to fix the storage issue on the chain level; hence, no weaknesses are mentioned yet.	As future work, the authors plan to work on the implementation of the proposed blockchain-based IoT architecture in more real IoT applications, and to thoroughly evaluate its other performances, such as latency and throughput.
[44]	1. It reduces the network load and latency. 2. Secure multi-party computation proposed that guarantees data security and privacy.	This architecture has proposed solutions to the expected weakness, such as the intercommunication between the on-chain and off-chain networks. As of now, no new weaknesses are witnessed.	The paper describes two applications of the architecture BPIIoT. However, further research can be conducted to ensure the use of blockchain to meet the legislative standards for industrial applications.
[43]	Since blockchain-based IoT systems offer solutions to the problems addressed by providing transparency, decentralization, efficient data storage, and most importantly the data is being protected because of the immense security offered by such systems; hence, the inventory can be maintained with great ease.	Since this paper only focuses on the benefits of implementing blockchain-based systems in the industrial sector, no such weaknesses have been discussed so far.	The presented overview will help the academic researchers to practically implement the architecture to automate the entire workflow of the supply chain management.
[45]	The proposed architecture offers the increased throughput and efficiency of the system, while providing an immensely secure network that provides privacy and access control over the data that greatly improves the performance of the system. Moreover, the proposed architecture makes it extremely difficult for the malicious nodes to initiate the attack as it would be computationally expensive to carry out such attacks.	The weaknesses of the proposed architecture include the limitations in terms of storing great amounts of data, as well as the lack of control over the quality of data coming through the sensors.	In the future, the authors can carry out extensive research for establishing quality control over the sensory information in blockchain-based frameworks and a few strategies to store immense measures of information.

Table 3. *Cont.*

Paper Title	Strengths	Weaknesses	Future Scope for Improvement
[46]	Blockchain-based IoT frameworks offer answers for the issues addressed, by giving straightforwardness, decentralization, effective information stockpiling, and, in particular, the information is being ensured on account of the high security presented by such frameworks; consequently, stock can be kept up effortlessly.	This paper discusses the limitations in research directed towards the use of blockchain-based systems and their effects on IIoT.	As blockchain and its changes settle in the thought process of industrial giants and implementation increases, more techniques with better outcomes will come to the platform.
[47]	In this paper, the different applications of blockchain-enabled IIoT have been addressed with emphasis. The discussions of the increase in implementation will lead to efficient, scalable, and secure working.	Since the implementation and research of blockchains are still in their infancy, the systems that rely on the blockchain cannot fully utilize the benefits of blockchain integrated systems and, hence, there are some limitations.	With an increase in research in blockchains and fully utilizing it, industries will soon be able to work on blockchain-based systems more comfortably.
[14]	A broader range of protocols and devices are compared and discussed. Their setups are thoroughly examined.	The research was limited to technical comparisons. There were no use cases available for the specific protocols and devices.	The researchers proposed the work of controlling and monitoring IoT devices and protocols remotely, and effectively in terms of cost.
[16]	This study depicts the observations about the acceptance of IIoT by the survey data of real industries, so that it can help in our further researches concerning what our industrial sector thinks about IIoT.	This study highlights the factors that are affecting the adaptation of IoT in the industrial sector, but do not discuss the possible solutions that can minimize these factors' effects.	If authors can reduce the challenges and effects of factors affecting the adaptation of IIoT discussed in this paper, in the future, users will see the great industrial revolution in which IoT will have a greater contribution, as the authors discuss the contribution of IIoT in minimizing the wastage of energy resources, reduction in bills, well-organized maintenance can offer higher merits to the industrial sector.
[17]	The concept of automation is described more precisely with methods and types, and this paper also introduces the concept to integrate artificial intelligence in the IIoT.	It should further describe some ways to integrate the AI in IIoT so it would be more interesting.	Industrial automation with an artificial intelligence-based IoT system, so that the system will be capable to intelligently make decisions.
[30]	The paper briefly explains all the research challenges that are faced in IoT in a very simple and easy way.	The paper should also provide some ways to manage the challenges.	As blockchain algorithms consume a lot of energy, there is a need for energy-efficient devices to cope with this challenge.
[28]	The architecture for industrial automation and the technologies used for security in IoT applications are thoroughly explained in this paper.	It should further address some challenges for IoT.	As the processing of data and the management of data is computationally expensive, there is a need for adequate techniques to address this.

Table 3. *Cont.*

Paper Title	Strengths	Weaknesses	Future Scope for Improvement
[7]	A proper architecture is proposed with strong research simulated for the real environment using Simulink and MATLAB, the quantitative measures presented.	Does not discuss the future improvements. Does not mention the challenges faced in implementing the IoT for the system.	The different architectures that improve the energy efficiency and performance of factories even further.
[21]	Mentions research questions, aims, scope, and background, and discusses all the required technology for implementing IIoT with protocols and describes what has already been applied in the field, challenges, future considerations. Surveys a solution in the sector (electricity supply chain).	Does not explore how to solve the issues associated with IoT (privacy, interoperability, and others).	Smart grids need to adjust the network balance based on situational awareness. In practice, protection relays and transformers and creating this information for downstream uses. IoT infrastructure enables remote controls and complex strategies utilizing future contracts and the virtualizations of power plants. Enabling charging for electric cars on a larger scale through IoT as the trend increases.
[46]	(1) The proposed techniques have many industrial applications with a good number of industrial benefits. The issues proposed have solutions, such as the use of proper layer architectures in the implementation	(1) No feasibility studies were proposed for the adaptation of these IoT-based techniques	(1) There are 3 main areas discussed, in which future improvements are possible. Firstly, using a lot of sensors can increase energy consumption so that energy-efficient IoT systems are needed. Secondly, the use of social media should be implemented to create a wide network. Lastly, AI should be implemented to create smart objects that can have good adaptability.
[4]	IoT technologies enable smart manufacturing using technologies, such as WSN, smart sensors, big data analytics, and cloud computing.	Opening up a large number of connected devices to the cloud provides an attacker with multiple points of entry. Sensor equipment is expensive, and data ownership is a legal concern. Manufacturing applications that demand real-time feedback control may be unable to withstand data transfer latency caused by IoT.	Emerging IoT applications in manufacturing present new research challenges, necessitating technical standards and solutions that can harness enormous streams of real-time data to enhance operations throughout the production life cycle.

Table 3. *Cont.*

Paper Title	Strengths	Weaknesses	Future Scope for Improvement
[6]	A growing number of industrial firms are embracing the IoT to change their processes. For retrieving and altering the knowledge of inventory materials, information systems architecture has been widely employed in development, production methods, and condition monitoring. A more effective production reduction is achieved, thanks to the thorough integration between operating systems. RFID uses electromagnetic fields to transfer data. Wireless sensor networks are self-organized nodes that maintain the connectivity in data transfer. Cloud computing effectively manages the shared pool of computing resources.	Several of the attempts are examined using the manufacture hardware's instruction set limits that are closely linked to the vehicle's physical attributes and offer malware limits of assaults.	The next phase will be to create an analytical tool that will be used to simulate the existing Internet of Things production process. Additionally, investigate how to end data can be used to detect attacks and create an algorithm for detecting intrusions in cellular manufacturing techniques by digesting background.
[21]	IoT provided an improved operational environment and led to efficient decision making.	IoT in logistics application requires good communication and participation. Introverts cannot work very well in such a system.	IoT in transport and industry will contribute to an efficient logistics activity.
[22]	IoT enables resources to support remote management, facility management, auto supervision, and inventory management.	Power outages create connectivity issues and integration between operational, and information technology can cause data loss.	Involving decentralization and using more edge computing can reduce costs.

4. Observations and Derivations

4.1. Major Industrial Challenges

With the boom of IoT, industrialists face challenges of the protection and privacy of their data, as traditional security methods cannot be applied in IoT. Additionally, the increase in electronic gadgets makes scalability a challenge. Therefore, a flexible and scalable architecture should be proposed. Real-time monitoring and storage space is also a great hurdle faced by industrialists [37]. IIoT deals with complicated physical machinery having industrial sensors and relevant software. The challenge is to provide real-time connectivity between humans and machines, which is possible by providing a presentation layer for error-free systems.

It thus requires a connection of the IoT device with IP. IP plays a key role in exchanging information to the devices to which it is connected. IoT is used at the enterprise level and each enterprise comprises of different infrastructures and builds the different architectures of an IoT system. The major challenge here is that no such repetition can occur in a specific industry, as IoT devices are solely based on enterprise operation. The major challenge it involves is making the data actionable from machines to software [48]. The traditional electricity supply chain is changing from uni-directional to bi-directional, but to further utilize the full efficacy, IoT would need to work with the existing smart grid and data analysis.

Along with the different advantages of IoT in every field, it also becomes a challenge, especially for industries in third world countries. To implement IoT 4.0 and 5.0 with IoT in third-world countries, finding good quality hardware devices, sensors, and IoT devices is difficult. Moreover, adopting IoT in the industry requires a huge cost. That is why industries do not opt for the Industrial IoT and automation, without thinking that these technologies are great cost-savers after the adoption of IoT. One of the most important challenges is the skilled persons required, who know about implementing IoT with complex automation techniques and real-time data handling on a large industrial scale [49].

If manufacturing plants use IoT with blockchain technology to ensure security and privacy, then by using blockchain technology, they have to face high costs and long-term issues to create a block of transactions.

4.2. Key Findings

The transformation from IoT to IIoT, leading to a great change in efficiency and sustainability around the world [39]. It was discovered that IIoT is a key component that local industries must adopt to optimize efficiency and profitability. In addition to the numerous benefits of IoT in the industrial sector, some critical aspects need to be addressed to face the challenges that arise while adopting IoT on a larger scale [50]. Wireless sensor networks (WSN) and radio frequency identification sensors form the basis of IoT technology. RFID is a non-contact, automated identifying technique that does not require human involvement. WSNs are self-configuring, infrastructure-free wireless networks that are used to monitor physical or environmental conditions [51].

This study focuses on the merits that Industrial IoT brings to the industries operating in different parts of the world, along with the challenges that arise due to IIoT. A proper architecture is proposed with strong research simulated for the real environment using Simulink and MATLAB; the quantitative measures are presented [52]. It also mentions the research questions, aims, scope, and background, and discusses all the required technology for implementing IIoT with protocols. It also describes the methods that have already been applied in the field, as well as the challenges and future considerations. Moreover, it surveys a solution in the sector (the electricity supply chain).

4.3. Implementation Analysis

This paper sheds light on the temperature monitoring system, and other different parameters to review the gas, oil, chemicals, and other manufacturing industries. The research is limited to the different parameters to be used based on technical comparisons;

therefore, no specific implementation analysis can be entitled. This paper also presents the key components of IIoT architecture, which include devices, such as sensors, interpreters, the transient data store, which temporarily stores transient data objects to avoid data loss, and local processors serving as low latency data processing systems [45]. Application is a presentation layer that helps staff to understand things interactively. Channels are a medium to exchange data; they include IP routers, switches, and other networking protocols. Gateways are used to ensure a connection with other networks. Collectors provide help to collect data from different gateways [46]. Processors are used to transform data, detect various signals, and other complex event processing. Permanent data store provides storage, such as cloud storage, RDBMS, data repositories, open-source data, and website data. The models in IIoT comprised of analytical models and data models. These analytical models are trained using artificial intelligence. Security includes encryption, authentication, and firewalls [47]. Computing environments differ from enterprise to enterprise. Fog computing is used for analytics purposes. Cloud computing is used to scale things globally. Hybrid computing is a mixture of fog and cloud computing.

This paper discusses a conceptual-based implementation of IIoT by dividing them into three layers: the sensor layer, communication layer, and presentation layer. This paper also discusses the big data applications in IIoT [53]. This article proposes an EMS based on the IoT (IoT) network that boosts power quality for smart factories to establish an energy-efficient system. In addition, the architecture for improving the power quality in industries that follow ISO 50001 standards is suggested. Before implementing IoT in warehouses and production plants, there are some key requirements, such as domain requirement knowledge; IT office in industry; good quality hardware; large scale or big data handling; real-time monitoring; interoperability with other software or interfaces; the scalability of IoT devices to expand the business; and the reliability of device functionality [31]. The bandwidth of the network is also a great problem to transmit the data in real-time, such as NBIoT devices.

Implementing IoT in industrial sectors requires the consideration of various aspects to elicit the requirements. It includes the identification of the particular industrial sector, understanding of the business requirements of that particular industrial area, infrastructure requirements, addressing integrating issues in case of the up-gradation of the existing IoT system, and an understanding of human and social aspects in the case that training would be required for the people who are expected to interact with the system [38]. Depending upon the requirements, a threshold needs to be set for the quality factors of the system as well as leaving provisions in the systems for integrating functionalities and capabilities that can be required to be added in the future.

4.4. Development of IIoT in the Future

IIoT's future advancement will envelop an assortment of cloud providers, which will all be observed from a distance while remembering the costs [54]. This paper presents an application guide and portrays how future improvement will be centered around IIoT gadget wellbeing and security. Assuming the users can diminish the boundaries and outcomes of the factors affecting IIoT adaption, as referenced in this review, the authors will see critical modern unrest later on, with IoT assuming a larger role [42]. Different plans further increment fabricating energy effectiveness and execution. Brilliant matrices' organization balance should be adjusted, relying upon situational mindfulness. Practically speaking, this information is created by the defensive transfers and transformers for downstream applications. Controllers and confounded strategies dependent on future agreements and power plant virtualizations are conceivable with IoT innovation. IoT will be used to empower greater scope charging for electric vehicles, as the pattern extends. The IoT (IoT) can extend and turn into the following flood of mechanical development. In the present quick-moving climate, innovations are being created to make IoT establishment simpler. One technique is to create "IoT as a Service" innovation, which will expand the scope of IoT applications, all things considered [41].

More research can be conducted in the integration of blockchain technology with IoT topics, to improve blockchain blocks creating time by using other coins, such as Ethereum and Altcoins. The practical implementation of different frameworks in IoT should be focused on instead of theory. IoT with quantum computing, deep learning, and blockchain can be explored to an extensive level. As a result of the IoT paradigm, the industry will be converted into "cyber-production systems" that are adaptive, flexible, and fully aware of the production circumstances. New techniques of filtering and processing data should be developed, however, to minimize the amount of data created and transmitted [39]. The production components must be able to self-identify, see intelligently, make autonomous decisions, and acquire new knowledge to achieve intelligent production. It is necessary to conduct further study into IoT technologies for manufacturing, artificial intelligence, and machine learning approaches. If the authors can reduce the challenges and the effects of factors affecting IIoT adaptation, people will observe a great industrial revolution in the future, in which IoT will play a bigger role. IIoT's contribution to minimizing energy waste and well-organized maintenance can offer greater benefits to the industrial sector [40].

5. Discussion

The term IoT was coined keeping "Smart World" in mind. Mark Weiser was the first person who started the concept, which is now called IoT. Later, MIT raised it again. IoT can be explained as the concatenation of different sensors, gadgets, and programs that can provide the measurement and are capable of acting all around the world. IoT is majorly used in smart cities and smart homes to achieve security and surveillance, health care, smart industry, environmental monitoring, and almost all major industries. This paper also highlights the major elements used in IoT. There are almost three elements used in every IoT application:

- Hardware, including actuators, sensors, modules, and other gadgets;
- A middleware for data storage and analytics purposes;
- Frontend presentation.

Furthermore, the paper provides temperature monitoring architecture and key findings. In industries, such as petroleum, cement, and brick, the temperature element plays a key role; therefore, the IoT sensor results in such industries should be accurate enough for the different processes involved from exploration to extraction, refining, and other purposes of different petrochemical by-products [52]. Likewise, food industries also need to monitor the temperature changes. The effective functioning of each sensor and each gadget should be involved, otherwise great losses will occur in such industries. These sensors can be wired or can be wireless. The overall working of an IoT application starts with collecting data through the sensors.

Then, that data should be sent to multiple devices connected (wired or wireless) through different networking protocols. Usually, wired sensors are used so that data can go through the process of refining or the conversion of data from digital to analog signals. The microcontroller then makes decisions based on the collected data [44]. All these things should be reviewed by keeping security, reliability, scalability, safety concerns, and also the cost involved in the production. The authors can conclude that in almost all IoT applications the process is to gather, record, and report. This paper also provides a comparison of the different communication protocols and also compared different IoT platforms. Based on their research, the most effective communication protocol is the LoRaWAN LoRa protocol, and ARM Cortex is the most efficient IoT platform [38].

IoT is a field of technology that utilizes information interrelationships to associate actual things to the web, without the necessity of human-to-machine or human-to-human contact. In 2011, Gartner incorporated the "Web of Things" to their rundown of arising patterns. The IoT is for business use, though the Industrial IoT (IIoT) is for modern use. The advancement of IoT, the change from IoT to IIoT, execution investigation, the association of IIoT to the fourth modern upset, IIoT administrations to modern robotization, the job of information examination, the contextual analyses of organizations utilizing IIoT, and its advantages for business applications are canvassed in this paper [43].

The standard computerization approaches are investigated in this work, just as mechanized engineering and, likewise, it contributes to the eventual fate of IIoT and how it will be coordinated with digital actual frameworks (CPSs). The utilization of comparable methodologies in the working environment has likewise been thought of. This review offers a power electronic framework plan for bringing down energy utilization and improving power quality [55]. Additionally, it handles concerns, for example, power factor decreases and consonant rates. It likewise proposes an energy-productive arrangement dependent on an IoT organization to further develop fabricating power quality [51]. Modern automation is quite possibly the most fundamental sector that incorporates with the business to create superior grade, reliable merchandise at a sensible cost. Modern automation is a specialized framework wherein process administrators, specialized cycles, and PCs and IoT gadgets are completely interconnected. Modern robotization area vaults require a space-explicit improvement climate with restricted time and assets, just as a few groups in different positions. The area archive's construction likewise incorporates a domain repository motor, a fundamental layer with parts, and network layers [32].

Exploitation and monetary development in stockrooms with IoT and Industry 5.0 is a difficult issue in the current world when innovation is enhancing a standard premise. Ventures are experiencing issues sending these creating advancements because of the absence of a reasonable development of the executive's structure. An "Outright Innovation Framework" (AIM) is proposed to make developments a customary part of modern schedules. By applying novel ideas, the AIM proposes to tackle the issue of bombed modern cycles [44]. Organizations will be prepared to convey IoT and industry 5.0, assuming they consolidate configuration thinking, inventiveness, and mechanical drives. Assembling and creation utilizing IoT, supportability, and energy productivity in processes are needed for an enormous scope. Narrowband IoT (NBIoT) is a kind of IoT that provides energy production and long-haul processes. NBIoT utilizes incredibly little power and transfer speed. It is likewise utilized in cell networks; thus, in independent assembling plants and capacity frameworks, NBIoT is the most ideal choice for emerging countries [48].

The reliance and correspondence between IoT gadgets are uncertain, bringing about security and protection issues. A protected remote technique is introduced that utilizes blockchain innovation to keep up with the security and straightforwardness of every sensor movement, keeping programmers from obtaining the information. To contrast the security of IoT gadgets with the old strategy, the proposed approach is created and reproduced against various measurements, such as the shot at simple discovery, distortion assault, and the likelihood of an effective attack [17]. The stylish subjects of Industry 4.0, blockchain, business analytics, and the IoT drew countless specialists and scholastics. The fourth modern insurgency (Industry 4.0) means to make a brilliant assembling framework that utilizes innovation to make digital actual frameworks. The IoT (IoT) is an organization of numerous gadgets that utilize sensors, systems administration, and data innovations to convey the possible answers for changing the working and activities of many distribution centers and assembling plant frameworks [36]. Blockchain is a dispersed, decentralized innovation that endeavors to make frameworks with security, transparency, trustworthiness, namelessness, and genuineness for some reasons.

6. IoT Contribution in Performance Indication

Following digital and IoT innovations helps to track and improve the logistics performance indications. These will be explained below.

6.1. RFID for Identification and Tracking

RFID flags are classified into two types: passive RFID flags, which retro modulate the incoming wave from the interrogator to transmit information, and active RFID flags, which do not have any RF transmitters and instead rely on electromagnetic waves to power the on-board circuitry. This tag typically includes a power transmission source as well as humidity and temperature indicators/sensors. However, there are some limitations to this because the manufacturing costs are quite high, limiting the use of this technology, and companies still prefer to label each of their products to improve traceability [54]. RFID usually provides solutions to the problems in which the demand distortion that travels throughout the supply chain is larger than that of the sales; therefore, its benefits in the supply chain can reduce error rates, customer relationship management, and security.

6.2. Logistics Indicators

They provide us with a clear quantitative and qualitative analysis of the ongoing SCM project, and identify the regulation at each level, ultimately improving the ongoing process. These performance indicators are commonly referred to as KPIs, and they are aggregated to the total deployment of RFID in inventory management. These different indicators can include KPI in inventory turns, service level, resource optimization, production cost, quality, and productivity [12].

6.3. Industry Regulations and Process Control

The significance and impact of the modern web of things on how businesses run all through the world, just as the worth added to society by web associated innovation, are the subject of this examination. Industry 4.0 and the web of things (IoT), empowered advances to help modern proficiency by permitting merchandise, frameworks, and machines to speak with each other [37]. The IoT (IoT) is gradually yet consistently becoming perceived as the following stage in the development of the internet. Modern IoT centers around expanding functional effectiveness, wellbeing, and usefulness, while also zeroing in on the profit from the venture, although IIoT centers around working on functional proficiency, security, and efficiency while additionally focusing on profit from speculation. The Industrial IoT (IIoT) is regularly portrayed as an insurgency that is rapidly and keenly changing the industry, savvy cities, intelligent factories, self-regulating buildings, and other creating IIoT applications [1].

6.4. Production Turnover

Ongoing progressions in RFID, brilliant sensors, correspondence advances, and internet conventions have empowered the IoT. The IoT's underlying stage may respect the current internet, be portable, and cause (M2M) machine-to-machine upset. The IoT (IoT) is relied upon to associate an assortment of advances to empower new applications by interfacing actual items to further develop canny and compelling decision-production [53]. Industrial automation is one of the most prominent use cases of IoT in the industrial sector, which requires a substantial number of hardware technologies. A large-scale industrial automation system covers various areas of an enterprise that includes sales and customer support, finance, and an entire supply chain of the system. The implication is that lower-level automation systems, on the other hand, rely on hardware, electronics, and embedded computers rather than IT to communicate with a single machine or, at best, a group of machines [2].

6.5. Testing and Surveillance Advancement

The IoT aims to enable objects to connect with other objects and persons at any time and from any location utilizing the internet. The IoT (IoT) is progressively becoming recognized as the next step in the growth of the internet. Currently, it is expected that over 50 billion gadgets globally have been connected to the internet [25]. The IoT (IoT) is predicted to keep growing in terms of the number of gadgets and functionalities it can support. IoT applications span a wide range of industries, including manufacturing, healthcare, agriculture, smart cities, security, disaster relief, and retail and logistics to name a few. There is still a slew of issues that need to be addressed, clearing the door for new types of study to be conducted, which include privacy and security, data management, and the selection of communication protocols [3].

6.6. Humanless Manufacturing and Control

As enterprises revamp, the utilization of IoT in assembling considers the exchange of existing creation frameworks into new digitalized ones, bringing about monstrous monetary possibilities. Modern IoT assists present-day firms with conveying information-driven techniques and methodologies to manage worldwide cutthroat strain [56]. The usage of the IoT (IoT) in the assembling business expands the general volume of information produced, bringing about the transformation of modern information into modern big data [35]. Organizations will want to improve their presentation by gathering and investigating information using information-driven philosophies all through the item lifecycle. Moreover, by using the accumulated information, groundbreaking firms can utilize prescient investigations to acquire a benefit and increment their seriousness. Despite the expanded organization of the IoT in assembling, financially savvy and attachment and play framework interoperability arrangements are as yet restricted [4].

6.7. Supply Chain and Production Management

The organization's item advancement is based on the establishment of the creative studio. Fabricating IoT (IoT) is another assembling mode that incorporates IoT innovation with assembling innovation to empower dynamic perception, intellectual handling, and the ideal administration of assembling and data assets across the item life cycle [43]. They introduced a framework for checking the creation lines, in which the programmed gathering of continuous shop floor information offers a strong dynamic establishment for the upper-level arranging the board office. Anti-interference, rapid deployment capabilities, convenient expansion, and security are the important performance factors for the systems that are used for production line data monitoring to achieve intelligent manufacturing [50]. The functional model of the system comprises of six modules that are the monitoring of workshop, system login, DNC (direct numerical control), warehouse management, statistical analysis, and product tracking. The client/server model is currently the most used computer mode. As the system involves a huge volume of data exchange, multithread real-time data collection, as well as quick real-time interactive responsiveness and data security, is required. As a result, the traditional client/server architecture is used, and the field-level end-devices and the workshop are linked via IoT [5].

7. Challenges on the Platform Shift

7.1. Challenges

Consumer Privacy and security against cybercrime:

IoT is now commonly used, so it needs appropriate security. the flaws in the system are commonly known to everyone. Many IoT devices already possess these. Furthermore, because IIoT is built on top of existing wireless sensor networks (WSN), it, therefore, has the same issues of privacy and security as WSN. Various attacks and flaws in IoT systems demonstrate the necessity for comprehensive security designs that secure data and systems from start to end [31]. This security barrier necessitates complete security solutions, which include efficient research in cryptographic solutions and security systems that help developers to develop secure systems. The integrity of messages sent and received, and the confidentiality and authenticity in a conversation between communicating parties should be considered. These can include features, such as the ability to prevent several parties from communicating with each other [19].

7.2. Data Management

A vast amount of data has been produced in the period of big data, but the management of data is very difficult. Currently, centralized systems are used for computationally expensive tasks on platforms of the cloud [31]. Nonetheless, there is a persistent concern that traditional cloud designs may fail to transfer the vast volumes of data produced, to be used by devices, and to load, which happens on computation; keeping time constraints is, at the same time, also a challenge to current cloud designs [5]. Other challenges also arise from the fact that, once the data are collected, they are then to be used intelligently to gain insights, but machine-learning models and algorithms that work on the neural network can perform automated decision making, which is not always accurate.

7.3. Monitoring and Sensing

The technologies of sensing and monitoring have advanced significantly; they are always changing, with a special focus on energy efficiency and shape. As sensors are working continuously and constantly to obtain all data instantly or to acquire real-time data, this makes them more energy-efficient; furthermore, the breakthroughs in nanotechnology made it possible to develop sensors at the nanoscale [27].

7.4. Protocols

Device communication protocols are commonly called the major driver behind IoT applications, and they serve as the primary route for the flowing of data between sensors and the outside world. Meanwhile many MAC algorithms with frequency division multiple access have been proposed for several domains free of collision and traffic [14]. The transport layer has protocols similar to TCP, which is used for providing reliable communication and controlling the congestion between communicating devices; however, the communication protocols do not usually provide a high level of reliability.

7.5. Interoperability

As the devices that are connected in communication are of different types in IoT as they use different encoding and different protocols, interoperability has always been and continues to be a core essential ideal. Currently, several standards are used to support diverse industries' applications [40]. As a result of the large amounts of data, different interconnected devices also have to adopt standards for collaboration, which is very difficult to perform, as well as within a variety of system restrictions. As a result, IoT systems are being developed to manage increasingly greater levels of interconnection.

7.6. Standardization

A major challenge for IoT is standardization. There are no specific guidelines for IoT solutions. It all depends on the individual vendor as to what they are providing and how they are developing their technology or service [57]. This is mainly due to its rapid development, varying fields of implementation with different hardware and software as well as it being a relatively newer technology [11]. There are four categories in which to divide the IoT standardization: platform, connectivity, business model, and killer applications (to control, collect, and analyze data). They are interrelated so that even a single break would cause the IoT system and standardization to collapse.

7.7. Legal Aspects

It is fairly difficult to deal with the legal implications of evaluating consumer behavior in real-time. One also has to consider data minimization—the company must not collect more data than necessary, and such fine optimization of the object can prove to be a real challenge [23]. Then, there is also the question of what cases can be taken to the court by the consumers or producers about IoT, how much responsibility the producer bears, and what shall be the repercussions. If great amounts of investments are made in this uncertain legal environment, they can pose a serious business risk [30].

8. Industrial Achievements of IIoT

8.1. Economic Impact

A regulation related to the user's data privacy and their rights in this regard, known as GDPR, was passed in 2018. It has several directives and regulations, all of which focus on the consent to use personal information gathered over the internet and the right to compensation in case of any breach or threat to the information [53]. It can be very well inferred that this particular regulation would affect the industry of IoT more than anything else, as the major operative behind this industry is the collection of data through different means [23]. IoT can go as far as collecting data from search patterns and inferring the choices and behavior of an individual; this seriously collides with the consent clause of the GDPR as it becomes hard to obtain consent for this kind of information gathering. Moreover, maintaining security is a great issue in IoT devices as it has become the prime target of hackers and, with a large number of devices or "things", it is difficult to keep every device updated according to the current security standards and updates [29]. In the related researched article, a model, namely Gordon and Loeb, was employed in addition to the statistical inference. Apart from the GDPR, the coronavirus pandemic also economically impacted the IoT market in the years 2019–20. In a report in Forbes, it was indicated that the transportation industry's revenue decreased from USD 43 billion to USD 34 billion, whereas the IoT-based automotive enterprise took a hit of USD 42 billion as it was downgraded from USD 393 billion to USD 351 billion [38].

8.2. Social Impacts

IoT brings a revolutionary change in the industrial sector. It has countless benefits for the industry. While some believe that IoT will result in positive changes for society, there might be effects of IoT that can negatively impact the society. Researchers conducted a study in Japan for which data was collected to obtain the social impacts of IoT on the industry [42]. They gathered information in terms of the independent variables, such as the number of job vacancies available, average annual hours worked, average power consumption per year, number of researcher vacancies, and employment percentage. They collected 5 years of data (2013–2017) for these entities and used the ANOVA statistical method to find the social trends [23]. The study concluded that the employment percentage in the industrial sector is decreasing as automation is increasing. This is creating unemployment issues among some labor classes in Japan. Research opportunities are increasing because more innovative ideas are needed and this can bring a positive change in society as more and more people are encouraged to join research centers and influence the standing of IoT [32]. One of the worst trends they observed was increased power consumption. The electricity requirements drastically increased over the years. This led to a deficiency of power, which is compensated by nonrenewable resources, such as gas and petrol. This can result in negative changes in the environment, such as excess carbon emissions and global warming. To conclude the social impacts, IoT can have both positive and negative impacts on society, and a proper feasibility study should be initially conducted in IoT innovation, so that the negative effects can be catered to properly [40].

8.3. Security

Notwithstanding its many benefits, IoT security is a major worry, since caricaturing endeavors and unlawful access have imperiled the client's information honesty. Network protection and security concerns have been a wellspring of worry for various organizations and government offices. The weaknesses emerge because of IoT network interconnectivity, which takes into account mysterious and untrusted web access [58]. At the point when IoT is redirected from conventional PCs, it turns out to be more defenseless against security dangers [43]. Since IoT gadgets are appropriated for an enormous scope and have practically equivalent properties, they are indistinguishable. This shared characteristic expands the measure of defenselessness, which can altogether affect most gadgets. One more component of IoT that is defenseless is data security. Contactless cards, for instance, permit card numbers and names to be perused without requiring pin codes for confirmation, making it more straightforward for a programmer to obtain the cardholder's character and card number [17].

9. Future Scope Directions

9.1. Cyber Security and Data Analytics

One of the things keeping industries away from IoT is their concern about privacy and security requirements. When it comes to the security of IoT-implemented devices, industrialists should be familiar with the terms of cyber security and data analytics. Data analysis is critical to the effectiveness of operational actions [25]. Thus, automating the industry coins the development of the fifth industrial revolution (Industry 5.0), making it evident to include the cyber risks to obtain secure and persistent security strategies for Industry 5.0.

9.2. Combination of Blockchain and IoT

Blockchain technologies, such as IoT, became popular in 2018 [11]. Even though blockchain was first employed as the underpinning technology for the Bitcoin cryptocurrency, it is now being used in a variety of non-financial applications. IoT suffers from security issues. On the other hand, the innate security, the immutability of blockchains are the major reasons for its adoption in monetary and nonmonetary applications [12]. Blockchain made this possible through its consensus approach and by using its ledger, which is distributed, i.e., not controlled, by only one node. As a result, the combination of these two technologies provide an additional layer of security [5]. Furthermore, the security of devices will increase while also benefiting from one another.

In Industry 5.0, blockchain technology will play a vital role in deploying and designing real-time applications to increase productivity and create a proper working environment.

9.3. Cyber-Physical Production Systems

CPS, otherwise called CPPSs, depend on the current improvements in software engineering and data correspondence advances, similar to the development of assembling science and innovation. CPSs interface this present reality with the virtual universe of instructive innovation and programming, allowing clients to attain a different arrangement of information, administrations, and advanced correspondence decisions [10]. In any case, taking on CPS through IoT produces large volumes of information that require explicit administration, handling, and examination to execute considerable thinking and possibly concentrate on helpful experiences, particularly in the modern area. To take care of this issue, a large information examination occurs as an impetus for eliminating IoT information bottlenecks. The CPS worldview stresses the utilization of observing gadgets that go beyond conventional ways for on-location information gathering, handling, and show [38] as a feature of the IoT thought.

10. Conclusions

Industry 5.0 has taken a step forward, it emphasizes the objective to strengthen the collaboration between creative productions of human beings and advanced, improved machinery and new technologies, such as IoT. It means that an automation system facilitates humans for faster and more efficient development. Numerous production plants and warehouse management have adopted new technologies to increase the overall performance of their employees. This combination of new technologies and human efficiency and intelligence clears the way for multiple benefits in manufacturing. The aim of Industry 5.0 is not the replacement of human beings; instead, its main goal is to empower humans. Robots can cope with different tasks repeatedly with more accuracy, but they are not able to point out the issues and solve them on their own. Industry 5.0 highlights the need for the cooperation of robots with humans. It empowers humans to control the robots to perform numerous tasks. The intelligence of human beings is required in Industry 5.0 to resolve the problems, and robots are needed to fix them accurately and quickly. This pairing of machines and humans provides multiple unique advantages for the manufacturers.

The research was based upon the advancement of IoT and its impact upon the supply chain architecture, and the authors discussed the origins of the SCM, its manual and automation model, how IoT impacted the supply chain cycle. Essentially, the world is evolving fast and people are living in the world of digitalization where IoT blockchain and big data technologies that automate human work in all sectors especially in the industry are common. For the integration of IoT in the supply chain, the authors had to consider several key indicators and analyzed strong architectures, and discussed both its pros and cons while discussing the side effects and the hardware that are used or should be used [36]. From our research, it is found that the IoT (IIoT) is an important feature that industries must adapt to improve efficiency and revenues. This would benefit consumers by lowering prices and ensuring a consistent supply [59,60]. The incorporation of IoT technology in the industrial sector is thoroughly addressed in our research. Industrial IoT is the basis of Industry 4.0. The authors have presented the evolution of this disruptive industrial advancement along with the objectives of its adoption. The widely used and emerging applications of IIoT are also represented in our research. The related challenges in adopting IIoT are also discussed. Our research concludes that IIoT is a revolutionary technology that is transforming the course of the work of some of the major industries, such as the manufacturing industry, transportation industry, and power and energy-related industries. IIoT aims to efficiently connect resources that can work as a system, eventually leading to smart industrial sectors.

Author Contributions: Conceptualization, Z.F., L.F.N. and M.H.T.; methodology, Z.F., W. and S.Z.; software, H.K.; validation, Z.F., L.F.N., M.T. and N.A.; formal analysis, Z.F. and H.K.; investigation, N.A. and M.T.; resources, L.F.N. and H.K.; data curation, M.T.; writing—original draft preparation, Z.F., M.T. and N.A.; writing—review and editing, N.A., H.K., L.F.N., Z.F. and M.T.; visualization, H.K.; supervision, Z.F.; project administration, Z.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Following are the sources from where authors gathered the data to conduct this research; IEEE (https://www.ieee.org/publications/; accessed on 28 November 2021), ACM (https://dl.acm.org/journals; accessed on 28 November 2021), Elsevier (https://www.elsevier.com/; accessed on 28 November 2021), Springer (https://link.springer.com/; accessed on 28 November 2021), Google Scholar (https://scholar.google.com/; accessed on 28 November 2021).

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.

References

1. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
2. Xu, L.D.; He, W.; Li, S. Internet of Things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]
3. Khaleel, H.; Conzon, D.; Kasinathan, P.; Brizzi, P.; Pastrone, C.; Pramudianto, F.; Eisenhauer, M.; Cultrona, P.A.; Rusinà, F.; Lukáč, G.; et al. 'Heterogeneous applications, tools and methodologies in the car manufacturing industry through an IoT approach' 2015. *IEEE Syst. J.* **2017**, *11*, 1412–1423. [CrossRef]
4. Badarinath, R.; Prabhu, V.V. Advances in IoT (IoT) in Manufacturing. In *Advances in Production Management Systems. The Path to Intelligent, Collaborative and Sustainable Manufacturing*; Springer: Cham, Switzerland, 2017; pp. 111–118. [CrossRef]
5. Yang, C.; Shen, W.; Wang, X. Applications of IoT in manufacturing. In Proceedings of the 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanchang, China, 4–6 May 2016; pp. 670–675.
6. Pan, Y.; White, J.; Schmidt, D.; Elhabashy, A.; Sturm, L.; Camelio, J.; Williams, C. Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems. *IJIMAI* **2017**, *4*, 45–54. [CrossRef]

7. Gomaa, N.N.; Youssef, K.Y.; Abouelatta, M. An IoT-based energy-efficient system for the industrial sector. In Proceedings of the 2019 15th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 29–30 December 2019; 1109. [CrossRef]
8. Lin, J.D.; Cheng, A.M.K.; Gercek, G. Partitioning Real-Time Tasks With Replications on Multiprocessor Embedded Systems. *IEEE Embed. Syst. Lett.* **2016**, *8*, 89–92. [CrossRef]
9. Brusakova, I.A.; Borisov, A.D.; Gusko, G.R.; Nekrasov, D.Y.; Malenkova, K.E. Prospects for the development of IIoT technology in Russia. In Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg/Moscow, Russia, 1–3 February 2017.
10. Zhou, L.; Guo, H. Anomaly Detection Methods for IIoT Networks. In Proceedings of the IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Singapore, 31 July–2 August 2018.
11. Zhang, C.; Chen, Y. A Review of Research Relevant to the Emerging Industry Trends: Industry 4.0, IoT, Blockchain, and Business Analytics. *J. Ind. Integr. Manag.* **2020**, *5*, 165–180. [CrossRef]
12. Aleksic, S. A Survey on Optical Technologies for IoT, Smart Industry, and Smart Infrastructures. *J. Sens. Actuator Netw.* **2019**, *8*, 47. [CrossRef]
13. Karmakar, A.; Dey, N.; Baral, T.; Chowdhury, M.; Rehan, M. Industrial Internet of Things: A Review. In Proceedings of the 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, India, 18–20 March 2019. [CrossRef]
14. Maheswari, C.; Perinchery, A.A.B.; Priyanka, E.; Ambika, K.; Narmatha, S.; Prenitha, A.; Monisha, M. Review on Online Monitoring and Control in Industrial Automation–An IoT Perspective. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1055*, 012034. [CrossRef]
15. Arsénio, A.; Serra, H.; Francisco, R.; Nabais, F.; Andrade, J.; Serrano, E. Internet of Intelligent Things: Bringing artificial intelligence into things and communication networks. In *Inter-Cooperative Collective Intelligence: Techniques and Applications*; Springer: Berlin/Heidelberg, Germany, 2014; Volume 495, pp. 1–37.
16. Goundar, S.; Bhardwaj, A.; Nur, S.S.; Kumar, S.S.; Harish, R. Industrial Internet of Things: Benefit, Applications, and Challenges. In *Innovations in the Industrial Internet of Things (IIoT) and Smart Factory*; IGI Global: Wellington, New Zealand, 2021; pp. 133–148. [CrossRef]
17. Yadav, S.K.; Sharma, K. Industrial Automation: Overview of the IoT (IoT). *Int. J. Sci. Eng. Res.* **2017**, *8*, 75–81.
18. Rao, P.; Saluia, P.; Sharma, N.; Mittal, A.; Sharma, S.V. Cloud computing for IoT & sensing-based applications. In Proceedings of the 2012 6th International Conference on Sensing Technologies (ICST), Kolkata, India, 18–21 December 2012; pp. 374–380.
19. Mahmud, B. IoT (IoT) for Manufacturing Logistics on SAP ERP Applications. *J. Telecommun. Electron. Comput. Eng.* **2017**, *9*, 43–47.
20. Lahti, J.P.; Helo, P.; Shamsuzzoha, A.; Phusavat, K. IoT in electricity supply chain: Review and evaluation. In Proceedings of the 2017 15th International Conference on ICT and Knowledge Engineering (ICT&KE), Bangkok, Thailand, 22–24 November 2017; pp. 1–6. [CrossRef]
21. Salah, B. Real-Time Implementation of a Fully Automated Industrial System Based on IR 4.0 Concept. *Actuators* **2021**, *10*, 318. [CrossRef]
22. Sciforce Article. Available online: https://medium.com/sciforce/how-to-recognize-industrial-internet-of-things-f27ccae1ac69 (accessed on 28 November 2021).
23. González, I.; Calderón, A.J.; Figueiredo, J.; Sousa, J.M.C. A Literature Survey on Open Platform Communications (OPC) Applied to Advanced Industrial Environments. *Electronics* **2019**, *8*, 510. [CrossRef]
24. Ungurean, I.; Gaitan, N.-C.; Gaitan, V.G. An IoT architecture for things from the industrial environment. In Proceedings of the 2014 10th International Conference on Communications (COMM), Bucharest, Romania, 29–31 May 2014; pp. 1–4.
25. Rathee, G.; Balasaraswathi, M.; Chandran, K.P.; Gupta, S.D.; Boopathi, C.S. A secure IoT sensors communication in industry 4.0 using blockchain technology. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 533–545. [CrossRef]
26. Chen, W. Intelligent manufacturing production line data monitoring system for industrial internet of things. *Comput. Commun.* **2020**, *151*, 31–41. [CrossRef]
27. Hussein, A.H. IoT (IoT): Research Challenges and Future Applications. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 77–82. [CrossRef]
28. Mondal, D. The internet of thing (IoT) and industrial automation: A future perspective. *World J. Model. Simul.* **2019**, *15*, 140–149.
29. Mourtzis, D.; Vlachou, E.; Milas, N. Industrial Big Data as a result of IoT adoption in Manufacturing. *Procedia CIRP* **2016**, *55*, 290–295. [CrossRef]
30. Routray, S.K.; Sharmila, K.P.; Javali, A.; Ghosh, A.D.; Sarangi, S. An Outlook of Narrowband IoT for Industry 4.0. In Proceedings of the 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 15–17 July 2020; pp. 923–926.
31. Aslam, F.; Aimin, W.; Li, M.; Ur Rehman, K. Innovation in the Era of IoT and Industry 5.0: Absolute Innovation Management (AIM) Framework. *Information* **2020**, *11*, 124. [CrossRef]
32. Maga, C.; Jazdi, N. Concept of a domain repository for industrial automation. In Proceedings of the First International Workshop on Domain Engineering, Amsterdam, The Netherlands, 8–12 June 2009.
33. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial IoT (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
34. Sujay, L. *Vailshery IoT (IoT)—Statistics & Facts*; Statista Research Department: Hamburg, Germany, 2021.
35. Ding, L.; Jiang, W.; Zhou, Y.; Zhou, C.; Liu, S. BIM-based task-level planning for robotic brick assembly through image-based 3D modeling. *Adv. Eng. Inform.* **2019**, *43*, 100993. [CrossRef]

36. 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]
37. Chang, K.-H. Bluetooth: A viable solution for IoT? [Industry Perspectives]. *IEEE Wirel. Commun.* **2014**, *21*, 6–7. [CrossRef]
38. Aich, S.; Chakraborty, S.; Sain, M.; Lee, H.-I.; Kim, H.-C. A Review on Benefits of IoT Integrated Blockchain based Supply Chain Management Implementations across Different Sectors with Case Study. In Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 17–20 February 2019; pp. 138–141. [CrossRef]
39. Wang, G.; Shi, Z.; Nixon, M.; Han, S. ChainS plitter: Towards Blockchain-Based Industrial IoT Architecture for Supporting Hierarchical Storage. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 166–175.
40. Bai, L.; Hu, M.; Liu, M.; Wang, J. BPIIoT: A Light-Weighted Blockchain-Based Platform for Industrial IoT. *IEEE Access* **2019**, *7*, 58381–58393. [CrossRef]
41. Xu, Y.; Ren, J.; Wang, G.; Zhang, C.; Yang, J.; Zhang, Y. A Blockchain-Based Nonrepudiation Network Computing Service Scheme for Industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3632–3641. [CrossRef]
42. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet Things* **2020**, *10*. [CrossRef]
43. Kumar, A.S.; Iyer, E. An Industrial IoT in Engineering and Manufacturing Industries—Benefits and Challenges. *Int. J. Mech. Prod. Eng. Res. Dev.* **2019**, *9*, 151–160. [CrossRef]
44. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain-based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
45. Breivold, H.P.; Jansen, A.; Sandström, K.; Crnkovic, I. Virtualize for architecture sustainability in industrial automation. In Proceedings of the 2013 IEEE 16th International Conference on Computational Science and Engineering, Sydney, NSW, Australia, 3–5 December 2013; pp. 409–415.
46. Arvind, R.V.; Raj, R.R.; Raj, R.R.; Prakash, N.K. Industrial automation using wireless sensor networks. *Indian J. Sci. Technol.* **2016**, *9*, 1–8. [CrossRef]
47. Breivold, H.P.; Sandström, K. Virtualize for test environment in industrial automation. In Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA), Barcelona, Spain, 16–19 September 2014; pp. 1–8.
48. Huang, J.; Kong, L.; Chen, G.; Wu, M.-Y.; Liu, X.; Zeng, P. Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3680–3689. [CrossRef]
49. Zhao, S.; Li, S.; Yao, Y. Blockchain-Enabled Industrial IoT Technology. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1442–1453. [CrossRef]
50. Santhosh, N.; Srinivasan, M.; Ragupathy, K. IoT (IoT) in smart manufacturing. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *76*, 012025. [CrossRef]
51. Cano, J.C.; Berrios, V.; Garcia, B.; Toh, C.K. Evolution of IoT: An Industry Perspective. *IEEE Internet Things Mag.* **2018**, *1*, 12–17. [CrossRef]
52. Faul, A.; Jazdi, N.; Weyrich, M. Approach to interconnect existing industrial automation systems with the Industrial Internet. In Proceedings of the 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany, 6–9 September 2016; pp. 1–4.
53. Okano, M.T. IoT and industry 4.0: The industrial new revolution. In Proceedings of the International Conference on Management and Information Systems, İstanbul, Turkey, 17–20 October 2017; Volume 25, p. 26.
54. Teslya, N.; Ryabchikov, I. Blockchain-based platform architecture for industrial IoT. In Proceedings of the 2017 21st Conference of Open Innovations Association (FRUCT), Helsinki, Finland, 6–10 November 2017; pp. 321–329. [CrossRef]
55. Minchala, L.I.; Peralta, J.; Mata-Quevedo, P.; Rojas, J. An Approach to Industrial Automation Based on Low-Cost Embedded Platforms and Open Software. *Appl. Sci.* **2020**, *10*, 4696. [CrossRef]
56. Trunzer, E.; Calà, A.; Leitão, P.; Gepp, M.; Kinghorst, J.; Lüder, A.; Schauerte, H.; Reifferscheid, M.; Vogel-Heuser, B. System architectures for Industrie 4.0 applications. *Prod. Eng.* **2019**, *13*, 247–257. [CrossRef]
57. Givehchi, O.; Landsdorf, K.; Simoens, P.; Colombo, A.W. Interoperability for Industrial Cyber-Physical Systems: An Approach for Legacy Systems. *IEEE Trans. Ind. Inform.* **2017**, *13*, 3370–3378. [CrossRef]
58. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
59. Shenkoya, T.; Dae-Woo, C. Impact of IoT on social innovation in Japan. *Asia Pac. J. Innov. Entrep.* **2019**, *13*, 341–353. [CrossRef]
60. Google Trends: Industry 5.0. Available online: https://trends.google.com/trends/explore?date=today%205-y&q=industry%205.0 (accessed on 28 November 2021).