

Review

A Survey on the Role of Industrial IoT in Manufacturing for Implementation of Smart Industry

Muhammad Shoaib Farooq ¹, Muhammad Abdullah ¹, Shamyla Riaz ¹, Atif Alvi ¹, Furqan Rustam ², Miguel Angel López Flores ^{3,4,5}, Juan Castanedo Galán ^{3,6,7}, Md Abdus Samad ^{8,*} and Imran Ashraf ^{8,*}

¹ Department of Computer Science, University of Management and Technology, Lahore 54000, Pakistan; shoaib.farooq@umt.edu.pk (M.S.F); abdullah.muhammad001144@gmail.com (M.A.); shamyla.riaz@umt.edu.pk (S.R.); atif.alvi@umt.edu.pk (A.A.)

² School of Computer Science, University College Dublin, D04 V1W8 Dublin, Ireland; furqan.rustam1@gmail.com

³ Research Group on Foods, Universidad Europea del Atlántico, Isabel Torres 21, 39011 Santander, Spain; miguelangel.lopez@uneatlantico.es (M.A.L.F.); juan.castanedo@uneatlantico.es (J.C.G.)

⁴ Research Group on Foods, Universidad Internacional Iberoamericana, Campeche 24560, Mexico

⁵ Instituto Politécnico Nacional, UPIICSA, Ciudad de México 04510, Mexico

⁶ Universidad Internacional Iberoamericana, Arecibo, PR 00613, USA

⁷ Department of Projects, Universidade Internacional do Cuanza, Cuito EN250, Bie, Angola

⁸ Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea

* Correspondence: masamad@yu.ac.kr (M.A.S.); imranashraf@ynu.ac.kr (I.A.)

Abstract: The Internet of Things (IoT) is an innovative technology that presents effective and attractive solutions to revolutionize various domains. Numerous solutions based on the IoT have been designed to automate industries, manufacturing units, and production houses to mitigate human involvement in hazardous operations. Owing to the large number of publications in the IoT paradigm, in particular those focusing on industrial IoT (IIoT), a comprehensive survey is significantly important to provide insights into recent developments. This survey presents the workings of the IoT-based smart industry and its major components and proposes the state-of-the-art network infrastructure, including structured layers of IIoT architecture, IIoT network topologies, protocols, and devices. Furthermore, the relationship between IoT-based industries and key technologies is analyzed, including big data storage, cloud computing, and data analytics. A detailed discussion of IIoT-based application domains, smartphone application solutions, and sensor- and device-based IIoT applications developed for the management of the smart industry is also presented. Consequently, IIoT-based security attacks and their relevant countermeasures are highlighted. By analyzing the essential components, their security risks, and available solutions, future research directions regarding the implementation of IIoT are outlined. Finally, a comprehensive discussion of open research challenges and issues related to the smart industry is also presented.



Citation: Farooq, M.S.; Abdullah, M.; Riaz, S.; Alvi, A.; Rustam, F.; Flores, M.A.L.; Galán, J.C.; Samad, M.A.; Ashraf, I. A Survey on the Role of Industrial IoT in Manufacturing for Implementation of Smart Industry. *Sensors* **2023**, *23*, 8958. <https://doi.org/10.3390/s23218958>

Academic Editors: Arslan Musaddiq, Fredrik Ahlgren, Neda Maleki and Jorge L. Zapico

Received: 1 October 2023

Revised: 24 October 2023

Accepted: 31 October 2023

Published: 3 November 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: Internet of Things; industrial IoT; smart industry; network protocols

1. Introduction

The Internet of Things (IoT), originally introduced in the early 1990s, acquired significant attention during the late 1990s after an investigation by the Massachusetts Institute of Technology (MIT), Auto-ID Labs, which raised its overall publication market [1]. Conceptually, the IoT is a combination of virtual domains that use the internet to exchange information. Various real-world applications have adopted IoT-based technologies that have made life easy. The wide applications of the IoT include smart healthcare, smart agriculture, automatic security systems, smart factories, and smart industries [2].

Although a lot of work has been conducted in the IoT-enabled smart industry, further efforts are needed to overcome issues related to security and privacy [3]. The smart industry

has initiated an extremely positive effort by integrating IoT technology in the industrial domain. As predicted, advanced technologies and industry could solve numerous problems by implementing pervasive security countermeasures through the effective implementation of the IoT [4]. The state-of-the-art implementation of the IoT is solving industrial security issues by providing productive and cost-effective solutions [5]. The industrial IoT process depends on the cyber-physical system (CPS). Therefore, the CPS is considered a pillar of IIoT and is used in the industrial wireless network to monitor and control the physical processes among IoT devices, sensors, controllers, and actuators [6]. Furthermore, IIoT provides cost-effective and well-organized scheduling of limited resources to boost production.

Figure 1 shows the recent IIoT trends, which offer cost-effective, secure, and authorized connectivity among smart factories, workers, smart healthcare, transportation, and logistics. In addition, IIoT-based networks using wireless technologies require real-time monitoring, CPS, and smartphone-based IIoT applications. Moreover, smart IoT sensors monitor temperature, airflow, and humidity, keep safe historical records, and enable smoke and heat alarms. Similarly, smart industry servers, IIoT-based servers, and gateways play a crucial role in securing smart industry data and offer on-demand IIoT assistance to permissible subscribers. The top research trends in the IIoT domain consist of IIoT applications, network topologies, network architecture, communication protocols, and security challenges [7,8]. Soori et al. [9] present a review of the impact of IoT in the smart industry. Various applications of the IoT in smart factory environments are covered, like asset tracking, quality control, monitoring, energy optimization, etc. In addition, current challenges are identified to outline future directions. Although a significant amount of work has been conducted in the IIoT field, a comprehensive survey is required to identify the recent research trends in the smart industry.

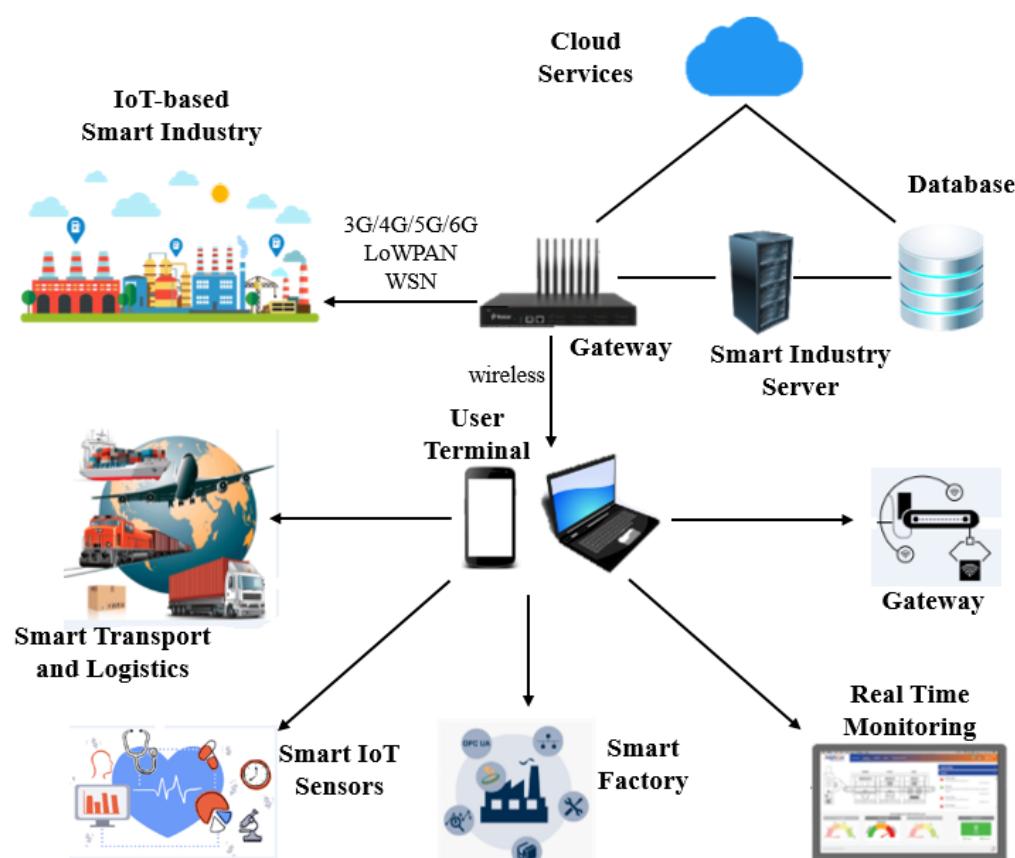


Figure 1. Industrial IoT trends show recent applications for industrial IoT.

1.1. Survey Contributions and Comparison with Related Work

In existing research, many surveys focus on the dependencies of IIoT components, security challenges, solutions, and characteristics. For example, the work presented by [10,11] focuses only on the research landscape of security challenges of IIoT but misses major attacks and their related countermeasures, while the current survey presents a comprehensive overview of attacks and countermeasures. On the other hand, [12] presents blockchain solutions for IIoT and attack taxonomies but does not provide a clear explanation for real-world mapping incidents. Comparatively, this study presents an extensive survey of recent research efforts and also provides real-world examples.

Similarly, in [13,14], a software-based and fog-based IIoT architecture is presented only. In contrast, this work not only describes IIoT network architecture but also presents comprehensive and updated literature on the layered structure of IIoT architecture. In a similar fashion, [15] proposed a fog cloud architecture between IIoT devices to briefly control the network traffic. However, the proposed architecture does not fulfill the security requirements; the current study presents an updated view of security-related needs and solutions for different IIoT sectors, security attacks, and threats.

The work illustrated in [16,17] explains the IIoT framework taxonomies to help researchers discover the security, network, and technology gaps but misses the security threats and their existing solutions. The current study briefly discusses attack taxonomies and their solutions. IIoT security research can significantly impact the industrial security process. Strong bonding between security and safety in IIoT is identified by [18]. Similarly, Ref. [19] propose a security solution and identify the security challenges in IIoT but lack taxonomy attacks and their solutions.

In comparison to the above-cited works, the current survey presents a comprehensive and extensive survey of IIoT attacks, weaknesses, and vulnerabilities, as well as measurements to overcome the identified security threats and challenges. In [20] the research gap of the manufacturing system between different layers of industry 4.0 is presented. Similarly, the survey [21] describes the scope of the study and challenges of intelligent factories extensively but does not explain the current modern applications of IIoT. In comparison to these, this survey presents an updated and comprehensive survey on IIoT applications, sensors, and smartphone applications. Table 1 provides the contributions of the current survey in comparison to existing works.

Table 1. Comparative analysis of existing related work.

Ref.	IIoT Security	Major Attacks	Countermeasures	Blockchain	Software-Based IIoT	Fog-Based IIoT
[10]	Yes	No	Yes	No	No	No
[11]	Yes	No	Yes	No	No	No
[12]	Yes	Yes	Yes	No	No	No
[13]	No	No	Yes	No	Yes	Yes
[14]	No	No	Yes	No	Yes	Yes
[15]	No	Yes	Yes	No	No	Yes
[16]	Yes	No	No	Yes	No	No
[17]	Yes	No	No	Yes	No	No
Current	Yes	Yes	Yes	Yes	Yes	Yes

The contributions of this survey are not limited to the classification of privacy and security issues in IIoT; it also identifies the weaknesses, risks, problems, and challenges and provides future research directions to overcome these attacks. Many researchers have surveyed IIoT security challenges, attacks, and related countermeasures; however, the current work is more comprehensive than these studies. We present a state-of-the-art

network infrastructure covering network topologies, network platforms, and network architecture based on big data and cloud computing.

1.2. Organization of Survey

Section 2 presents key components of the IoT-based smart industry together with the related technologies. In Section 3, the state-of-the-art network infrastructure is introduced, which includes a structural layer of IIoT architecture, IIoT network topologies, IIoT network platforms, and protocols. In Section 4, various IIoT application domains, smartphone applications, and sensor applications are presented. Section 5 presents IIoT-based security attacks and their countermeasures. In Section 6, research directions and future implementation of IIoT are discussed. Finally, in Section 7, open research challenges faced by technologists while implementing the IoT in the smart industry are discussed.

2. Major Components Related to IoT-Based Smart Industry

The IoT industry comprises four elements, including data acquisition, physical structure, data analytics, and data processing, as illustrated in Figure 2. The most crucial aspect of the smart industry to avoid critical situations is the physical structure that controls all sensors, actuators, and devices. A sensor is responsible for various tasks, such as temperature monitoring, humidity monitoring, vibration sensing, current monitoring, pressure detection, etc. IoT gadgets, on the other hand, conduct various control functions, such as device identification, node discovery, and naming services. Any sensor or device controlled by a microcontroller can perform all these tasks. Each control activity can be remotely performed by any computer or remote device linked to the internet.

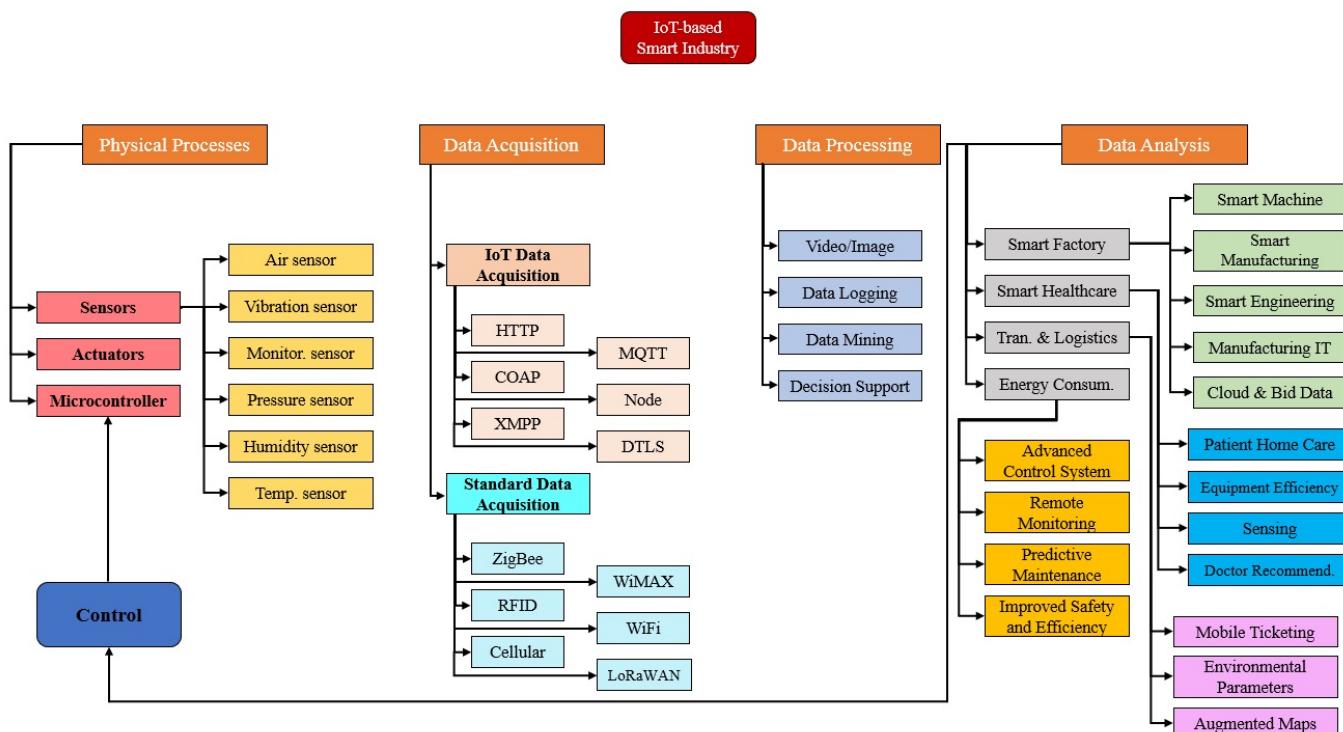


Figure 2. Key components of IoT smart industry.

Data acquisition is the process of monitoring and analyzing various sensors, collected data, and hardware and is categorized into two sub-components: standard data acquisition and IoT data acquisition. The IoT data acquisition has six protocols: (i) node, (ii) message queuing telemetry transport (MQTT), (iii) datagram transport layer security (DTLS), (iv) constrained application protocol (CoAP), (v) extensible messaging and presence protocol (XMPP), and (vi) hypertext transfer protocol (HTTP). However, more protocols can be added or removed depending on the conditions and requirements of the designed system. The most commonly used protocols for standard data acquisition are ZigBee, Lora WAN, WiFi, mobile cellular networks, radio frequency identification (RFID), and WiMAX. Data processing includes several components, such as video or image processing, data mining, decision support systems, and data loading. Therefore, any feature can be implemented according to the system requirements and executed in parallel to offer additional services.

Data analytics aims to reduce costs by identifying more efficient methods of storing large amounts of data. Data analytics involves four sub-applications: smart factories, transportation and logistics, smart healthcare, and energy consumption in IIoT. Each device in a smart factory is connected to the internet and linked to actuators and sensors. The IIoT allows manufacturing devices to exchange data between service providers and users in smart factories [22]. Similarly, improved patient care, a faster and more accurate diagnosis, and more personalized treatment are also possible with the utilization of IIoT in healthcare [23]. Smart transportation-based IIoT helps to improve multiple devices and sensors, such as vehicle control systems, car navigation systems, traffic signal management systems, and speed monitoring systems [24]. In addition, the IIoT can reduce energy consumption, increase sustainable energy usage, and reduce the environmental impact of energy use [25].

3. IIoT Network Infrastructure

The IIoT network infrastructure is the backbone of the IoT for industries, and helps to connect many sensory, physical, and network devices to improve product quality and the manufacturing process, thereby playing an important part in the growth of IIoT. The infrastructure in IoT-enabled industrial network architecture comprises the industrial network platform, the network topology, and protocols.

3.1. Layered Structure of IoT-Enabled Industrial Network Architecture

The most important aspect of IIoT is the IIoT network, which connects devices, actuators, sensors, processors, cyber-physical systems, and production flow to make smart decisions [26]. The three-layer architecture, including the network layer, the perception layer, and the application or support layer, was initially presented by the researchers [27,28]. However, the three-layered architecture is weak from a security perspective and unable to fulfill the IoT network requirements [29]. For example, [28,29] points out several attacks on IIoT and various other security weaknesses. For that reason, the three-layer architecture has been shifted into a four-layer infrastructure (the perception layer, the network layer, the application layer, and the processing layer) to enhance the security of IoT networks [30]. After a comprehensive study of these four layers, two more solutions are IPv6 and 6LoWPAN, as shown in Figure 3. The support layer is the last stage of abstraction in the network architecture, which makes it more secure and robust. At this stage, communication protocols are used to keep track of several smart industry characteristics, like energy usage, cost reduction, and productivity enhancement. The network architecture includes sensors/devices at the first layer, communication devices at the second layer, data processing and storage at the processing layer, and smart applications at the fourth layer, as shown in Figure 4.

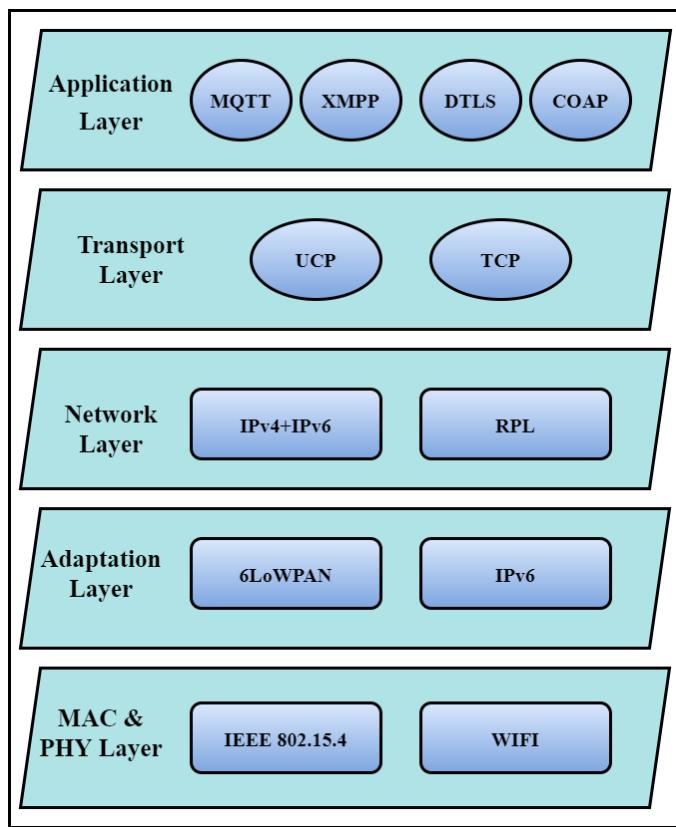


Figure 3. The 6LoWPAN layer structure.

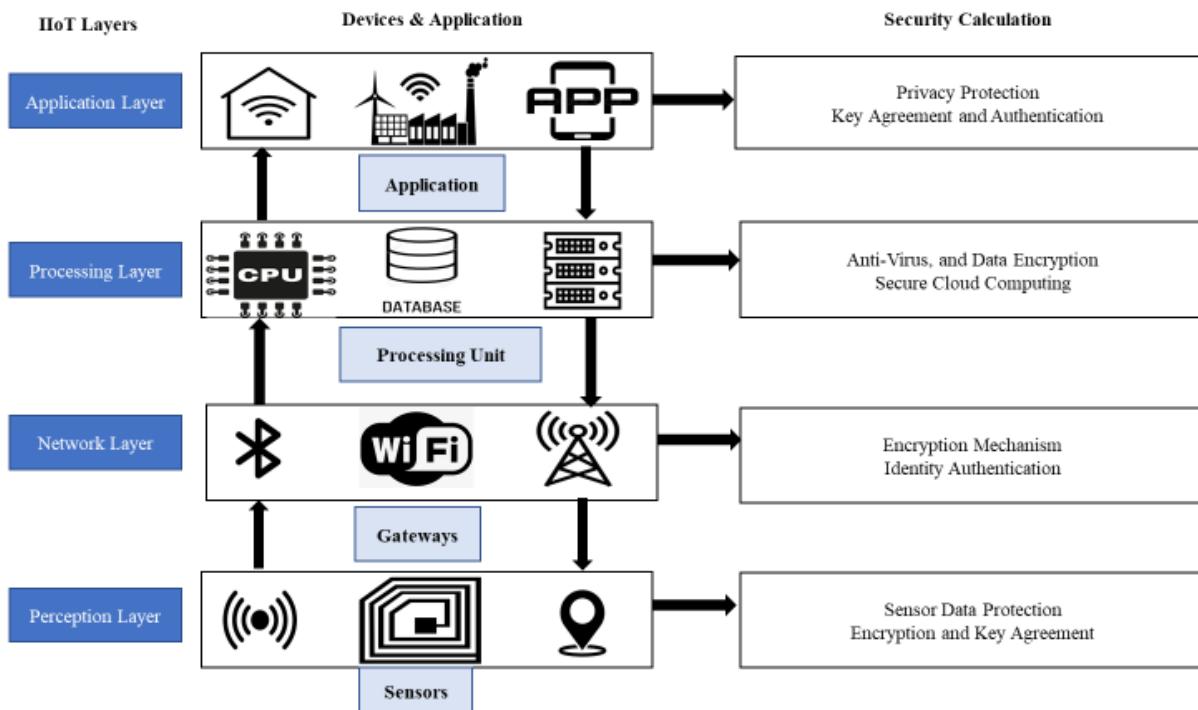


Figure 4. IIoT four-layer architecture.

3.1.1. Perception Layer

The perception layer is also defined as the sensor layer. It is a mixture of sensor and physical devices, global positioning system (GPS) modules, RFID, 2-D barcode, and closed-circuit television (CCTV) cameras [27]. It gathers data from all connected devices and sends

them to the servers. In the industrial environment, devices are responsible for transporting raw items, monitoring production areas, and catching sensory data, industrial robots, automated guided vehicles (AGVs), and transporter systems. It is a sensitive layer and can be attacked easily. The security threats for the perception layer include node injection, tampering, eavesdropping, reply attacks, radio frequency (RF) interference, timing attacks, and node capturing [31].

3.1.2. Network Layer

The network layer, also called data transmission, is responsible for receiving and transferring industrial information between physical objects, smart things, devices, sensors, networks, and servers using a wired or wireless medium [28]. It consists of protocols like IPv4, IPv6, WiFi, ZigBee, etc., and helps the connection between the perception (or sensor) layer. As a result, the network layer is susceptible to various attacks. Man-in-the-middle attacks (MITM), Sybil attacks, spoofing, denial of service (DoS), and sinkhole attacks are the riskiest and most well-known attacks on the network layer [31].

3.1.3. Application Layer

The application layer is responsible for transferring IIoT applications from a connected device to the user. It works as a bridge between the end nodes and the network of IIoT, allowing them to communicate with approved software components [29]. The smart home, smart factory, and smart robotics are famous IIoT applications [32]. Securing the application layer is extremely challenging as security is a critical issue. Smart home applications are fragile to security issues because they are insecure from the inside and outside, which can introduce vulnerabilities. The security attacks on the application layer can be Trojan horses, malicious code attacks, cross-site scripting, and side-channel attacks [33].

3.1.4. Processing Layer

The main reason for creating the fourth processing (or support layer) layer is various security issues in different layers of IIoT. The three-level architecture is not secure enough to pass data directly to the network layers; this layer overcomes multiple threats. The fourth-level architecture was proposed to overcome security issues in IIoT. Authentication is prioritized using passwords, pre-shared secrets, and keys and then sending collected data to the network layers. It contains databases and servers that can run various tasks like decision-making, storing vast amounts of data, and computer algorithms [13].

3.2. IoT-Enabled Industrial Network Platform

Big data analytics and cloud models have been included in the IIoT network platform.

3.2.1. IIoT Network Platform Based on Big Data Analytics

Big data analysis collects essential and useful information from massive data and various types of data. The increasing deployment of sensors and IoT devices has resulted in a big data source in the IIoT. In IIoT systems, big data analytics is utilized for both functional and customer data. The big data-based IIoT network platform is shown in Figure 5. It is divided into six parts: big data analysis, employee experience, storage devices, monitoring and sensing, communication protocols, and physical implementation. This platform allows users to connect to the IoT backbone and collect data on equipment's health monitoring, indoor climate, miniaturization, manufacturing process automation, etc. [34].

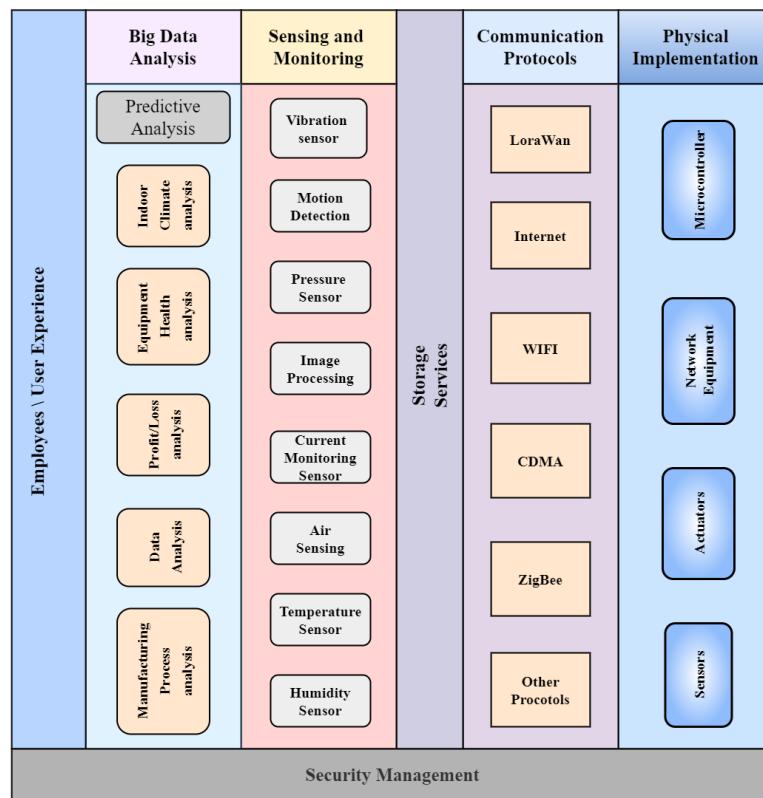


Figure 5. IIoT network-based platform on big data analytics.

Employee's Experience: The employee experience layer is created to benefit employees by monitoring equipment health and identifying temperature, humidity, air, pressure, and moisture-based indoor climate change. This identification helps industries to resolve production risks and increase income.

Predictive Analysis: Predictive analysis uses smart IIoT technology and market intelligence to make a smart environment. The key role of predictive analysis is to monitor, examine, and progress smart industrial technology for digital wakefulness. In addition, predictive analysis is used to check if the manufacturing process is working in the right direction without technical faults and risks. Based on manufacturing process management, different detection devices are used to identify indoor climate changes, equipment health, profit/loss estimation, and data analysis.

Sensing and Monitoring Analysis: The sensing and monitoring process is performed using various sensing and detecting equipment to store information about the manufacturing process. The sensing layer automatically analyzes the data collected from different resources. In addition, statistical analysis is performed on data received from sensors to actuate the production risks. Sensors such as vibration sensors, air sensors, temperature sensors, current monitoring, and humidity sensors provide crucial data regarding production units and help the smart industry run smoothly.

Storage Service: The data related to the smart industry are saved to perform future analyses to enhance manufacturing productivity appropriately.

Communication Protocols: Smart industrial data are collected and summarized in communication protocols. Therefore, the central pillar of IIoT analyzes and transmits data using different protocols. Third-party service providers like code division multiple access (CDMA), long-term evolution (LTE), or the global system for mobile communications (GSM) are no longer available. Researchers across the globe recommend ZigBee as the leading protocol for communication over long distances.

Physical Implementations: Several sensors, actuators, and microcontrollers monitor various IIoT applications. In addition, additional devices in the network such as routers, switches, and gateways are major components of the physical layer. This layer detects the whole

environment and activates according to specified commands. The microcontroller works as a controller and performs network-related tasks and other functions handled by sensors and actuators.

3.2.2. IIoT Network Platform Based on Cloud Computing

Cloud computing delivers a huge amount of storage via large virtualized computers linked together. In addition, cloud computing and big data consist of the latest high-performance computing, IIoT technologies, service-oriented technologies, and cloud services [35]. Figure 6 shows the cloud computing-based IIoT network platform with four layers: cloud storage, gateway, fog computing, and hardware modules. The IIoT-related data, including manufacturing processes, indoor climate change, moisturizing, and smart industry marketing, are stored in the cloud. The networked infrastructure provides on-demand resources. In addition, online services and analytical resources are also stored and accessed via cloud computing [36].

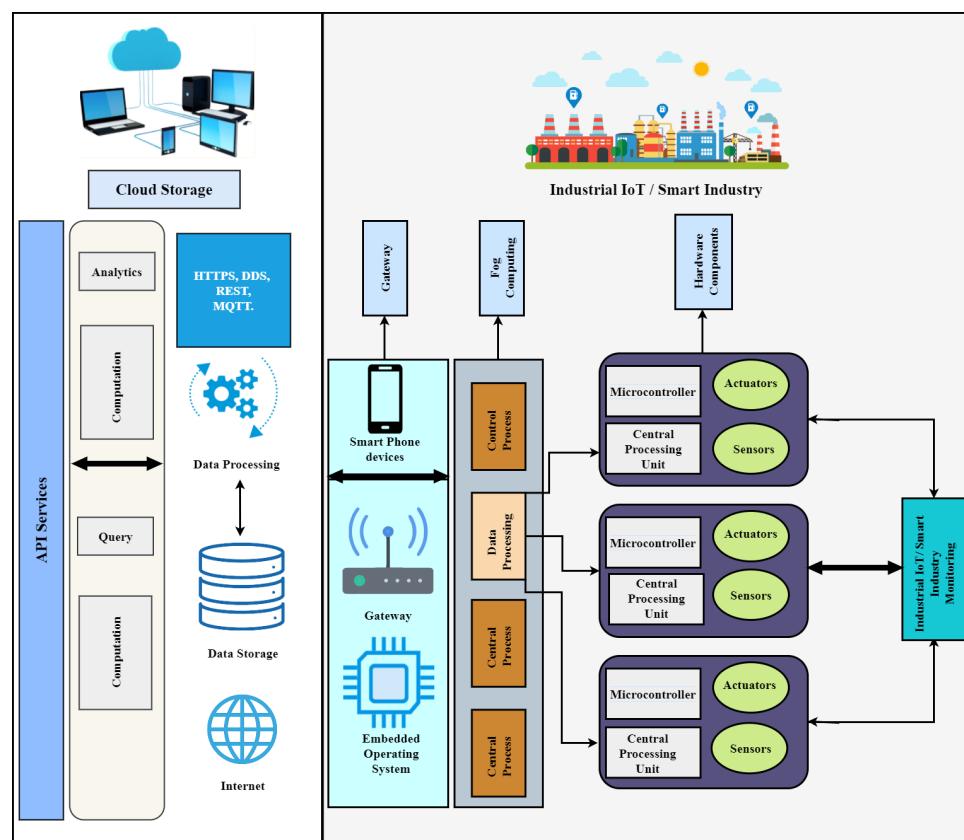


Figure 6. The cloud computing-based industrial IoT network platform.

Connecting a large number of devices to the internet for data sharing is not appropriate or safe. Instead, local gateways are designed to solve data-sharing problems by connecting all hardware devices and sensors for security, connectivity, and controllability. For example, a gateway in a production process or productivity unit controls a real-time manufacturing monitoring system and enhances automation. Similarly, fog computing allows the distribution of hardware components, cloud services, and the combination of available resources [37]. In addition, fog computing ensures real-time processing and reduces cloud computational load. The main objective of fog computing is to take advantage of both edge and cloud computing to maximize cloud computing resources and on-demand scalability.

Multiple sensors, actuators, microcontrollers, and a central processing unit are applied to components to sense and monitor different IIoT variables. Hardware components are delivered worldwide or locally and utilized to provide services or processes. A fast response time and the ability to exchange information are required for smart manufacturing

deployment. MQTT and representational state transfer (REST) are two protocols that meet both the requirements of a quick response time and the ability to communicate information. Using a big data center, a distributed system is made more efficient for smart manufacturing [38]. It also divides large computations into simple and smaller jobs, such as controlling temperature, floor moisture, indoor climate, and production units.

3.3. IoT-Enabled Industrial Network Topology and Protocols

An IIoT network's topology describes how different network elements of the IIoT are connected and provides an ideal smart industry scenario. Several IoT connection protocols are commonly used in the industrial field for the smart industry [39]. Using these protocols, employees/workers can communicate more easily and make effective decision-making for the smart industry to improve and monitor the manufacturing productivity of the unit.

3.3.1. IoT-Enabled Industrial Network Platform

IIoT network topology provides a state-of-the-art network topology for the smart industry. IIoT network topology combines different sensors, actuators, and physical devices like pressure, temperature, humidity current monitoring, vibration, and water detecting sensors, as depicted in Figure 7. Moreover, the ideal scenario (conceptual design) for future smart industry solutions includes the help of storage devices such as laptops, tablets, smartphones, grid computing, and actuators [40].

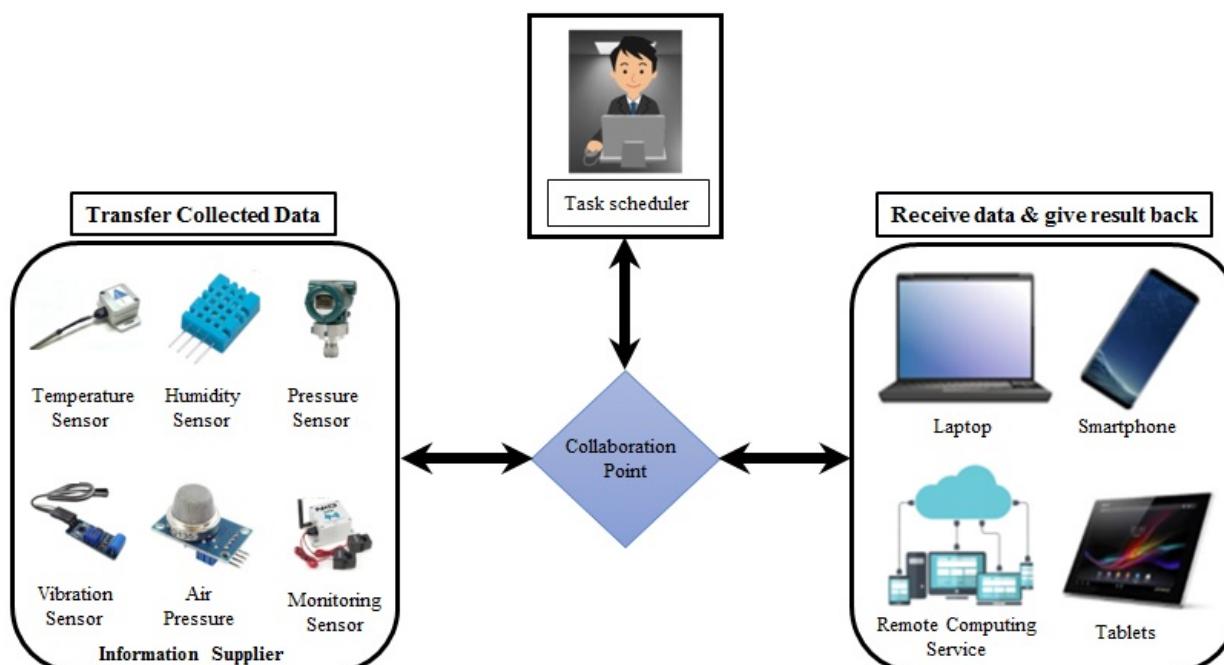


Figure 7. Conceptual design for smart industry.

A structural framework of IIoT network topology is given in Figure 8. The production unit and manufacturing sector are monitored with the help of different protocols and devices. Data from various sensors and devices are useful for aggregated data. Data are then processed and stored. Industrialists/employees can remotely monitor different manufacturing unit aggregations and analyses. Furthermore, topology comprises an appropriate network configuration for industrial video streaming [41].

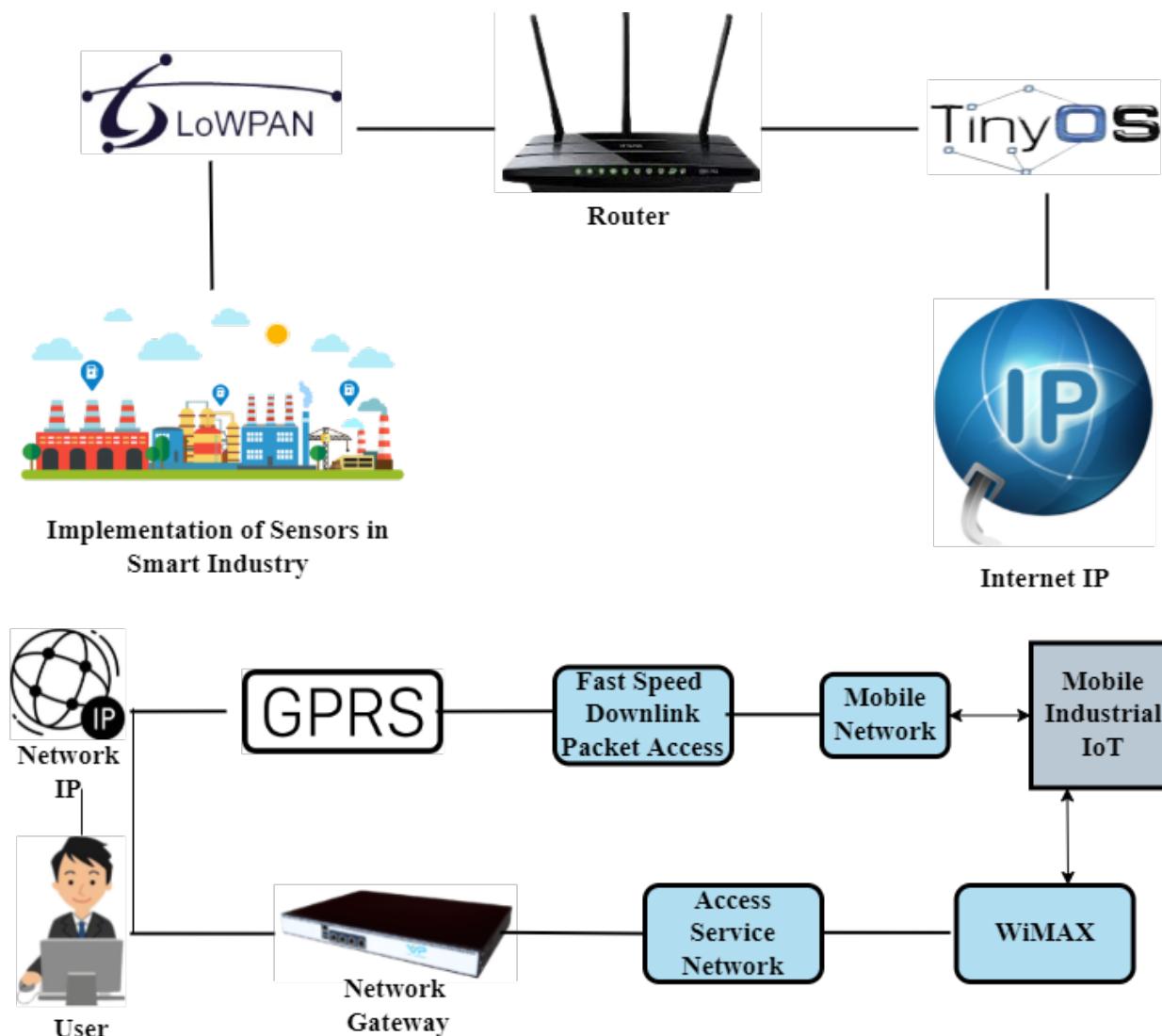


Figure 8. Remote monitoring topology in a manufacturing unit of smart industry.

Similarly, Figure 9 shows an interconnected network comprising internet protocol (IP), GSM, WiMAX, access service network gateway, and manufacturing units. A wireless sensor network is used to monitor (the manufacturing process) and control (power consumption) in many fields of the smart industry. ZigBee is used in network topology; the function of ZigBee is to transfer data or sensitive information through routers, sensors, base stations, and end devices. In addition, sensors like air sensors, temperature sensors, vibration sensors, humidity sensors, current monitoring sensors, and microcontrollers are used [42]. The router and microcontroller are connected directly to the end devices, and the microcontroller communicates with the base station through the serial port to examine the collected data. According to software monitoring, each end device is configured properly, and attached sensors are enabled. When the sensors are turned on, each device follows the router to connect in the designed way. End devices can connect to the base station, which analyzes the information. Data are transferred through ZigBee to the controller or router when end-device sensors are read. The bidirectional communication via ZigBee is the main strength of this network topology.

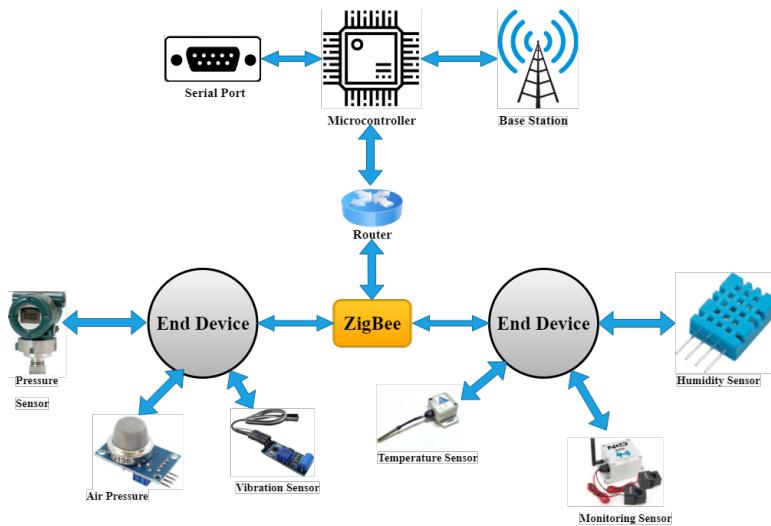


Figure 9. Low-power wireless sensor network topology.

3.3.2. IIoT Communication Protocols

Various IoT communication protocols have been widely used in the smart manufacturing industry. Therefore, it is very useful to use smart manufacturing and monitor the rise in industry productivity by employing these protocols [39]. The most popular wireless protocols are ZigBee, Bluetooth, WiFi, MQTT, Lora WAN, mobile cellular networks, RFID, WiMAX, and LR-WPAN. Table 2 provides a summary of wireless protocols utilized in IIoT communication. These protocols are discussed from several aspects. For example, protocols are described with respect to operating frequency, IEEE standard, and transmission range. In addition, data rate, cost, and energy usage are also given. LoraWAN and WiMAX are better choices for long-range communication, but LoraWAN consumes less energy compared to WiMAX.

Table 2. Comparison between current wireless protocols.

Protocols	Frequency Band	Standards	Transmission Range	Data Rate	Cost	Energy Usage
ZigBee	2.4 GHz	IEEE 802.15.4	10–20 m	20–250 Kilobyte	Low	Low
Bluetooth	24 GHz	IEEE 802.15.1	8–10 m	1–24 Mbs	Low	Very Low
WiFi	5–60 GHz	IEEE 802.11	20–100 m	1 Mbegabit–7 Gigabyte	High	High
MQTT	2.4 GHz	OASIS	-	250 kilobyte per second	Low	Low
Lora WAN	868/900 MHz	Lora WAN R1.0	<30 KM	0.3–50 Kb per second	High	Very Low
Mobile Cellular Networks	865–MHz, 2.4 GHz	2G–GSM, CDMS–3GUMTS, CDMA2000, 4G–LTE	Entire Cellular Area	2G: 50–100 Kb per second 3G 200 Kb per second 4G: 0.1–1 Gb/s	Medium	Medium
RFID	860–960 MHz	ISO 18,000–6C	1–5 m	40–160 Kb per second	Low	Low
WiMAX	2 GHz–66 GHz	IEEE 802.16	<50 KM	1 Mb per second–1 Gb per second (Fixed) 50–100 Mb/s (mobile)	High	Medium
LR-WPAN	868/915–MHz, 2.4 GHz	IEEE 802.15.4	10–20 m	40–250 Kb per second	Low	Low

ZigBee: ZigBee technology is a low-data-rate, low-power consumption, and low-cost wireless networking protocol developed by the ZigBee Alliance for automation and sensor networks. The ZigBee network can contain many nodes in an industrial environment and connect them into a single control network [43].

Bluetooth: Bluetooth is a low-power, short-range personal area network (PAN). It was developed by Ericsson but operated under the auspices of the Bluetooth special interest group (SIG), which created the Bluetooth standards (IEEE 802.15.1). Moreover, to close the energy efficiency gap between Zigbee and Bluetooth for no-streaming sensor node-type applications, the low energy standard for IIoT-based Bluetooth has been modified [44].

WiFi: In the current era of modern advancements, the availability of WiFi has become a necessity. WiFi stands for wireless fidelity, and was introduced by the Institute of Electrical and Electronics Engineers (IEEE) and is a communication standard for wireless local area networks (WLANs). WiFi operates on physical and data link layers. Furthermore, these standards operate at different bandwidths, ranging from 5 GHz to 60 GHz. The communication and manufacturing processes are discussed in [45].

MQTT: MQTT is a remote connection between two messages queuing telemetry transport protocols in the IoT. It is a combination of low-power protocols with high bandwidth efficiency. In the smart manufacturing industry, MQTT is utilized for monitoring and development. The use of MQTT to track, monitor, and investigate the manufacturing process and improve efficiency has been presented as a low-cost, web-based IoT solution [46].

Lora Wan: Lora WAN is a long-distance communication protocol designed for IoT and mobile-to-mobile (M2M) applications that provide a cellular-style, low-data-rate communications network. The primary goal of the Lora WAN protocol is to ensure interoperability across several operators in the IIoT [47].

Mobile Cellular Networks: There are many generations of mobile communication standards, including 2G, 3G, 4G, and 5G. Each generation of mobile phones has its own challenges and capabilities. For example, smart manufacturing based on cyber-physical manufacturing systems helps IIoT in automation, real-time monitoring, and collaborative control. Although 3G and 4G cannot meet the CPMS standard requirements, 5G can support IIoT [48].

RFID: RFID records data by assigning a unique number to each object. RFID systems comprise readers, hosts, and tags that receive and broadcast radio waves, also known as the communicators. RFID tags can be active or passive, and they come in a range of sizes and designs. Passive tags are less expensive than active tags and are more profitable. Tags have unique ID numbers and IIoT environmental information, such as moisture level, temperature condition, humidity, etc. In the IIoT, RFID monitors the manufacturing process [49].

WiMax: The data transfer rate of WiMAX ranges from 1.5 Mb to 1 Gb per second. However, technical advancements have improved the data transfer rate in recent years. Furthermore, WiMAX offers multi-access connectivity, including wired and wireless connectivity for fixed, mobile, portable, and mobile communication, used in IIoT [50].

LR-WPAN: In recent years, advancements in high-level communication protocols such as ZigBee have developed low-rate wireless personal area network (LR-WPAN) standards. LR-WPAN offers data rates ranging from 40 to 250 Kb per second. This standard's key feature is that it delivers low-speed and low-cost communication services. It has a frequency band that ranges from 868/915 MHz to 2.4 GHz. LR-WPAN has been used in IIoT control applications and manufacturing monitoring systems [51].

4. IIoT Applications

The IIoT system is used as an order in many fields, such as smart factories, healthcare, energy consumption, transportation, logistics, etc. There are three types of industrial applications: IIoT applications, sensor-based applications, and smartphone-based applications. The classification of IIoT-based applications is presented in Figure 10, which was created to examine the industry's current IoT solutions.

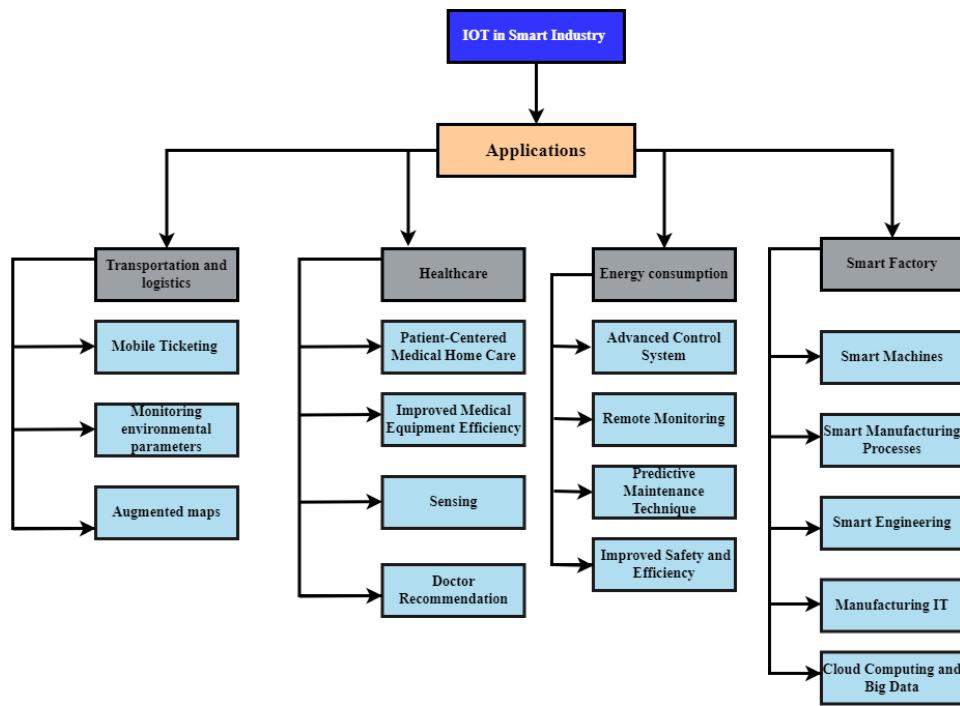


Figure 10. IoT applications in smart industry.

4.1. IIoT Sub-Applications

Many IIoT applications have been used to create more effective resources for the fast growth of industry productivity. However, depending on the proposed industrial application, designers may trade off these goals to balance costs and benefits. Different types of industrial applications are discussed in the subsections that follow.

4.1.1. Transportation and Logistics

The IoT is essential to the rapid growth of transportation, logistics, and industrial manufacturing processes [52]. Transportation and logistics companies can manage the real-time monitoring of the movement of physical objects from one place to another over the complete supply chain, including distribution, manufacturing, and shipping [53].

IIoT offers advanced technologies and solutions for the automobile and transportation industry [54]. IoT technologies have improved networking, communication, sensing, and data-processing capabilities for underused vehicles in parking spaces or on the road. IoT technologies make it possible to track vehicles, monitor their movement, and predict current and future locations. For example, a very effective and intelligent technology (iDrive system) made by BMW (Rolls Royce Phantom) uses different sensors and tags to monitor the environment, such as road conditions, to provide driving directions and trace the vehicle location [55]. Zhang et al. [56] built an intelligent monitoring system that uses RFID, sensors, tags, and wireless communication technologies to monitor humidity and temperature within refrigerator trucks. Tesla makes autopilot (advanced driving assistance system) vehicles that can monitor vehicles' movement and be controlled remotely at any place [57]. IIoT technology such as RFID, autopilot systems, computer vision, and robotics have helped the transportation and logistics industry increase productivity and automate processes [58].

Mobile Ticketing: Smart transportation uses near-field communication (NFC) tags, a numeric identifier, and a visual marker [59]. Using IIoT technologies, consumers obtain information about various possibilities from the web services by passing their mobile phone over the NFC tag or directing their mobile phone toward the visual markers. The mobile phone obtains data from connected web services (stations, passengers, pricing, available seats, and type of services) and allows users to purchase equivalent tickets [60].

Monitoring Environmental Parameters: IIoT technology can help monitor our daily environment, like the temperature and humidity [61]. For example, food manufactured in a factory and traveling thousands of kilometers to reach customers must be monitored to reduce the risk of food spoilage. IoT-based advanced technologies, sensor technologies, and pervasive computing improve the productivity of the food supply chain [62].

Augmented Maps: IIoT-based applications make tourist maps, tags, and NFC-enabled smartphones available for browsing [63]. In addition, IIoT technologies help provide information on restaurants, monuments, hotels, and other locations relevant to users' interests [64].

4.1.2. Healthcare

The healthcare industry is benefiting greatly from IIoT applications [65]. They reduce cost and provide remote control of medical equipment, home-bound patient care, modeling, and monitoring [66]. As a result, hospitals benefit from smart equipment that decreases a patient's waiting time and improves equipment performance. The popularity of mobile internet services has promoted the faster growth of IIoT-powered in-home healthcare (IHH) services [67]. Different health application domains can be helped, as mentioned below.

Patient-Centered Medical Home Care: Patient-centered medical home (PCMH) care is a simple solution to many problems faced by the healthcare industry, such as chronic disease management, overuse of emergency rooms, patient satisfaction, high medical costs, and accessibility [68,69]. The IIoT has completely changed the healthcare industry. The use of modern technology saves time and allows nursing staff to perform more work in less time, such as taking blood pressure without wasting time. IIoT devices can be utilized to collect patient data, upload it to the cloud, and have a doctor make a fast diagnosis and suggest appropriate therapy. Moreover, a doctor can make a timely decision for appropriate treatment. For example, Cambridge consultants' flow health hub (FHH) IIoT home diagnostics can gather samples and promptly deliver blood pressure, cholesterol, and diabetes medication [66]. In addition, this method automatically alerts doctors that their patients need or want assistance.

Improved Medical Equipment Efficiency: The fast growth of IIoT technology gives doctors more useful information. With a concept known as medical device plug-and-play (MD PnP), IIoT allows modern medical equipment to be connected instantly. MD PnP is a cyber-physical system for medical devices [70]. The healthcare industry is affected by two sides of CPSs. The first involves discrete computer logic of various secured medical equipment in the cyber-world. The second is that it offers a complicated biochemical system that includes a patient-in-the-loop mechanism [71]. As a result, CPSs offer valuable data and reduce patients' waiting times. Thus, CPS sensors provide real-time data to guide doctors in making the best decisions for their patients [72].

Sensing: Sensor devices provide valuable information on patient health and diagnosing patient disease [73]. In addition, the IIoT application domain offers telemedicine solutions such as informing patient welfare and monitoring patient health with advanced medical equipment [74]. Sensors are useful for both in-patient and out-patient treatment. In addition, wireless-based remote monitoring systems are generally employed to outreach to patients anywhere in the world through the employment of multiple wireless technologies paired with real-time bio-signal monitoring systems to capture the patient's movements dynamically [75].

Doctor Recommendation: Today, choosing the right doctor online and getting an appointment is a tough job for patients. Patients have a big problem without real-time data and valuable information about professional doctors [76]. In this capacity, IIoT-based applications have developed a doctor recommendation system to get an online appointment with a doctor [77]. In addition, recommendation systems are still a hot topic in machine learning, image processing, and data mining [78]. The sensor data received from patients, feedback for qualifying doctor suggestions, and doctor appointment policies have been updated in the doctor recommendation system [38].

4.1.3. Smart Factory

Smart factories utilize IIoT technologies to connect machines to humans (M2P) by using controlling devices like operation devices, field devices, mobile devices, and so on [39]. The purpose of smart factories is to provide smart products, services, and feedback to the client. Furthermore, cloud computing and big data are used to build smart factories' manufacturing processes, hardware, and software [79]. Wang et al. [80] present a smart factory design that describes how to link cloud computing, an industrial wireless network, and workstations with smart shop-floor devices. Smart machinery, smart manufacturing, smart engineering, manufacturing information technology (IT), cloud computing, and big data are the essential components of a smart factory [40].

Smart Machine: A smart machine combines an autonomous, networked system, sensors, processing capabilities, and communication devices in IIoT [81]. Smart machines have also been linked to other field devices and humans and can work remotely. In addition, smart machines use IIoT to perform self-operability, self-maintenance, and self-awareness [16].

Smart Manufacturing: The IIoT directly impacts the manufacturing industry by merging cyber-physical production systems and the IoT, resulting in smart manufacturing, which connects the practical and physical worlds [41]. The smart manufacturing process is automated, efficient, and effective, and its real-time performance is one of its key characteristics [82]. Smart manufacturing processes require industries to dynamically fulfill customer requests based on the interconnectivity provided by the IIoT to manage personalization [44]. Furthermore, customer feedback plays a vital role in manufacturing [83]. As a result, both the cyber-physical production system and the IIoT concepts are integrated into the smart manufacturing concept [84]. IIoT consists of smart sensors that can send information about machines, fleets, and components and monitor the production system [85].

Smart Engineering: Smart engineering in smart factories creates product engineering, product design, and product development [86]. Big data analytics are generally employed to attain continuous feedback, providing a more effective engineering process in IIoT, dispensing efficient optimization, and improving productivity.

Manufacturing IT: Manufacturing IT refers to smart factories' information technology infrastructure [79]. Manufacturing IT involves the production system's algorithms, software, and hardware infrastructure, such as sensors and actuators that offer smart monitoring and control of physical devices. In addition, IIoT enables production management systems to integrate many technologies and maintain all data generated during manufacturing.

Cloud Computing and Big Data: The latest high-performance computing, IIoT technologies, service-oriented technologies, and cloud services are part of cloud computing and big data [35]. In addition, cloud computing and big data built a business model for the manufacturing industry, creating smart factory networks that support productive collaboration and helping it adjust product innovation with business policy [36]. Cloud computing fulfills customers' requests for services, including product design, management, manufacturing, and testing. Moreover, trends in smart manufacturing, innovation, and future methodologies focus on the cloud, the CPS, and the IoT [37]. For example, the design of smart manufacturing has been reviewed by Saldivar et al. [87]. In addition, Rugman et al. [88] explain the benefits for the manufacturing industry and highlight the latest technologies, such as big data analytics, autonomous robots, cyber security, system integration, cloud computing, augmented reality, simulation, and additive manufacturing.

4.1.4. Energy Consumption

IIoT technologies have modified the energy sector, and efficient sensor monitoring systems have decreased factory energy usage [89]. Therefore, the industrial energy system is an important component of the IIoT. In addition, IIoT technologies have increased the performance of new energy systems. Furthermore, a new energy system increases environmental security [90]. The study [91] provides an energy-efficient design for energy-constrained mobile devices. The authors consider multiple-antenna access points for radio

frequency energy harvesting using non-orthogonal multiple access (NOMA). For obtaining a better system performance, the communication protocol comprises four phases. Results indicate a 3 to 30% improved performance of successful computation probability. When compared to traditional energy systems in IIoT, the new energy system has the following characteristics:

Advance Control System: The management and control of old energy systems require many workers, whereas the new IIoT energy system requires less labor [92]. Furthermore, the effective application of new technologies in connectivity and interoperability improves system operability. The latest communication and information technologies have a tremendous change in the IIoT energy system, such as big data analytics, software-defined machines, and smart sensing [13]. These new technologies have continually been improving the system's operational performances.

Remote Monitoring: Old energy systems needed a large amount of labor to run them. In contrast, the new energy production systems use remote monitoring systems to build a safe environment in IIoT. The IIoT system utilizes communication and sensor technologies to operate the production system remotely. Remote monitoring technologies can help the energy industry enhance its production performance while also reducing the risk for workers [93].

Predictive Maintenance Technique: Energy production systems in the IIoT hold data analytics and big data to generate predictive analytics information to help prevent unplanned downtime and major losses and minimize the risk of a complete shutdown [94]. However, the energy production industry faces a big problem in maintaining good conditions of the equipment.

Improved Safety and Efficiency: Different security policies exist for IIoT risk management and system control security principles [95]. In addition, the IIoT energy system can detect faults and energy consumption of multiple components through continuous monitoring and real-time data processing. As a result, the system can reduce serious and dangerous incidents and unnecessary losses and increase overall energy efficiency [42].

4.2. Smartphone Applications Solutions for IIoT

Smartphone applications (apps), an innovative technology that combines electronic devices, are used to drive IoT. Smartphone applications have been created for the industrial sector. In [96], the authors present smartphone apps that provide industry solutions. The categorization design of smartphone apps for the smart industry is shown in Figure 11. All of the smartphone apps are presented in Figure 11, with a brief description of each app. Developers from all over the world have built many e-industry apps; this survey highlights a few selected apps based on their popularity. Apps are divided into different categories:

- **Remote Equipment Management and Monitoring Apps:** Apps used to manage and monitor the equipment remotely, like Atera, Domotz Pro, etc.
- **Production Implementation Apps:** Apps providing platforms for administrators for production control.
- **Quality Control Apps:** Apps aiming to provide quality control for single and multiple software, while others provide long-term tracking solutions.
- **Safety Management Apps:** Apps that focus on providing different kinds of security controls like hazard management, audit management, and corrective and preventive action.
- **Predictive Maintenance Apps:** Apps that provide predictive tools for predicting asset maintenance.
- **Supply Chain Optimization Apps:** These apps offer platforms to optimize supply chain operations.

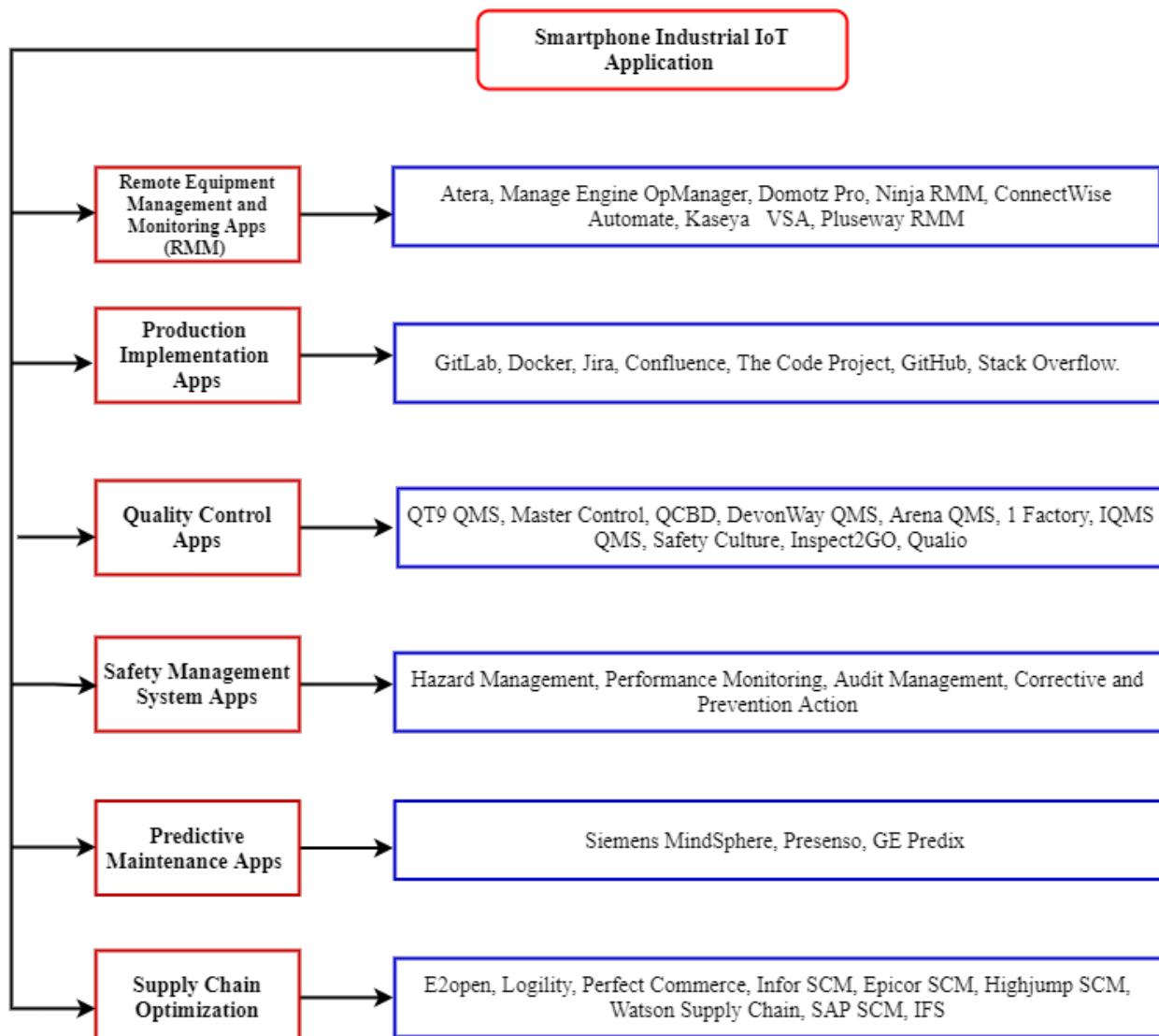


Figure 11. Smartphone applications for Industrial IoT.

4.3. Sensors and Devices in Industrial IoT

Everything needs to be automated with fewer human resources by using less time in today's world. The sensor is one such device that can fulfill a specific need by detecting and responding to the same input from the current physical environment [96]. Users configure some settings on sensing equipment to execute tasks without using human resources. Users set some settings over sensing devices to complete their jobs without the involvement of human resources in some major IoT sensors. Temperature, humidity, pressure, current-monitoring, vibration, and water-detection sensors are important IoT sensors. Sensor-based industrial applications are shown in Table 3. The table describes various industrial sensors used in IIoT, including humidity, pressure, temperature sensors, etc. These sensors are discussed with their attributes and shortcomings.

Table 3. Industrial IoT sensor-based applications description.

Sensors	Description of Sensors, IoT Connections/Roles
Temperature Sensor	One of the most important requirements for this sensor is to help prevent moisture on a large production floor. In addition, temperature sensors also help detect extremely high temperatures in manufacturing processes and display our performance rating [97].
Humidity Sensor	Humidity sensors, which monitor the quantity of moisture in the air, are the most useful IIoT sensors. The humidity would build in our customer's application, and the flooring would become completely soaked. The production line was severely affected by wet feet. IIoT humidity sensors could be used during the production line to monitor the humidity [98].
Pressure Sensor	IIoT sensors generally require the ability to read pressure. Therefore, choosing the correct pressure sensor for every application, from detecting air pressure to harmful gases and liquids, requires some research. In industrial applications, pressure sensor designs detect leaks or flow blockages. Other transmissions may be issued if pressure fluctuations surpass predefined limitations. Pressure sensors provide a fast payback period, especially when faults are found [99].
Current-monitoring Sensor	When IIoT sensor procedures are used, power consumption monitoring cannot be minimized [100]. The current monitoring method helps you to check utility bills. Unfortunately, the current monitoring devices do not help predict the system's failure [101]. When an application fails on an industrial motor, the first thing that happens is friction. A larger load on an engine is caused by friction. When power consumption exceeds expected levels, motor utilization can detect failures. The most significant utilization evidence has come from industrial freezers. When compressors fail, for example, one of two things can happen: current consumption is significantly lowered (allowing the motor to spin freely without load) due to internal component failure, or recent consumption increases due to friction [102].
Vibration Sensor	Vibration sensors are crucial components of IIoT sensors. Vibration sensors can alert the user to frequent faults with working machinery and devices, making them a solution for many predictive preservation applications. Accelerometers are used in vibration sensors to read microchanges over a wide range of frequencies. NCD vibration sensors can detect malfunctioning items from heavy machinery and motors to industrial pipe flow vibration monitoring. However, this sensor can save lives when utilized appropriately, making it the top-ranked sensor for predictive maintenance applications because of its early detection abilities. Furthermore, the vibration sensor is the most commonly utilized in industrial applications that do not require human intervention [103].
Water-Detection Sensor	Water-detection sensors are essential sensors for industrial applications. When water is exposed, they send an alert, and when the sensor has been restored to its dry state, they send another alert. Water detection sensors also communicate data regularly, letting you know they are still watching out for you. The battery state is also communicated, as it is with all NCD sensors, to control the sensor's overall health. Water detection sensors have been used to detect floods in unexpectedly large numbers of applications. In addition, this sensor is commonly used to detect water in basements. Detecting water on solid floors and walls is one of the most fundamental detecting applications [104].

5. IIoT Security Threats

Many researchers have briefly discussed IIoT security and privacy threats; this work highlights the attacks on each layer of the four-level architecture of IIoT and provides its countermeasures equally [105–107]. For example, [108] analyzed the security technology trends for smart factories regarding IIoT. Security protocols are discussed from an automation and manufacturing industry point of view. In addition, recent IIoT-related security solutions and technological advancements are discussed in particular. This research reviews the literature on IIoT security attacks and presents countermeasures in the following sections. The IIoT security attacks are summarized into three parts: physical attacks, network attacks, and software and data link attacks. The effects of these attacks on the four-level IIoT architecture are shown in Figure 12 [109]. A thorough analysis of IIoT and Ir 4.0 security protocols is presented in [110]. Recent research developments are analyzed, particularly those involving blockchain. In addition, the challenges of implementing cryptocurrency are also explored.

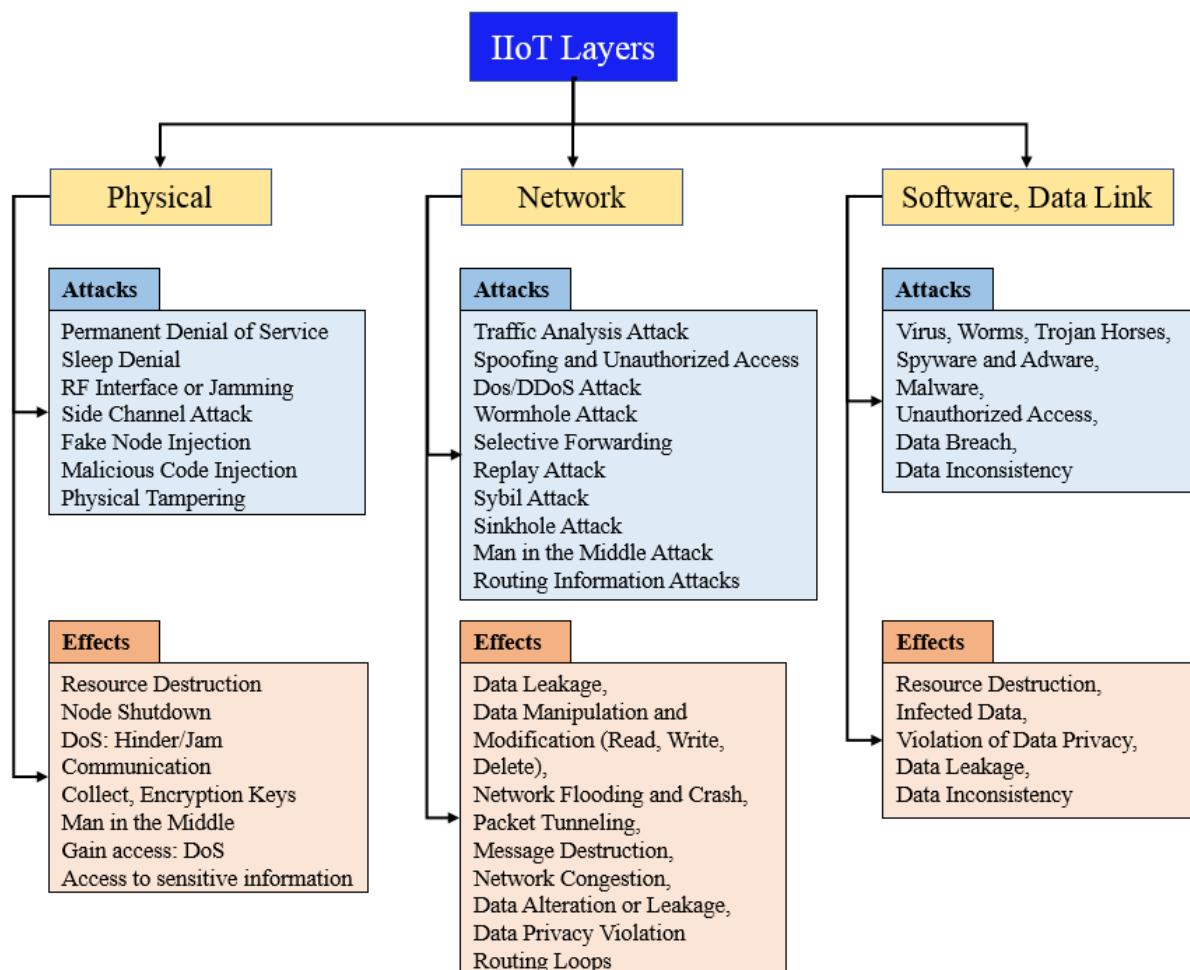


Figure 12. Industrial IoT attacks.

5.1. Physical Attacks

These attacks include IoT hardware and physical devices, and attackers remain close to the device or network of the system [109]. Physical attacks harm the user's sensitive information like passwords. A description of the different types of physical attacks is provided here.

5.1.1. Permanent Denial-of-Service

Permanent denial-of-service (PDoS) is a denial-of-service (DoS) attack that can harm the hardware of IoT devices [111]. Phishing is another term for this type of attack. PDoS disables a system's functionality and firmware [112].

5.1.2. Denial of Sleep

An attack prevents battery-powered sensor nodes from entering sleep mode, causing network performance issues [113]. In addition, it is also possible to target networking devices to prevent communication and block traffic resulting from denial of sleep attacks.

5.1.3. RF Interface/Jamming

Through RF, the attacker can create and transfer noise signals to distract communication and DoS attacks in RFID nodes [114]. In general, the function of a radio frequency interface (RFI) attack is to divert the user to get themselves connected to a fake rogue base station (RBS) while abandoning the legitimate operator signal. These attacks are based on a suitable combination of targeted jamming signals.

5.1.4. Side-Channel Attack

A cloud service provider secures IoT security, and industries are aware of that kind of attack. Encryption keys are the focus area of the attacker; these keys encrypt/decrypt users' sensitive data [115]. The side-channel attacks (SCAs) are generally grounded on power consumption, electromagnetic, timing, and laser-based attacks. Contemporary IoT technologies include mechanisms to prevent these attacks through the use of cryptographic security.

5.1.5. Fake Node Injection

Many nodes work together to create a fake report and inject it between the control data flow and the system's network [116]. Later on, faulty information is provided by the applications that impact the effectiveness of the IoT platform.

5.1.6. Malicious Code Injection

The malicious code injection (MCI) functions to force users to act unknowingly as their information is stolen, usually through cookies. Hackers can target users by sending malicious links via social media sites or email. After clicking the link, the user is redirected to an untrusted server, reflecting the attack on the user's browser [117].

5.1.7. Tampering

The attacker has physical access to modify the device interface like communication devices and RFID [118]. The function of tampering is to manipulate application information that is transferred between server and client. In this case, every bit of information is sent to the application through a POST request.

5.1.8. Countermeasures for Physical Attacks

Many approaches have been published to overview the critical research work on countermeasures [119,120]. For example, Sicari et al. [121] proposed solutions against network smart object (NOS) middleware and REATO, which is attacked by DoS in the IoT environment. This technique involves sending HTTP connection requests to NOS and receiving authentic information in return. Hsiao et al. [122] developed a support vector machine (SVM) technique to organize a model that avoids security risks in IoT applications. The author of [123] predicts the results with the help of SVM to show how effective it is in the medical field. SVM highlights resource depletion as the leading cause of sleep denial attacks. The author of [124] proposed a model named smart-fusion2 SoC, which prevents attacks like jamming. The author also presents the architecture model of (Cute Mote) for better performance and energy production. A side-channel attack is dangerous for IoT devices; a technique known as physically unclonable function (PUF) that protects from side-channel attacks is shown in [125]. Saivarun et al. [126] provide a solution to monitor a smart industry and alert in case of any threats. For data analysis from the IoT sensors, cloud service is utilized. Porambage et al. [127] describe the PAAuthKey protocol, which builds implicit certificates connecting the peer sensor node and end-users. This mechanism creates a security boundary with the help of sensor node protection from different attacks like fake node injection. Deepa et al. [128] highlight various attacks (tampering and malicious code injection) that access users' sensitive information. PUF-based authentication prevents these attacks. A list and short description of countermeasures for physical attacks are shown in Table 4. Each physical attack is discussed concerning its possible impact on the network. In addition, probable countermeasures and solutions are also suggested for each attack.

Table 4. Countermeasures of physical layer attacks.

Ref.	Countermeasures/Solutions	Physical Attacks	Effects
[121]	NOS middleware	Permanent denial-of-service (PDoS)	Resource destruction
[122,123]	Support vector machine (SVM)	Sleep denial	Node shutdown
[124]	CUTE Mote; packets' rerouting to alternative routes	RF interference/jamming	DoS; hinder/jam communication
[125]	Masking technique; authentication using PUF	Side-channel attack	Collect encryption keys
[127]	PAuthKey	Fake node injection	Control data flow; man-in-the-middle
[128]	PUF-based authentication	Malicious code injection and physical tampering	DoS attacks; leak sensitive information

5.2. Network Attacks

The network layer is a sensitive layer that can easily attack and damage network devices [129]. Information integrity and confidentiality are generally threatened by the general security issues of the network layer. The description of attacks is as follows:

5.2.1. Traffic Analysis Attack

The attacker gains access to network-sensitive information without entering into the network [130]. In addition, various forms of malicious behavior can be launched by the attackers such as back attacks and hop-by-hop tracing to attain the precise position of the key nodes.

5.2.2. Spoofing Unauthorized Access

The attacker acts on behalf of another person and gains access to sensitive data through RFID signals. In this type of attack, attackers quickly change the IP address packets and send malicious code [131].

5.2.3. Distributed Denial of Service Attacks

The reverse of a DoS attack is a distributed DoS (DDoS) attack, which brings down a server or network system. DDoS can target a specific flooding message with a node attack [132].

5.2.4. Wormhole Attack

Tunnel packets are moved from one place to another over a low-latency link created by an attacker [133]. The primary objective of a wormhole attack is to dislocate the flow of traffic and the network topology. This type of attack is executed by producing a tunnel between two attackers and transmitting all the traffic toward the targeted node.

5.2.5. Selective Forwarding

The attacker can send malicious code messages and drop them into one network node, but data cannot reach its location [134]. In addition, the selective forwarding attacks are concealed by the normal packet losses, which complicate the attack detection. Hence, it is generally stimulating to identify selective forwarding attacks and enhance network efficiency.

5.2.6. Replay Attack

This attack is the leading cause of the DoS attack. The attacker often sends signed packets with wrong values to the same destination [135]. The increased risk of replay attacks is because the attacker does not need high-level hacking skills to attain information by decrypting after capturing the information. In general, attackers are successful by resending all the information.

5.2.7. Sybil Attack

The Sybil attack targets the compromisation of the privacy of users' information. In this type of attack, the hacker can breach the IoT-distributed cloud storage nodes and become a participating member of the network. In addition, the compromised users let the hacker detain some amount of distributed storage [136]. An attacker creates a false identity and authenticated access to WiFi.

5.2.8. Man-in-the-Middle Attack

This type of attack infects both the wireless and wired users present on the IoT network. A practical scenario of this attack can be related to a football case where the third player tried to intercept while the other two players tried to pass it. Hence, this type of attack threatens the overall network communication. An attacker drops eavesdropped messages between two communication IoT devices and accesses their sensitive information [137].

5.2.9. Routing Information Attacks

These attacks are produced through modification in routing data. These attacks are highly damaging to the network as they input the wrong routing table entries into the routing table. Then, attackers send malicious messages and leak the network's routing information [138].

5.2.10. Countermeasures for Network Attacks

This section focuses on published works to overcome the attacks faced in the network layer. Liu et al. [139] provide a framework for privacy-preserving traffic obfuscation and defenses against traffic analysis attacks in various IoT applications. The results show that network utility cost and privacy protection are better than others. Farha et al. [140] describe a secure static random-access memory (SRAM)-PUF-based entity authentication technique for IoT device authentication. This technique uses challenge-response pairs (CRPs) to overcome the challenges and increases the response time of SRAM cell values. The value result shows that this scheme is better for resources constrained with a low memory size in IoT devices.

The study [141] proposed a secure routing protocol for low power (SRPL), which is resistant to skin-hole and routing attacks and prevents malicious code by using secure authentication hash values. Tao et al. [142] proposed the great-alternative-region (GAR)-based approaches that overcome the physical attacks problem. Intrusion detection systems (IDS) create attack detection techniques to prevent IoT devices from threats [143,144]. IDS protects from sinkhole and wormhole attacks. Djedjig et al. [145] introduced the measure-based RPL trustworthiness scheme (MRTS), which benefits energy usage, a trust-based routing metric, packet delivery ratio, consistency, and node rank changes. Haripriya et al. [146] proposed a secure MQTT system to avoid intrusion detection. It can protect IoT applications from DoS attacks. The experiment results show that the proposed scheme detects malicious nodes between IoT devices better than existing techniques. Thus, MQTT-based authorization shows better performance and privacy protection systems in IoT networks [147]. Karati et al. [148] proposed that encryption is perfect for data confidentiality and the authenticity of data transmission in IIoT systems. On the other hand, Yin [149] proposed two frameworks. Firstly, software-defined IoT (SD-IoT) uses IoT devices and gateways, and second, an algorithm is used to prevent and protect from DDoS attacks. The results of both models show that the algorithm presents better performance countermeasures, as shown in Table 5. It provides an overview of network attacks launched on the IIoT network. Various types of attacks are summarized along with their possible damage and probable countermeasures.

Table 5. Countermeasures of network layer attacks.

Ref.	Countermeasures/Solutions	Network Attacks	Effects
[139]	Privacy-preserving traffic obfuscation framework	Traffic analysis attack	Data leakage
[140]	SRAM-based PUF	RFID spoofing and unauthorized access	Data manipulation and modification (read, write, delete)
[141]	Hash chain authentication	Routing information attacks	Routing loops
[142]	Hash chain authentication; monitor-based approach	Selective forwarding	Message destruction
[143]	Hash chain authentication; intrusion detection	Sinkhole attack	Data alteration or leakage
[144]	Clustering-based intrusion detection system	Wormhole attack	Packet tunneling
[145]	Trust aware protocol	Sybil attack	Unfair resource allocation; redundancy
[146,147]	Secure MQTT; inter-device authentication	Man-in-the-middle attack	Data privacy violation
[148]	Signcryption	Replay attack	Network congestion; DoS
[149]	DDoS server; SDN-based IoT framework	DoS/DDoS attack	Network flooding; network crash

5.3. Software and Data Link Attacks

With the rapid development of IoT/IIoT, attacks on IoT devices, applications, software, and networks have also increased [7]. In the following, a description of attacks faced by the IoT world is provided.

5.3.1. Trojan Horses, Virus, Adware, Worms, and Spyware

Contemporary IoT appliances include programmable embedded systems. Moreover, most IoT devices run complex software for general purposes. Therefore, such devices are always at a security risk. For instance, a computer can become infected through the internet by a virus or Trojan. These are malware software that gain access to a user's system without permission and spy on sensitive information. Then, they perform a malicious task and are ready for further attacks [150].

5.3.2. Malware

In general, this type of attack is called a cyber attack in which malicious software executes unauthorized actions on the targeted user node. The malware virus is launched in various forms and encapsulates various forms of attacks, for instance, ransomware, spyware, command, and control. Malware corrupts data centers or the cloud and destroys sensitive data stored in IoT devices. Security firewalls and anti-virus are two possible ways to prevent malware [151].

5.3.3. Data Breach

A data breach is a general issue where the sensitive information is leaked. The protected information no longer remains trustworthy and is linked to an untrusted environment. In general, an information breach occurs as a result of a hacker attack or inside a corporation by an individual or a previously employed individual, leading to exposed data. The data breach is an attack to gain access to users' sensitive information [152].

5.3.4. Data Inconsistency

In general, issues related to data inconsistency or redundancy commonly occur in IoT devices. Data inconsistency leads to the complication of multiple tables within the same database creating database issues. The data become inconsistent and redundant, having various inputs for the same entries. In addition, data inconsistency is usually compounded by redundancy. For example, multiple tables have the same data but different inputs [153].

5.3.5. Countermeasures for Software and Data Link Layer Attacks

Researchers highlight various solutions that help to prevent different attacks. For example, Batra et al. [154] proposed two solutions using secure security solutions like a lightweight IoT-based framework wireless network system (WNS). The proposed security solutions provide outstanding results. In addition, high-level synthesis (HLS) presents a secure high-level architecture protected from malicious activity [155]. Latif et al. [156] proposed a lightweight prediction model based on a random neural network (RaNN). The prediction accuracy of this model is better than other models. The accuracy of the proposed approach is better compared to IoT-based machine learning schemes. Zheng et al. [157] use an attribute bloom filter to cover all the characteristics in the access control system and present a privacy-preserving attribute-based online–offline encryption (ABE) for medical data exchange. As a result, only medical users encrypt the message to the server and decrypt the message using access control technology. Jiansheng et al. [158] propose two privacy-preserving technologies: attribute-based encryption (ABE) and blockchain-based access control data privacy schemes for IoT systems. The proposed scheme is more secure and efficient and solves authentication challenges.

A data breach is a harmful attack to gain access to users' sensitive information. To overcome these threats, the author in [159] propose two-factor authentication dynamic privacy protection (DPP) and improved secure directed diffusion (ISDD). The authors utilize dynamic programming to obtain better results for privacy protection security in IoT devices. Furthermore, Gope et al. [160] proposed a two-factor authentication approach based on PUFs that were both privacy-preserving and lightweight. These authentication models show higher performance and security against attacks on IoT devices.

Song et al. [161] investigated IoT attacks and proposed a chaos-based privacy-preserving cryptographic system as well as a message authentication code (MAC) to protect data transmissions within a smart home. The suggested chaotic system generates symmetric keys using a logistic map to protect data transmissions and ensure integrity. Furthermore, in [162], the authors present secure blockchain-based framework solutions for the image encryption algorithm to prevent different attacks. A brief overview of the discussed countermeasures is provided in Table 6. This table presents trojan horses, malware, unauthorized access, data breach, and data inconsistency attacks, which are launched on the link layer. These attacks can cause resource destruction, data infection, privacy violation, data leakage, and data inconsistency. Possible solutions to avoid these attacks include high-level synthesis, neural network frameworks, privacy-preserving and blockchain-based solutions, and two-factor authentication.

Table 6. Countermeasures of software and data link layer attacks.

Refs.	Countermeasures/Solutions	Physical Attacks	Effects
[154,155]	Lightweight framework; high-level synthesis (HLS)	Trojan horses, virus, adware, worms, and spyware.	Resource destruction
[156,157]	Lightweight neural network framework; malware image classification	Malware	Infected data
[158]	Privacy-preserving ABE; blockchain-based ABE	Unauthorized access	Violation of data privacy
[159,160]	Two-factor authentication; DPP; ISDD	Data breach	Data leakage
[161,162]	Chaos-based scheme; blockchain architecture	Data inconsistency	Data inconsistency

6. Research Directions and Future Implementation

This survey presents an overview of the taxonomy of IIoT security attacks and their countermeasures and challenges. The IIoT sector is facing multiple challenges, including high traffic, regular dataset updates, data confidentiality, lack of IoT dataset availability, a complicated network topology, security, and privacy [150]. These challenges heavily influence the IIoT system and manufacturing processes. The IIoT sector faces various intrusion and application-specific flaws as well. These factors include a lack of maintenance

in IIoT appliances, accidental vulnerability, and major financial, technical, and human loss [12]. This survey also presents challenges and solutions to ensure security regarding IIoT implementations for future applications.

6.1. Blockchain and 5G Technologies

Blockchain and 5G technologies are expected to play a major role in developing future IIoT. For example, Ling Liu et al. [163] investigated how 5G can work for efficient energy management in the IIoT. In [164], the author investigated how blockchain can be used for shared data storage in the IIoT. However, in this survey, a four-layer architecture and strategy are presented for combining IIoT with other technologies. This architecture considers different IIoT deployments, security requirements, compatibility, timeliness, scalability, and other related factors [165].

6.2. IIoT Integration with Security Systems

There is no integrated model for edge and data-level security in IIoT devices [166]. Furthermore, no model is a suitable fit for various automatic functions of IIoT. As a result, the compatibility and verifiability of the system integration should be further investigated.

6.3. IIoT High-Power Secured Communication Model

Data transmission through a public network causes vulnerability and increases security risks since IIoT devices are not secure. Data access problems can be reduced by introducing a high-power secured protocol [167].

6.4. Detective and Preventive Measures

A lack of preventative measures causes virus and injection attacks. The majority of attacks are detected through analysis rather than prevention. As a result, some effective measures for detecting assaults and preventing them from happening again are required. There is a major need to introduce sophisticated malware detection technologies to protect IIoT devices from attacks [168].

6.5. Advanced IIoT Support Architecture

Advanced IIoT architecture must be created for platforms with low feedback latency. Furthermore, few security systems in IIoT can support heterogeneous platforms, and backward compatibility has also been a research challenge [169].

6.6. IIoT Security Authorization Models

Authorization models with double-layer validation should be available in the future to improve IIoT security [170]. Furthermore, user modification should be provided in a way that is consistent with all application frameworks. Deep learning algorithms and a game-theoretic approach can build an application-based security measure for sensitive data. Table 7 shows some leading technologies from well-known companies along with their future trends and directions. These companies offer different solutions for IoT networks. IBM provides AI-supported visual inspection of components for quality control workers. Intel enables the deployment of smart factory solutions. Samsung provides an SDS platform to interconnect various IoT devices.

Table 7. Description of IIoT trends and directions in some popular technology industries.

Firms	Directions and Trends
IBM, Armonk, NY, USA	IBM can increase process product quality, capabilities, and insights, decrease production errors, and save money and time by applying AI-powered visual inspection of components and assemblies. Quality control workers can use a smartphone connected to the cloud to monitor manufacturing operations from anywhere at no cost. Furthermore, manufacturers can spot mistakes earlier rather than later using machine learning algorithms when more expensive repair work is needed [171].
Intel, Santa Clara, CA, USA	Intel can help quicken the time of value data-driven, interoperable IIoT solutions. The ecosystem of innovators and a collection of flexible solutions help develop and integrate intelligent industrial edge solutions that reduce costs, increase profits, and move you ahead of the competition. In addition, Intel enables the deployment of smart factory solutions to achieve new productivity levels while exposing new opportunities to maximize income [172].
Samsung, Seoul, Korea	Samsung takes action in the world of IoT. Samsung SDS's IoT platform lets users connect with various devices and many IoT communication protocols like Zigbee, Lora WAN, MQTT, BLE, and Modbus [173].
Oracle, Austin, TX, USA	Oracle's digital world applications include customer experience (CX), supply chain, HR, and ERP to increase operational efficiency, boost worker productivity, improve CX, generate new business models and prospects, and support intelligent, predictive algorithms, and digital twins [174].
Microsoft, Redmond, WA, USA	Microsoft is the reason behind the digital transformation of smart manufacturing to improve in productivity and grow industrial processes. In addition, Microsoft also helps IIoT sensors communicate with artificial intelligence (AI) to create smart machines and equipment that communicate. In addition, since IIoT generates massive volumes of big data, it needs a fast, powerful system [175].
HQ Software, New York, NY, USA	HQ Software gives solutions for IIoT services to make the whole process of manufacturing more efficient. One of the efficiency parameters is a shorter manufacturing cycle; IIoT results in choosing the right IoT automation software to decrease the manufacturing cycle time and cut costs [176].
Cisco, San Jose, CA, USA	Cisco gives a solution for a secure and strong network infrastructure for the success of Industry IoT [177].
Google, Mountain View, CA, USA	Google Cloud Open System infrastructure provides an IIoT solution for developing opportunities, new devices, technologies, and business models.

7. Industrial IoT Challenges

The key motive for manufacturers, healthcare providers, utility companies, industry automation, and agricultural producers to deploy IIoT is to boost production and efficiency. IIoT has various technical challenges, including efficiency, security, privacy, connectivity, interoperability, scalability, flexibility, and resource management. A few critical challenges that need to be resolved are discussed here.

7.1. Energy Consumption and Management Schemes

Industries are the greatest electricity users in a country, demanding energy-efficient power management methods. Some IIoT applications run on batteries for years, and this costly energy consumption needs low-power sensors and actuators that do not require batteries. Therefore, energy consumption affects network life, robotic devices, sensors, and actuators, so is an essential factor of IIoT. In addition, data packets continuously exchanging results is a leading cause of energy consumption. LPWAN technology enables low-power and low-cost operation in energy efficiency and consumption systems [178]. Although there are many technologies for energy consumption and efficiency, energy harvesting is a promising and emerging approach for IIoT [179]. Solar, radiofrequency, and thermal energy harvesting techniques provide low-power, availability, and low-cost benefits and should be enhanced further to increase efficiency [180].

7.2. Energy Optimization

Energy optimization is an area of increased research attention in IIoT. The lifetime of IIoT systems is affected by limited resources, so energy-optimized schemes are significantly important [179,181]. IIoT comprises various sensors and devices that require substantial amounts of energy [182]. It also leads to a higher carbon footprint. Energy-efficient communication is the need of the hour for IIoT systems [183]. Similarly, since IIoT devices also involve computation, energy-efficient computing is also needed [184].

7.3. Data Confidentiality

The IIoT collects increasing amounts of data; for example, cloud services [185] use processes and meta information for control and optimization. Customer information and company secrets are among the data that must be kept safe from unauthorized access. The main problem is maintaining confidentiality while allowing approved IIoT services to process and analyze the data.

7.4. High Connectivity in IIoT

The IIoT's major advantages are strong connectivity between IT, operating technology, and the internet, which allows for more efficient and adaptable industrial production [186]. However, the separation and isolation of IIoT devices based on their functionality and preventing unauthorized access have become increasingly challenging. Nevertheless, the National Institute of Standards and Technology (NIST) [187] network segmentation is a reasonable option for securing industrial control systems (ICSSs), controlling high connectivity, and requiring further investigation for IIoT applications.

7.5. Network Latency

Network latency challenges increase as the number of shared devices increase in IIoT [188]. Fog computing or edge computing is used to reduce latency in the network. Fog or edge computing applications require an end device or to be pushed towards the network edge to minimize response time and latency. The edge computing paradigm is built on the cloud computing paradigm by relocating services that are not fit for cloud execution to end devices.

The paradigm shift lowers overall network latency while improving the quality of service (QoS). Fog computing is ideal for IIoT systems that require low-latency and real-time performance [189]. Cloud offloading is another model in which computation-intensive tasks are uploaded to the cloud for quick and predictable execution [190]. Non-real-time apps are placed on the cloud, whereas latency-sensitive applications are executed in local networks using machine-to-machine communications [191].

7.6. Limitations of Sensors in Industries

IIoT uses many sensors to increase efficiency and improve product quality, and such sensors are temperature, ethnography, motion, sound, laser scanner, radar, color, light, and X-ray [192]. Moreover, recent advancements in microelectronics linked with improvements in solid-state sensors have drastically lowered the complexity of simple sensors and are less of an issue for the future. Instead, the challenge has been making them more selective in congested, noisy, and complicated conditions. Applying algorithms related to fuzzy logic guarantees to reduce such issues for future applications [193].

7.7. Co-Existence and Interoperability

Many subsystems and external systems would connect in the IIoT, resulting in interoperability problems [194]. For example, a smart industry is linked to an external smart grid, a production plant is linked to the WoT service, and the factory's production system is linked to the same factory's storage system. In addition, a variety of sensors and techniques would be used. As a result, integrating systems and sensors, as well as interoperability protocols, becomes more challenging. In the future, IIoT devices based on detection, identification, and reduction in external interference can achieve successful coexistence. Because many of the tasks (such as those in a production setting where actuators are required to initiate actions) are time-sensitive, the integration and interoperability must be perfect to offer excellent performance.

7.8. Scalability

The scalability of machines and factories becomes a basic problem in IIoT as the number of linked devices increases [195]. The scalability problem in the IIoT is caused by three factors:

- i. Scalability of data. The increasing number of sensors in IIoT creates a considerable amount of sensing data continually. As a result, the process required for industrial control applications, such as motion-control applications, is typically very high.
- ii. Furthermore, the high-frequency data scalable combination affects the system's scalability. For example, control systems are usually controlled independently in traditional industrial approaches and do not scale. As a result, enabling heterogeneous devices and approaches to communicate becomes challenging.
- iii. Collaboration. Scalable management becomes a challenge for heterogeneous devices. The horizontal and vertical integration of numerous industrial components and systems presents a non-trivial management and maintenance challenge to system administrators. As a result, to achieve scalability, current management technologies must be integrated into the system management process.

High-frequency data overcome the problem of data scalability by reducing bandwidth and improving system scalability. Furthermore, when multiple systems integrate and collaborate, combination scalability requires the lowering of the human effort in configuration. As a result, several communication protocols such as data distribution service (DDS), advanced message queueing protocol (AMQP), and MQTT have been proposed to overcome scalability in IIoT [196].

7.9. Fault Detection and Reconfiguration

The chances of failure rise as the IIoT system becomes more automated and more heterogeneous devices are used [197]. Some common examples include device failure, delayed communication, and connectivity issues. An efficient IIoT system must be robust, identify and endure common errors, and detect problems in real time. Advanced defect detection algorithms have been used at the hub, gateway, or middleware to coordinate various machines and devices. To detect problems, accuracy and timeliness are also essential. A single malfunctioning object can take control of a whole manufacturing or industrial process, resulting in financial, energy, and other resource losses. Without the need for human involvement, a faulty network of sensors or equipment should reconfigure itself. If a sensor stops working due to a fault, it can be put to sleep until it is replaced, and the sensor network configurations can be changed. In this manner, it ensures robustness while also saving energy.

7.10. Long-Lived Components

Consumer IoT devices have a far shorter lifespan than IIoT devices [198]. This increases the need to consider application and communication security during device creation and, more significantly, to update the software after devices are deployed. However, this problem is not limited to newly deployed devices; it directly impacts existing devices delivered with few or no security features and a complex upgrade method, despite being supposed to be used for decades. Furthermore, as the IIoT becomes more connected, the potential of security breaches rises, especially if formerly isolated older components become part of the network.

7.11. Security and Privacy Challenges

IIoT requires security assurance [199]. However, it becomes difficult to maintain the authenticity and data secrecy of the system when distributed sensor nodes, actuators, and machines are coupled in a production system. Moreover, the possibility for attackers to exploit and take control of the system is high due to self-configuration and automation. Furthermore, the storage of industrial production-related data on the cloud is a problem for data privacy [200]. As a result, industrial internet software must secure linked devices

and generate data against various threats. Furthermore, to secure automation processes continually, security upgrades must not interfere with control processes and must be seamlessly integrated with the usual control cycle.

8. Conclusions

IoT technology is expanding at a fast-paced rate and various testbeds have been developed to improve smart industry productivity. With a large number of studies published over recent years, a comprehensive overview of the state-of-the-art technologies for IIoT in the industry holds significant importance. This study examined state-of-the-art IIoT network architecture, platforms, topologies, and protocols that enable the smart industry to improve manufacturing productivity by facilitating access to the IoT backbone. Furthermore, we include a comprehensive review of the present and future developments in industrial IoT applications, devices/sensors, communication protocols, and many other linked technologies. Consequently, for a better understanding of IoT smart industry security, we covered a variety of industrial IoT challenges and security requirements.

The analysis reveals several important and crucial aspects of IoT-based industries and key technologies, such as cloud computing, big data storage, and analytics. It is found that energy consumption, data privacy and confidentiality, network latency, and high connectivity are major challenges in IIoT. With the expanding network, scalability is an obvious challenge for the IIoT network. Moreover, due to the heterogeneity of sensors deployed in the IIoT network, interoperability is becoming challenging. Due to the shorter span of consumer IoT devices, implementing complex security protocols is also difficult and raises security and privacy issues.

Recently, governments have begun to support IIoT, and in the near future, traditional industrial techniques are anticipated to be transitioned into the IoT industry. Moreover, many popular firms also began investing and creating new strategies to improve manufacturing productivity using IoT technologies. Finally, researchers, experts, industrialists, and policymakers working in the IoT sector and industrial technologies are likely to find this comprehensive survey to be highly important and helpful.

This survey provides a comprehensive overview of the role of IoT in the manufacturing industry in general. Key components of IIoT smart industry are discussed concerning their features and flaws. Existing surveys explore different aspects of IIoT, like security challenges, blockchain-based solutions, software-based and fog-based IIoT solutions, etc.; this survey provides an extensive survey of attacks, weaknesses, and vulnerabilities of IIoT and provides probable solutions to overcome these issues. With an increased number of articles publishing rapidly, the survey might have missed the most recent articles on IIoT security. The survey covered only traditional solutions for IIoT attacks. Quantum computing-based attacks have been launched recently and traditional security protocols are unable to detect such attacks. Exploring quantum cryptography solutions to overcome such attacks on IIoT would be an interesting avenue.

Author Contributions: Conceptualization, M.S.F. and M.A.; methodology, S.R. and A.A.; software, A.A. and F.R.; validation, J.C.G. and M.A.S.; formal analysis, M.S.F. and S.R.; investigation, M.A.L.F., M.A.S. and I.A.; resources, J.C.G. and M.A.S.; data curation, M.A. and S.R.; writing—original draft preparation, M.S.F. and M.A.; writing—review and editing, I.A.; visualization, A.A. and F.R.; supervision, I.A.; project administration, F.R. and M.A.L.F.; funding acquisition, M.A.L.F. and J.C.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the European University of the Atlantic.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Ma, H.D. Internet of things: Objectives and scientific challenges. *J. Comput. Sci. Technol.* **2011**, *26*, 919–924. [[CrossRef](#)]
2. Okano, M.T. IOT and industry 4.0: The industrial new revolution. In Proceedings of the International Conference on Management and Information Systems, Istanbul, Turkey, 17–20 October 2017; Volume 25, p. 26.
3. Tabaa, M.; Monteiro, F.; Bensag, H.; Dandache, A. Green Industrial Internet of Things from a smart industry perspectives. *Energy Rep.* **2020**, *6*, 430–446. [[CrossRef](#)]
4. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [[CrossRef](#)]
5. Salman, T.; Zolanvari, M.; Erbad, A.; Jain, R.; Samaka, M. Security services using blockchains: A state of the art survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 858–880. [[CrossRef](#)]
6. Cardenas, A.A.; Amin, S.; Sastry, S. Secure control: Towards survivable cyber-physical systems. In Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 495–500.
7. Khan, W.Z.; Rehman, M.; Zangoti, H.M.; Afzal, M.K.; Armi, N.; Salah, K. Industrial internet of things: Recent advances, enabling technologies and open challenges. *Comput. Electr. Eng.* **2020**, *81*, 106522. [[CrossRef](#)]
8. Chen, B.; Wan, J.; Shu, L.; Li, P.; Mukherjee, M.; Yin, B. Smart factory of industry 4.0: Key technologies, application case, and challenges. *IEEE Access* **2017**, *6*, 6505–6519. [[CrossRef](#)]
9. Soori, M.; Arezoo, B.; Dastres, R. Internet of things for smart factories in industry 4.0, a review. *Internet Things-Cyber-Phys. Syst.* **2023**, *3*, 192–204. [[CrossRef](#)]
10. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. Towards a systematic survey of industrial IoT security requirements: Research method and quantitative analysis. In Proceedings of the Workshop on Fog Computing and the IoT, New York, NY, USA, 15 April 2019; pp. 56–63.
11. Yu, X.; Guo, H. A survey on IIoT security. In Proceedings of the 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), Singapore, 28–30 August 2019; pp. 1–5.
12. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [[CrossRef](#)]
13. Wan, J.; Tang, S.; Shu, Z.; Li, D.; Wang, S.; Imran, M.; Vasilakos, A.V. Software-defined industrial internet of things in the context of industry 4.0. *IEEE Sens. J.* **2016**, *16*, 7373–7380. [[CrossRef](#)]
14. Aazam, M.; Zeadally, S.; Harras, K.A. Deploying fog computing in industrial internet of things and industry 4.0. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4674–4682. [[CrossRef](#)]
15. Omoniwa, B.; Hussain, R.; Javed, M.A.; Bouk, S.H.; Malik, S.A. Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues. *IEEE Internet Things J.* **2018**, *6*, 4118–4149. [[CrossRef](#)]
16. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [[CrossRef](#)]
17. 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. *Int. J. Interact. Multimed. Artif. Intell.* **2017**, *4*, 45–54. [[CrossRef](#)]
18. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. *Comput. Netw.* **2018**, *141*, 199–221. [[CrossRef](#)]
19. Chhetri, S.R.; Rashid, N.; Faezi, S.; Al Faruque, M.A. Security trends and advances in manufacturing systems in the era of industry 4.0. In Proceedings of the 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Irvine, CA, USA, 13–16 November 2017; pp. 1039–1046.
20. Alcácer, V.; Cruz-Machado, V. Scanning the industry 4.0: A literature review on technologies for manufacturing systems. *Eng. Sci. Technol. Int. J.* **2019**, *22*, 899–919. [[CrossRef](#)]
21. Oztemel, E.; Gursev, S. Literature review of Industry 4.0 and related technologies. *J. Intell. Manuf.* **2020**, *31*, 127–182. [[CrossRef](#)]
22. Mabkhout, M.M.; Al-Ahmari, A.M.; Salah, B.; Alkhalefah, H. Requirements of the smart factory system: A survey and perspective. *Machines* **2018**, *6*, 23. [[CrossRef](#)]
23. Saheb, T.; Izadi, L. Paradigm of IoT big data analytics in the healthcare industry: A review of scientific literature and mapping of research trends. *Telemat. Inform.* **2019**, *41*, 70–85. [[CrossRef](#)]
24. Babar, M.; Arif, F. Real-time data processing scheme using big data analytics in internet of things based smart transportation environment. *J. Ambient. Intell. Humaniz. Comput.* **2019**, *10*, 4167–4177. [[CrossRef](#)]
25. Hossein Motlagh, N.; Mohammadrezaei, M.; Hunt, J.; Zakeri, B. Internet of Things (IoT) and the energy sector. *Energies* **2020**, *13*, 494. [[CrossRef](#)]
26. Chen, C.H.; Lin, M.Y.; Guo, X.C. High-level modeling and synthesis of smart sensor networks for Industrial Internet of Things. *Comput. Electr. Eng.* **2017**, *61*, 48–66. [[CrossRef](#)]
27. Jayalaxmi, P.; Saha, R.; Kumar, G.; Kumar, N.; Kim, T.H. A taxonomy of security issues in Industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges. *IEEE Access* **2021**, *9*, 25344–25359. [[CrossRef](#)]
28. Domingo, M.C. An overview of the Internet of Things for people with disabilities. *J. Netw. Comput. Appl.* **2012**, *35*, 584–596. [[CrossRef](#)]

29. Jia, X.; Feng, Q.; Fan, T.; Lei, Q. RFID technology and its applications in Internet of Things (IoT). In Proceedings of the 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, China, 21–23 April 2012; pp. 1282–1285.
30. Darwish, D. Improved layered architecture for Internet of Things. *Int. J. Comput. Acad. Res.* **2015**, *4*, 214–223.
31. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors* **2018**, *18*, 2796. [CrossRef]
32. Iqbal, F.; Altaf, A.; Waris, Z.; Aray, D.G.; Flores, M.A.L.; Díez, I.d.I.T.; Ashraf, I. Blockchain-Modeled Edge-Computing-Based Smart Home Monitoring System with Energy Usage Prediction. *Sensors* **2023**, *23*, 5263. [CrossRef]
33. Ashraf, I.; Park, Y.; Hur, S.; Kim, S.W.; Alroobaea, R.; Zikria, Y.B.; Nosheen, S. A survey on cyber security threats in iot-enabled maritime industry. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 2677–2690. [CrossRef]
34. Almujally, N.A.; Aljrees, T.; Saidani, O.; Umer, M.; Faheem, Z.B.; Abuzinadah, N.; Alnowaiser, K.; Ashraf, I. Monitoring Acute Heart Failure Patients Using Internet-of-Things-Based Smart Monitoring System. *Sensors* **2023**, *23*, 4580. [CrossRef]
35. Kaur, K.; Garg, S.; Aujla, G.S.; Kumar, N.; Rodrigues, J.J.; Guizani, M. Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud interplay. *IEEE Commun. Mag.* **2018**, *56*, 44–51. [CrossRef]
36. Ibarra, D.; Ganzarain, J.; Igartua, J.I. Business model innovation through Industry 4.0: A review. *Procedia Manuf.* **2018**, *22*, 4–10. [CrossRef]
37. Kang, H.S.; Lee, J.Y.; Choi, S.; Kim, H.; Park, J.H.; Son, J.Y.; Kim, B.H.; Noh, S.D. Smart manufacturing: Past research, present findings, and future directions. *Int. J. Precis. Eng.-Manuf.-Green Technol.* **2016**, *3*, 111–128. [CrossRef]
38. Jiang, H.; Xu, W. How to find your appropriate doctor: An integrated recommendation framework in big data context. In Proceedings of the 2014 IEEE Symposium on Computational Intelligence in Healthcare and e-Health (CICARE), Orlando, FL, USA, 9–12 December 2014; pp. 154–158.
39. Mantravadi, S.; Möller, C.; Chen, L.; Schnyder, R. Design choices for next-generation IIoT-connected MES/MOM: An empirical study on smart factories. *Robot.-Comput.-Integr. Manuf.* **2022**, *73*, 102225. [CrossRef]
40. Shrouf, F.; Ordieres, J.; Miragliotta, G. Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm. In Proceedings of the 2014 IEEE International Conference on Industrial Engineering and Engineering Management, Selangor, Malaysia, 9–12 December 2014; pp. 697–701.
41. Vogel-Heuser, B.; Weber, J.; Folmer, J. Evaluating reconfiguration abilities of automated production systems in Industrie 4.0 with metrics. In Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, 8–11 September 2015; pp. 1–6.
42. Garetti, M.; Taisch, M. Sustainable manufacturing: Trends and research challenges. *Prod. Plan. Control* **2012**, *23*, 83–104. [CrossRef]
43. Souza, V.; Cruz, R.; Silva, W.; Lins, S.; Lucena, V. A digital twin architecture based on the industrial internet of things technologies. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–2.
44. Qi, Q.; Tao, F. A smart manufacturing service system based on edge computing, fog computing, and cloud computing. *IEEE Access* **2019**, *7*, 86769–86777. [CrossRef]
45. Olivares, E.; Ye, H.; Herrero, A.; Nia, B.A.; Ren, Y.; Donovan, R. Applications of information channels to physics-informed neural networks for WiFi signal propagation simulation at the edge of the industrial internet of things. *Neurocomputing* **2021**, *454*, 405–416. [CrossRef]
46. Dobrilovic, D.; Brtka, V.; Stojanov, Z.; Jotanovic, G.; Perakovic, D.; Jausevac, G. A Model for Working Environment Monitoring in Smart Manufacturing. *Appl. Sci.* **2021**, *11*, 2850. [CrossRef]
47. Pötsch, A.; Hammer, F. Towards end-to-end latency of LoRaWAN: Experimental analysis and IIoT applicability. In Proceedings of the 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS), Sundsvall, Sweden, 27–29 May 2019; pp. 1–4.
48. Cheng, J.; Chen, W.; Tao, F.; Lin, C.L. Industrial IoT in 5G environment towards smart manufacturing. *J. Ind. Inf. Integr.* **2018**, *10*, 10–19. [CrossRef]
49. Zhai, C.; Zou, Z.; Chen, Q.; Xu, L.; Zheng, L.R.; Tenhunen, H. Delay-aware and reliability-aware contention-free MF-TDMA protocol for automated RFID monitoring in industrial IoT. *J. Ind. Inf. Integr.* **2016**, *3*, 8–19. [CrossRef]
50. Goudarzi, S.; Anisi, M.H.; Abdullah, A.H.; Lloret, J.; Soleymani, S.A.; Hassan, W.H. A hybrid intelligent model for network selection in the industrial Internet of Things. *Appl. Soft Comput.* **2019**, *74*, 529–546. [CrossRef]
51. Shahzad, K.; O’Nils, M. Condition monitoring in industry 4.0—design challenges and possibilities: A case study. In Proceedings of the 2018 Workshop on Metrology for Industry 4.0 and IoT, Brescia, Italy, 16–18 April 2018; pp. 101–106.
52. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
53. Karakostas, B. A DNS architecture for the internet of things: A case study in transport logistics. *Procedia Comput. Sci.* **2013**, *19*, 594–601. [CrossRef]
54. Riasanow, T.; Jäntgen, L.; Hermes, S.; Böhm, M.; Krcmar, H. Core, intertwined, and ecosystem-specific clusters in platform ecosystems: Analyzing similarities in the digital transformation of the automotive, blockchain, financial, insurance and IIoT industry. *Electron. Mark.* **2021**, *31*, 89–104. [CrossRef]
55. Suchy, J.; Paces, P. BMW iDrive automotive hid device in EFIS control. In Proceedings of the 2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC), Atlanta, GA, USA, 16–18 December 2014; pp. 1–11.

56. Zhang, Y.; Chen, B.; Lu, X. Intelligent monitoring system on refrigerator trucks based on the internet of things. In *International Conference on Wireless Communications and Applications*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 201–206.
57. Dikmen, M.; Burns, C. Trust in autonomous vehicles: The case of Tesla autopilot and summon. In Proceedings of the 2017 IEEE International Conference on Systems, MAN, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; pp. 1093–1098.
58. Shahzad, Y.; Javed, H.; Farman, H.; Ahmad, J.; Jan, B.; Zubair, M. Internet of energy: Opportunities, applications, architectures and challenges in smart industries. *Comput. Electr. Eng.* **2020**, *86*, 106739. [\[CrossRef\]](#)
59. Broll, G.; Rukzio, E.; Paolucci, M.; Wagner, M.; Schmidt, A.; Hussmann, H. Perci: Pervasive service interaction with the internet of things. *IEEE Internet Comput.* **2009**, *13*, 74–81. [\[CrossRef\]](#)
60. Qiu, T.; Chi, J.; Zhou, X.; Ning, Z.; Atiquzzaman, M.; Wu, D.O. Edge computing in industrial internet of things: Architecture, advances and challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2462–2488. [\[CrossRef\]](#)
61. Wang, T.; Wang, P.; Cai, S.; Ma, Y.; Liu, A.; Xie, M. A unified trustworthy environment establishment based on edge computing in industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 6083–6091. [\[CrossRef\]](#)
62. Rejeb, A.; Keogh, J.G.; Treiblmaier, H. Leveraging the internet of things and blockchain technology in supply chain management. *Future Internet* **2019**, *11*, 161. [\[CrossRef\]](#)
63. Cerruela García, G.; Luque Ruiz, I.; Gómez-Nieto, M.Á. State of the art, trends and future of bluetooth low energy, near field communication and visible light communication in the development of smart cities. *Sensors* **2016**, *16*, 1968. [\[CrossRef\]](#)
64. Verma, A.; Shukla, V.K.; Sharma, R. Convergence of IOT in Tourism Industry: A Pragmatic Analysis. *J. Phys. Conf. Ser. IOP Publ.* **2021**, *1714*, 012037. [\[CrossRef\]](#)
65. Al-Turjman, F.; Alturjman, S. Context-sensitive access in industrial internet of things (IIoT) healthcare applications. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2736–2744. [\[CrossRef\]](#)
66. Li, J.Q.; Yu, F.R.; Deng, G.; Luo, C.; Ming, Z.; Yan, Q. Industrial internet: A survey on the enabling technologies, applications, and challenges. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1504–1526. [\[CrossRef\]](#)
67. Pang, Z.; Chen, Q.; Tian, J.; Zheng, L.; Dubrova, E. Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things. In Proceedings of the 2013 15th International Conference on Advanced Communications Technology (ICACT), PyeongChang, Republic of Korea, 27–30 January 2013; pp. 529–534.
68. Driscoll, D.L.; Hiratsuka, V.; Johnston, J.M.; Norman, S.; Reilly, K.M.; Shaw, J.; Smith, J.; Szafran, Q.N.; Dillard, D. Process and outcomes of patient-centered medical care with Alaska Native people at Southcentral Foundation. *Ann. Fam. Med.* **2013**, *11*, S41–S49. [\[CrossRef\]](#) [\[PubMed\]](#)
69. Crabtree, B.F.; Nutting, P.A.; Miller, W.L.; McDaniel, R.R.; Strange, K.C.; Jaen, C.R.; Stewart, E. Primary care practice transformation is hard work: Insights from a 15-year developmental program of research. *Med. Care* **2011**, *49*, S28. [\[CrossRef\]](#) [\[PubMed\]](#)
70. Sha, L.; Gopalakrishnan, S.; Liu, X.; Wang, Q. Cyber-physical systems: A new frontier. In Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008), Taichung, Taiwan, 11–13 June 2008; pp. 1–9.
71. Li, T.; Tan, F.; Wang, Q.; Bu, L.; Cao, J.N.; Liu, X. From offline toward real time: A hybrid systems model checking and CPS codesign approach for medical device plug-and-play collaborations. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *25*, 642–652.
72. Zhang, Y.; Qiu, M.; Tsai, C.W.; Hassan, M.M.; Alamri, A. Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Syst. J.* **2015**, *11*, 88–95. [\[CrossRef\]](#)
73. Kumar, P.M.; Lokesh, S.; Varatharajan, R.; Babu, G.C.; Parthasarathy, P. Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. *Future Gener. Comput. Syst.* **2018**, *86*, 527–534. [\[CrossRef\]](#)
74. Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. *J. Ind. Inf. Integr.* **2020**, *18*, 100129. [\[CrossRef\]](#)
75. Niyato, D.; Hossain, E.; Camorlinga, S. Remote patient monitoring service using heterogeneous wireless access networks: Architecture and optimization. *IEEE J. Sel. Areas Commun.* **2009**, *27*, 412–423. [\[CrossRef\]](#)
76. Huang, Y.F.; Liu, P.; Pan, Q.; Lin, J.S. A doctor recommendation algorithm based on doctor performances and patient preferences. In Proceedings of the 2012 International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP), Chengdu, China, 17–19 December 2012; pp. 92–95.
77. Hossain, M.S.; Muhammad, G. Cloud-assisted industrial internet of things (iiot)-enabled framework for health monitoring. *Comput. Netw.* **2016**, *101*, 192–202. [\[CrossRef\]](#)
78. Chen, F.; Deng, P.; Wan, J.; Zhang, D.; Vasilakos, A.V.; Rong, X. Data mining for the internet of things: Literature review and challenges. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 431047. [\[CrossRef\]](#)
79. Lee, J.Y.; Yoon, J.S.; Kim, B.H. A big data analytics platform for smart factories in small and medium-sized manufacturing enterprises: An empirical case study of a die casting factory. *Int. J. Precis. Eng. Manuf.* **2017**, *18*, 1353–1361. [\[CrossRef\]](#)
80. Wang, S.; Wan, J.; Li, D.; Zhang, C. Implementing smart factory of industrie 4.0: An outlook. *Int. J. Distrib. Sens. Netw.* **2016**, *12*, 3159805. [\[CrossRef\]](#)
81. Bu, L.; Zhang, Y.; Liu, H.; Yuan, X.; Guo, J.; Han, S. An IIoT-driven and AI-enabled framework for smart manufacturing system based on three-terminal collaborative platform. *Adv. Eng. Inform.* **2021**, *50*, 101370. [\[CrossRef\]](#)
82. Scheuermann, C.; Verclas, S.; Bruegge, B. Agile factory—an example of an industry 4.0 manufacturing process. In Proceedings of the 2015 IEEE 3rd International Conference on Cyber-Physical Systems, Networks, and Applications, Kowloon, Hong Kong, 19–21 August 2015; pp. 43–47.

83. Sundar, R.; Balaji, A.; Kumar, R.S. A review on lean manufacturing implementation techniques. *Procedia Eng.* **2014**, *97*, 1875–1885. [[CrossRef](#)]
84. Park, K.T.; Lee, J.; Kim, H.J.; Noh, S.D. Digital twin-based cyber physical production system architectural framework for personalized production. *Int. J. Adv. Manuf. Technol.* **2020**, *106*, 1787–1810. [[CrossRef](#)]
85. Moens, P.; Bracke, V.; Soete, C.; Vanden Hautte, S.; Nieves Avendano, D.; Ooijevaar, T.; Devos, S.; Volckaert, B.; Van Hoecke, S. Scalable fleet monitoring and visualization for smart machine maintenance and industrial IoT applications. *Sensors* **2020**, *20*, 4308. [[CrossRef](#)]
86. ur Rehman, M.H.; Yaqoob, I.; Salah, K.; Imran, M.; Jayaraman, P.P.; Perera, C. The role of big data analytics in industrial Internet of Things. *Future Gener. Comput. Syst.* **2019**, *99*, 247–259. [[CrossRef](#)]
87. Saldivar, A.A.F.; Li, Y.; Chen, W.n.; Zhan, Z.h.; Zhang, J.; Chen, L.Y. Industry 4.0 with cyber-physical integration: A design and manufacture perspective. In Proceedings of the 2015 21st International Conference on Automation and Computing (ICAC), Glasgow, UK, 11–12 September 2015; pp. 1–6.
88. Rüßmann, M.; Lorenz, M.; Gerbert, P.; Waldner, M.; Justus, J.; Engel, P.; Harnisch, M. Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston Consult. Group* **2015**, *9*, 54–89.
89. Judge, M.A.; Manzoor, A.; Khattak, H.A.; Din, I.U.; Almogren, A.; Adnan, M. Secure transmission lines monitoring and efficient electricity management in ultra-reliable low latency industrial Internet of Things. *Comput. Stand. Interfaces* **2021**, *77*, 103500. [[CrossRef](#)]
90. Bhattacharjee, S.; Nandi, C. Implementation of industrial internet of things in the renewable energy sector. In *The Internet of Things in the Industrial Sector*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 223–259.
91. Truong, V.T.; Ha, D.B.; Nayyar, A.; Bilal, M.; Kwak, D. Performance analysis and optimization of multiple IIoT devices radio frequency energy harvesting NOMA mobile edge computing networks. *Alex. Eng. J.* **2023**, *79*, 1–20. [[CrossRef](#)]
92. Beier, G.; Niehoff, S.; Ziems, T.; Xue, B. Sustainability aspects of a digitalized industry—A comparative study from China and Germany. *Int. J. Precis. Eng.-Manuf.-Green Technol.* **2017**, *4*, 227–234. [[CrossRef](#)]
93. Huang, X. Intelligent remote monitoring and manufacturing system of production line based on industrial Internet of Things. *Comput. Commun.* **2020**, *150*, 421–428. [[CrossRef](#)]
94. Civerchia, F.; Bocchino, S.; Salvadori, C.; Rossi, E.; Maggiani, L.; Petracca, M. Industrial Internet of Things monitoring solution for advanced predictive maintenance applications. *J. Ind. Inf. Integr.* **2017**, *7*, 4–12. [[CrossRef](#)]
95. Mouratidis, H.; Diamantopoulou, V. A security analysis method for industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4093–4100. [[CrossRef](#)]
96. Perera, C.; Liu, C.H.; Jayawardena, S. The emerging internet of things marketplace from an industrial perspective: A survey. *IEEE Trans. Emerg. Top. Comput.* **2015**, *3*, 585–598. [[CrossRef](#)]
97. Chang, V.; Martin, C. An industrial IoT sensor system for high-temperature measurement. *Comput. Electr. Eng.* **2021**, *95*, 107439. [[CrossRef](#)]
98. Chavhan, S.; Kulkarni, R.A.; Zilpe, A.R. Smart Sensors for IIoT in Autonomous Vehicles. In *Smart Sensors for Industrial Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 51–61.
99. Park, D.; Kim, S.; An, Y.; Jung, J.Y. LiReD: A light-weight real-time fault detection system for edge computing using LSTM recurrent neural networks. *Sensors* **2018**, *18*, 2110. [[CrossRef](#)]
100. Ghosh, A.; Mukherjee, A.; Misra, S. SEGA: Secured Edge Gateway Microservices Architecture for IIoT-based Machine Monitoring. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1949–1956. [[CrossRef](#)]
101. Strauß, P.; Schmitz, M.; Wöstmann, R.; Deuse, J. Enabling of predictive maintenance in the brownfield through low-cost sensors, an IIoT-architecture and machine learning. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 12–13 October 2018; pp. 1474–1483.
102. Sinha, N.; Pujitha, K.E.; Alex, J.S.R. Xively based sensing and monitoring system for IoT. In Proceedings of the 2015 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 8–10 January 2015; pp. 1–6.
103. Ali, J.B.; Fnaiech, N.; Saidi, L.; Chebel-Morello, B.; Fnaiech, F. Application of empirical mode decomposition and artificial neural network for automatic bearing fault diagnosis based on vibration signals. *Appl. Acoust.* **2015**, *89*, 16–27.
104. Budiarti, R.P.N.; Tjahjono, A.; Hariadi, M.; Purnomo, M.H. Development of IoT for automated water quality monitoring system. In Proceedings of the 2019 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE), Jember, Indonesia, 16–17 October 2019; pp. 211–216.
105. Ashraf, I.; Narra, M.; Umer, M.; Majeed, R.; Sadiq, S.; Javaid, F.; Rasool, N. A deep learning-based smart framework for cyber-physical and satellite system security threats detection. *Electronics* **2022**, *11*, 667. [[CrossRef](#)]
106. El Akrami, N.; Hanine, M.; Flores, E.S.; Aray, D.G.; Ashraf, I. Unleashing the Potential of Blockchain and Machine Learning: Insights and Emerging Trends from Bibliometric Analysis. *IEEE Access* **2023**, *11*, 78879–78903. [[CrossRef](#)]
107. Akram, U.; Sharif, W.; Shahroz, M.; Mushtaq, M.F.; Aray, D.G.; Thompson, E.B.; Diez, I.d.I.T.; Djuraev, S.; Ashraf, I. IoTPPS: Ensemble RK SVM Model-Based Internet of Things Threat Protection System. *Sensors* **2023**, *23*, 6379. [[CrossRef](#)]
108. Kim, J.; Park, J.; Lee, J.H. Analysis of recent IIoT security technology trends in a smart factory environment. In Proceedings of the 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC), Bali, Indonesia, 20–23 February 2023; pp. 840–845.

109. Nawir, M.; Amir, A.; Yaakob, N.; Lynn, O.B. Internet of Things (IoT): Taxonomy of security attacks. In Proceedings of the 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 11–12 August 2016; pp. 321–326.
110. Tamilmani, S.; Mohan, T.; Jeyalakshmi, S.; Shukla, G.P.; Gehlot, A.; Shukla, S.K. Blockchain integrated with Industrial IOT towards Industry 4.0. In Proceedings of the 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, 27–29 January 2023; pp. 575–581.
111. Rustam, F.; Mushtaq, M.F.; Hamza, A.; Farooq, M.S.; Jurcut, A.D.; Ashraf, I. Denial of service attack classification using machine learning with multi-features. *Electronics* **2022**, *11*, 3817. [[CrossRef](#)]
112. Kambourakis, G.; Kolias, C.; Stavrou, A. The mirai botnet and the iot zombie armies. In Proceedings of the MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 267–272.
113. Raymond, D.R.; Midkiff, S.F. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Comput.* **2008**, *7*, 74–81. [[CrossRef](#)]
114. Seneviratne, S.; Hu, Y.; Nguyen, T.; Lan, G.; Khalifa, S.; Thilakarathna, K.; Hassan, M.; Seneviratne, A. A survey of wearable devices and challenges. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2573–2620. [[CrossRef](#)]
115. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access* **2019**, *7*, 82721–82743. [[CrossRef](#)]
116. Ye, F.; Luo, H.; Lu, S.; Zhang, L. Statistical en-route filtering of injected false data in sensor networks. *IEEE J. Sel. Areas Commun.* **2005**, *23*, 839–850.
117. Al-Khurafi, O.B.; Al-Ahmad, M.A. Survey of web application vulnerability attacks. In Proceedings of the 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, Malaysia, 8–10 December 2015; pp. 154–158.
118. Shah, S.; Simnani, S.S.A.; Banday, M.T. A study of security attacks on internet of things and its possible solutions. In Proceedings of the 2018 International Conference on Automation and Computational Engineering (ICACE), Greater Noida, India, 3–4 October 2018; pp. 203–209.
119. Rustam, F.; Ashraf, I.; Jurcut, A.D.; Bashir, A.K.; Zikria, Y.B. Malware detection using image representation of malware data and transfer learning. *J. Parallel Distrib. Comput.* **2023**, *172*, 32–50. [[CrossRef](#)]
120. Chaganti, R.; Boppana, R.V.; Ravi, V.; Munir, K.; Almutairi, M.; Rustam, F.; Lee, E.; Ashraf, I. A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. *IEEE Access* **2022**, *10*, 96538–96555. [[CrossRef](#)]
121. Sicari, S.; Rizziardi, A.; Miorandi, D.; Coen-Porisini, A. Dynamic policies in internet of things: Enforcement and synchronization. *IEEE Internet Things J.* **2017**, *4*, 2228–2238. [[CrossRef](#)]
122. Le, D.N.; Parvathy, V.S.; Gupta, D.; Khanna, A.; Rodrigues, J.J.; Shankar, K. IoT enabled depthwise separable convolution neural network with deep support vector machine for COVID-19 diagnosis and classification. *Int. J. Mach. Learn. Cybern.* **2021**, *12*, 3235–3248. [[CrossRef](#)]
123. Shen, M.; Tang, X.; Zhu, L.; Du, X.; Guizani, M. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet Things J.* **2019**, *6*, 7702–7712. [[CrossRef](#)]
124. Gomes, T.; Salgado, F.; Tavares, A.; Cabral, J. Cute mote, a customizable and trustable end-device for the internet of things. *IEEE Sens. J.* **2017**, *17*, 6816–6824. [[CrossRef](#)]
125. Bolotnyy, L.; Robins, G. Physically unclonable function-based security and privacy in RFID systems. In Proceedings of the 5th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'07), White Plains, NY, USA, 19–23 March 2007; pp. 211–220.
126. Saivarun, K.; Ramakrishnan, R.; Kishore, M. IoT Based Smart Industry Monitoring And Alerting System. In Proceedings of the 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), Bengaluru, India, 18–19 November 2022; pp. 1108–1111.
127. Porambage, P.; Schmitt, C.; Kumar, P.; Gurto, A.; Ylianttila, M. PAAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 357430. [[CrossRef](#)]
128. Deepa, G.; Thilagam, P.S. Securing web applications from injection and logic vulnerabilities: Approaches and challenges. *Inf. Softw. Technol.* **2016**, *74*, 160–180. [[CrossRef](#)]
129. Chahid, Y.; Benabdellah, M.; Azizi, A. Internet of things security. In Proceedings of the 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), Fez, Morocco, 19–20 April 2017; pp. 1–6.
130. Jiang, J.; Han, G.; Wang, H.; Guizani, M. A survey on location privacy protection in wireless sensor networks. *J. Netw. Comput. Appl.* **2019**, *125*, 93–114. [[CrossRef](#)]
131. Damghani, H.; Damghani, L.; Hosseiniyan, H.; Sharifi, R. Classification of attacks on IoT. In Proceedings of the 4th International Conference on Combinatorics, Cryptography, Computer Science and Computation, Tehran City, Iran, 20–21 November 2019.
132. Sonar, K.; Upadhyay, H. A survey: DDOS attack on Internet of Things. *Int. J. Eng. Res. Dev.* **2014**, *10*, 58–63.
133. Pongle, P.; Chavan, G. Real time intrusion and wormhole attack detection in internet of things. *Int. J. Comput. Appl.* **2015**, *121*, 840–847. [[CrossRef](#)]
134. Liu, A.; Liu, X.; Li, H.; Long, J. MDMA: A multi-data and multi-ACK verified Selective Forwarding Attack Detection Scheme in WSNs. *IEICE Trans. Inf. Syst.* **2016**, *99*, 2010–2018. [[CrossRef](#)]

135. Yang, X.; Karampatzakis, E.; Doerr, C.; Kuipers, F. Security Vulnerabilities in LoRaWAN. In Proceedings of the 2018 IEEE/ACM 3rd International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, FL, USA, 17–20 April 2018; pp. 129–140.
136. Mishra, A.K.; Tripathy, A.K.; Puthal, D.; Yang, L.T. Analytical model for sybil attack phases in internet of things. *IEEE Internet Things J.* **2018**, *6*, 379–387. [[CrossRef](#)]
137. Mohapatra, H.; Rath, S.; Panda, S.; Kumar, R. Handling of man-in-the-middle attack in wsn through intrusion detection system. *Int. J.* **2020**, *8*, 1503–1510. [[CrossRef](#)]
138. Perazzo, P.; Vallati, C.; Anastasi, G.; Dini, G. DIO suppression attack against routing in the Internet of Things. *IEEE Commun. Lett.* **2017**, *21*, 2524–2527. [[CrossRef](#)]
139. Liu, J.; Zhang, C.; Fang, Y. Epic: A differential privacy framework to defend smart homes against internet traffic analysis. *IEEE Internet Things J.* **2018**, *5*, 1206–1217. [[CrossRef](#)]
140. Farha, F.; Ning, H.; Ali, K.; Chen, L.; Nugent, C. SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices. *IEEE Internet Things J.* **2020**, *8*, 5904–5913. [[CrossRef](#)]
141. Glissa, G.; Rachedi, A.; Meddeb, A. A secure routing protocol based on RPL for Internet of Things. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–7.
142. Tao, M.; Ota, K.; Dong, M. Locating compromised data sources in IoT-enabled smart cities: A great-alternative-region-based approach. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2579–2587. [[CrossRef](#)]
143. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37. [[CrossRef](#)]
144. Anju, J.; Smimesh, C. An improved clustering-based approach for wormhole attack detection in MANET. In Proceedings of the 2014 3rd International Conference on Eco-Friendly Computing and Communication Systems, Mangalore, India, 18–21 December 2014; pp. 149–154.
145. Djedjig, N.; Tandjaoui, D.; Medjek, F.; Romdhani, I. Trust-aware and cooperative routing protocol for IoT security. *J. Inf. Secur. Appl.* **2020**, *52*, 102467. [[CrossRef](#)]
146. Haripriya, A.; Kulothungan, K. Secure-MQTT: An efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 90.
147. Lohachab, A.; Karambir. ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. *J. Inf. Secur. Appl.* **2019**, *46*, 1–12. [[CrossRef](#)]
148. Karati, A.; Islam, S.H.; Biswas, G.; Bhuiyan, M.Z.A.; Vijayakumar, P.; Karuppiah, M. Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments. *IEEE Internet Things J.* **2017**, *5*, 2904–2914. [[CrossRef](#)]
149. Yin, D.; Zhang, L.; Yang, K. A DDoS attack detection and mitigation with software-defined Internet of Things framework. *IEEE Access* **2018**, *6*, 24694–24705. [[CrossRef](#)]
150. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258. [[CrossRef](#)]
151. Costin, A.; Zaddach, J. Iot malware: Comprehensive survey, analysis framework and case studies. *BlackHat USA* **2018**, *1*, 1–9.
152. Fisher, J.A. Secure my data or pay the price: Consumer remedy for the negligent enablement of data breach. *Wm. Mary Bus. L. Rev.* **2012**, *4*, 215.
153. Miao, D.; Cai, Z.; Li, J.; Gao, X.; Liu, X. Complexity and efficient algorithms for data inconsistency evaluating and repairing. *arXiv* **2020**, arXiv:2001.00315.
154. Batra, I.; Verma, S.; Alazab, M. A lightweight IoT-based security framework for inventory automation using wireless sensor network. *Int. J. Commun. Syst.* **2020**, *33*, e4228. [[CrossRef](#)]
155. Pilato, C.; Garg, S.; Wu, K.; Karri, R.; Regazzoni, F. Securing hardware accelerators: A new challenge for high-level synthesis. *IEEE Embed. Syst. Lett.* **2017**, *10*, 77–80. [[CrossRef](#)]
156. Latif, S.; Zou, Z.; Idrees, Z.; Ahmad, J. A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. *IEEE Access* **2020**, *8*, 89337–89350. [[CrossRef](#)]
157. Zheng, D.; Wu, A.; Zhang, Y.; Zhao, Q. Efficient and privacy-preserving medical data sharing in Internet of Things with limited computing power. *IEEE Access* **2018**, *6*, 28019–28027. [[CrossRef](#)]
158. Zhang, J.; Xin, Y.; Gao, Y.; Lei, X.; Yang, Y. Secure ABE scheme for access management in blockchain-based IoT. *IEEE Access* **2021**, *9*, 54840–54849. [[CrossRef](#)]
159. Gai, K.; Choo, K.K.R.; Qiu, M.; Zhu, L. Privacy-preserving content-oriented wireless communication in internet-of-things. *IEEE Internet Things J.* **2018**, *5*, 3059–3067. [[CrossRef](#)]
160. Gope, P.; Sikdar, B. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet Things J.* **2018**, *6*, 580–589. [[CrossRef](#)]
161. Song, T.; Li, R.; Mei, B.; Yu, J.; Xing, X.; Cheng, X. A privacy preserving communication protocol for IoT applications in smart homes. *IEEE Internet Things J.* **2017**, *4*, 1844–1852. [[CrossRef](#)]
162. Khan, P.W.; Byun, Y. A blockchain-based secure image encryption scheme for the industrial Internet of Things. *Entropy* **2020**, *22*, 175. [[CrossRef](#)]
163. Lyu, L.; Chen, C.; Zhu, S.; Guan, X. 5G enabled codesign of energy-efficient transmission and estimation for industrial IoT systems. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2690–2704. [[CrossRef](#)]

164. Bahga, A.; Madisetti, V.K. Blockchain platform for industrial internet of things. *J. Softw. Eng. Appl.* **2016**, *9*, 533–546. [CrossRef]
165. Stankovic, J.A. Research directions for the internet of things. *IEEE Internet Things J.* **2014**, *1*, 3–9. [CrossRef]
166. Mumtaz, S.; Alsohaily, A.; Pang, Z.; Rayes, A.; Tsang, K.F.; Rodriguez, J. Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation. *IEEE Ind. Electron. Mag.* **2017**, *11*, 28–33. [CrossRef]
167. Haseeb, K.; Saba, T.; Rehman, A.; Ahmed, I.; Lloret, J. Efficient data uncertainty management for health industrial internet of things using machine learning. *Int. J. Commun. Syst.* **2021**, *34*, e4948. [CrossRef]
168. Astarloa, A.; Bidarte, U.; Jiménez, J.; Zuloaga, A.; Lázaro, J. Intelligent gateway for Industry 4.0-compliant production. In Proceedings of the IECON 2016—42nd Annual Conference of the IEEE Industrial Electronics Society, Florence, Italy, 24–27 October 2016; pp. 4902–4907.
169. Bouachir, O.; Aloqaily, M.; Tseng, L.; Boukerche, A. Blockchain and fog computing for cyberphysical systems: The case of smart industry. *Computer* **2020**, *53*, 36–45. [CrossRef]
170. Sharma, P.; Jain, S.; Gupta, S.; Chamola, V. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Netw.* **2021**, *123*, 102685. [CrossRef]
171. IBM. What Is Industry 4.0? 2021. Available online: <https://www.ibm.com/topics/industry-4-0> (accessed on 20 October 2023).
172. Intel. Industrial IoT (IIOT) and Automation Technology. 2021. Available online: <https://www.intel.com/content/www/us/en/manufacturing/manufacturing-industrial-overview.html> (accessed on 20 October 2023).
173. Oracle. Remote Monitoring & Maintenance: Mission Critical Operations at the Competitive Edge. 2021. Available online: <https://www.oracle.com/us/solutions/internetofthings/iot-remote-monitoring-brief-2881653.pdf> (accessed on 2 March 2023).
174. Oracle. What Is IoT? 2021. Available online: <https://www.oracle.com/internet-of-things/what-is-iot/> (accessed on 2 March 2023).
175. Microsoft. Microsoft and Nokia Collaborate to Accelerate Digital Transformation and Industry 4.0 for Communications Service Providers and Enterprises. 2021. Available online: <https://news.microsoft.com/2019/11/05/microsoft-and-nokia-collaborate-to-accelerate-digital-transformation-and-industry-4-0-for-communications-service-providers-and-enterprises/> (accessed on 2 March 2023).
176. HQ Software. Development and Industrial IoT Solutions. 2021. Available online: <https://hqsoftwarelab.com/solutions/internet-of-things/industrial-iot/> (accessed on 22 March 2023).
177. Cisco. Industrial IoT Solutions for Digital Manufacturing. 2021. Available online: <https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-digital-manufacturing-solution.html> (accessed on 22 March 2023).
178. Bembe, M.; Abu-Mahfouz, A.; Masonta, M.; Ngondi, T. A survey on low-power wide area networks for IoT applications. *Telecommun. Syst.* **2019**, *71*, 249–274. [CrossRef]
179. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
180. Kantareddy, S.N.R.; Mathews, I.; Sun, S.; Layurova, M.; Thapa, J.; Correa-Baena, J.P.; Bhattacharyya, R.; Buonassis, T.; Sarma, S.E.; Peters, I.M. Perovskite PV-powered RFID: Enabling low-cost self-powered IoT sensors. *IEEE Sensors J.* **2019**, *20*, 471–478. [CrossRef]
181. Mao, W.; Zhao, Z.; Chang, Z.; Min, G.; Gao, W. Energy-efficient industrial internet of things: Overview and open issues. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7225–7237. [CrossRef]
182. Younan, M.; Houssein, E.H.; Elhoseny, M.; Ali, A.A. Challenges and recommended technologies for the industrial internet of things: A comprehensive review. *Measurement* **2020**, *151*, 107198. [CrossRef]
183. Humayun, M.; Jhanjhi, N.; Alruwaili, M.; Amalathas, S.S.; Balasubramanian, V.; Selvaraj, B. Privacy protection and energy optimization for 5G-aided industrial Internet of Things. *IEEE Access* **2020**, *8*, 183665–183677. [CrossRef]
184. del Campo, G.; Calatrava, S.; Cañada, G.; Olloqui, J.; Martinez, R.; Santamaria, A. IoT Solution for Energy Optimization in Industry 4.0: Issues of a Real-life Implementation. In Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018; pp. 1–6.
185. Sajid, A.; Abbas, H.; Saleem, K. Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access* **2016**, *4*, 1375–1384. [CrossRef]
186. Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. Challenges and opportunities in securing the industrial internet of things. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2985–2996. [CrossRef]
187. Stouffer, K.; Falco, J.; Scarfone, K. *Guide to Industrial Control Systems (ICS) Security*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2008.
188. Dolui, K.; Datta, S.K. Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. In Proceedings of the 2017 Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6.
189. Shi, C.; Ren, Z.; Yang, K.; Chen, C.; Zhang, H.; Xiao, Y.; Hou, X. Ultra-low latency cloud-fog computing for industrial internet of things. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
190. Hong, Z.; Chen, W.; Huang, H.; Guo, S.; Zheng, Z. Multi-hop cooperative computation offloading for industrial IoT-edge-cloud computing environments. *IEEE Trans. Parallel Distrib. Syst.* **2019**, *30*, 2759–2774. [CrossRef]
191. Pei-Brevold, H.; Sandström, K. Internet of things for industrial automation-challenges and technical. In Proceedings of the iThings 2015: The 8th IEEE International Conference on Internet of Things, Sydney, Australia, 11–13 December 2015; pp. 532–539.

192. Munirathinam, S. Industry 4.0: Industrial internet of things (IIOT). In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2020; Volume 117, pp. 129–164.
193. Ghorpade, S.; Zennaro, M.; Chaudhari, B. Survey of localization for internet of things nodes: Approaches, challenges and open issues. *Future Internet* **2021**, *13*, 210. [[CrossRef](#)]
194. Saqlain, M.; Piao, M.; Shim, Y.; Lee, J.Y. Framework of an IoT-based industrial data management for smart manufacturing. *J. Sens. Actuator Netw.* **2019**, *8*, 25. [[CrossRef](#)]
195. Wu, Y.; Dai, H.N.; Wang, H. Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet Things J.* **2020**, *8*, 2300–2317. [[CrossRef](#)]
196. Iglesias-Urkia, M.; Orive, A.; Barcelo, M.; Moran, A.; Bilbao, J.; Urbieta, A. Towards a lightweight protocol for Industry 4.0: An implementation based benchmark. In Proceedings of the 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and Their Application to Mechatronics (ECMSM), Donostia, Spain, 24–26 May 2017; pp. 1–6.
197. Gebremichael, T.; Ledwaba, L.P.; Eldefrawy, M.H.; Hancke, G.P.; Pereira, N.; Gidlund, M.; Akerberg, J. Security and privacy in the industrial internet of things: Current standards and future challenges. *IEEE Access* **2020**, *8*, 152351–152366. [[CrossRef](#)]
198. Grüner, S.; Pfrommer, J.; Palm, F. RESTful industrial communication with OPC UA. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1832–1841. [[CrossRef](#)]
199. Ankele, R.; Marksteiner, S.; Nahrgang, K.; Vallant, H. Requirements and recommendations for IoT/IIoT models to automate security assurance through threat modelling, security analysis and penetration testing. In Proceedings of the 14th International Conference on Availability, Reliability and Security, Vienna, Austria, 26–29 August 2019; pp. 1–8.
200. Feng, J.; Yang, L.T.; Zhang, R.; Qiang, W.; Chen, J. Privacy preserving high-order bi-lanczos in cloud-fog computing for industrial applications. *IEEE Trans. Ind. Inform.* **2020**, *18*, 7009–7018. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.