applied sciences

MDPI

Review

Analysis of Security Issues and Countermeasures for the Industrial Internet of Things

Shantanu Pal [1,*] and Zahra Jadidi [2]

[1] School of Computer Science, Faculty of Science, Queensland University of Technology, Brisbane, QLD 4000, Australia
[2] Cyber Security Cooperative Research Centre, Queensland University of Technology, Brisbane, QLD 4000, Australia; zahra.jadidi@qut.edu.au
* Correspondence: shantanu.pal@qut.edu.au; Tel.: +61-7-3138-2419

Abstract: Industrial Internet of Things (IIoT) can be seen as an extension of the Internet of Things (IoT) services and applications to industry with the inclusion of Industry 4.0 that provides automation, reliability, and control in production and manufacturing. IIoT has tremendous potential to accelerate industry automation in many areas, including transportation, manufacturing, automobile, marketing, to name a few places. When the benefits of IIoT are visible, the development of large-scale IIoT systems faces various security challenges resulting in many large-scale cyber-attacks, including fraudulent transactions or damage to critical infrastructure. Moreover, a large number of connected devices over the Internet and resource limitations of the devices (e.g., battery, memory, and processing capability) further pose challenges to the system. The IIoT inherits the insecurities of the traditional communication and networking technologies; however, the IIoT requires further effort to customize the available security solutions with more focus on critical industrial control systems. Several proposals discuss the issue of security, privacy, and trust in IIoT systems, but comprehensive literature considering the several aspects (e.g., users, devices, applications, cascading services, or the emergence of resources) of an IIoT system is missing in the present state of the art IIoT research. In other words, the need for considering a vision for securing an IIoT system with broader security analysis and its potential countermeasures is missing in recent times. To address this issue, in this paper, we provide a comparative analysis of the available security issues present in an IIoT system. We identify a list of security issues comprising logical, technological, and architectural points of view and consider the different IIoT security requirements. We also discuss the available IIoT architectures to examine these security concerns in a systematic way. We show how the functioning of different layers of an IIoT architecture is affected by various security issues and report a list of potential countermeasures against them. This study also presents a list of future research directions towards the development of a large-scale, secure, and trustworthy IIoT system. The study helps understand the various security issues by indicating various threats and attacks present in an IIoT system.

Keywords: Industrial Internet of Things; security; architecture; threats; attacks; countermeasures

Citation: Pal, S.; Jadidi, Z. Analysis of Security Issues and Countermeasures for the Industrial Internet of Things. *Appl. Sci.* **2021**, *11*, 9393. https://doi.org/10.3390/app11209393

Academic Editor: Eui-Nam Huh

Received: 27 August 2021
Accepted: 28 September 2021
Published: 10 October 2021

1. Introduction

In recent years, there has been an increasing trend in the use of Internet of Things (IoT) applications in the industrial sectors [1]. The emergence of IoT is already well noted in industry, e.g., linked to Supervisory Control And Data Acquisition (SCADA) for control and monitoring production chains and addressing specific use cases involved in Cyber-Physical System (CPS) [2]. Moreover, with the advancements of Industry 4.0 (also known as the fourth industrial revolution), it is possible to perform interconnected operations that bring digital and physical technologies together with IoT operations. This is achieved by a large number of interconnected devices or machines, applications, as well as people with industrial applications at scale [3]. This paradigm is commonly known as the Industrial IoT

(IIoT) that aims to improve the efficiency in operations and product quality of an industry in real-time. IIoT requires minimal human intervention for performing a task. In other words, it is more automated than traditional computer-assisted industrial systems. It is predicted that the IIoT marketplace will be worth USD 106.1 billion by 2026, and it is worth USD 76.7 billion in 2021 [4].

In Figure 1, we illustrate the relationship among IoT, CPS, Industry 4.0, and IIoT [5]. In the figure, we can precisely see the intersection between IoT and Industry 4.0, IoT and CPS, and CPS and Industry 4.0. Common concepts provided in these intersections are as follows: (1) *IoT and Industry 4.0* deals with human-to-machine communications, inter-connectivity, low-cost sensors applications, machine-to-machine communications, and cloud computing-based services; (2) *IoT and CPS* considers fog computing enabling IIoT, efficient resource sharing, real-time systems, and applications that are coupled with the physical and virtual computing environment; (3) *CPS and Industry 4.0* delivers innovative functionalities through Web of Things (WoB) with appropriate computing and communication infrastructures [6,7].

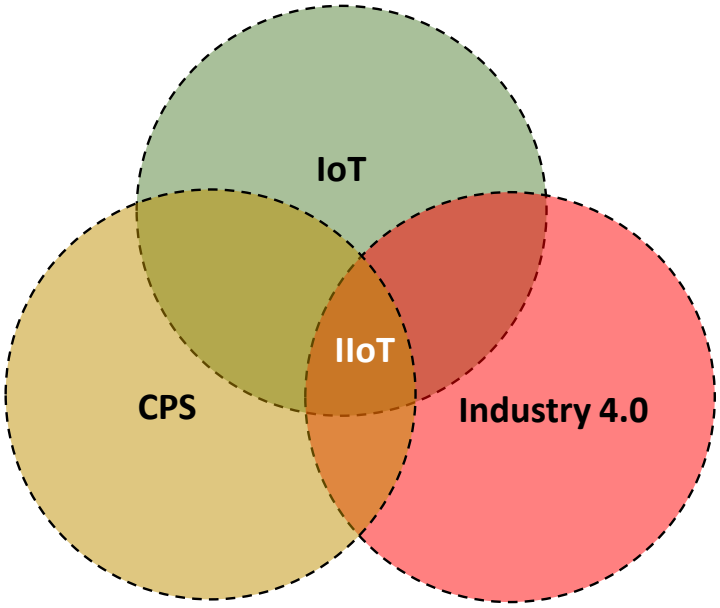

Figure 1. Relationship among IoT, CPS, Industry 4.0, and IIoT.

We note that an important requirement for IIoT systems is dependability, which has different facets [8]. Some basic needs of dependability are *reliability*, *safety*, *availability*, *maintainability*, and *security*. Reliability implies to what extent a system operates correctly. Safety guarantees that no catastrophe occurs when there is a failure. Availability is related to the readiness of a system for usage. Highly available systems provide their functionality even when there is a system failure. High maintainability means that changing the configuration of a system or replacing failed components is an easy task. Finally, security is another critical requirement for dependable systems. There are different applications of IIoT with varying issues of dependability. An example of an IIoT application is the industrial automation of smart digital factories. To this end, wireless IIoT networks can be used for real-time monitoring and industrial control [9].

Pervasive [10] and ubiquitous computing [11] have a long tradition of looking into the integration of physical objects with the digital world. The IIoT combines the components of the digital and physical worlds of IoT, CPS, and Industry 4.0 by bringing diverse concepts and technological components of ubiquitous and pervasive computing together for large-scale industrial sectors. On the one hand, ubiquitous computing is a concept in software engineering where general-purpose machines (e.g., personal computers) are replaced by many specialized computers embedded into everyday objects and can be used for

identifying, sensing, networking, etc., data processing. A typical application for this is the smart home, whereby with the use of such technology, users can control and monitor the lighting, thermostat, or even a microwave from a smart phone. Therefore, ubiquitous computing makes much greater use of technology. It deals with the question of how entities would communicate in a digital environment, i.e., with digital functionality. On the other hand, the term pervasive computing refers to the vision of connecting real-world objects in our everyday life to allow them to communicate with one another embedded by microprocessors. An example of pervasive computing is smart meters, where the smart meters send usage data over the Internet to the managing companies. Therefore, along with the IoT, CPS, and Industry 4.0, IIoT potentially represents one of the most promising technologies, enabling both the ubiquitous and pervasive computing scenarios to the smart and innovative industrial operations [12,13].

The Internet is a compelling example of a scalable global network of computers that interoperates across heterogeneous hardware and software platforms. However, the IoT is not merely the Internet, and it does not rely on IP (Internet Protocol), but it is a new application trend for the next generation of Internet users [14,15]. The IoT extends the principles of the Internet as a network organization concept to physical things, in which everything has a unique identification, based on standard communication protocols, e.g., IPV6. This should be machine-readable and associated with a digital representation on the Web. This paradigm can be envisioned as a *things-connected* network where the *things* are connected with each other using a communication medium. That said, IoT and IIoT can not be interpreted as the same. A major difference between them is the scale of interconnected devices/machines, users, applications, and associated services. An IIoT system can achieve higher scale than an IoT system [16,17].

1.1. Problem Statement and Motivation

There are several interpretations to define an IIoT system. For example, according to [18], it is combined with *"machines, computers and people enabling intelligent industrial operations using advanced data analytics for transformational business outcomes"*. According to [5], IIoT *"covers the domains of machine-to-machine (M2M) and industrial communication technologies with automation applications"*. The optimization of IIoT can be seen as a transformation rather than an evolutionary technological progression for both conventional and non-conventional fields of application. From a logical point of view, IIoT can be seen as a collaborative and interconnected system with the help of smart devices/machines to share a common objective as Industry 4.0 and CPSs. From a technological point of view, IIoT combines and adopts various architectures, communication and networking technologies, processing methodologies, and design concepts to fulfill a common goal based on their target. That said, the IIoT uses a broad range of communication platforms, which integrates a broad range of technologies, including sensing, networking, service-oriented architecture (SOA), or even intelligent information processing technologies that deal with complex system information and its uncertainty [19,20]. In Figure 2, we illustrate the basic concept of an IIoT infrastructure.

The benefits of IIoT are promising, for example, for reducing human errors, lowering the need for manual labor, cost-effectiveness, etc. In addition, it indicates the significant improvement towards the automation that IIoT brings to industry, and at the same time provides affordability and flexibility in applications for end-users [21]. However, there are numerous security issues that must be addressed to provide a flexible, scalable, and trustworthy IIoT environment to both the client and users [22]. Recent attacks on IIoT elevate a significant security concern for industry [23–27]. These attacks can cause a large amount of business failure/damage and also sometimes may bring about life-threatening situations. Among others, data security is one of the core issues in an IIoT system (along with the Industry 4.0 infrastructure). Typically, the nature (e.g., resource-constrained) and the properties (e.g., heterogeneity, mobility) of an IIoT system make it difficult where the traditional heavy-weight security architectures cannot be applied directly to address such

issues. Instead, they require additional mechanisms and frameworks that can capture the particular requirements of an IIoT system. That said, there is a need for a seamless data exchange platform across companies that allow for efficient data acquisition and collection, transfer, and analysis of various data sources, for example, in a supply chain network [28]. Thus, in addition to the technical considerations, organizational aspects, e.g., cross-company information sharing and collaboration (through data exchange and data transparency), are highly demanding. As IIoT is an interconnected network of multiple platforms, networks, services, and applications, a potential vulnerability in one part of the system can make an impact on the overall performance of the system to a greater extent [29]. For instance, in 2021, a Canadian manufacturer of business jets called Bombardier was compromised by a cyber attack. The attackers entered into the network and tried to steal sensitive information associated with employees, customers, and suppliers [30]. In 2021, Harris Federation, a multi-academy trust based in London was compromised by a cyber attack. The attackers disabled the devices and email systems for academics for a short period of time [31]. In 2017, WannaCry ransomware attacks disrupted the services of several manufacturers and spread rapidly across many computer networks to collapse the interconnected systems. It has one of the most significant impacts on the medical facilities in the United Kingdom's National Health Services (NHS), where MRI scanners, blood-storage refrigerators, and other types of operation theatre equipment were compromised [32].

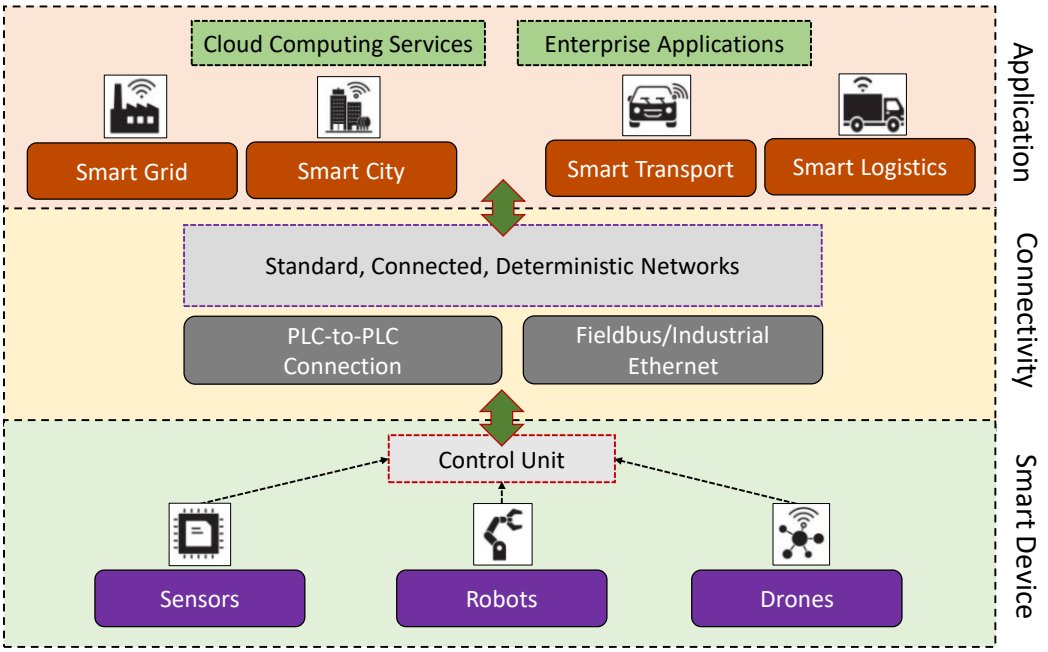

Figure 2. A simple outline of the basic concept of an IIoT infrastructure.

Commonly, IIoT inherits security issues from IoT systems [33]. Although the heterogeneity in the IIoT system further produces complexity in designing a comprehensive and cohesive system. This requires further studies to investigate the security issues in IIoT systems. Several surveys discuss the security issues in IIoT. For instance, Yu and Guo [34] present a survey on IIoT security, focusing on four key features, namely data confidentiality, CPSs integrity, secure key establishment, and device management. Tange et al. [35] provide a survey on research methodologies in existing surveys on IIoT security requirements. The key focus of their survey is to investigate the feasibility of adaptive fog computing services as a potential security solution for IIoT systems. In particular, it discusses the benefits of edge intelligence of fog computing applications to IIoT applications. Vallois et al. [36] present security challenges, issues, and requirements for the IIoT systems based on three security services. The focus of their survey is limited to information assurance, access control, and dependability, which are common to any of the network systems. Panchal et al. [37]

present a survey on IIoT security highly focused on an Industrial Control Systems (ICS) point of view. They focus on IT (Information Technology) and OT (Operational Technology) layers specifically. Xu et al. [38] discuss IIoT security issues from a CPS perspective. The discussion is limited to control, networking, and computing without the system-specific needs for cascading services or the emergence of resources. Similar to [36], Jayalaxmi et al. [39] present a security taxonomy for the IIoT system based on six specific security services, namely authentication, confidentiality, non-repudiation, availability, integrity, and privacy. While these surveys present state-of-the-art security issues in IIoT systems, their contributions are specific to certain scenarios. They do not consider the wider aspects of IIoT systems, e.g., communication, heterogeneity in users and devices, and their interactions at scale from consumers and enterprises' points of view. Further, these approaches do not consider the combination of confidentiality, integrity, and availability for IIoT services and applications (especially how data are used and shared) to provide more fine-grained security controls that are immensely important for IIoT security issues.

1.2. Contributions

The business, cultural, technological, and personal advantages are expected to rise significantly by IIoT commerce and support. This includes smarter cities, creative infrastructure, intelligent communications and information sharing platforms, smart healthcare systems, energy-saving uses, autonomous supply chain management, and smart transportation [40]. However, protecting IIoT systems is challenging due to the security, privacy, and trust issues that constrain the convenience of a digital world into the physical world. Apart from the security, privacy, and trust concerns, the scale of the number of different devices, administrations, services, resource-constrained nature of the devices, and the curtailment of well-known standards and design considerations for an IIoT system further makes it difficult to enforce traditional security approaches within it [26]. Therefore, the baseline security requirements must be robust and scalable. This paper is motivated by the following research questions: (1) Are the current security requirements enough to develop a secure IIoT system? (2) What are the potential threats and attacks that are primary concerns for a seamless IIoT application that operates in a multi-organizational heterogeneous network environment? (3) How can one design dynamic security mechanisms for managing authentication, authorization, and access control seamlessly over billions of interconnected entities in an IIoT system? The goals of this paper are two-fold: (1) to discuss the various security issues of an IIoT system (note, we use the term security issue to represent attacks, threats, and the potential vulnerabilities), and (2) to use an IIoT layered architecture to demonstrate the various threats and attacks specific to each layer. The significant contributions of this paper can be summarized as follows:

- We review the existing IIoT security issues in a systematic way. We consider broader aspects of an IIoT system (e.g., integration of IoT, Industry 4.0, and various communication and networking issues related to multi-organizational communications) and list a set of security issues for the IIoT systems.
- We discuss an example use case of IIoT architecture based on layers and examine the identified security issues in each layer. We provide a detailed discussion of the potential countermeasures against these security issues. It helps to understand the system-specific security needs in an IIoT architecture at a more fine-grained level.
- We discuss a set of unique open research issues and list the future research directions that require further study to ensure the security of an IIoT system at scale.

1.3. Paper Organization and Roadmap

The rest of the paper is organized as follows. In Section 2, we discuss different IIoT architectures based on layers. In Section 3, we provide a detailed categorization of existing security issues in an IIoT system. We list the security issues and show potential threats and attacks within them. In Section 4, we consider a four-layer IIoT architecture and show how the functioning of different layers is affected by the various security issues.

We also provide countermeasures against such security issues. In Section 5, we provide a discussion on lessons learned. Finally, we conclude the paper with future research development in Section 6.

2. IIoT Architecture

There is no single and well-accepted IIoT architecture at present. We consider an IIoT architecture to be dependent on the system's requirements and the designer's choice. We observe that a single vendor does not propose an ideal IIoT architecture. Therefore, using standards can help the architecture take advantage of evolving technologies and standards. Consequently, it can use powerful IIoT devices when they become available. Different vendors support standards such as WirelessHART [41] and Foundation Fieldbus [42]. The advantage of using standards is that if a particular type of sensor from one vendor fails, it is possible to replace it with another vendor as long as they use the same protocol standard and network technology. This is the crucial part of interoperability. When a sensor is changed, typically, the system does not need to replace the other sensors or the higher levels of the IIoT architecture. This signifies the use of standard protocols and networks for the IIoT systems. On the other hand, new standards have begun to emerge due to the need to monitor industrial systems and processes, for example, new industrial wireless sensor network (IWSN) standards of ZigBee, WirelessHART, ISA 100.11a wireless, and Wireless network for Industrial Automation-Process Automation (WIA-PA), to name a few [43].

Before going to a detailed discussion of security issues and their potential countermeasures, in this section, we discuss the foundation of a basic IIoT architecture within which these security issues would function. Several proposals present various architectures for IIoT. Mostly, these architectures are classified based on layers. Significantly, these layers typically overlap with IoT architecture. However, significant differences are from the business, usage, functional, scalability, and implementation points of view. Next, we discuss some basic architectures of an IoT system and then see how these architectures can be integrated into the IIoT space.

A three-layer IoT architecture is discussed in [44]. The layers are perception (sensing information from the physical layer), network (provides communication between the layers), and application layers (facilitates communication between the end-users via different apps). To provide more granularity in the system, [45] proposes a four-layer IoT architecture. These layers are sensing, network, service, and application interface. The sensing layer is responsible for the collection of data sensing from the physical environment. The network layer helps in communications among the various components with the architecture, supports data aggregation, and maintains Quality of Service (QoS). The major functionalities of the service layer are service processing, divisions, monitoring, and configuration. Finally, the top layer (i.e., the application interface layer) is responsible to provide smart IoT services to the end-users.

Proposals [46–48] present a five-layer IoT architecture. These layers are object, object abstraction, networking, service composition, and application. The object layer (also known as the perception layer) is the bottom layer of the architecture. It is composed of vast and heterogeneous sensors, actuators, and other smart-sensing objects. The object abstraction layer passes the collected data to the next layer, called the networking layer. It is responsible for providing networking between the other layers of the architecture. The service management layer performs the service decisions tasks. The service composition layer helps to aggregate various services using specific hardware platforms. Finally, the application layer renders desired interfaces for the end-users to access the services via apps.

Al-Qaseemi et al. [49] present another five-layer architecture for the IoT. These layers are perception, access gateway, network, middleware, and application layers. The middleware layer is introduced to provide a more flexible association between the hardware devices and effective communications to various applications by enabling real-time information flow. In [50], the authors propose another five-layer IoT architecture. These layers are objects, object-abstraction, service management, application, and business manage-

ment layers. The newly provisioned business management layer is the topmost layer of the architecture. It controls IoT system activities and manages services using dedicated business models applied to the received data from the service management layer (through the application layer).

In proposal [51], authors illustrate a relationship between a three-layer (e.g., [52]) and a five-layer (e.g., [50]) IoT architectures. In comparing these architectures, the authors argue that the object and the object abstraction layers in a five-layer architecture are the same as the perception and network layers in a three-layer architecture, where the application layer in a three-layer architecture is composed of the core functionality compounding of the service management layer, application layer, and business management layer of a five-layer architecture.

CISCO provides a seven-layer IoT reference architecture [53]. From bottom to top, these layers are physical devices and controllers, connectivity, edge (fog) computing, data accumulation, data abstraction, applications and collaboration, and processes.

For IIoT, a three-layer architecture is discussed in [5]. The layers are sensors, networks, and services. Another three-layer architecture for IIoT is discussed in [38]. Unlike [5], it is composed of physical, communication, and application layers. Proposal [36] discusses a four-layer IIoT architecture composed of thing, network, middleware, and application layers. The newly introduced middleware layer is the central point of the architecture that consists of different applications, middleware services, databases, and management software. In [54], a four-layer IIoT architecture is presented. These layers are perception fog, cloud, and application layers. Fog layer has been introduced to minimize the latency in decision making at the edge devices, consider the resource-constraint nature of the devices, and improve battery life of the devices in offloading the intensive computations. Another four-layer IIoT architecture is presented in [39], composed of perception, network, support, and application layers. The functioning of the support layer can be regarded as a data layer performing data analytics tasks. In [37], a five-layer IIoT architecture is discussed. The first layer is composed of embedded devices, sensors, and actuators. The second layer is composed of Distributed Control Systems (DCS), Programmable Logic Control (PLC), and Gateways. The third layer is composed of SCADA systems. The fourth layer is composed of office applications, Intranet services, Web services, etc. Finally, the fifth layer is composed of enterprise applications, and cloud computing services. In Figure 3, we present an outline of three distinct IIoT layer architecture (three-layer [5], four-layer [39], and five-layer [37]) discussed above.

We argue that an layered IIoT architecture must support an industrial platform's scale and diverse nature of connected objects, applications, and associated services. At the same time, the architecture must be flexible to collect contextual information, store processed data, analyze the operation and detect anomalies, visualize the performance, and execute the instruction with high efficiency. The architecture also needs to handle the essential elements in traditional information security, i.e., communication, control, and computation [55]. We argue that an ideal view of an IIoT architecture should contain the different requirements of the IIoT system, and simultaneously fulfill the dynamic nature of the system. This also needs to include operational efficiencies with wireless cellular connectivity while maintaining seamless communications and semantic between the layers [56].

For our purpose, in this paper, we consider an IIoT architecture discussed in [39]. Note that we select a four-layer architecture that can be potentially used in different IIoT systems. It has the ability to hold the components of a three-layer IIoT architecture, and at the same time, a four-layer architecture can easily be enhanced with more components to represent a fine-grained five-layer IIoT architecture. That said, our present study on IIoT security issues can easily be fit into any of the architectures that we discussed above. Recall, [39] consists of four distinct layers (i.e., perception, network, support, and application layers). Further, we argue that this architecture can deliver the basic functionalities and is able to maintain seamless communication to the end users. Recall's perception layer collects

information from the physical environment and sends the collected information to the next layer (i.e.,the network layer). The network layer manages and transforms information to the next layer (i.e., the support layer). The support layer performs data analytics tasks (e.g., data division, composition, etc). Finally, through the application layer, end users can access the desired services.

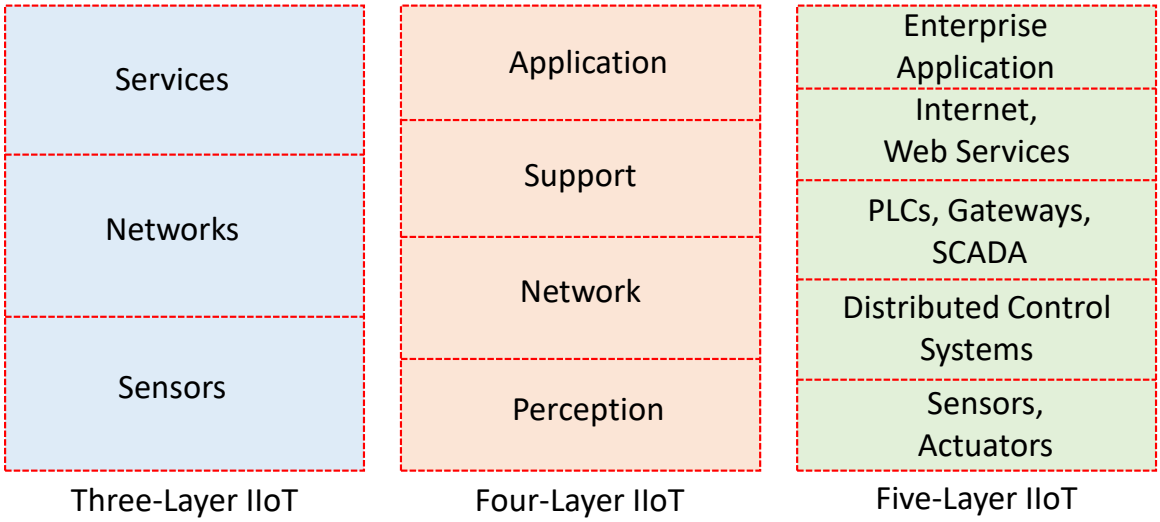

Figure 3. Outline of various available IIoT architectures based on layers (three-layer [5], four-layer [39], and five-layer [37]).

3. Security Issues in IIoT Systems

In this section, first, we discuss an application scenario of IIoT infrastructure to motivate the need for security. Then, we discuss the various security issues present in an IIoT system in detail.

3.1. An Application Scenario

There are various applications for IIoT, for example, automation industry, smart manufacturing, logistics, automobile and construction, smart healthcare systems, supply chain optimization and management, etc. [5,57–59]. In this section, we employ a use case of a smart healthcare system as an IIoT application. We select a smart healthcare system as an example, as it deals with sensitive, private, and critical information where security is a significant concern [60]. We examine the smart healthcare system based on the four layers of an IIoT architecture, which is discussed in [39] (cf. Section 2). In Figure 4, we illustrate the employed scenario. Different sensors are attached to the patients, and the perception layer collects information from the patients. Then this information is transferred to the hospital's internal database through the network layer, which is responsible for communication. Next, records are analyzed in the service layer, and appropriate recommendations (e.g., alteration of meditation or associated examinations) are made for the specific needs of the patients. Finally, doctors and caregivers can access this information through the application layer.

3.2. Security Issues

As noted earlier, some security issues in IIoT are inherited from IoT. Thus, a few of them can be overlapped for both IIoT and IoT systems [61–67]. For instance, Sicari et al. [68] suggest developing a scalable, robust, and structured (i.e., divided into layers) security infrastructure for the IoT systems. Roman et al. discuss IoT security issues from a distributed IoT architecture point of view. They also enhance the edge intelligence of the devices and collaboration between them to satisfy a common goal [69]. They emphasize edge intelligence, resource-constrained IoT device provision to the services at the edge of the network (e.g., edge computing [70]), and collaboration. In such a case, the devices generate a diverse collaborative resource sharing environment among other devices located

in proximity. This is also envisioned for the IIoT discussed in proposal [34]. Both of the proposals address the issues of communication, control, and computation, as well as the potential security issues related to authentication, authorization, and access control. Proposal [71] discusses IoT security requirements looking at logical and technological points of view (includes device interactions, and technological device collaborations), which further advance the necessity of the IoT security requirements discussed in [69,71]. These features are significantly relevant for IIoT systems as well.

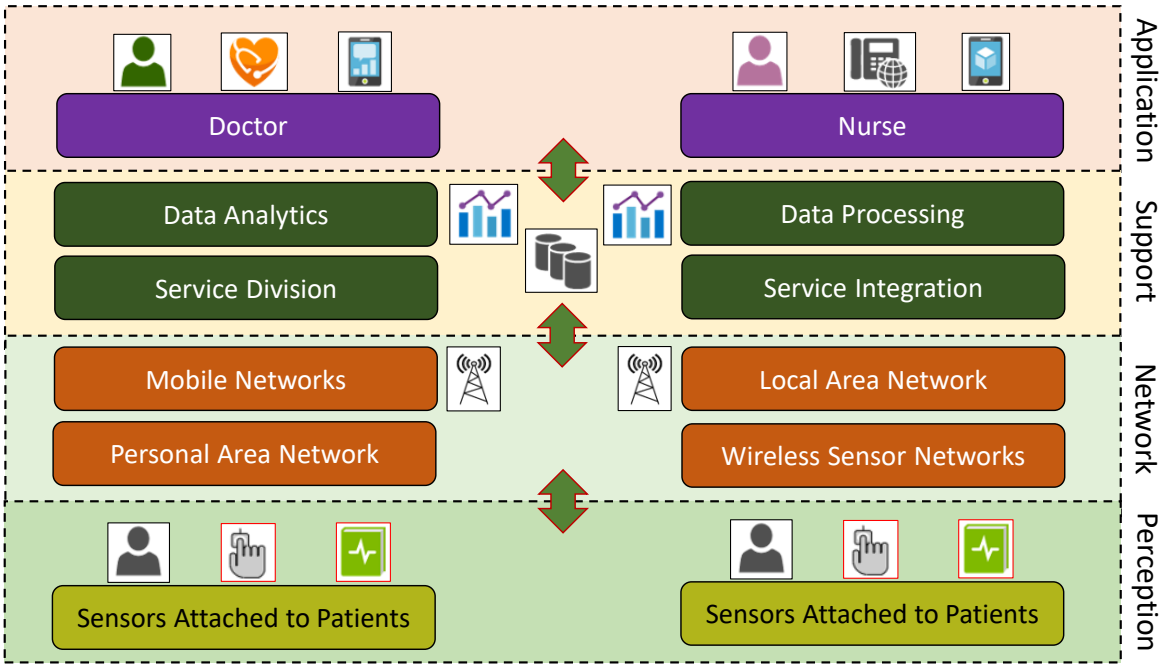

Figure 4. An illustration of a smart healthcare application scenario used in our paper.

Monjur et al. [72] present the state of the art security in distributed decentralized IIoT, focused on three core issues, i.e., privacy for humans, the confidentiality of the business process, and third-party dependability, which supports scalability and usability issues. The authors analyze the most recent approaches related to IoT security based on integrity, confidentiality, authentication, privacy, trust, and mobility management.

Apart from the logical, technological, and architectural points of view, the integration of different IIoT security requirements poses several legal challenges over multiple jurisdictions. Further, the IIoT system must adjust to node failures and avoid a single point of failure for resilience to attacks. For data authentication, the client identity and the object information must be authenticated and then authorized for providing the desired assistance. From an access control point of view, successfully providing the information/resources to the authorized users also brings new security issues of trust. That said, the information/resources must be shared between trusted parties authorized to access the information/resources. Finally, the privacy of a specific user must be secured by the service provider within the system. We consider a wider context of IIoT and examine potential security issues that may come from communication, devices, networking, users, applications, and services. That said, we consider the broad range of areas, including CPS, Industry 4.0, and IoT. In Figure 5, we illustrate the core security issues of an IIoT system [39]. Note that these are security issues common for general IoT systems; however, in the case of an IIoT system, its scale and nature of adversary are different. Based on these core security issues, we list a number of potential security concerns as follows:

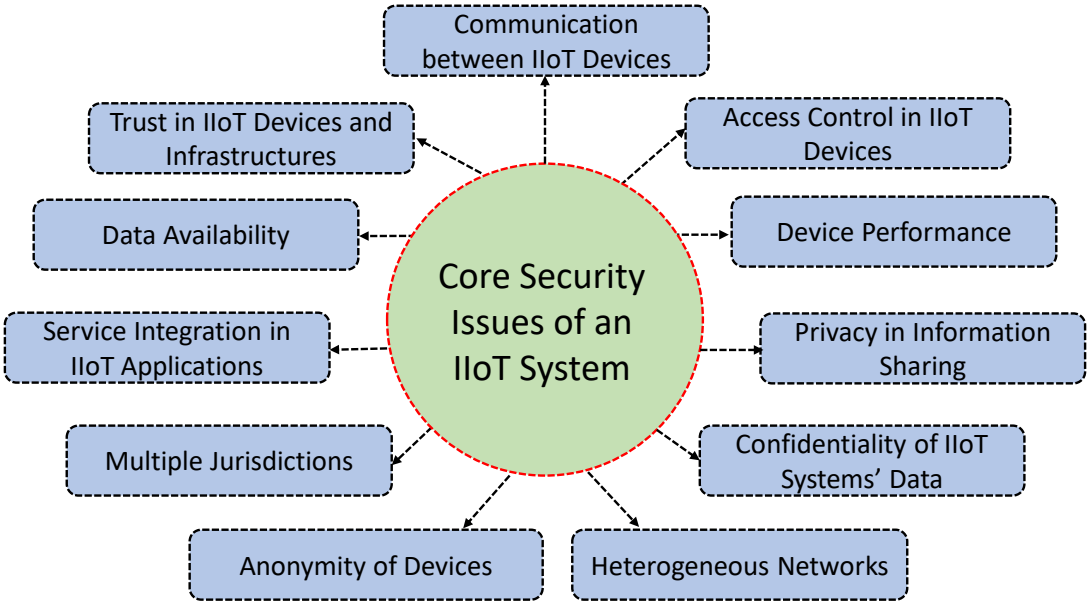

Figure 5. Outline of the core security issues in an IIoT system.

3.3. Security Issue 1—Controlling Over Communication

In this case, an attacker targets routing protocols and network traffic, and redirects the routing path from the original receiver to an insecure destination. Due to the high network dynamics and unpredictable nature of the IIoT systems, it is challenging to enforce a fixed and secure routing mechanism for the present IIoT systems. Therefore, with the lack of a predefined routing infrastructure, it is difficult to cooperate and communicate securely with one another in such systems. In a routing attack, an attacker can misconfigure routers, gateways, and even DNS (Domain Name System) servers and selectively drop messages unfavorably [73]. In a *DNS spoofing* attack, an attacker takes control over the DNS server and unlawfully diverts network traffic to the attacker's devices that further launch attacks against the user's data confidentiality and network hosts [74]. Moreover, an attacker can spoof the identity of an attacked node's IP address and create a TCP (Transmission Control Protocol) session hijacking by impersonating a victim node. In such cases, attackers first capture an IIoT device and inject malicious codes into the router to impersonate a device's identity.

The most common forms of this types of routing attacks are blackhole, wormhole, sybil, and pharming attacks [75]. In a blackhole attack, the compromised nodes divert data packets to another insecure location by falsely declaring a new direction to some targeted (i.e., malicious) destination and drops them before reaching the original destination. In a wormhole attack, an attacker makes a tunnel and secretly captures data packets from a specific location in the routing path and then transmits them to another insecure location. In a Sybil attack, an attacker creates a false identity (by providing false credentials) and uses this "Sybil" identity with another node to masquerade untrusted information to compromise the whole network [76]. In the case of a pharming attack, an attacker infects a large number of trusted nodes in a DNS server with malicious codes or changes the host files on a compromised computer. This redirects a legitimate website's data traffic to an insecure and fake site created by the attacker [77]. Returning to our use case of smart healthcare infrastructure, these are potential threats towards users' (i.e., patients) and devices' (i.e., the sensors attached to the patients) data privacy. In such cases, the attackers can masquerade a reputation system for gaining unauthorized control over the data traffic of the communications [78].

3.4. Security Issue 2—Infecting Data Packets

In this type of attack, an attacker controls an IIoT device by injecting malicious codes into the data packet [79]. Attackers mostly try to gain extensive control over the resource of a victim node (e.g., source, destination, number, size, as well as the transmission time). This can be done in two different ways, via an *active attack* and a *passive attack* [80]. These are discussed as follows:

In the former case (i.e., the active attack), one of the most frequent attacks is the *Man in the Middle* (MITM) attack. In this case, the attacker joins the network as a legitimate user and gains control over the nodes through the active attack path to sniff information. In an MITM attack, an attacker sits in between two nodes (the sender and the receiver) and creates an independent connection by secretly relaying traffic between the nodes, making the attacked nodes believe that they are directly communicating with one another (by impersonating the sender for transmitting information to the receiver) [47]. This is a potential threat to the IIoT systems towards data modification and data fabrication.

In such cases (i.e., data modification and data fabrication), the attacker captures data packets and collects its information (e.g., destination header) and then tampers (i.e., doing intentional alteration of data packets) with the information to inject a malicious code and makes an unauthorized attempt to channel the modified data packet to another unsecured network direction rather than its actual destination [81]. By tampering with the data packets, attackers get unauthorized access to the data traffic as they drop data packets while passing through the unsecured channe, or cause a further delay in forwarding other data packets.

Another form of the active attack is the *jamming channels* attack. In this type of attack, attackers exploit the transmission and stuff the network with the infected data packets to disrupt normal communications. This can be done by re-sending a data packet over a long period of time to saturate the system's buffer [47]. Furthermore, unauthorized data manipulation via spoofing of identities (e.g., manipulation of a node's digital identity by impersonating falsified data) can allow an attacker to successfully gain control over the data packets of the victim node [82].

In the latter case (i.e., the passive attack), the most common form of attack is *eavesdropping*, where an attacker takes unauthorized control over an IIoT node and silently listens to the real-time conversations between the users and captures the information transmitted. This allows the attackers the ability to capture and manipulate sensitive information in real-time through *traffic analysis* and *traffic monitoring* that intercepts and reads different communication patterns and other secret information (e.g., decipher the payload) between the victimized nodes [83].

3.5. Security Issue 3—Flooding Attack

In this type of attack, attackers send an extremely high volume of traffic that causes service unavailability to its users. The most common form of this type of attack is *DoS* and *DDoS* attacks [84]. In these attacks, attackers take control over the network and make the network traffic unavailable to the users connected to the network. These types of attacks are more vulnerable for IIoT systems because of the resource-limited nature of the IIoT devices (e.g., memory size, processing capability, or battery power). That is, these resource-constrained devices are running out of memory with unwanted information rather than holding a piece of actual information. In such cases, a compromised device can make an impact on the services of other interconnected devices for delivering dedicated performances [85].

In a similar way to the DoS and DDoS attacks, attackers can also flood the network by the *SYN flooding* attacks [86]. In this attack, attackers exploit the transmission and stuff the network by sending a succession of SYN requests over a long period to saturate a system's computational resource, making the system unresponsive to legitimate traffic. The SYN requests are the half-opened TCP connections that are generated by the victim's node. The fundamental of this attack is that when two nodes communicate with one another

over the Internet's TCP, they must establish three-way handshaking before a successful communication occurs. However, in such attacks, the attackers flood the network with the SYN requests, which does not allow the other nodes to complete handshaking to make a full open connection between them. One of such significant attacks in the smart healthcare sector is the "WannaCry" ransomware attack [32].

It is also possible that the attackers flood the victim's routing table to make the routing path unavailable to an authorized node within the system [87]. In such a case, the attacker node creates excessive numbers of route advertisements and channels them to the network to flood the routing table. Recall that, due to the high mobility of the IIoT systems, it is impractical to enforce a predefined routing path for them. In addition, this type of attack makes the device more vulnerable resulting in legitimate devices becoming unable to communicate with one another [88].

3.6. Security Issue 4—Attack on Physical Devices

As the majority of IIoT devices function in open and unrestricted settings, this poses high-security threats for those devices against physical attacks [89]. The most common damage could be device damage and disconnection, which may cause serious disruption over the network. For instance, an attacker physically disconnects a device (e.g., laptop, smartphone, air-conditioner machine) from the Internet.

Control over IIoT devices can be made in two ways when an attacker controls a single device and collectively controls several devices. In the first case, an attacker can insert a user's home network and disconnect a device from the Internet [90]. We argue that this kind of attack is not uncommon to IIoT systems. This can be applied to any networked computing system. However, the resource-limited characteristics of some devices make them further endangered where conventional security mechanisms cannot be embedded properly [61,91]. This will disrupt the system as data will be coming from various sources.

In the latter case, an attacker can control the functionality of many IIoT devices and manipulate services by disrupting the operation, e.g., block the service of the monitors in a traffic controlling unit to make unavailable the current traffic transport flows [92]. Furthermore, most of today's televisions (TVs) in the marketplace are embedded with a feature to surf the Internet in real-time, but in a TV, there are no firewall, antivirus protection, or monthly software update features. Thus, it is possible for an attacker to lock and jam the TV screen with unwanted advertisements for extortion of payment by money (e.g., bitcoins) to unlock the screen. Likewise, an attacker can lock the door of a refrigerator and turn down the cooling system, and demand payments to return the refrigerator to its normal operations. It is also possible that having compromised a smart physical device, an attacker can capture and control a remote car or the other IIoT devices that are connected to that device, e.g., taking control over an aircraft operating system [93].

In addition, attackers can malfunction devices through data exfiltration. In an IIoT system, data exfiltration can be done by an attacker when performing various malicious activities through different techniques. For instance, rotate the service of an electric heater in an unauthorized way, so that it cools during winter and heats during summer, and turn on the lights of a room when a person leaves the house [92,94].

3.7. Security Issue 5—Impact on Devices' Performance

In these types of attacks, one or more devices are compromised by the attackers. Then, a collection of malicious devices are controlled by the attackers to enact malevolent performances on the sensitive data without the user's knowledge. For example, in an IoT-enabled healthcare system, if an attacker gains access to a portable mobile device (e.g., Fitbit, or smartphone), it can then enter and hack the hospital's internal database management system through identity spoofing. Attackers can collect a patient's health record or even steal the identity of the patient [95].

It further helps attackers to perform replay attacks to the IIoT systems by transmitting copies of a stream of messages between the devices to make delays in a valid data

transmission [96]. Combined with device controlling and analysis of the devices' data, it becomes a possible threat towards the privacy in the IIoT systems.

An attacker can attack an IIoT device to degrade the memory space and battery capacity by memory exhaustion and battery corruption attacks [71]. In the former (i.e., memory space), the IIoT devices, in general, are restrained from extended processing capabilities due to less memory and processing power. Thus, attacking these resource-limited devices on a mass scale can be a potential threat to break down the entire system's operations that are connected to these devices. This attack can be made by state manipulating both the "memory performance" and "memory allocation", for instance, a heatstroke attack, in which an attacker repeatedly accesses a shared memory/resource and makes the space unavailable to other definite applications [97]. In the latter (i.e., battery capacity), a DoS/DDoS attack can drain a huge amount of power, and it would potentially affect the device to gain further service availability for computational processing and data transmission by keeping them in a busy state [98].

3.8. Security Issue 6—Device Impersonation

This is defined as the use of another person's identity, pretending to be someone else. Device impersonations in IIoT are becoming a critical issue because a particular service in IIoT is constructed by a collection of data sources that come from various devices, contexts, locations, and users [99]. In the case of a heterogeneous, dynamic IIoT system, each device has its own unique identity, but they may not be known to each other in advance. Therefore, securing identity management is crucial to protect fraud against device impersonation [89,100].

Identity in a system establishes the authorization of a device or another system that is allowed to access certain information [82]. Damage can be done by distorting a device's identity (using identity fabrication) and aggravating the reputation of a system. Further, this can be performed via identity spoofing, where malicious entities gain unlawful entry into IIoT regularities. This can lead to an attack that can block or manipulate a system's resources and disrupt the integrity of a database by data forgery. We note that design of an identity management mechanism would not only consider the device's identifiable information but also take into consideration the attributes and the context of the systems [101].

3.9. Security Issue 7—Privacy

The massive scale of IIoT and the dynamics in communications, make the system more vulnerable from the privacy point of view for protecting personally identifiable information (PII) [102]. The device's privacy protection (e.g., information related to a device's daily tasks, frequency of interactions with other devices, etc.) requires dynamic security protections to make IIoT systems more secure from potential threats and attacks.

An attacker may try to break a communication path and make a replay of interactions to perform transactions under a falsified identity. Further, the attacker can manipulate unauthorized logging data of a system and can generate trust-related attacks, e.g., self-promoting attack (a malicious node provides a positive reference for itself), bad-mounting attack (a malicious node provides a negative reference against an exemplary, i.e., good node), and good-mounting attack (where a malicious node giving good recommendations for themselves) [68].

Another dimension of privacy is important for IIoT systems, i.e., context-aware privacy mechanisms. This will help to implement security protection by taking into account the current environmental requirements (e.g., location, device, user, etc.) [69] and privacy-by-design principles [103]. Further, an attacker can disclose a user's privacy by taking explicit control over devices via device capturing and tracking and tag tracking (e.g., RFID tag tracking). One considerable issue is the theft of credentials (e.g., logging information and password) in such cases. This can be done by the device's identity spoofing, in which an attacker can enforce non-authorized IIoT device's control (e.g., medical equipment) by

violating the elevation of privileges and bringing a malicious action (e.g., changing the dose of an insulin pump) into an authorized session [104].

3.10. Security Issue 8—Data Confidentiality

Confidentiality ensures that the data are protected from unauthorized entities. In a centralized IIoT system, a user's confidential data are stored inside a traditional server,; however, in the case of a large-scale IIoT system, sensitive information can also be stored in distributed locations. Therefore, IIoT systems experence issues, e.g., protecting business's confidential information and individual confidential information [105,106]

One of the common ways to get a user's confidential and private information (e.g., username, password, bank details, etc.) unlawfully is a phishing attack. This can be done by sending emails, seemingly legitimate emails, that contain a malicious link (e.g., malware or spyware), and when a user clicks on the link, their sensitive information is transferred online to the attacker's device [107]. Another possible attack on data confidentially could be the MITM attack, which may be caused due to insufficient authentication and authorization mechanisms, lack of transport encryption schemes, and weak access control enforcement. It could be a potential threat of *disclosure* of users' sensitive data unlawfully by the attackers. Therefore, protecting the databases as well as taking security measures for local data (i.e., data located inside an IIoT device) is important in the context of data confidentiality in an IIoT system [69]. It is also imperative to design security protocols for resource limited IIoT devices that require a minimum of identifiable information of users and devices.

3.11. Security Issue 9—Heterogeneity of Networks

The improvement and demand on wireless and mobile communications enhance the various IoT applications by improving energy consumption of the devices, overall throughput, and communication techniques that apply directly or indirectly on the devices [108]. These communications include various networks (e.g., Wireless Sensor Networks (WSN), Wireless Mesh Network (WMN), SCADA, etc. Such highly dynamic network environments make an IIoT system more vulnerable, especially for the devices located at the edge networks [109]. One common security issue is the exposure of secret (private and sensitive) information via packet dropping attack [64]. A packet-dropping attack is one kind of DoS attack, where the compromised nodes drop packets to make the connection path unavailable between the source (i.e., sender) and destination (i.e., receiver) nodes.

3.12. Security Issue 10—Non-Trusted Network Connection

In an IIoT system, the majority of the devices often perform networking functions in an open (and maybe public) wireless networking environment [110]. The edge devices could be attacked by the de-synchronization attack in which an attacker can take control over communication between two devices and disconnect an established dialogue [111]. In this attack, an attacker de-synchronizes a tag's key (e.g., RFID tag) that is stored in the back-end server and the key that is located in the tag's memory. Therefore, in a future session establishment, it is impossible to get synchronized with the correct pair of keys required for authentication. In addition, in a non-trusted network connection environment, the IIoT systems can face DoS attacks where an attacked node would send more and more data packets to a trusted node to disintegrate the whole network [68,94].

3.13. Security Issue 11—Dynamic Infrastructure

One of the significant characteristics of IIoT is that the interaction between the objects is dynamic [112]. However, the nature of the communication does not rely directly upon human interventions. Therefore, these dynamics of the IIoT system must be considered when designing architecture. From an organization's point of view, with the rapid development of IIoT, companies try to put every end node to the Internet or their private networks or public and private cloud infrastructure. However, the nodes do not necessitate connecting across a public Internet infrastructure for communication. Still, they can connect via any

network (e.g., Wireless Local Area Network (WLAN), Personal Area Network (PAN), or Wireless Body Area Network (WBAN), which can be uniquely identified and are addressable [113]. This infrastructure is not only composed of a large number of networks, but it also contains billions of resource-limited IIoT devices, which further generates security challenges (e.g., threats and attacks on automatic cars, power grid systems, etc.) for the developers, designers, and business processes that come from a dynamic infrastructure. Therefore, this diversified infrastructure of networks and devices requires better security protections that could safely integrate a real-time IIoT state into the physical world [114]. This is significant in a dynamic network infrastructure like healthcare, where a patient's registration to a diagnosis is highly dependent on the communication infrastructure.

3.14. Security Issue 12—Anonymity

IIoT devices can transmit beacons that can be collected by a server and generate information of real-time activities, e.g., the device's physical locations, and different activities in a certain time frame performing locally or remotely [115]. Moreover, an IIoT device can communicate with another device with real-time notifications using Bluetooth low-power communication techniques to share a range of possible applications and information e.g., traffic information, retail, or shopping information (e.g., Google Physical Web [116]).

This location-based information is a popular choice for attackers. More specifically, "the idea is to build a map reflecting on the activities, mobility behavior, and other mobile patterns of an entity using the data gathered from other attacks" [117]. The location- and tracking-related attacks (sometimes referred to as *inference attacks*) are major concerns in such cases, where a device may wish to keep its information confidential from a group of other devices [118]. With such location-based information, an attacker can take control over a device through device tracking or tag tracking and can be vulnerable to the other devices that are connected to them and sharing real-time information [119].

Due to the massive scale of IIoT systems, dynamics in interactions, and resource-constrained (e.g., memory and battery) characteristics of the devices, as well as bandwidth-constraints, traditional TCP-based security mechanisms cannot be applied directly to them [47]. Therefore, it is a major challenge for securing access control by rejecting unauthorized data monitoring and unauthorized access [91].

Anonymity refers to the situation where an entity performs a task but remains anonymous to others [120]. The anonymity in the system must ensure that the attacker can never be able to discover the entity's personal information to breach privacy and pose further privacy-related attacks. For example, an attacker can guess the initiator's information (through tracked stream) in an anonymous connection and, on that basis, modify the communication path to another insecure destination [121]. To ensure a device's or user's anonymity, the system should employ a robust authentication scheme. However, in the case of IIoT, the devices themselves lack insufficient resources (e.g., memory and storage) to run heavy-weight security mechanisms. This further suggests the need for lightweight security mechanisms for the IIoT systems [78,122].

3.15. Security Issue 13—Cross-Domain Jurisdictions

Jurisdiction refers to a particular area (or territory) defined with a specific set of rules and regulations that are granted by some administrative authorities. In an IIoT context, it can be referred to as various networks of devices within one jurisdiction or spreading over multiple jurisdictions (cf. Figure 6). The data that reside in multiple jurisdictions, depending upon the various locations, may directly or indirectly be affected by various legal and law enforcement agencies [123]. For instance, in an industrial supply-chain network, communication is necessary over cross-domain jurisdictions from product manufacturing to delivery to the end users [124]. However, how to manage and coordinate such information among various service providers while preserving the device's privacy is a challenging task. This is due to the lack of dedicated interoperable communication protocols that autonomously trigger actions with or without physical human intervention [125,126].

3.16. Security Issue 14—Heterogeneous Infrastructure

Unlike the emergence of the Internet, which focuses solely on online services and applications, the IIoT integrates various infrastructures and services in a more scalable and usable paradigm to better serve the society beyond its connectivity. An IIoT system can include IoT, cloud computing [127], fog computing [128], mobile computing [129], and industrial networks [130]. This helps with the more widespread distribution of information not only for human users but also for the billions of pervasively interconnected smart devices.

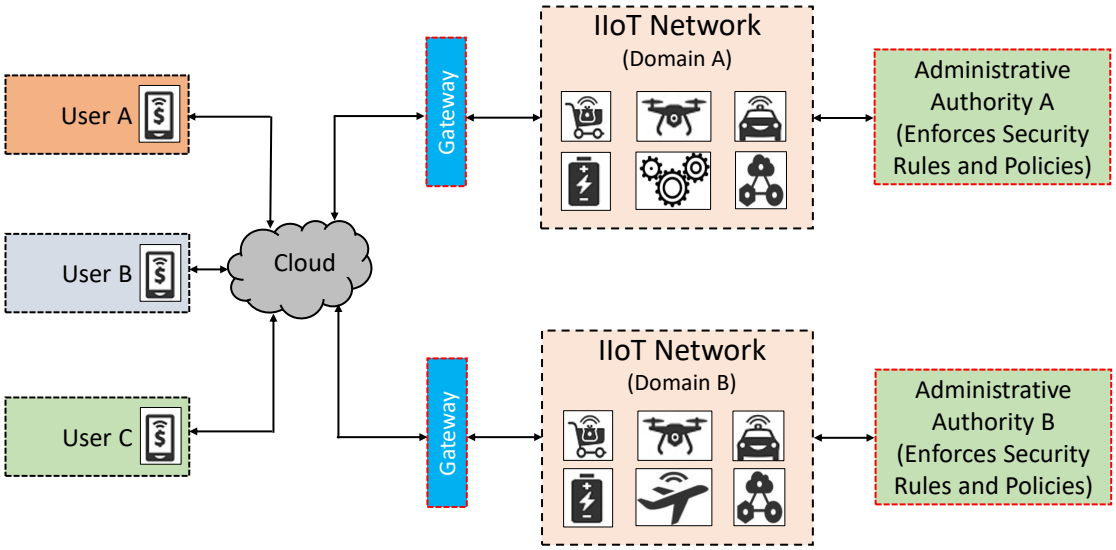

Figure 6. A view of cross-domain jurisdictions in an IIoT setting.

Notably, IoT device by themselves, in isolation, cannot compute, analyze, or store the massive amounts of data collected from the physical environment. This, in other ways, advances the dependency of the IoT over the infrastructures mentioned above. The integration of IoT and such infrastructures are challenging and introduce numerous security and privacy issues for them. For example, in a heterogeneous IoT-based healthcare system, a patient's health-related records are captured via a blipcare (a Wi-Fi blood pressure monitor) and transfer information to the cloud-based infrastructure in the hospital. Doctors can view the record using their smartphone, which uses a mobile cloud infrastructure. Further, a doctor can generate health alerts to the patient's family members, who are connected over a social network infrastructure with the doctor. Therefore, any of these stages of data collection, their transmissions, processing, analysis, storage, and sharing of medical information with others are vulnerable to attackers who can breach user's personal information by penetrating any of the communication networks between the infrastructures [131,132].

This heterogeneous infrastructure and service introduce trust-related attacks for users as well as for organizations by making possible the disclosure of a user's identity and unauthorized data access. We argue that, while global connectivity is important for IIoT, it is also significant to ensure security in local areas to minimize the overall impact of an attack [133].

3.17. Security Issue 15—Cascading Services

The cascading of service refers to the combination of two or more different services into a single service that allows access by several others in order to use those services [134]. This is significant for IIoT as it combines a massive number of cooperative services due to the rapid growth of Service-Oriented Computing (SOC). In such cascading services, IIoT devices represent the services, and the links between the devices represent the dependency among the services [135]. The potential security issue in IIoT is the failure of cascading

services and misuse of the services by malicious actors. The failure of cascading service is unique in IIoT than in other traditional services due to the pervasiveness in interactions of devices within the system. As a result, this is vulnerable since the cascading failure leads to the failure of other services that are interconnected [136].

3.18. Security Issue 16—Emergence of Resources

With the growing demand for IoT-based applications in industrial sectors and the rapid improvements of low-cost and low-powered IoT devices, from large companies to small investors there is a greater need to shift their specific market segments for a quicker adaptation with the emergence of this resources [137]. While the emergence of resources needs better data management, the major challenges for a widespread adoption of IoT are the lack of skilled and experienced professionals for collection, integration, and distribution of these resources [138].

Furthermore, the big volume of data (i.e., Big Data) in the IIoT makes it more challenging to secure management of the resources [139]. Moreover, the massive number of data attributes in big data (e.g., medical records in an organization) can potentially target attackers to manipulate sensitive information and perform unauthorized data access. This further breaches the trust relationships between various users that enhance the risk towards user's privacy with an *automated invasion attack* [117]. In such an attack, the attacker illegally collects a vast amount of information about a system and conducts automated data mining to gather the essential information. Importantly, the way to provide trustworthiness of resources in an IIoT system is an emerging research concern [133].

4. Security Countermeasures in IIoT systems

In this section, we discuss the potential security countermeasures of an IIoT system. For this purpose, in particular, we revisit the four-layer IIoT smart healthcare architecture discussed in Section 3.1. Next, we see how different layers of the IIoT architecture are affected by the various security issues we identified in the earlier section and then consider their potential countermeasures. They are as follows:

4.1. Perception Layer

This layer consists of a large number of sensors and actuators. These components can automatically sense (i.e., identify) things and collect parameters (i.e., information) from the physical environment. The scale in the number of devices in an IIoT system shows that these devices can be stationed at once or incrementally upon the context and practical requirements [63]. Some unique security requirements in this layer are related to devices' authentication (prove its identity), authorization (whether it is allowed to access a resource), and securing access control of these devices for authorized data acquisition.

Returning to our list of devised security issues, among others, we observe that security issues 4 (i.e., attack on physical devices), 5 (i.e., impact on devices' performance), 12 (i.e., anonymity), and 13 (i.e., cross-domain jurisdictions) are major concerns in this layer. To protect the devices from security issue 4, a more practical approach should be taken; e.g., the devices should be checked and monitored frequently and enhance the protection in the server storage. Moreover, the hardware of the device should be checked and evaluated frequently, particularly those that are unattended for a long time. Finally, we note that the SCADA system can play an important role in IIoT applications [140]. To protect a SCADA system, some physical security measures (standards) must be taken. For this purpose the employed hardware components should meet the NIST (National Institute of Standards and Technology) and FIPS (Federal Information Processing Standards) standards [141].

We observe that trustworthy data sensing systems can be enforced to address security issues 4 and 5. Service requests are granted in such a trustworthy system based on specific trust values calculated by a trust management system. However, trust management is highly dependent on how the trust is collected. Trust can be collected in two

ways, directly (i.e., direct interactions between the entities) and indirectly (i.e., based on recommendations) [142]. In Figure 7, we illustrated a simple trust management process.

For instance, an identity-based trust management model, e.g., [143], can be employed. This model follows a key-based trust agreement at the beginning of communication within a network domain. The novelty of this approach is that it can determine malicious objects coming from an outside network and is then able to update the other nodes within the network reading this malicious node information (with a specific trust value). Therefore, it can improve the authentication and authorization security of a network by reducing abnormal communications between the trusted and malicious nodes. It ensures protection for unauthorized control over the devices.

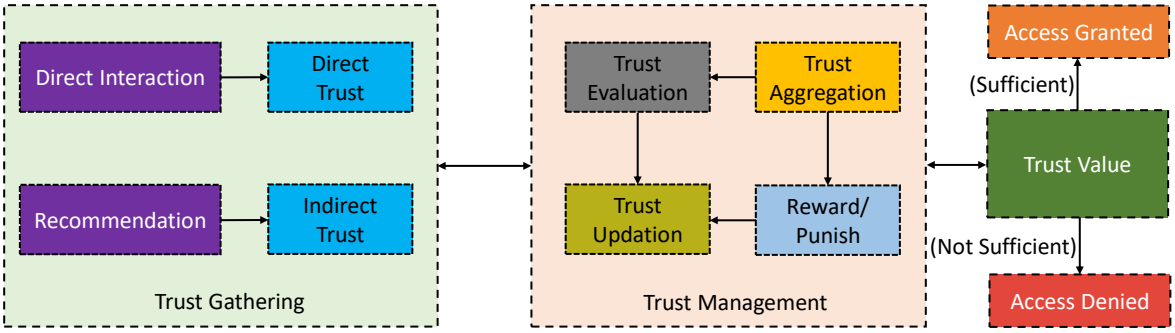

Figure 7. An outline of a simple trust management process.

To address security issue 12, a mobility-aware policy-based security technique can be employed [144]. This uses Quantum Lifecycle Management (QLM), a messaging standard that provides generic and standardized application-level interfaces for the IoT to achieve secure two-way communication in a privacy-preserving manner. Furthermore, this security technique enables real-time control over devices, and thus an entity can control a device's movements and restrict the device's information (e.g., location and activities) to others. In addition, IP-based security management protocols that are usable to a distributed system can be used for achieving end-to-end encryption and integrity protection between edge devices [145].

To address security issue 13, there is a need for seamless integration between various service providers and service users within the IIoT system. Importantly, this is to ensure that when a device is collecting data from other devices that reside in cross-domain jurisdictions, the legal issues (including policy enforcements) should be taken into consideration for acquiring resources and their distributions [146]. However, it is difficult for an IIoT system to seamlessly integrate the vast number of members of devices and their services. In such cases, privacy-preserving authentication and data control schemes can be employed that ensure the security and privacy requirements for cross-domain jurisdictions [147]. This scheme helps seamless integration of two underlying cryptographic primitives, called blind-signature and hash-chain, and delivers them into a single authentication and key establishment protocol that is flexible and lightweight in nature. The blind signature is defined as a digital signature that is used by another party to gain access to a message using the first party's signature without revealing any information. The usefulness of this scheme is that, on the one hand, the service provider can authenticate the authorized users using digital signatures, and on the other hand, the user can maintain their privacy without being tracked by the activities they performed.

4.2. Network Layer

This layer consists of various wired and wireless networks. The major functionality of this layer is to provide seamless communication to other layers. It is also accountable for transferring information from the perception layer to the support layer. The immense heterogeneous networks in this layer are WSNs, WLANs, 3G, 4G, Wi-Fi, Bluetooth, etc. [148].

Returning to our devised security issues, we find that the security issues 1 (i.e., controlling over communication), 2 (i.e., infecting data packets), 3 (i.e., flooding attacks), 9 (i.e., heterogeneity of networks), 10 (i.e., non-trusted network connections), and 11 (i.e., dynamic infrastructure) are major concerns in this layer. To address security issue 1, an attack-resistance trust-management-based routing protocol can be employed [149]. The proposed routing protocol can evaluate propagation reputation in a distributed system using a beta function (i.e., probability density function). This protocol is useful for the IIoT systems where a reliable trust relationship can easily be established among the self-organized nodes that are known to each other and interacted with previously.

Further, a context-aware, secure multi-hop routing protocol can also be employed to address the security issue 1 [150]. Nodes need to authenticate themselves before joining a network using multi-level security parameters (e.g., authentication, authorization, and trust) in this routing. The protocol is based on a user-controllable multi-layer (UML)-aware secure algorithm [151], which further enhances IIoT security issues by improving inter-connectivity using trust levels among the devices. It is also useful when applied in IIoT systems, as this protocol reduces significant overhead in the network. In this, users are located at the application layer. The UML layer provides appropriate network addressing by the routing agents. The address unit checks the users' pre-assigned applications and addresses to access a particular resource. The User-Controllable Entry (UCID) and Unique Code Generator (CG) are two modules that also help to verify the pre-assigned applications.

To address security issue 2, intrusion detection system (IDS)-based security architecture, e.g., [152], can be used. This architecture provides end-to-end security between two IoT nodes connected in a 6LoWPAN-based network. To address security issue 3, privacy-preserving data mining (PPDM) techniques can be used [153]. This technique integrates a random number generator in the IoT tag and readers and applies cryptographic one-way hash functions on them; thus, if an IoT node is attacked, it is infeasible to invert the number. This minimizes sensitive data disclosure by a compromised node and thus protects the resources' privacy.

A privacy preserved access control protocol [154] can be used to address security issue 9. This protocol helps entities to understand and locate who is collecting and accessing their data and which part of the data is being collected and accessed and at what time it is happening. Using this protocol, a user can separate and place their data in different privacy levels in an IIoT system. Then, according to the data privacy level, they give appropriate access control permission to other users. This helps to balance data authenticity and data integrity in the system. Moreover, the access control permission is performed based on the context-aware k-anonymity technology and role-based (e.g., authority and responsibility) access policies [155], in which access control systems can determine a user's access privileges based on their roles assigned to different privacy levels.

To address security issues 10 and 11, secure mobile handshake mechanisms e.g., [156,157], can be employed. The proposed mechanisms verify insecure mobile nodes over an insecure channel using attribute-based encryption matching handshaking scheme. In this, a node's attributes (e.g., IP-address, location, timestamp, etc.) are checked with handshaking factors (e.g., bilinear pairings) with fuzzy authentication and data fusion techniques before negotiation can happen in a communication. In the context of IIoT, this further helps to balance data confidentiality and service availability in a larger and complex service hierarchy.

4.3. Support Layer

The core functionality of this layer is analysis and processing of data received from the network layer. From the architectural analysis (cf. Section 2), we noted that the middleware technology is the base of the support layer. This layer is designed based on the usability of applications and the scale of the number of devices in an IIoT system that satisfies the common service requirements.

We argue that to design an effective security strategy in this layer, security issues 3 (i.e., flooding attacks), 5 (i.e., impacts on devices' performance), 6 (i.e., device impersonation), 8 (i.e., data confidentiality), 9 (i.e., heterogeneity of networks), and 15 (i.e., cascading services) are necessary address. To address security issue 3, in this layer, lightweight security and privacy-enhanced middleware infrastructure can be employed [158]. The infrastructure uses lightweight symmetric encryption for data and asymmetric encryption for key exchange in Trivial File Transfer Protocol (TFTP). The infrastructure ensures security, privacy, and trust in service compositions by employing a secure TFTP protocol. In an IIoT system, because of its high number of devices and their distributed nature in data processing, sometimes protecting users' confidentiality is more computationally intensive than traditional server-based data processing and computation systems. Towards this, to address security issue 5, a secure and dynamic trust management system can be used [159]. This system helps when building trust-based service composition applications in IIoT systems based on a dynamic trust management protocol, which allows detecting misbehaving nodes that change their behavior more often. This is useful in IIoT systems where a centralized trust management authority may not be present. Furthermore, the system is capable of adaptively adjusting the trust parameters (following the autonomous and independent interactions with objects) in response to dynamically changing systems to maximize application performance, thus, in turn, helping to address data confidentiality from non-trusted entities.

To address security issue 6, attribute-based signature schemes that support user's privacy can be employed [160]. In this scheme, a service requester is required to generate a signature with attributes (i.e., attribute-based encryption and attribute-based signature) that satisfies certain policies before accessing any information. Therefore, a user is not able to forge or tamper information, nor consume resources using a false signature and attributes that they do not possess. To address security issue 8, policy-based access control mechanisms e.g., [161] can be enforced. The proposed mechanism is based on a role-based access control model. The use of role-based access control has improved service composition and service division by using roles to manage the relationship between subjects and policies. It is beneficial within an organizational context that controls resources locally.

To address security issue 9, security countermeasures i.e., [154], can be employed. To address security issue 15, strong access control mechanisms can be applied. For this, a hierarchical access control model, e.g., [162], can be exercised. This model proposes an access control technique for resource-limited devices with short processing power and storage capacity. Moreover, the model uses key-based authentication systems to protect the communications of hierarchical data access. The novelty of the proposed model is that the authentication is done using a single key and allows it limited distribution among entities, which further strengthens the resource security and reduces storage costs.

4.4. Application Layer

This layer provides structure, behavior, and interaction of the applications to the end-users. The different functional components of this layer are commerce applications, e.g., smart healthcare, smart grid, and smart logistics. That said, this layer represents the various utilizations to regulate and monitor the connected devices. However, the application layer is likely to target the attackers as this layer provides typical e-commerce services. Furthermore, the application layer strongly depends on various applications, and therefore, security issues in those applications are a major concern.

Returning to our devised security issues, the security issues 7 (i.e., privacy disclosure), 9 (i.e., heterogeneity of networks), 12 (i.e., anonymity), 14 (i.e., heterogeneous infrastructure), 15 (i.e., cascading services), and 16 (i.e., the emergence of resources) are significant concerns in this layer. To address security issue 7, a privacy-preserving data mining technique can be employed [163]. This technique helps to minimize sensitive data disclosure and protects sensitive content analysis from attackers in a distributed system, using sensitivity detection, analysis, and a privacy content quantification detection scheme. To address

security issue 9, a two-way authentication security scheme can be used [164]. This scheme absorbs the existing Internet standards, specifically the Datagram Transport Layer Security (DTLS) protocol. This scheme further uses a public key cryptography system (e.g., RSA) for securing communications over standard communication stacks that offer UDP/IPv6 networking for 6LoWPANs.

To address security issue 12, an identity-based encryption scheme, e.g., [165], can be used. The usefulness of this scheme is that it uses a secure generic model that helps anonymous communications between the various edge IIoT nodes and WSN. Moreover, this scheme protects the sender's and receiver's anonymities from the malicious actors (e.g., hackers) trying to steal a real identity. Further, to address security issue 14, a distributed capability-based access control (DCapBAC) framework that is used for IoT devices can be employed [166], where the edged IoT devices are capable of being authorized themselves without any centralized control systems. That is, the authorization is performed at the edge devices in real-time, improving the disadvantages of a highly centralized system. A capability can be defined as a communicable token. This token is associated with an object and the corresponding access rights (along with the specified conditions of access). Such a framework also considers context-aware access control based on local conditions, which is highly applicable to IIoT scenarios. This approach, in general, uses public-key cryptography while managing the scalability and interoperability among devices with a strong security foundation. Furthermore, in [166], a highly optimized version of the Elliptic Curve Digital Signature Algorithm (ECDSA) has been implemented inside the end devices (i.e., the edge devices), which ensure end-to-end authentication, integrity, and non-repudiation. In Figure 8, we provide an outline of the process.

To address security issue 15, a capability-based delegation model for the federated networks can be employed [167]. This model supports a delegation process that supports a context-aware access control mechanism. The intention of this model reclines in the principle of identity-based access control supported by capability, where capability becomes the pivotal point on access control mechanisms. It also uses an identifier that is used to improve the scalability and control the capability propagation through access control delegation.

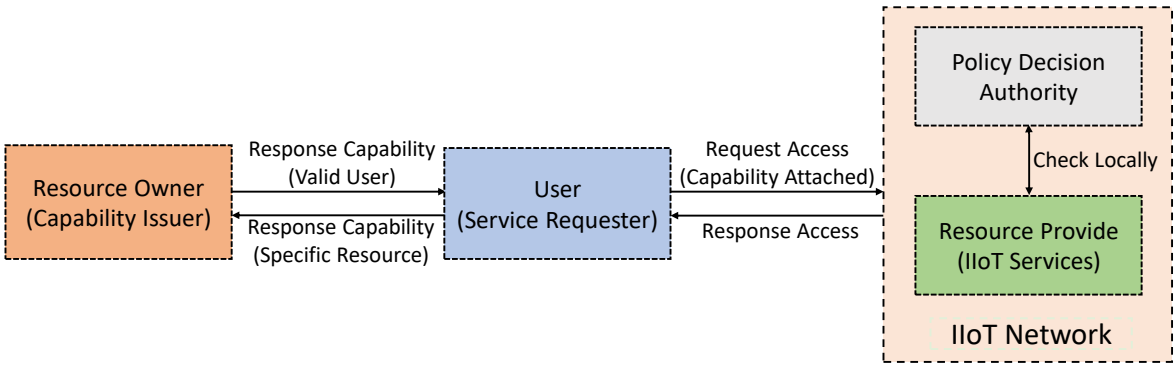

Figure 8. A simple outline of a DCapBAC process discussed in [166].

To address security issue 16, a cryptography-based security mechanism can be used [168]. The proposed security mechanism is based on the public key infrastructure (PKI) that includes a set of roles, policies, and procedures to create, manage, and distribute resources in a large-scale IIoT system. The usefulness of the PKI in IIoT is that it can manage a large number of certificates for securing network-connected devices all along, further enhancing and expanding its use for the millions of interconnected IIoT devices.

5. Discussion and Future Research Direction

IoT devices are an integral part of an IIoT system. However, IIoT is designed for heavy-duty tasks, for instance, manufacturing, monitoring, and maintenance in an industrial

setting. IIoT devices can be seen as more durable and resistant to specific criteria, e.g., heat, cold, etc. However, this is to note that the IoT and IIoT share the basic principles of data management, network communication, security, infrastructure, etc. That said, the primary difference between IoT and IIoT is the scale of data and their management issues [13]. We observe that security is a significant concern for the deployment of IIoT systems at scale. The present IIoT architectures lack the ability to address all of the security issues that we devised in this paper. That said, these architectures are not able to deploy a generic and scalable solution that can address all of these possible threats and attacks in a consistent and comprehensible way. This further reinforces the employment of system-specific security solutions based on the context and requirements. This can intuitively structure and manage those requirements (service and applications) of both the service providers and service consumers [169].

In Table 1, we summarize various security issues along with their potential countermeasures in different layers in an IIoT architecture. Note that it is also possible to have the same security issues in two or multiple layers of an IIoT architecture. However, their context and requirements may be different. One of the major research questions that have arisen is: which is the base layer of the security in this architecture? We observe that each layer has its distinct characteristics to address various threats and attacks. For instance, in the network layer, network firewalls and protocols can manage high-level traffic controlling through the Internet, but the challenge is how to protect the resource-constrained embedded IoT device's deeply embedded endpoint from possible threats and attacks in the perception layer? Some of the existing security solutions attempt to improve security in each device by embedding them into IoT objects. However, this requires changing the existing communication mechanisms and protocols. Further, these embedded solutions aim at enhancing encryption, authentication, and key management. This does not seem feasible to deploy on a large scale because this requires additional costs compared to the cost of IIoT systems and resource-intensive overheads in terms of computational processing and power consumption. There could also be a redesign of the physical structure, but this may not be a feasible option for some IIoT systems due to their high-security issues.

Our study presents a comprehensive discussion on the potential threats and attacks in an IIoT system that widely covers attributes, including devices, users, services, resources, and applications. In addition, an IIoT system typically needs to be monitored in real-time from virtually anywhere. It is fundamental for monitor manufacturing processes, including discrete and process manufacturing. This aspect also needs to be considered for better decision-making [170]. Our study covers threats and attacks on communications between various devices and users in an IIoT system. The communications in IIoT occur via wired or wireless mediums, and this communication channel is a potential target point for an attacker to enter into the system. For instance, an attacker can absorb network traffic and redirect the routing path to an insecure destination. We also argue that the attackers can further attack a communication without redirecting the whole data packet; instead, the attackers can infect selected data packets for specific information. Finally, an attacker can flood the network with unnecessary data packets to collapse the bandwidth or resources of an attacked system, which will consequently impact the performance of the complete system [171].

Our study also includes the possible vulnerabilities in smart IIoT devices and associated services. With the limited battery and memory capacity of the IIoT devices, many IIoT devices have restricted abilities to patch and update their software, making them vulnerable to attacks (e.g., DDoS attacks). Looking towards these issues, we explore various threats and attacks from devices' data access points. It helps to understand the attack scenarios and possible issues for the need to protect information flows, which are essential to consider in areas such as Industry 4.0 [172].

Despite the device's autonomy, humans are an integral part of the IIoT ecosystems. Given that humans (i.e., a user in general) are a valuable foundation in IIoT e-commerce, attention is therefore required to protect the issues related to their security. We identified the

issues, e.g., privacy disclosure and user impersonation, in this area. In the future, potential research can be conducted with the help of advances in Artificial Technologies (AI) [173] and digital twins [174] to address such issues. The advantages of both emerging technologies (i.e., AI and digital twins) in the IIoT are promising, but at the same time, they bring various security concerns related to identity issues. Furthermore, low-powered wireless communication technologies are critical for building various IIoT smart applications that need further investigation. In such cases, this could pose potential threats to the system and require dynamic identification, authentication, and privacy-protection mechanisms that we identified in our paper [85].

Table 1. Identified security issues and their potential countermeasures in different layers of an IIoT architecture.

IIoT Architectural Layer	Security Issues	Potential Countermeasures
Perception	Attack on Physical Devices	The devices' hardware must be checked and evaluated frequently [140]. In addition, the hardware components should meet the standard (e.g., NIST, FIPS, etc.).
	Impact on Devices' Performance	Employment of identity0based trust management model for trusted data sharing is beneficial [143].
	Anonymity	Mobility-aware policy-based security techniques, e.g., Quantum Lifecycle Management (QLM), can be employed [144], and IP-based security management protocols that are usable to a distributed system can be used for achieving end-to-end encryption [145].
	Cross-Domain Jurisdictions	Privacy-preserving authentication and data control schemes can be employed for cross-domain jurisdictions [147].
Network	Controlling Over Communication	An attack-resistance trust-management-based routing protocol can be employed for a reliable trust relationship [149], and a context-aware, secure multi-hop routing protocol can also be employed [150].
	Infecting Data Packets	Intrusion detection system (IDS)-based security architecture can be used [152].
	Flooding Attacks	Privacy-preserving data mining (PPDM) techniques can be placed [153].
	Heterogeneity of Networks	A privacy preserved access control protocol can be employed [154].
	Non-Trusted Network Connections	A secure mobile handshake mechanism that verifies insecure mobile nodes over an insecure channel using attribute-based encryption matching handshaking scheme can be used [156].
	Dynamic Infrastructure	A lightweight and end-to-end security mechanism with less overheads, e.g., [157], can be used.
Support	Flooding Attacks	A light weight security and privacy enhanced middleware infrastructure can be employed [158].
	Impact on Devices' Performance	A secure and dynamic trust-management system based on a dynamic trust management protocol can be used [159].
	Device Impersonation	An attribute-based signature scheme that supports user's privacy can be employed [160].
	Data Confidentiality	Policy-based access control mechanisms e.g., [161], can be enforced.
	Heterogeneity of Networks	A privacy-preserving access control protocol can be employed [154].
	Cascading Services	A hierarchical access control model, e.g., [162], can be exercised for resource-limited devices.

Table 1. *Cont.*

IIoT Architectural Layer	Security Issues	Potential Countermeasures
Application	Privacy	A privacy-preserving data mining technique that helps to minimize sensitive data disclosure can be employed [163].
	Heterogeneity of Networks	A two-way authentication scheme can be used that absorbs the existing Internet standards, specifically the Datagram Transport Layer Security (DTLS) protocol [164].
	Anonymity	An identity-based encryption scheme, e.g., [165] can be used that helps to detect anonymous communications.
	Heterogeneous Infrastructure	A distributed capability-based access control (DCapBAC) framework for IIoT devices can be employed [166].
	Cascading Services	A capability-based delegation model for the federated networks can be employed [167].
	Emergence of Resources	Cryptography-based security mechanism, for instance, that involves public key infrastructure (PKI), can be used [168].

The IIoT is an integration of different technologies at scale, and therefore it is significant to capture various aspects from data processing to storage within the infrastructures. However, making a seamless integration between the various services coming from many devices and infrastructures is a challenging task [175]. Moreover, these control processes, monitoring, and management services create several security issues of privacy, identity, and trust. Our study identified potential security concerns related to the heterogeneous infrastructure, anonymity, or even cascading services.

To gain more fine-grained control over security and trust management, recent trends in security mechanisms are employing blockchain-based security solutions for IIoT systems [176–179]. Blockchain originated as a tool for developing crypto-currency (a new form of virtual currency) [180]. Blockchain is used for transactions to be verified with a group of actors that are not trusted. It provides a distributed and auditable ledger that holds the various blocks of previous transactions where the records within a blockchain are compounded by mathematical algorithms (called consensus), and whose data are shared between the various peers within the network [181]. In other words, blockchain can be seen as a distributed database where the information is verified with the previous data. That said, in a blockchain network, the previously stored information cannot be erased. Fundamentally, every node in the network has the same ledger, which ensures a complete consensus from all nodes for the transactions in the blockchain. Blockchain can enrich the IIoT systems by providing a platform for sharing information in a trustless environment, where information is reliable and translations are traceable, which provides the ability to identify sources at any time. That said, the use of blockchain can track, coordinate, and perform transactions for a large number of devices without the need for a centralized (trusted) authority, which complements the IIoT in various ways including reliability, security, and scalability [182]. Zero Trust is another strategic initiative that has the potential to secure an organization's network architecture (including expensive data, assets, applications, and services) without replying to a dedicated trust architecture. In other words, the zero-trust strategy provides restricted access control only to the authorized users and does not trust anyone by default [183,184]. Furthermore, blockchain supports fully distributed access control with a high degree of trust, integrity, and resiliency that are immensely important for securing an IIoT system [185,186].

Machine Learning (ML) is another avenue with enormous potential to secure IIoT infrastructure from threats and attacks [187,188]. ML uses past behaviors and helps identify

future patterns (i.e., analyze the patterns and learn from them and generate efficient models with changing parameters) that eventually help detect attacks. Importantly, ML can detect the type of attacks, including both known and unknown attacks. Some aspects of IIoT security that can be improved using ML are securing 5G-driven IIoT applications [189], malware defense [190], and false data injection attack detection [191]. However, there are several challenges in this area that need to be addressed in the future. We list a few of them as follows:

- Training datasets for ML-based solutions: generating training datasets with sufficient numbers of possible attacks and benign traffic is challenging for ML algorithms in IIoT security. In addition, high-quality training data are required for ML methods, as the noisy nature of IIoT data can affect the performance of ML-based intrusion detection. Deep Learning (DL) methods can be used for large-scale, heterogeneous, and noisy datasets in IIoT networks [192].
- Exploiting ML and DL algorithms: studies have shown that more severe attacks are possible using these methods. For instance, convolutional neural networks (CNN) have been used to break many cryptographic algorithms. These security issues must be taken into account in the design of IIoT networks.
- Privacy concerns: ML and DL algorithms may cause potential leakage of private data. For example, DL classifications can be broken easily, and it potentially causes privacy breaches. In addition, there are some adversarial attacks possible against the DL process, which exploit the detection methods used in the DL. Therefore, more research in this space is essential.
- Implementation of ML/DL at the edge: this is another challenging area that needs further research. In edge computing, these methods (i.e., ML and DL) can help minimize cloud dependency and delay processing. Further research in this area is required.

6. Conclusions

By bringing the existing technologies and applications (e.g., IoT, Industry 4.0, CPSs, control systems, etc.) together in a novel way, IIoT has the potential to re-shape the future industrial platforms. IIoT aims to provide higher efficiency and productivity with better asset management and monitoring product information between the industry and end-users with real-time tracking (accumulation, analysis, and exchange of application and service processes). However, IIoT must provide transparency to the data and assure appropriate security, privacy, and trust for service providers and consumers. Information sharing is another crucial aspect of an IIoT system to show how data are used and can be shared with other organizations. However, security is concern that increases for secure IIoT systems at scale. There are many proposals that discuss various threats and attacks of an IIoT system from security, privacy, and trust points of view. However, they lack significant attention to users, applications, services, and resources that are integral to an IIoT system.

This paper has reviewed the recent state-of-the-art security issues in IIoT systems and examined the implications of these various security issues in an IIoT architecture. To establish a secured automatic operation, we identify a set of security issues of an IIoT system. In addition, we have noticed that the prevailing IIoT security architectures cannot comprehensively address multiple threats and attacks at scale in a structured way. This increases the need to redesign and rethink the threat and attack taxonomy for the IIoT systems. To address this limitation, we consider a set of IIoT architectures available at present. We also noted that there is a need for security requirements that can fit well from small-scale companies to large-scale industrial sectors, which may consist of multiple jurisdictions. Future research in IIoT security must deal with various attributes, including system integration, energy efficiency, and communication. System integration is important to address the combination of edge IIoT devices to cloud-based services. Energy efficiency must focus on investigating lightweight and energy-efficient (i.e., uses minimal energy) mechanisms that can operate within the constrained devices. Finally, communication must

take appropriate security measures (e.g., lightweight encryption mechanisms) that can handle the security issues in cross-domain networks during data exchange. In the future, we also aim to study further different threat and attack models to assess the security issues and their impact in real-world scenarios for IIoT that we devised in this paper.

Author Contributions: S.P. and Z.J. planned the paper, structured the article, and contributed to the core research problem formulation. All authors reviewed the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors acknowledge the support of the Commonwealth of Australia and Cybersecurity Research Centre Limited.

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

References

1. Aleksic, S. A survey on optical technologies for IoT, smart industry, and smart infrastructures. *J. Sens. Actuator Netw.* **2019**, *8*, 47. [CrossRef]
2. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
3. Okano, M.T. IOT and industry 4.0: the industrial new revolution. *Int. Conf. Manag. Inf. Syst.* **2017**, *25*, 26.
4. Industrial IoT Market by Device & Technology. Available online: https://www.marketsandmarkets.com/Market-Reports/industrial-internet-of-things-market-129733727.html (accessed on 5 July 2021).
5. 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]
6. Iwanicki, K. A distributed systems perspective on industrial IoT. In Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2–6 July 2018; pp. 1164–1170.
7. Lu, Y. Cyber physical system (CPS)-based industry 4.0: A survey. *J. Ind. Integr. Manag.* **2017**, *2*, 1750014. [CrossRef]
8. Foukalas, F.; Pop, P.; Theoleyre, F.; Boano, C.A.; Buratti, C. Dependable wireless industrial iot networks: Recent advances and open challenges. In Proceedings of the 2019 IEEE European Test Symposium (ETS), Baden, Germany, 27–31 May 2019; pp. 1–10.
9. Raposo, D.; Rodrigues, A.; Sinche, S.; Sá Silva, J.; Boavida, F. Industrial IoT monitoring: Technologies and architecture proposal. *Sensors* **2018**, *18*, 3568. [CrossRef] [PubMed]
10. Satyanarayanan, M. Pervasive computing: Vision and challenges. *IEEE Pers. Commun.* **2001**, *8*, 10–17. [CrossRef]
11. Abowd, G.D.; Mynatt, E.D. Charting Past, Present, and Future Research in Ubiquitous Computing. *ACM Trans. Comput. Hum. Interact.* **2000**, *7*, 29–58. [CrossRef]
12. 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]
13. Sari, A.; Lekidis, A.; Butun, I. Industrial networks and IIoT: Now and future trends. In *Industrial IoT*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 3–55.
14. Jaidka, H.; Sharma, N.; Singh, R. Evolution of iot to iiot: Applications & challenges. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC), Delhi, India, 18 May 2020.
15. Pal, S.; Hitchens, M.; Varadharajan, V.; Rabehaja, T. Policy-based access control for constrained healthcare resources. In Proceedings of the 2018 IEEE 19th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Chania, Greece, 12–15 June 2018; pp. 588–599.
16. Pal, S.; Hitchens, M.; Varadharajan, V. Towards a secure access control architecture for the Internet of Things. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks (LCN), Singapore, 9–12 October 2017; pp. 219–222.
17. Pal, S. Limitations and Approaches in Access Control and Identity Management for Constrained IoT Resources. In Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 11–15 March 2019; pp. 431–432.
18. IIoT—The Industrial Internet of Things (IIoT) Explained. Available online: https://www.i-scoop.eu/ (accessed on 30 June 2021).
19. Bansal, M.; Goyal, A.; Choudhary, A. Industrial Internet of Things (IIoT): A Vivid Perspective. In *Inventive Systems and Control*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 939–949.
20. Rabehaja, T.; Pal, S.; Hitchens, M. Design and implementation of a secure and flexible access-right delegation for resource constrained environments. *Future Gener. Comput. Syst.* **2019**, *99*, 593–608. [CrossRef]

21. Luchian, R.A.; Stamatescu, G.; Stamatescu, I.; Fagarasan, I.; Popescu, D. IIoT Decentralized System Monitoring for Smart Industry Applications. In Proceedings of the 2021 29th Mediterranean Conference on Control and Automation (MED), Puglia, Italy, 22–25 June 2021; pp. 1161–1166.
22. Sadeghi, A.R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
23. Tsiknas, K.; Taketzis, D.; Demertzis, K.; Skianis, C. Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT* **2021**, *2*, 9. [CrossRef]
24. Ginter, A. *The Top 20 Cyberattacks on Industrial Control Systems*; Waterfall Security Solutions: 2017. Available online: https://waterfall-security.com/20-attacks (accessed on 30 August 2021).
25. Ly, K.; Jin, Y. Security challenges in CPS and IoT: From end-node to the system. In Proceedings of the 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh, PA, USA, 11–13 July 2016; pp. 63–68.
26. Attri, T.; Bhushan, B. Enabling Technologies, Attacks, and Machine Learning-Based Countermeasures for IoT and IIoT. In *Integration of WSNs into Internet of Things*; CRC Press: Boca Raton, FL, USA, 2021; pp. 249–272.
27. Pal, S. Wind energy—An innovative solution to global warming? In Proceedings of the 2009 1st International Conference on the Developements in Renewable Energy Technology (ICDRET), Dhaka, Bangladesh, 17–19 December 2009; pp. 1–3.
28. Ghadge, A.; Kara, M.E.; Moradlou, H.; Goswami, M. The impact of Industry 4.0 implementation on supply chains. *J. Manuf. Technol. Manag.* **2020**, *31*, 669–686. [CrossRef]
29. Müller, J.M.; Veile, J.W.; Voigt, K.I. Prerequisites and incentives for digital information sharing in Industry 4.0—An international comparison across data types. *Comput. Ind. Eng.* **2020**, *148*, 106733. [CrossRef]
30. Bombardier Statement on Cybersecurity Breach. Available online: https://bombardier.com/en/media/news/bombardier-statement-cybersecurity-breach (accessed on 3 July 2021).
31. School Cyber-Attack Affects 40,000 Pupils' Email. Available online: https://www.bbc.com/news/technology-56569873 (accessed on 3 July 2021).
32. Dwyer, A. The NHS cyber-attack: A look at the complex environmental conditions of WannaCry. *RAD Mag.* **2018**, *44*, 25–26.
33. Khujamatov, H.; Reypnazarov, E.; Khasanov, D.; Akhmedov, N. IoT, IIoT, and Cyber-Physical Systems Integration. In *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 31–50.
34. 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.
35. 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, Montreal, QC, Canada, 15–18 April 2019; pp. 56–63.
36. Valentin, V.; Mehaoua, A.; Guenane, F.A. *Security Challenges and Requirements for Industrial IoT Systems*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2020; pp. 117–136.
37. Panchal, A.C.; Khadse, V.M.; Mahalle, P.N. Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures. In Proceedings of the 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 23–24 November 2018; pp. 124–130.
38. Xu, H.; Yu, W.; Griffith, D.; Golmie, N. A survey on industrial Internet of Things: A cyber-physical systems perspective. *IEEE Access* **2018**, *6*, 78238–78259. [CrossRef]
39. 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]
40. 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]
41. Saifullah, A.; Xu, Y.; Lu, C.; Chen, Y. Real-time scheduling for WirelessHART networks. In Proceedings of the 2010 31st IEEE Real-Time Systems Symposium, San Diego, CA, USA, 30 November–3 December 2010; pp. 150–159.
42. Dirgantoro, K.P.; Nwadiugwu, W.P.; Lee, J.M.; Kim, D.S. Dual fieldbus industrial IoT networks using edge server architecture. *Manuf. Lett.* **2020**, *24*, 108–112. [CrossRef]
43. Devan, P.; Hussin, F.A.; Ibrahim, R.; Bingi, K.; Khanday, F.A. A Survey on the Application of WirelessHART for Industrial Process Monitoring and Control. *Sensors* **2021**, *21*, 4951. [CrossRef]
44. Pal, S.; Hitchens, M.; Varadharajan, V. Access control for Internet of Things—Enabled assistive technologies: An architecture, challenges and requirements. In *Assistive Technology for the Elderly*; Suryadevara, N.K., Mukhopadhyay, S.C., Eds.; Academic Press: Cambridge, MA, USA, 2020; pp. 1–43. [CrossRef]
45. Li, S.; Tryfonas, T.; Li, H. The Internet of Things: A security point of view. *Internet Res.* **2016**, *26*, 337–359. [CrossRef]
46. Ray, P. A Survey on Internet of Things Architectures—ScienceDirect. *J. King Saud Univ. Comput. Inf. Sci.* **2018**, *30*, 291–319.
47. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
48. Sethi, P.; Sarangi, S.R. Internet of things: Architectures, protocols, and applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 9324035. [CrossRef]
49. Al-Qaseemi, S.A.; Almulhim, H.A.; Almulhim, M.F.; Chaudhry, S.R. IoT architecture challenges and issues: Lack of standardization. In Proceedings of the 2016 Future Technologies Conference (FTC), San Francisco, CA, USA, 6–7 December 2016; pp. 731–738. [CrossRef]

50. Yun, M.; Yuxin, B. Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. In Proceedings of the 2010 International Conference on Advances in Energy Engineering, Beijing, China, 19–20 June 2010; pp. 69–72.
51. Silva, B.N.; Khan, M.; Han, K. Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. *IETE Tech. Rev.* **2018**, *35*, 205–220. [CrossRef]
52. Yang, Z.; Yue, Y.; Yang, Y.; Peng, Y.; Wang, X.; Liu, W. Study and application on the architecture and key technologies for IOT. In Proceedings of the 2011 International Conference on Multimedia Technology, Hangzhou, China, 26–28 July 2011; pp. 747–751. [CrossRef]
53. CISCO: The Internet of Things Reference Model. Available online: http://cdn.iotwf.com/ (accessed on 4 October 2018).
54. Sengupta, J.; Ruj, S.; Bit, S.D. A secure fog-based architecture for industrial Internet of Things and industry 4.0. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2316–2324. [CrossRef]
55. Pham, Q.V.; Dev, K.; Maddikunta, P.K.R.; Gadekallu, T.R.; Huynh-The, T. Fusion of federated learning and industrial internet of things: A survey. *arXiv* **2021**, arXiv:2101.00798.
56. Radanliev, P.; De Roure, D.; Nicolescu, R.; Huth, M. *A Reference Architecture for Integrating the Industrial Internet of Things in the Industry 4.0*; University of Oxford: Oxford, UK, 2019.
57. Varga, P.; Peto, J.; Franko, A.; Balla, D.; Haja, D.; Janky, F.; Soos, G.; Ficzere, D.; Maliosz, M.; Toka, L. 5G support for Industrial IoT Applications—Challenges, Solutions, and Research gaps. *Sensors* **2020**, *20*, 828. [CrossRef]
58. 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]
59. Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243.
60. Kumar, A.; Krishnamurthi, R.; Nayyar, A.; Sharma, K.; Grover, V.; Hossain, E. A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. *IEEE Access* **2020**, *8*, 118433–118471. [CrossRef]
61. Pal, S.; Hitchens, M.; Rabehaja, T.; Mukhopadhyay, S. Security requirements for the internet of things: A systematic approach. *Sensors* **2020**, *20*, 5897. [CrossRef] [PubMed]
62. Gluhak, A.; Krco, S.; Nati, M.; Pfisterer, D.; Mitton, N.; Razafindralambo, T. A survey on facilities for experimental internet of things research. *IEEE Commun. Mag.* **2011**, *49*, 58–67. [CrossRef]
63. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context Aware Computing for The Internet of Things: A Survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 414–454. [CrossRef]
64. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
65. Madakam, S.; Date, H. Security Mechanisms for Connectivity of Smart Devices in the Internet of Things. In *Connectivity Frameworks for Smart Devices*; Mahmood, Z., Ed.; Computer Communications and Networks; Springer International Publishing: Berlin/Heidelberg, Germany, 2016; pp. 23–41. [CrossRef]
66. Premalatha, J.; Rajasekar, V. Industrial Internet of Things Safety and Security. In *Internet of Things*; CRC Press: Boca Raton, FL, USA, 2020; pp. 135–152.
67. Ghosh, S.; Gourisaria, M.K.; Routaray, S.S.; Pandey, M. IIoT: A Survey and Review of Theoretical Concepts. In *Interoperability in IoT for Smart Systems*; CRC Press: Boca Raton, FL, USA, 2020; pp. 223–236.
68. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
69. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]
70. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge Computing: Vision and Challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646. [CrossRef]
71. Abomhara, M.; Køien, G.M. Security and privacy in the Internet of Things: Current status and open issues. In Proceedings of the International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, 11–14 May 2014; pp. 1–8. [CrossRef]
72. Ahmed, M.; Jaidka, S.; Sarkar, N.I. Security in Decentralised Computing, IoT and Industrial IoT. In *Industrial IoT*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 191–211.
73. Airehrour, D.; Gutierrez, J.; Ray, S.K. Secure routing for internet of things: A survey. *J. Netw. Comput. Appl.* **2016**, *66*, 198–213. [CrossRef]
74. Wang, Y.; Wen, Q. A privacy enhanced DNS scheme for the Internet of Things. In Proceedings of the IET International Conference on Communication Technology and Application (ICCTA), Beijing, China, 14–16 October 2011; IET: London, UK, 2011; pp. 699–702. [CrossRef]
75. Pongle, P.; Chavan, G. A survey: Attacks on RPL and 6LoWPAN in IoT. In Proceedings of the International Conference on Pervasive Computing (ICPC), Pune, India, 8–10 January 2015; pp. 1–6. [CrossRef]
76. Kannhavong, B.; Nakayama, H.; Nemoto, Y.; Kato, N.; Jamalipour, A. A survey of routing attacks in mobile ad hoc networks. *IEEE Wirel. Commun.* **2007**, *14*, 85–91. [CrossRef]
77. Ghafir, I.; Prenosil, V.; Alhejailan, A.; Hammoudeh, M. Social Engineering Attack Strategies and Defence Approaches. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 145–149. [CrossRef]

78. Pal, S.; Hitchens, M.; Varadharajan, V.; Rabehaja, T. Policy-based access control for constrained healthcare resources in the context of the Internet of Things. *J. Netw. Comput. Appl.* **2019**, *139*, 57–74. [CrossRef]
79. Mosteiro-Sanchez, A.; Barcelo, M.; Astorga, J.; Urbieta, A. Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0. *J. Manuf. Syst.* **2020**, *57*, 367–378. [CrossRef]
80. Shah, D.P.; Shah, P.G. Revisting of elliptical curve cryptography for securing Internet of Things (IOT). In Proceedings of the 2018 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, Sharjah, Abu Dhabi, United Arab Emirates, 6 February–5 April 2018; pp. 1–3.
81. Kozlov, D.; Veijalainen, J.; Ali, Y. Security and Privacy Threats in IoT Architectures. In Proceedings of the 7th International Conference on Body Area Networks, Oslo, Norway, 24–26 February 2012; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Brussels, Belgium, 2012; pp. 256–262.
82. Sarma, A.; Girão, J. Identities in the Future Internet of Things. *Wirel. Pers. Commun.* **2009**, *49*, 353–363. [CrossRef]
83. Welch, D.; Lathrop, S. Wireless security threat taxonomy. In Proceedings of the IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, West Point, NY, USA, 18–20 June 2003; pp. 76–83. [CrossRef]
84. Pacheco, L.A.; Gondim, J.J.C.; Barreto, P.A.; Alchieri, E. Evaluation of Distributed Denial of Service threat in the Internet of Things. In Proceedings of the 15th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 31 October–2 November 2016; pp. 89–92. [CrossRef]
85. Sharghivand, N.; Derakhshan, F. Data Security and Privacy in Industrial IoT. In *AI-Enabled Threat Detection and Security Analysis for Industrial IoT*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 21–39.
86. Xiao, B.; Chen, W.; He, Y.; Sha, E.H.M. An Active Detecting Method Against SYN Flooding Attack. In Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), Fukuoka, Japan, 20–22 July 2005; pp. 709–715. [CrossRef]
87. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors* **2021**, *21*, 3654. [CrossRef] [PubMed]
88. Jing, Q.; Vasilakos, A.; Wan, J.; Lu, J.; Qiu, D. Security of the Internet of Things: Perspectives and challenges. *Wirel. Netw.* **2014**, *20*, 2481–2501. [CrossRef]
89. Babar, S.; Mahalle, P.; Stango, A.; Prasad, N.; Prasad, R. Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In *Recent Trends in Network Security and Applications*; Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D., Eds.; Communications in Computer and Information Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 89, pp. 420–429. [CrossRef]
90. Coppolino, L.; DAlessandro, V.; DAntonio, S.; Levy, L.; Romano, L. My Smart Home is under Attack. In Proceedings of the 18th International Conference on Computational Science and Engineering, Porto, Portugal, 21–23 October 2015; pp. 145–151. [CrossRef]
91. Pal, S.; Hitchens, M.; Varadharajan, V. On the design of security mechanisms for the Internet of Things. In Proceedings of the 2017 Eleventh International Conference on Sensing Technology (ICST), Sydney, Australia, 4–6 December 2017; pp. 1–6.
92. Ronen, E.; Shamir, A. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. In Proceedings of the European Symposium on Security and Privacy (EuroS&P), Saarbruecken, Germany, 21–24 March 2016; pp. 3–12. [CrossRef]
93. Pal, S. *Internet of Things and Access Control: Sensing, Monitoring and Controlling Access in IoT-Enabled Healthcare Systems*; Springer Nature: Berlin/Heidelberg, Germany, 2021; Volume 37.
94. Pal, S. Extending Mobile Cloud Platforms Using Opportunistic Networks: Survey, Classification and Open Issues. *J. Univ. Comput. Sci.* **2015**, *21*, 1594–1634.
95. Catarinucci, L.; de Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet Things J.* **2015**, *2*, 515–526. [CrossRef]
96. Yang, J.; Fang, B. Security model and key technologies for the Internet of things. *J. China Univ. Posts Telecommun.* **2011**, *18*, 109–112. [CrossRef]
97. Moscibroda, T.; Mutlu, O. Memory Performance Attacks: Denial of Memory Service in Multi-core Systems. In Proceedings of the 16th USENIX Security Symposium, Boston, MA, USA, 6–10 August 2007; USENIX Association: Berkeley, CA, USA, 2007.
98. Ravi, N.; Scott, J.; Han, L.; Iftode, L. Context-aware Battery Management for Mobile Phones. In Proceedings of the Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom), Hong Kong, China, 17–21 March 2008; IEEE: Los Alamitos, CA, USA, 2008; pp. 224–233. [CrossRef]
99. Liu, J.; Xiao, Y.; Chen, P. Authentication and Access Control in the Internet of Things. In Proceedings of the 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012; pp. 588–592. [CrossRef]
100. Pal, S.; Hitchens, M.; Varadharajan, V. Modeling identity for the internet of things: Survey, classification and trends. In Proceedings of the 2018 12th International Conference on Sensing Technology (ICST), Limerick, Ireland, 4–6 December 2018; pp. 45–51.
101. Mahalle, P.; Babar, S.; Prasad, N.; Prasad, R. Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges. In *Recent Trends in Network Security and Applications*; Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D., Eds.; Communications in Computer and Information Science, Chapter 43; Springer: Berlin/Heidelberg, Germany, 2010; Volume 89, pp. 430–439. [CrossRef]

102. Suhardi.; Ramadhan, A. A Survey of Security Aspects for Internet of Things in Healthcare. In *Information Science and Applications (ICISA)*; Kim, K.J., Joukov, N., Eds.; Lecture Notes in Electrical Engineering; Springer: Singapore, 2016; Volume 376, pp. 1237–1247. [CrossRef]
103. Perera, C.; McCormick, C.; Bandara, A.; Price, B.; Nuseibeh, B. Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms. *arXiv* **2016**, arXiv:1609.04060v1.
104. Condry, M.W.; Nelson, C.B. Using Smart Edge IoT Devices for Safer, Rapid Response with Industry IoT Control Operations. *Proc. IEEE* **2016**, *104*, 938–946. [CrossRef]
105. Hwang, Y. IoT Security and Privacy: Threats and Challenges. In Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security, Singapore, 14–17 April 2015; ACM: New York, NY, USA, 2015; p. 1. [CrossRef]
106. Pal, S.; Hitchens, M.; Varadharajan, V.; Rabehaja, T. Fine-grained access control for smart healthcare systems in the Internet of Things. *EAI Endorsed Trans. Ind. Netw. Intell. Syst.* **2018**, *4*, e5. [CrossRef]
107. Gupta, B.B.; Tewari, A.; Jain, A.; Agrawal, D. Fighting against phishing attacks: state of the art and future challenges. *Neural Comput. Appl.* **2017**, 28, 3629–3654. [CrossRef]
108. Mattern, F.; Floerkemeier, C. From the Internet of Computers to the Internet of Things. In *From Active Data Management to Event-Based Systems and More*; Sachs, K., Petrov, I., Guerrero, P., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6462, pp. 242–259. [CrossRef]
109. Nahrstedt, K.; Li, H.; Nguyen, P.; Chang, S.; Vu, L. Internet of Mobile Things: Mobility-Driven Challenges, Designs and Implementations. In Proceedings of the First International Conference on Internet-of-Things Design and Implementation (IoTDI), Berlin, Germany, 4–8 April 2016; pp. 25–36. [CrossRef]
110. Satyanarayanan, M.; Simoens, P.; Xiao, Y.; Pillai, P.; Chen, Z.; Ha, K.; Hu, W.; Amos, B. Edge Analytics in the Internet of Things. *IEEE Pervasive Comput.* **2015**, *14*, 24–31. [CrossRef]
111. Ahmadian, Z.; Salmasizadeh, M.; Aref, M.R. Desynchronization attack on RAPP ultralightweight authentication protocol. *Inf. Process. Lett.* **2013**, *113*, 205–209. [CrossRef]
112. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516. [CrossRef]
113. Palattella, M.R.; Dohler, M.; Grieco, A.; Rizzo, G.; Torsner, J.; Engel, T.; Ladid, L. Internet of Things in the 5G Era: Enablers, Architecture, and Business Models. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 510–527. [CrossRef]
114. Guinard, D.; Trifa, V.; Karnouskos, S.; Spiess, P.; Savio, D. Interacting with the SOA-Based Internet of Things: Discovery, Query, Selection, and On-Demand Provisioning of Web Services. *IEEE Trans. Serv. Comput.* **2010**, *3*, 223–235. [CrossRef]
115. Zhou, L.; Chao, H. Multimedia traffic security architecture for the internet of things. *IEEE Netw.* **2011**, *25*, 35–40. [CrossRef]
116. Bhattacharya, D.; Canul, M.; Knight, S. Case study: impact of the physical web and BLE beacons. In Proceedings of the 50th Hawaii International Conference on System Sciences, Village, HI, USA, 4–7 January 2017.
117. Elkhodr, M.; Shahrestani, S.; Cheung, H. The Internet of Things: Vision & Challenges. In Proceedings of the Tencon-Spring, Sydney, Australia, 17–19 April 2013; pp. 218–222. [CrossRef]
118. Wernke, M.; Skvortsov, P.; Dürr, F.; Rothermel, K. A Classification of Location Privacy Attacks and Approaches. *Pers. Ubiquitous Comput.* **2014**, *18*, 163–175. [CrossRef]
119. Ho, G.; Leung, D.; Mishra, P.; Hosseini, A.; Song, D.; Wagner, D. Smart Locks: Lessons for Securing Commodity Internet of Things Devices. In Proceedings of the 11th Asia Conference on Computer and Communications Security, Xi'an, China, 30 May–3 June 2016; pp. 461–472. [CrossRef]
120. Christie, C.; Dill, E. Evaluating peers in cyberspace: The impact of anonymity. *Comput. Hum. Behav.* **2016**, *55*, 292–299. [CrossRef]
121. Wright, M.K.; Adler, M.; Levine, B.N.; Shields, C. The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems. *ACM Trans. Inf. Syst. Secur.* **2004**, *7*, 489–522. [CrossRef]
122. Gilchrist, A. *Industry 4.0: The Industrial Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2016.
123. Weber, R.H. Internet of Things—New security and privacy challenges. *Comput. Law Secur. Rev.* **2010**, *26*, 23–30. [CrossRef]
124. Kalmar, E.; Kertesz, A.; Varadi, S.; Garg, R.; Stiller, B. Legal and Regulative Aspects of IoT Cloud Systems. In Proceedings of the 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 15–20. [CrossRef]
125. Bader, A.; Ghazzai, H.; Kadri, A.; Alouini, M.S. Front-end intelligence for large-scale application-oriented internet-of-things. *IEEE Access* **2016**, *4*, 3257–3272. [CrossRef]
126. Zhang, Y.; Huang, X. Security and privacy techniques for the industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 245–268.
127. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; et al. A View of Cloud Computing. *Commun. ACM* **2010**, *53*, 50–58. [CrossRef]
128. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog Computing and Its Role in the Internet of Things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 13–17 August 2012; ACM: New York, NY, USA, 2012; pp. 13–16. [CrossRef]
129. Giurgiu, I.; Riva, O.; Juric, D.; Krivulev, I.; Alonso, G. Calling the cloud: enabling mobile phones as interfaces to cloud applications. In Proceedings of the ACM/IFIP/USENIX 10th International Conference on Middleware, Urbana, IL, USA, 30 November–4 December 2009; Springer: Berlin/Heidelberg, Germany, 2009; pp. 83–102.

130. Willig, A.; Matheus, K.; Wolisz, A. Wireless Technology in Industrial Networks. *Proc. IEEE* **2005**, *93*, 1130–1151. [CrossRef]
131. Zeadally, S.; Isaac, J.; Baig, Z. Security Attacks and Solutions in Electronic Health (E-health) Systems. *J. Med. Syst.* **2016**, *40*, 263. [CrossRef]
132. Pal, S.; Hitchens, M.; Varadharajan, V.; Rabehaja, T. On design of a fine-grained access control architecture for securing iot-enabled smart healthcare systems. In Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Melbourne, Australia, 7–10 November 2017; pp. 432–441.
133. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [CrossRef]
134. Chang, C.; Srirama, S.N.; Buyya, R. Mobile Cloud Business Process Management System for the Internet of Things: A Survey. *ACM Comput. Surv.* **2016**, *49*, 1–42. [CrossRef]
135. Lhaksmana, K.; Murakami, Y.; Ishida, T. Analysis of Large-Scale Service Network Tolerance to Cascading Failure. *IEEE Internet Things J.* **2016**, *3*, 1159–1170. [CrossRef]
136. Lhaksmana, K.M.; Murakami, Y.; Ishida, T. Cascading Failure Tolerance in Large-Scale Service Networks. In Proceedings of the International Conference on Services Computing, New York, NY, USA, 27 June–2 July 2015; pp. 1–8. [CrossRef]
137. Yu, S.; Liu, M.; Dou, W.; Liu, X.; Zhou, S. Networking for Big Data: A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 531–549. [CrossRef]
138. Gupta, Pooja, and M. A. Alam. *"Challenges in the Adaptation of IoT Technology"—A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems*; Springer: Cham, Switzerland, 2022; pp. 347–369.
139. O'Leary, D.E. 'Big data', the 'internet of things" and the 'internet of signs'. *Intell. Syst. Account. Financ. Manag.* **2013**, *20*, 53–65. [CrossRef]
140. Di Pietro, R.; Guarino, S.; Verde, N.V.; Ferrer, J.D. Review: Security in Wireless Ad-hoc Networks—A Survey. *Comput. Commun.* **2014**, *51*, 1–20. [CrossRef]
141. Li, S.; Xu, L.; Zhao, S. The internet of things: A survey. *Inf. Syst. Front.* **2015**, *17*, 243–259. [CrossRef]
142. Pal, S.; Hitchens, M.; Varadharajan, V. Towards the design of a trust management framework for the Internet of Things. In Proceedings of the 2019 13th International Conference on Sensing Technology (ICST), Sydney, Australia, 2–4 December 2019; pp. 1–7.
143. Liu, L.; Liu, T.; Guan, Y.W.; Yan, Y.Q.; Deng, Q.C. A WSN-Oriented Key Agreement Protocol in Internet of Things. Frontiers of Manufacturing Science and Measuring Technology III. Trans Tech Publications. *Appl. Mech. Mater.* **2013**, *401*, 1792–1795. [CrossRef]
144. Kubler, S.; Främling, K.; Buda, A. A standardized approach to deal with firewall and mobility policies in the IoT. *Pervasive Mob. Comput.* **2015**, *20*, 100–114. [CrossRef]
145. Heer, T.; Garcia, O.; Hummen, R.; Keoh, S.; Kumar, S.; Wehrle, K. Security Challenges in the IP-based Internet of Things. *Wirel. Pers. Commun.* **2011**, *61*, 527–542. [CrossRef]
146. Ward, B.T.; Sipior, J.C. The Internet Jurisdiction Risk of Cloud Computing. *Inf. Syst. Manag.* **2010**, *27*, 334–339. [CrossRef]
147. Ren, K.; Lou, W.; Kim, K.; Deng, R. A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environments. *IEEE Trans. Veh. Technol.* **2006**, *55*, 1373–1384. [CrossRef]
148. Wang, F.; Hu, L.; Hu, J.; Zhou, J.; Zhao, K. Recent Advances in the Internet of Things: Multiple Perspectives. *IETE Tech. Rev.* **2016**, *34*, 122–132. [CrossRef]
149. Dong, P.; Guan, J.; Xue, X.; Wang, H. Attack Resistant Trust Management Model Based on Beta Function for Distributed Routing in Internet of Things. *China Commun.* **2012**, *9*, 89–98.
150. Chze, P.; Leong, K. A secure multi-hop routing for IoT communication. In Proceedings of the World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 428–432. [CrossRef]
151. Chze, P.; Yan, W.; Leong, K. A User-Controllable Multi-Layer Secure Algorithm for MANET. In Proceedings of the 8th International Wireless Communications and Mobile Computing Conference (IWCMC), Limassol, Cyprus, 27–31 August 2012; pp. 1080–1084. [CrossRef]
152. Kasinathan, P.; Pastrone, C.; Spirito, M.A.; Vinkovits, M. Denial-of-Service detection in 6LoWPAN based Internet of Things. In Proceedings of the 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 7–9 Octobet 2013; pp. 600–607. [CrossRef]
153. Peng, L.; Ruchuan, W.; Xiaoyu, S.; Long, C. Privacy Protection Based on Key-changed Mutual Authentication Protocol in Internet of Things. In *Advances in Wireless Sensor Networks*; Sun, L., Ma, H., Hong, F., Eds.; Communications in Computer and Information Science; Springer: Berlin/Heidelberg, Germany, 2014; Volume 418, pp. 345–355. [CrossRef]
154. Huang, X.; Fu, R.; Chen, B.; Zhang, T. User interactive Internet of things privacy preserved access control. In Proceedings of the 7th International Conference for Internet Technology and Secured Transactions, London, UK, 10–12 December 2012; pp. 597–602.
155. Ferraiolo, D.; Sandhu, R.; Gavrila, S.; Kuhn, R.; Chandramouli, R. Proposed NIST Standard for Role-based Access Control. *ACM Trans. Inf. Syst. Secur.* **2001**, *4*, 224–274. [CrossRef]
156. Li, S.; Gong, P.; Yang, Q.; Li, M.; Kong, J.; Li, P. A secure handshake scheme for mobile-hierarchy city intelligent transportation system. In Proceedings of the Fifth International Conference on Ubiquitous and Future Networks (ICUFN), Da Nang, Vietnam, 2–5 July 2013; pp. 190–191. [CrossRef]

157. Diro, A.; Reda, H.; Chilamkurti, N.; Mahmood, A.; Zaman, N.; Nam, Y. Lightweight authenticated-encryption scheme for Internet of Things based on publish-subscribe communication. *IEEE Access* **2020**, *8*, 60539–60551. [CrossRef]
158. Isa, M.; Mohamed, N.; Hashim, H.; Adnan, S.; Manan, J.; Mahmod, R. A lightweight and secure TFTP protocol for smart environment. In Proceedings of the International Symposium on Computer Applications and Industrial Electronics (ISCAIE), Kota Kinabalu, Malaysia, 3–4 December 2012; pp. 302–306. [CrossRef]
159. Bao, F.; Chen, I. Dynamic Trust Management for Internet of Things Applications. In Proceedings of the International Workshop on Self-aware Internet of Things, Grenoble, France, 7–10 July 2012; ACM: New York, NY, USA, 2012; pp. 1–6. [CrossRef]
160. Su, J.; Cao, D.; Zhao, B.; Wang, X.; You, I. ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of Things. *Future Gener. Comput. Syst.* **2014**, *33*, 11–18. [CrossRef]
161. Carminati, B.; Ferrari, E.; Cao, J.; Tan, K. A Framework to Enforce Access Control over Data Streams. *ACM Trans. Inf. Syst. Secur.* **2010**, *13*, 1–31. [CrossRef]
162. Jun, M.; Yuanbo, G.; Jianfeng, M.; Jinbo, X.; Tao, Z. A Hierarchical Access Control Scheme for Perceptual Layer of IoT. *J. Comput. Res. Dev.* **2013**, *50*, 1267–1275.
163. Ukil, A.; Bandyopadhyay, S.; Pal, A. IoT-Privacy: To be private or not to be private. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 27 April–2 May 2014; pp. 123–124. [CrossRef]
164. Kothmayr, T.; Schmitt, C.; Hu, W.; Brünig, M.; Carle, G. DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2710–2723. [CrossRef]
165. Jebri, S.; Abid, M.; Bouallegue, A. An efficient scheme for anonymous communication in IoT. In Proceedings of the 11th International Conference on Information Assurance and Security (IAS), Marrakech, Morocco, 14–16 December 2015; pp. 7–12. [CrossRef]
166. Hernandez-Ramos, J.; Jara, A.; Marın, L.; Skarmeta, A. Distributed Capability-based Access Control for the Internet of Things. *J. Internet Serv. Inf. Secur.* **2013**, *3*, 1–16.
167. Mahalle, P.N.; Anggorojati, B.; Prasad, N.R.; Prasad, R. Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *J. Cyber Secur. Mobil.* **2013**, *1*, 309–348.
168. Hong, N., A Security Framework for the Internet of Things Based on Public Key Infrastructure. In *Information Technologies in Construction and Industry*; Huang, Y., Bao, T., Wang, H., Eds.; Trans Tech Publications Ltd.: Freinbach, Switzerland, 2013; Volume 671, pp. 3223–3226.
169. Hassaballah, M.; Hameed, M.A.; Awad, A.I.; Muhammad, K. A Novel Image Steganography Method for Industrial Internet of Things Security. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7743–7751. [CrossRef]
170. Prinsloo, J.; Sinha, S.; von Solms, B. A review of industry 4.0 manufacturing process security risks. *Appl. Sci.* **2019**, *9*, 5105. [CrossRef]
171. Xenofontos, C.; Zografopoulos, I.; Konstantinou, C.; Jolfaei, A.; Khan, M.K.; Choo, K.K.R. Consumer, commercial and industrial iot (in) security: attack taxonomy and case studies. *IEEE Internet Things J.* **2021**. [CrossRef]
172. Ainsworth, T.; Brake, J.; Gonzalez, P.; Toma, D.; Browne, A.F. A Comprehensive Survey of Industry 4.0, IIoT and Areas of Implementation. In Proceedings of the SoutheastCon 2021, Atlanta, GA, USA, 10–13 March 2021; pp. 1–6.
173. Bécue, A.; Praça, I.; Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artif. Intell. Rev.* **2021**, *54*, 3849–3886. [CrossRef]
174. Leng, J.; Wang, D.; Shen, W.; Li, X.; Liu, Q.; Chen, X. Digital twins-based smart manufacturing system design in Industry 4.0: A review. *J. Manuf. Syst.* **2021**, *60*, 119–137. [CrossRef]
175. Horak, T.; Strelec, P.; Huraj, L.; Tanuska, P.; Vaclavova, A.; Kebisek, M. The vulnerability of the production line using industrial IoT systems under ddos attack. *Electronics* **2021**, *10*, 381. [CrossRef]
176. Zelbst, P.J.; Green, K.W.; Sower, V.E.; Bond, P.L. The impact of RFID, IIoT, and Blockchain technologies on supply chain transparency. *J. Manuf. Technol. Manag.* **2019**, *31*, 441–457. [CrossRef]
177. Iqbal, A.; Amir, M.; Kumar, V.; Alam, A.; Umair, M. Integration of next generation IIoT with Blockchain for the development of smart industries. *Emerg. Sci. J.* **2020**, *4*, 1–17. [CrossRef]
178. Seitz, A.; Henze, D.; Miehle, D.; Bruegge, B.; Nickles, J.; Sauer, M. Fog computing as enabler for blockchain-based IIoT app marketplaces-A case study. In Proceedings of the 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, Valencia, Spain, 15–18 October 2018; pp. 182–188.
179. Puri, V.; Priyadarshini, I.; Kumar, R.; Kim, L.C. Blockchain meets IIoT: An architecture for privacy preservation and security in IIoT. In Proceedings of the 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 13–14 March 2020; pp. 1–7.
180. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
181. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [CrossRef]

182. Conoscenti, M.; Vetrò, A.; Martin, J.C.D. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6. [CrossRef]
183. Dhar, S.; Bose, I. Securing IoT Devices Using Zero Trust and Blockchain. *J. Organ. Comput. Electron. Commer.* **2021**, *31*, 18–34. [CrossRef]
184. Vanickis, R.; Jacob, P.; Dehghanzadeh, S.; Lee, B. Access control policy enforcement for zero-trust-networking. In Proceedings of the 2018 29th Irish Signals and Systems Conference (ISSC), Belfast, UK, 21–22 June 2018; pp. 1–6.
185. Pal, S.; Rabehaja, T.; Hitchens, M.; Varadharajan, V.; Hill, A. On the design of a flexible delegation model for the Internet of Things using blockchain. *IEEE Trans. Ind. Inform.* **2019**, *16*, 3521–3530. [CrossRef]
186. Pal, S.; Rabehaja, T.; Hill, A.; Hitchens, M.; Varadharajan, V. On the integration of blockchain to the internet of things for enabling access right delegation. *IEEE Internet Things J.* **2019**, *7*, 2630–2639. [CrossRef]
187. Banaie, F.; Hashemzadeh, M. Complementing IIoT Services through AI: Feasibility and Suitability. In *AI-Enabled Threat Detection and Security Analysis for Industrial IoT*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 7–19.
188. Angelopoulos, A.; Michailidis, E.T.; Nomikos, N.; Trakadas, P.; Hatziefremidis, A.; Voliotis, S.; Zahariadis, T. Tackling faults in the industry 4.0 era—A survey of machine-learning solutions and key aspects. *Sensors* **2020**, *20*, 109. [CrossRef]
189. 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]
190. Khoda, M.E.; Imam, T.; Kamruzzaman, J.; Gondal, I.; Rahman, A. Robust malware defense in industrial IoT applications using machine learning with selective adversarial samples. *IEEE Trans. Ind. Appl.* **2019**, *56*, 4415–4424. [CrossRef]
191. Aboelwafa, M.M.; Seddik, K.G.; Eldefrawy, M.H.; Gadallah, Y.; Gidlund, M. A machine-learning-based technique for false data injection attacks detection in industrial IoT. *IEEE Internet Things J.* **2020**, *7*, 8462–8471. [CrossRef]
192. Geluvaraj, B.; Satwik, P.; Kumar, T.A. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In *International Conference on Computer Networks and Communication Technologies*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 739–747.