future internet

MDPI

Review

Open Radio Access Networks For Smart IoT Systems: State of Art and Future Directions

Abubakar Ahmad Musa [1], Adamu Hussaini [1], Cheng Qian [2], Yifan Guo [1,*] and Wei Yu [1,*]

[1] Department of Computer and Information Sciences, Towson University, Towson, MD 21252, USA; aahmadm1@students.towson.edu (A.A.M.); ahussa7@students.towson.edu (A.H.)
[2] Department of Computer Science & Information Technology, Hood College, Frederick, MD 21701, USA; qian@hood.edu
* Correspondence: yguo@towson.edu (Y.G.); wyu@towson.edu (W.Y.)

Abstract: The Internet of Things (IoT) constitutes a vast network comprising various components such as physical devices, vehicles, buildings, and other items equipped with sensors, actuators, and software. These components are interconnected, facilitating the collection and exchange of copious data across networked communications. IoT empowers extensive monitoring and control over a myriad of objects, enabling them to gather and disseminate data that bolster applications, thereby enhancing the system's capacity for informed decision making, environmental surveillance, and autonomous inter-object interaction, all without the need for direct human involvement. These systems have achieved seamless connectivity requirements using the next-generation wireless network infrastructures (5G, 6G, etc.), while their diverse reliability and quality of service (QoS) requirements across various domains require more efficient solutions. Open RAN (O-RAN), i.e., open radio open access network (RAN), promotes flexibility and intelligence in the next-generation RAN. This article reviews the applications of O-RAN in supporting the next-generation smart world IoT systems by conducting a thorough survey. We propose a generic problem space, which consists of (i) *IoT Systems*: transportation, industry, healthcare, and energy; (ii) *targets*: reliable communication, real-time analytics, fault tolerance, interoperability, and integration; and (iii) *artificial intelligence and machine learning (AI/ML)*: reinforcement learning (RL), deep neural networks (DNNs), etc. Furthermore, we outline future research directions concerning robust and scalable solutions, interoperability and standardization, privacy, and security. We present a taxonomy to unveil the security threats to emerge from the O-RAN-assisted IoT systems and the feasible directions to move this research forward.

Keywords: O-RAN; smart IoT systems; machine learning

Citation: Musa, A.A.; Hussaini, A.; Qian, C.; Guo, Y.; Yu, W. Open Radio Access Networks For Smart IoT Systems: State of Art and Future Directions. *Future Internet* **2023**, *15*, 380. https://doi.org/10.3390/fi15120380

Academic Editor: Eirini Eleni Tsiropoulou

Received: 7 October 2023
Revised: 20 November 2023
Accepted: 23 November 2023
Published: 27 November 2023

1. Introduction

Smart *"Internet of Things"* (IoT) systems refer to interconnected networks of devices, sensors, and objects that communicate and interact, collect and analyze data, make smart decisions based on the accumulated data, and take actions that improve the systems' efficiency, productivity, and safety and security [1–10]. These systems leverage the capabilities of IoT and data science technologies, such as networking connectivity, data analytics, and automation, to enable intelligent and efficient operations across various application domains. Some of the representative application domains include energy [11,12], transportation [13,14], industry [15,16], and healthcare [17], among others.

The basic building blocks of these systems include the sensing, identification, and/or controlling unit consisting of sensors and actuators for perceiving their operating environments and executing the received instructions, the processing unit housing microprocessors and software applications for data processing and running computations within the network edge, a communication unit comprised of the radio access network (RAN) for connecting the different nodes to the core network and the services unit for orchestrating the other components of the system to provide the required services [18].

The advancement of IoT technology heavily depends on its three pillars of computing, communication, and things (sensors and actuators). As evident by Figure 1, smart IoT systems have diverse quality of service (QoS) and reliability requirements [15,19]. For example, healthcare wearables and energy grid smart meters are massive-connectivity-intensive. At the same time, self-driving vehicles and remote surgery are latency-intensive, while telemedicine and industrial control and monitoring systems are broadband-intensive [20–23].

In the last two decades, mobile technology has opened the wildest imaginations regarding innovation and creativity in the telecom sector by drastically changing how we communicate from the perspective of distance and geographical divide. As a result, the total user experience has been consistently and substantially improved by new technology generations launched on average every ten years [24]. In a report published in 2022 by Dell'Oro, it was predicted that the global Radio Access Network (RAN) industry will surpass $40 billion by 2026 and that Open-RAN deployment will represent more than 15% to 20% of RAN worldwide [24,25].

Traditional cellular networks such as 3G and 4G are built on monolithic, inflexible infrastructure, unlike 5G, which supports heterogeneity, allowing O-RAN to run on software-defined radio (SDR), an open loop instead of traditional analog hardware-based systems, which are closed-loop control [26]. The practical implementation of 5G systems requires drastically reworking existing plug-and-play methodologies instead of flexible, new, and open paradigms for network management, deployment, and control [27]. In this scenario, the cellular arena welcomes ground-breaking and cutting-edge networking solutions based on softwarization, openness, resource sharing, virtualization, and mobile edge-computing [28,29].

O-RAN technology aims at maximizing possible resource usage and sharing infrastructure, providing a unique market opportunity such as infrastructure leasing and connectivity-as-a-service (CaaS) technology. As a result, it is an appealing solution for network operators and infrastructure providers [30]. The monolithic nature of RAN components, which supported a few vendors and were viewed by operators as black boxes, gave rise to drawbacks such as network node cooperation restrictions, poor reconfiguration, and vendor lock-in [28].

Furthermore, O-RAN technology advocates for the disaggregation of the RAN into smaller modules: a radio unit (RU), distributed unit (DU), control unit (CU), and opening the interfaces between the different components to promote flexibility, interoperability, innovation, and reduce costs [31]. The O-RAN Alliance is a group of companies formed to develop and promote the O-RAN concept. The alliance includes numerous companies, including mobile network operators, equipment vendors, and software providers. The alliance has developed a set of specifications and reference architectures for O-RAN, which are designed to ensure interoperability between different vendors' equipment [32]. Even though the O-RAN idea was initially conceived to support traditional mobile networks, next-generation wireless networks and smart IoT systems are also covered [33]. For example, networks for IoT systems comprise a heterogeneous and growing number of devices, sensors, objects, and other components, which makes it challenging to manage and orchestrate the network. With the aid of O-RAN, the interface between the different network components can be standardized and opened for easier management and orchestration, leading to enhanced efficiency and cost savings. Furthermore, it can facilitate the development of open and standardized interfaces between IoT devices, gateways, and the edge and cloud to allow different vendors' devices and gateways to work together seamlessly. Similarly, O-RAN can promote the development of enhanced edge intelligence solutions, i.e., by processing data close to where it is generated for transmission latency reduction [33–36].

In this study, we have systematically reviewed the literature by querying the reputable research databases using AND operation between keywords to have precise results such as 'O-RAN' and 'IoT', 'O-RAN' and 'Transportation', 'O-RAN' and 'Industrial IoT', 'O-RAN' and 'Healthcare', 'O-RAN' and 'Energy'. Furthermore, the articles are scrutinized to ensure

that the O-RAN concept supports the IoT systems conceptually or technically. Articles not satisfying the above criteria are not included in this research. Table 1 lists the key terms and abbreviations in the paper.

Our major contributions to this paper are as follows.

- We systematically review the applications of O-RAN in smart IoT systems, i.e., transportation, industry, healthcare, and energy.
- We propose a generic three-dimensional problem space that considers IoT systems (e.g., transportation, industry, healthcare, energy), targets (e.g., reliable communication, real-time analytics, fault tolerance, interoperability, integration), and artificial intelligence and machine learning (AI/ML) schemes (e.g., reinforcement learning (RL), deep neural networks (DNNs).
- We outline future research directions concerning robust and scalable solutions, interoperability and standardizations, privacy, and security. We also present a taxonomy to unveil the security threats to emerge from the O-RAN-assisted IoT systems and the feasible directions to address those threats.

The remainder of this paper is organized as follows. Section 2 introduces the background of traditional radio access networks (RAN), the concept of O-RAN technology, AI/ML, and a brief literature review on O-RAN. Section 3 explores the O-RAN in smart IoT systems based on our defined problem space. Section 4 presents several challenges and future research directions. Finally, Section 5 gives the final remarks.

Table 1. List of terms and abbreviations.

Term	Full Meaning	Term	Full Meaning
AML	Adversarial machine learning	AMQP	Advanced message queuing protocol
AI	Artificial intelligence	BBU	Baseband unit
BLE	Bluetooth low energy	QoS	Quality of service
CaaS	Connectivity-as-a-service	CoAP	Constrained application protocol
CNN	Convolutional neural network	CPS	Cyber–physical system
CTDE	Centralized training distributed execution	CU	Control unit
DCS	Distributed control systems	DNN	Deep neural network
DoS	Denial of service	DU	Distributed unit
FL	Federated learning	emBB	Enhanced mobile broadband
eCPRI	Enhanced common public radio interface	GNN	Graph neural network
ICT	Information communication technology	ICS	Industrial control system
IIoT	Industrial Internet of Things	IP	Internet protocol
IoT	Internet of things	IoV	Internet of vehicle
LLM	Large language model	LoRaWAN	Long-range wide area network
LTE	Long-term evolution	ML	Machine learning
MIMO	Multiple-input and multiple-output	MITM	Man in the middle
emMTC	Enhanced massive machine type communication	MQTT	Message queuing telemetry transport
OT	Operational technology	P2P	Peer-to-peer
PMU	Phasor measurement unit	PLC	Programmable logic controller
QoS	Quality of service	RAN	Radio access network
RF	Radio frequency	RFID	Radio frequency identification
RIC	RAN intelligent controller	RNN	Recurrent neural network

Table 1. *Cont.*

Term	Full Meaning	Term	Full Meaning
NRT-RIC	Near-real-time RIC	RL	Reinforcement learning
N-NRT-RIC	Non-real-time RIC	RU	Radio unit
SCADA	Supervisory control and data acquisition	SDR	Software-defined-radio
SMS	Smart manufacturing system	STS	Smart transportation system
SWOT	Strengths weaknesses opportunities and threats	UAV	Unmanned aerial vehicle
3GPP	Third Generation Partnership Project	UE	User equipment
URLLC	Ultra-reliable and low-latency communication	ZTA	Zero-trust architecture

2. Background

This section begins with a briefing of the traditional RAN, the basic concept of O-RAN technology, such as disaggregation, virtualization, RAN intelligent controller (RIC), and open interfaces. Then, this section introduces AI/ML techniques to make optimal or sub-optimal decisions or pattern recognition and classification, and a brief literature review on O-RAN.

2.1. Traditional Radio Access Network (RAN)

The RAN, popularly known as the access network, is the radio component of the cellular network. It is an essential element of a wireless telecommunication system that employs radio links to connect each device to other network sections. The RAN connects user equipment (UEs) over a fiber or wireless backhaul connection, such as a phone, computer, or any remotely operated machine. From the first generation (1G) of cellular networking to the fifth generation (5G), RANs have undergone several developments. The core network and radio access network underwent a significant change due to the introduction of long-term evolution (LTE) RAN by the Third Generation Partnership Project (3GPP) in the 2000s with the advent of fourth-generation (4G) technology. With 4G, system connectivity was replaced by circuit-based networks for the first time and was based on the internet protocol (IP). The first cellular networks were developed in the early years of the 2000s. Text messages, voice calls, streaming video, and audio have all become part of RAN's capabilities. Many more types of UEs use these networks, including autonomous cars, drones, and IoT devices.

Despite these remarkable advancements, traditional RANs are monolithic nowadays (i.e., inflexible, protocol-based, proprietary-driven), and inefficient in handling a number of vast dynamic requirements brought by 5G and future 6G. This calls for open, flexible, intelligent, software-driven connectivity solutions capable of handling these requirements and resolving the traditional RAN's deficiencies in a more cost-effective and energy-efficient manner. To address the shortcomings posed by RAN architecture, a number of research and standardization initiatives proposed O-RAN as the new paradigm shift for the future of RAN. Notwithstanding, O-RAN implementations use software-based, virtualized, and disaggregated components that are interoperable across multiple vendors and connected by open, standardized interfaces [37,38].

2.2. Concept of O-RAN Technology

The new O-RAN paradigm approach is software-based and adaptable, enabling data-informed smart control loops for cellular systems and openness, virtualization, and programmability of RAN functionality and components. As a result, network engineers can support new customized services on common physical infrastructures and vigorously rearrange them in response to user demand and network conditions thanks to the Open RAN. In addition, the network's operating expenses could decrease due to greater efficiency [26].

Disaggregation: It entails breaking down the RAN components into smaller chunks of functional modules that different vendors can implement. The following units emerged

by disaggregating the O-RAN components: the baseband unit (BBU), i.e., the control unit (CU), which is responsible for control plane functions, such as radio resource management and mobility management; the distributed unit (DU), which is responsible for radio frequency (RF) processing and data plane functions, such as user data forwarding; and finally, the radio unit (RU), which is responsible for radio frequency (RF) signal reception and transmission.

Virtualization: It encompasses separating the RAN software components from the underlying hardware to allow greater flexibility and agility in the RAN and the potential for cost savings. Since software components are tightly coupled to the underlying hardware in a traditional RAN, virtualization decouples the software components from the underlying hardware to optimize the RAN's performance for different application environments or even gives room for creating a responsive cloud-based RAN that scales or shrinks based on the available demand to ease the management of the RAN.

RAN intelligent controller (RIC): It is a key component of the O-RAN architecture. It carries out controlling and managing the RAN, and it uses software-based intelligence to optimize the performance of the network. The RIC is divided into the near-real-time RIC (NRT-RIC) and the non-real-time RIC (N-NRT-RIC). The N-NRT-RIC operates on a timescale greater than 1 s to handle non-real-time events and their respective control loops, such as configuration changes and performance optimization. The NRT-RIC operates between the 10 ms and 1 s timescale to handle near real-time events and their respective control loops, such as handovers and admission control.

D'Oro et al. [39] proposed the concept of dApps operating in the CU and DU to extend the RIC capabilities towards handling real-time control loops such as scheduling and beamforming working on timescales of less than 10 ms, even though efforts extending the RIC concept to the RU are yet to be recorded at the time of this writing. For instance, Ko et al. [40] proposed edgeRic to confirm that decoupling the RIC from the RAN stack and co-locating it close to the DU can support control loops operating within sub milliseconds and even microseconds. These proposed contributions extended the RIC capabilities toward addressing the latency requirements of the next-generation smart IoT systems.

Open interface: It involves the collection of standardized interfaces that enable the different components of the RAN to communicate with each other. The interfaces are designed to be open and interoperable to facilitate the seamless cooperation of different vendors.

Some of the interfaces that are defined and standardized by the O-RAN Alliance include the following: The **O1** interface, which connects the SMO with the remaining components (CU, DU, RU, and near-RT RIC) of the RAN stack to manage and orchestrate the RAN as well as enable the integration of the third-party apps. The **A1** interface, which provides a connection between the non-RT-RIC and the N-RT-RIC to send intelligent policies and telemetries to the N-RT-RIC and allow the N-RT-RIC to control the RAN intelligently. The **E2** interface, which connects the N-RT-RIC with the E2 nodes, enabling different RAN optimization and automation services like RAN control, monitoring, and configuration. Other interfaces include the **fronthaul**, which connects the RU with the DU. **Midhaul** enables connections between the DU and the CU, and backhaul connects the RAN with the core network. Figure 2 describes the architecture of O-RAN as defined by O-RAN Alliance [32]. The alliance is a global industry consortium that promotes developing and adopting open and intelligent RAN technologies. It was initiated to transform traditional RAN infrastructure by enabling greater interoperability, flexibility, and innovation in the mobile telecommunications industry. The alliance plays a pivotal role in driving innovation and openness in RAN technology, which is essential for the evolution of 5G networks and the deployment of future wireless communication technologies.

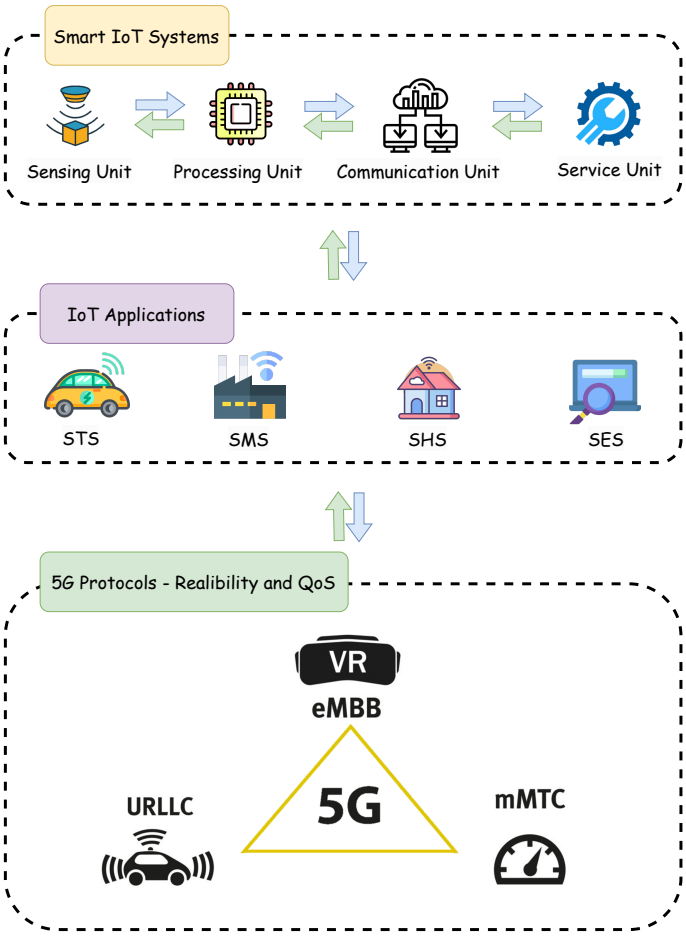

Figure 1. Building block of IoT systems.

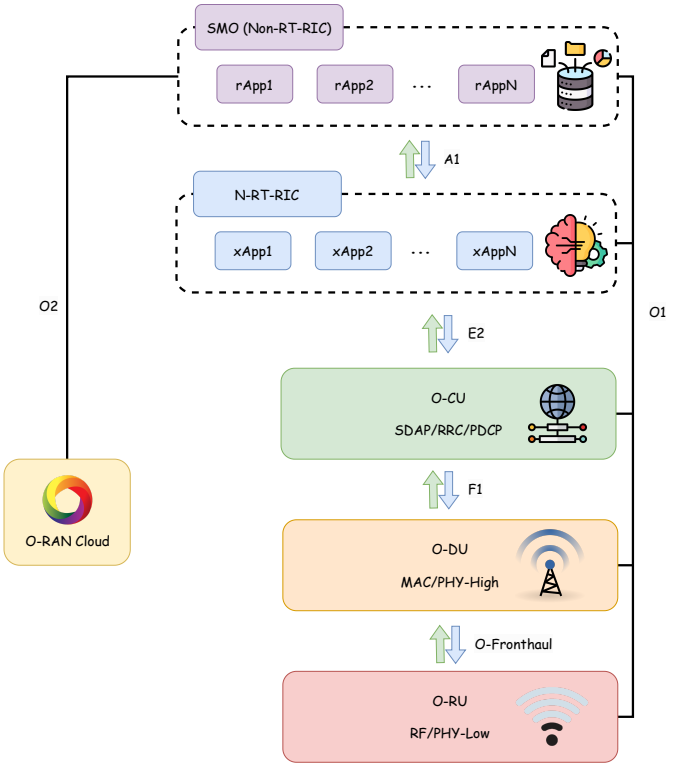

Figure 2. O-RAN architecture as defined by the O-RAN Alliance [32].

2.3. Artificial Intelligence and Machine Learning (AI/ML)

Simply put, AI is the art of enabling machines with human-like thought, reasoning, and decision-making power. It is the grand quest to breathe life into algorithms, allowing them to perceive the world, learn from experience to build a model that can reflect the target system, adapt to changing circumstances, and provide solutions to complex problems [7,41,42]. The ML, which is a subset of AI, learns from the given data about the past to make better futuristic predictions. It is the digital detective, discovering patterns and insights that elude human senses in pursuing more intelligent and autonomous machines.

In this context, the typical applications of AI/ML methods include dynamic control decision-making and pattern recognition/classification techniques as described below.

Reinforcement learning (RL) is a branch of the dynamic ML paradigm where software agents learn to make decisions in an environment by receiving feedback as rewards [43]. Through a cycle of observations, actions, and learning, the agents gradually improve their decision-making abilities to achieve long-term goals. Several RL types range from value-based, policy-based, deep RL, or actor–critic learning, which combines the two for optimized decision making in dynamic environments.

RL is applied in the O-RAN context to optimize the management and performance of the network. For example, RL dynamically allocates resources (bandwidth, power, frequencies, etc.) to different IoT devices or network slices based on real-time conditions and demands. Similarly, RL can control power consumption by optimizing transmission power levels and sleep modes of devices while ensuring connectivity and QoS. Again, RL agents can be trained to detect network anomalies and failures and then decide to implement self-healing mechanisms. This proactive approach ensures network resilience and reduces downtime. Despite RL's promising capabilities for optimizing O-RAN and the emerging O-RAN-based IoT systems, challenges related to training data, model robustness, and real-time adaptation, among others, remain open for the research community to solve [43,44].

Deep neural networks (DNNs): This refers to the stacked neural network architectures that recognize patterns and extract information from structured or unstructured data. They are well suited for tasks involving images, sequences, and graph data [41]. Convolutional neural networks (CNNs), as a good example, are applied to tasks involving grid-like data, such as images and videos. They are proficient at capturing spatial relationships within data. Recurrent neural networks (RNNs) on the other hand, are designed for handling sequential data. The architecture has connections that allow information to persist over time, which makes it exemplary at capturing temporal relationships within the data. Graph neural networks (GNNs) are essential for data representation involving graphs, i.e., data consisting of several nodes and edges. They are mostly used in applications with essential relationships between data points, such as network traffic analysis [45].

In this context, these techniques are applied to learn the latent characteristics of the network and its users, which will guide the effective management of the network in several ways. For example, these techniques can learn the operating pattern of the network from its data to predict traffic and performance degradation, detect anomalies and intrusions, and optimize energy efficiency. However, despite DNN's potential, striking a balance between their complexity and the complexity of the emerging O-RAN-based IoT system to satisfy the real-time performance requirement of their operating environment remains open for further research [41,46,47].

2.4. Brief Review on O-RAN

A number of recent research works have shown that O-RAN can support the next-generation smart IoT systems in several ways. For example, in two separate works, researchers in Pham et al. [48] and Pham et al. [49] considered the Internet of drones by integrating UAVs with O-RAN architecture to optimize user routes to the core network to improve resource allocation and enhance offloading tasks. Similarly, Wang et al. [36] proposed a computation offloading strategy that minimizes energy consumption and re-

duces the communication latency of O-RAN-based IoT systems. Riccio et al. [50] leveraged the RAN intelligent controller (RIC) to enhance IoT handover management. Lini et al. [51] emphasized that merging AI with 5G is essential in facilitating open networking (vendor independence) as well as realizing the next-generation smart IoT systems. Firouzi et al. [35] adopted O-RAN to optimize federated learning (FL) operation in supporting distributed edge intelligence of 5G-based IoT systems. Liu et al. [52] addressed network slicing security in cyber–physical systems (CPS), while Kougioumzidis et al. [53] considered extending O-RAN capabilities to virtual reality applications. Vila et al. [54] presented the network digital twins (DT) concept to reflect the RAN's operation for taking the appropriate action. Likewise, Masaracchia et al. [55] demonstrated the integration of DT with O-RAN as inevitable for yielding the 6G RAN.

Similarly, there are several surveys and reviews on O-RAN, its application areas, and areas of challenges. For example, Polese et al. [31] presented a comprehensive tutorial on O-RAN, discussing its architecture, interfaces, and workflows, giving a big picture of how O-RAN aims to transform the next-generation cellular networks. In addition to covering the areas of research successes and challenges, Liyanage et al. [56] presented both threats and possible solutions that are associated with O-RAN's security and privacy concerns. Bitton et al. [57] presented a systematic adversarial machine learning (AML) threat analysis for O-RAN, discussing some of the possible AML countermeasures and a method for conducting risk assessments. Abdalla et al. [58] reviewed O-RAN capabilities. Likewise, Wu et al. [59] reviewed network slicing management in Industrial IoT. Thus, there is room for more effort within the public domain to provide a holistic investigation of the applications of O-RAN in smart IoT systems.

3. O-RAN in Smart IoT Systems

This section explores the smart IoT systems and the O-RAN contribution in each selected domain. In particular, we first describe the problem system and then present the O-RAN application to some representative IoT systems.

3.1. Problem Space

We propose a three-dimensional problem space, as detailed by Figure 3, where the X-axis indicates the IoT systems (e.g., STS, SMS, others), the Y-axis displays the targets (e.g., reliable communication, real-time analytics, fault tolerance, interoperability and integration), and the Z-axis covers the AI/ML techniques (i.e., RL, DNN).

As shown in Figure 3, four targets were adopted to represent the research objectives achieved by O-RAN while supporting the smart IoT systems. The targets derived from the adopted research methodology and the diligent consideration of the objectives achieved by O-RAN in these domains. The dimension of targets (Y) are detailed below:

- *Reliable communication (Y_1):* It entails the achievement of reliable, optimized, and secure communication infrastructure for seamless connectivity and data exchange within and between these systems by addressing challenges related to latency, bandwidth, privacy, authentication protocols, interference, etc. For example, V2X communication represents optimal transmission latency [60], IoE beamforming represents optimized interference in the transmission medium [61], and telemedicine represents optimum end-to-end healthcare service delivery [62].
- *Real-time analytics (Y_2):* It involves improving data collection, analysis, decision-making, and control by integrating edge computing, distributed analytics, and machine learning techniques to support extracting valuable insights and real-time monitoring. It also enables predictive maintenance, personalized services, etc. For example, resource allocation represents the dynamic assignment of network resources in real time [34], and edge intelligence represents data analytics close to where it is generated for improved performance [63,64].
- *Fault tolerance (Y_3):* It implies using the O-RAN concept to enhance IoT systems' resilience and self-healing capabilities by improving the robustness of fault detec-

tion and recovery mechanisms to ensure uninterrupted operation, quick response to disruptions and security threats to minimize downtime. Some of the examples are signaling storm detection [65] and Industrial IoT data security [66].

- *Interoperability and integration (Y_4):* It entails using the O-RAN concept to promote interoperability and integration among IoT devices, systems, and platforms using the standardized interfaces to enable seamless connectivity, data exchange, and integration of diverse components for efficient operations. For example, O-RAN can be used to facilitate interoperability between two or more IoT domains [59].

It is worth noting that to make O-RAN a viable wireless network infrastructure to support IoT applications, it is critical to perform quantitative analysis with performance metrics (latency, bandwidth, scalability, capacity, coverage, range, etc.) for IoT applications based on O-RAN. For example, related to smart manufacturing systems, to carry out monitoring capability of industrial systems, the latency range must be below 100 ms, bandwidth must be in the range of 0.1–0.5 Mp/s, and reliability needs to be larger than 99.9% [67]. In our prior study [15], we emphasized the importance of understanding the key parameters and performance requirements of smart manufacturing systems, including types of manufacturing applications, key parameters (network size, etc.) and performance requirements (latency, reliability, etc.), discussed the challenges and limitations of existing static networking infrastructure to support applications in smart manufacturing systems with diversified performance requirements, and called for the necessity of developing dynamic and flexible/re-configurable networking infrastructures (e.g., software-defined networking) to support IoT applications with different performance requirements. Additionally, for energy-based IoT systems such as smart grids [68], it is critical to understand the performance requirements of smart grid applications in both the transmission and distribution side based on the standardization and carry out performance evaluation of different networking architectures and protocols. As the O-RAN is a new network infrastructure, the standardization and research community shall have joint efforts on the performance gap of O-RAN to support IoT applications via modeling, simulation, and testbed development.

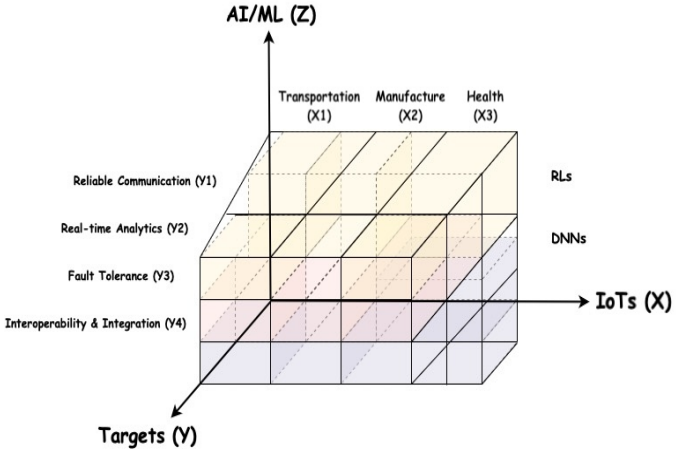

Figure 3. Problem space.

3.2. Smart Transportation Systems

The smart transportation system leverages advanced information communication technologies (ICT) to enhance transportation systems' safety, efficiency, reliability, and sustainability. It integrates sensors, communication systems, data analytics, and control systems to collect and process data, providing real-time decisions, and optimize transportation operations. Nowadays, the smart transportation system is used to support the automatic control of vehicles, monitor traffic conditions, handle traffic flow, provide real-time information updates to drivers, reduce environmental pollution, and even improve air quality. With the advent of 5G, the next-generation smart transportation system aims to improve

road safety, traffic efficiency, environmental sustainability, and user experience through enhanced communication and data-driven technologies [69]. Just like the *"ultra-reliable and low-latency communication (URLLC)"* capabilities to support real-time applications like autonomous driving, improving the reliability, range, and capacity of V2X communication promotes better coordination among road users [70]. The *"enhanced mobile broadband (emBB)"* applications like in-vehicle entertainment and infotainments require high-quality multimedia streaming, augmented reality navigation, and other entertainment services to passengers in moving vehicles [71]. The *"massive machine type communication (mMTC)"* enables more effective traffic management and congestion reduction strategies using dynamic traffic signal control, adaptive routing, and predictive traffic flow analysis, etc. [72,73].

At the same time, O-RAN could build on that to promote automation, interoperability, and cost-efficiency in the next-generation ITS by enhancing vehicular communication optimization, traffic management and control, cooperative autonomous driving, etc. For example, Huang et al. [63] presented an improved edge intelligence supporting IoV networks. Hammami et al. [74] leveraged the O-RAN concept to implement a centralized training but distributed execution (CTDE) strategy to enable cooperation among diverging agents operating in vehicular networks. In this manner, they addressed the resource allocation problem of V2V and V2I while satisfying their reliability and QoS requirements. Likewise, Ndikumana et al. [64] used the NRT-RIC to create a collaboration area in a network of multiple radios and edges. Their approach can balance computation and communication, translating to a latency reduction in autonomous vehicles network [75].

Abolhasan et al. [76] utilized the RIC to control the proposed fuzzy-based routing protocol. The RIC handles the dynamic network topology and arrives at the optimum traffic route by generating and maintaining the link state database, which guides the multi-hop peer-to-peer (P2P) communication. Linsalata et al. [60] presented O-RAN as a promising enabler of the next-generation vehicular communication orchestration, together with open research considerations militating against integrating the two technologies. V2X resource allocation, beam selection, relay assignment, and network DTs are among the feasible research directions in their work.

Takeaways from smart transportation systems: Supported by Table 2, the reviewed efforts in smart transportation covered Y_1 and Y_2, while Y_3 and Y_4 are less explored. However, despite O-RAN's achievements in smart transportation, there is a need for smart-transportation-compatible specifications, standards, and tools facilitating the development of robust, secure, energy-efficient, adaptive solutions that operate in real life.

Table 2. Summary of O-RAN in smart transportation systems.

Reference, Year	Objective	Gap	Contribution	Remarks
Ref. [63], 2021	X_1, Y_2	Computation-intensive solutions are not suitable for delay-sensitive Internet of vehicle (IoV) networks	Leveraged O-RAN concept to improve IoV's edge intelligence	The solution was technically presented and supported with a prototype but calls for the open-source community's support to be standardised
Ref. [74], 2022	X_1, Y_2	Traditional vehicular networks cannot facilitate cooperation among diverging agents in a resource constraint environment	Adopts O-RAN concept to implement *"centralized training distributed execution (CTDE)"* which promotes cooperation between diverging agents in a given environment	Despite the solution being technically presented and supported with results, it appears to be computation-expensive for its real application
Ref. [64], 2022	X_1, Y_2	Balancing between computation and communication in a network of multiple radios and edges is expensive in delay-sensitive systems	Utilizing the O-RAN concept to create a cooperation space in a network consisting of multiple radios and edges to improve autonomous vehicles' edge intelligence	The solution appears to be technically solid for operating in a static network. However, the solution may not scale to accommodate today's network dynamics
Ref. [76], 2022	X_1, Y_1	Multi-hop routing protocols do not consider the changing dynamics of the network participants	Proposed a fuzzy-based routing protocol guided by the RIC to accommodate the changing dynamics of multi-hop peer-to-peer communication	Despite the idea's novelty, the solution extends the system's complexity by increasing the processing overhead in today's delay-sensitive smart transportation systems.
Ref.[60], 2023	X_1, Y_1	Traditional RANs cannot support the emerging dynamic V2X communication	Presented O-RAN as a viable candidate for supporting dynamic control in V2X	The contribution was visionary; calls for the modification of the open interfaces to be V2X compatible

3.3. Smart Manufacturing Systems

Smart manufacturing applies cutting-edge technology that uses Internet-connected equipment to increase production efficiency and track processes by employing computer controls, modeling, big data, and other automation [15]. The Industrial Internet of Things (IIoT) has specific applications, one of which is smart manufacturing. The IIoT aims to increase the reachability, effectiveness, and decision making in industrial control systems (ICS). It also offers intelligent functions, including energy consumption monitoring, environmental release management, and general safety and security for the ICS network. ICSs are hardware and software-based systems that monitor and manage industrial activities. The networking hardware and protocols that serve the ICS are known as operational technologies (OT). Supervisory control and data acquisition (SCADA), plant distribution control systems (DCSs), as well as programmable logic controllers (PLCs) are some of the common examples of OT employed in ICS [77]. This entails integrating inter-connected IoT devices, technologies, and principles in industrial settings to improve operational efficiency, optimize processes, and enhance productivity. The smart manufacturing system leverages sensors, devices, and intelligent systems to connect and collect data from various industrial assets, machines, and equipment, enabling real-time monitoring, control of environmental activities, analysis, and automation.

From the 5G era and beyond, the smart manufacturing system targets improving seamless connectivity, ultra-reliable communication, high data rate, low latency, efficient data processing, and optimal resource allocation for various industrial applications, for example, industrial automation and remote robotics, where minimal transmission latency is the principal objective, video surveillance for real-time monitoring of industrial assets where high-speed data rates are targeted, and industrial assets tracking, where massive machine connectivity is preferred, among others [78–80].

O-RAN will build on 5G's intervention to yield open, scalable, resilient, cost-effective solutions that lead to a more efficient, productive, resilient, and sustainable industrial setting. This can be achieved in several ways. For example, Rahman et al. [67] conducted a *"SWOT Analysis"* to determine O-RAN's areas of strengths that could be leveraged to support the next-generation smart manufacturing applications in satisfying their seamless connectivity requirements. Lin et al. [81] proposed *"zero-touch"* architecture to connect the diverse components of a smart factory together. The RIC was used to control the connectivity using AI/ML in a distributed passion.

Abedin et al. [34] proposed a flexible and scalable method of slicing the IIoT network in RIC while considering the diverse QoS requirements and the available resources within the network. Their approach reduces the problem's complexity by employing distributed game theory to match each slice to its corresponding cell base stations and then applying actor–critic learning to achieve an optimum resource allocation that facilitates IIoT monitoring and control.

Hoffmann et al. [65] proposed an xApp that examines the control plane messages to detect malicious threats targeting IIoT devices. Tselikis et al. [66] presented IIoT data security as critical for effectively monitoring and controlling the ecosystem, thereby examining O-RAN's readiness towards ensuring the privacy and security of the data.

Takeaways from smart manufacturing systems: As supported by Table 3, the reviewed efforts in smart manufacturing systems covered Υ_1, Υ_2, and Υ_3 while Υ_4 still needs further exploration. However, despite O-RAN's achievements in smart manufacturing, there is a need for more efforts on SMS-compatible specifications, standards, and development, as well as testing tools facilitating the development of scalable, robust, adaptive solutions that keep the end-to-end security and privacy of the operating environment and its data in mind.

Table 3. Summary of O-RAN in smart manufacturing systems.

Reference, Year	Objective	Gap	Contribution	Remarks
Ref. [34], 2022	X_2, Y_2	Traditional RAN slicing is achieved using proprietary solutions	Applied game theory and actor–critic learning in the RIC, to address the resource allocation problem of IIoT	Despite the solution's robustness in preserving the system's QoS, security must be kept in mind as well
Ref. [81], 2022	X_2, Y_2	distributed AI/ML solutions in IIoT are implemented in small scales	Used the RIC to control the large-scale connectivity of diverse smart factory components	Large-scale solutions require dedicated testing and validation tools while considering safety threats targeting the model and the system
Ref. [65], 2023	X_2, Y_3	signaling messages evaluation is hard to achieve with monolithic solutions	xApp that studies the IIoT control plane messages statistics and detects any outlier as malicious right from the registration stage	Anomaly detection methods in a dynamic, heterogeneous environment that encourages interoperability needs to be robust, resilient, scalable and operate in real time
Ref. [66], 2023	X_2, Y_3	IIoT data security cannot be guaranteed by single scale solutions	Examines O-RAN's readiness to provide an interoperable ecosystem housing diverse security solutions working together to preserve IIoT QoS requirements	Security by design principles needs detailed investigation in this context
Ref. [67], 2023	X_2, Y_2	5G-based IIoT solutions are monolithic	Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of O-RAN in addressing the connectivity requirements of IIoT applications, i.e., in terms of monitoring and control	O-RAN potentials can only be uncovered by IIoT applications if the solutions are tested thoroughly, standardized for effective deployment

3.4. Smart Healthcare Systems

The smart healthcare system entails leveraging technological advancements in AI/ML and IoT to improve healthcare delivery, enhance medical services, improve patient outcomes, and streamline healthcare processes. The fundamental objective of smart healthcare is to provide personalized, efficient, and effective healthcare services while minimizing costs and enhancing the general quality of caregiving.

Some of the critical components of smart healthcare include IoT devices (sensors/actuators) and healthcare wearables for collecting patients' data remotely. The data are analyzed using AI/ML models to predict the required action, processed and stored with the aid of computing infrastructures like the network edge, cloud, data centers, and other networking equipment, and supported with a user interface to guide user interaction with the system. Due to the critical nature of the system and the data in circulation, the system is supported with authentication, encryption, access control, and intrusion detection mechanisms to ensure the security and privacy of the system and data [82].

With the benefits realized from the advancements in cellular networks like the 5G/6G, O-RAN can improve the services rendered by IHS by providing a flexible, scalable, and interoperable architecture that can support many devices, users, and systems to operate more cost-effectively and energy-efficiently.

For example, De et al. [62] presented "OpenCare5G", a project aimed at demonstrating 5G-enabled telemedicine, i.e., remote digital healthcare examinations in real-time. The project employs the O-RAN concept to disaggregate the network components, giving room for customization and updates and making the solution flexible and cost-effective. Likewise, Trifonov et al. [83] demonstrated how O-RAN uses AI/ML to improve network performance and supported that a policy-driven use case could control the inactivity timer prediction of narrow-band medical IoT devices.

Takeaways from smart healthcare systems: Supported by Table 4, the reviewed efforts in smart healthcare covered Y_1 and Y_2, while Y_3 and Y_4 are yet to be explored. However, despite O-RAN's achievements in smart healthcare, there is a need for more efforts to transition the several objectives in smart healthcare to reality as well as healthcare-compatible

specifications, standards and tools facilitating the development of enhanced solutions that preserve the end-to-end privacy and security of the patient's data.

Table 4. Summary of O-RAN in smart healthcare systems.

Reference, Year	Objective	Gap	Contribution	Remarks
Ref. [62], 2023	X_3, Y_1	5G facilitates the seamless connectivity required by remote healthcare services but with additional cost	Employs O-RAN to extend remote healthcare services to rural areas cost-effectively	Smart healthcare solutions will remain incomplete if end-to-end privacy and security of patients data is not considered
Ref. [83], 2022	X_3, Y_2	5G-based inactivity timer prediction methods are not adaptive	Employ O-RAN concept to propose an adaptive policy that embeds intelligence in the RAN, guiding the efficient energy utilization of remote narrow-band medical devices	The effort is conceptual; needs to be transited to real implementation

3.5. Smart Energy Systems

The smart energy system, such as the smart grid, involves integrating modern communication and information technologies with the energy sector to create a more interconnected, efficient, and sustainable energy ecosystem by applying digital solutions to energy generation, distribution, consumption, and management. The smart energy system leverages data analytics, automation, and real-time communication to optimize energy systems, enhance grid stability, and support the integration of distributed energy resources (DER). Some candidate systems in smart energy systems include smart grids, energy management and optimization systems, renewable energy integration mechanisms, demand response programs, microgrids, and energy trading schemes.

With 5G and beyond 5G (B5G) networks, the smart energy system targets the revolution of the entire energy sector by supporting efficient, flexible, and responsive energy systems. This can be achieved in several ways. Starting from ensuring low latency, facilitating real-time communication between various energy assets, sensors, and control systems to maintain grid stability, respond quickly to supply and demand fluctuations, and ensure the reliability of energy services to providing the massive connectivity required by the smart energy system to connect a wide range of devices, like the smart meters, sensors, DERs, energy storage systems, and electric vehicles as well as providing the necessary bandwidth required for transmitting large amounts of data in real-time, especially for the essential applications requiring high-resolution energy consumption monitoring, real-time analytics, and video surveillance of energy infrastructures [84]. When the O-RAN concept is extended to smart energy applications, it will yield more flexibly connected, efficient, and collaborative energy systems supporting enhanced communication, improved management of DERs, better grid stability, and increased flexibility in adapting to evolving energy demands.

For example, Mongay et al. [61] presented 5G as a promising enabler of smart energy systems and supported that with an O-RAN-based beamforming case study. Similarly, Kundacina et al. [85] proposed how 5G will support the next generation's smart distributed state estimation of PMU-based WAMS in near-real-time.

Takeaways from smart energy systems: Supported by Table 5, the reviewed efforts in smart energy systems covered Y_1 and Y_2, while Y_3 and Y_4 remain open for further investigation. However, despite O-RAN's achievements in smart energy systems, there is a need for more real-time operating ideas to maintain the integrity of the operating environment's data, minimizing interference in the transmission medium, which will improve the system's resilience to threats.

Finally, as depicted in Table 6, the O-RAN-IoT convergence helps to minimize IoT devices' energy consumption. In particular, computation tasks can be offloaded from the participating nodes to the network edge in the representative CPS (smart transportation, smart manufacturing, smart energy grids, smart healthcare, etc). The network edge can

leverage the O-RAN to promote openness and intelligence in addition to virtualization, scalability, and flexibility provided by the proprietary C-RAN and V-RAN. The openness in the edge offers the opportunity for heterogeneous computation and communication tasks to be jointly optimized and executed for latency reduction, which translates to the cost-effective energy consumption of participating IoT devices. Taking the computation offloading case [86] as an example, offloading points, processing speed, offloading ratio, and transmission power were jointly optimized within the edge. Since computation is carried out in the O-RAN-based edge and only the results are sent back to the participating nodes (IoT devices) via the downlink channel; this avoids traffic congestion, drastically reducing the energy consumption of IoT devices. Illustratively, in the smart transportation system, by minimizing the offloading delay in an open collaborative edge [64], the convergence leads to a massive communication latency reduction, a stringent requirement for the effective communication of autonomous vehicles. Likewise, in the smart healthcare system, the convergence can considerably reduce the cost associated with remote healthcare giving, just like the case of the OpenCare5G project [62], where the O-RAN concept was used to realize an interoperable architecture housing hardware and software, virtual machines and cloud-based open interfaces developed by different healthcare vendors.

Table 5. Summary of O-RAN in smart energy systems.

Reference, Year	Objective	Gap	Contribution	Remarks
Ref. [61], 2022	X_3, Y_1	Beamforming based on massive multiple-input and multiple-output (MIMO) in O-RAN is an open problem	Implemented zero-forcing in O-RAN to prove digital beamforming reduces fronthaul traffic and minimizes interference in IoE's communication channels	An effective smart energy-based beamforming solution should be scalable, adaptive, and prevent unauthorized access.
Ref. [85], 2022	X_3, Y_2	Model-based state estimation methods are inefficient nowadays	O-RAN for intelligent data-driven distributed state estimation of phasor measurement units (PMUs)	Effective PMU monitoring requires solutions that consider real-time performance, data quality and integrity, and privacy and security

Table 6. State-of-the-art benefits of O-RAN-based IoT systems.

Reference, Domain	Task	Gain
Ref. [86], IoT devices	Computation offloading from IoT devices to the network edge	20 % reduction in energy consumption among for IoT devices
Ref. [64], Transportation	Age of processing offloading for minimizing communication latency	More than 90 % reduction in computation cost leading to an effective communication for vehicular networks
Ref. [61], Energy	Digital beamforming for IoE	Efficient beamforming network parameters required by the IoE
Ref. [62], Healthcare	Healthcare remedies covering rural communities	Cost effective remote healthcare services
Ref. [34], Manufacturing	Network slicing for IIoT	Robust network for an effective monitoring and control in IIoT

4. Challenges and Future Research Directions

This section outlines several challenges and suggests some future research directions. Some of the challenges listed are interoperability and standardization, robust, scalable solutions, AI for O-RAN, and security and privacy. Future research directions include O-RAN for IoT applications, security and privacy in O-RAN, explainable AI for IoT and O-RAN integration and standardization, and research and development.

4.1. Challenges

Based on the investigation conducted in this study, it is clear that O-RAN can support IoT systems in several ways. However, these systems comprise diverse devices used by different application domains with different communication protocols to achieve their respective goals. This could lead to several challenges that need to be addressed before

these systems can be widely deployed. We have summarized the challenges based on the dimensions below.

4.1.1. Interoperability and Standardization

Interoperability between IoT and O-RAN will be a significant challenge for integrating the two systems because they comprise various devices from different manufacturers, cross-layer networking topologies, and edge computing vendors, having their respective communication protocols and standards. These devices span various application domains (transportation, industry, healthcare, energy, etc.), where each application has its unique requirements and data formats.

Second, O-RAN uses standard communication protocols like the 5G NR. In contrast, IoT devices use various IoT-specific protocols (e.g., MQTT, CoAP, AMQP, etc.). Most IoT devices have limited battery power. At the same time, the O-RAN concept is more complex and battery-demanding than the traditional RANs.

Lastly, the development, validation, and testing tools are imperfect for extending the O-RAN concept into IoT systems. Most of the efforts reviewed in this study are either complex (computation-expensive), static (does not scale to environmental changes and demands), visionary (theory/hypothesis, yet to be implemented), vulnerable to threats, or even undeployable (needs thorough testing/validation) in some cases. There is a need for standards, tools, and specifications that guarantee the integration and interoperability operation of these systems.

The O-RAN Alliance has dedicated several focus groups working to ensure that the O-RAN vision comes to fruition [87]. Similarly, there is a need for a dedicated group that engages O-RAN and IoT standardization and research communities to investigate the feasible ways O-RAN could be an idea match for IoT systems. At this juncture, there is not much published research reporting the possible ways of integrating O-RAN interfaces with IoT applications. How to implement IoT-specific protocols, such as RFID, NB-IoT, LoRAWAN, etc., in O-RAN still needs to be discovered and investigated. Most of the research efforts are visions and discussions for the future study. However, it is critical to dedicate a focus group within the O-RAN Alliance community that engages the IoT research community to develop standards and specifications for O-RAN to IoT integration. After that, the yielded specifications will be helpful to the research on a theoretical foundation and analysis, modeling and simulation testbeds, among others.

4.1.2. Robust and Scalable Solutions

Realising robust, dynamic, and adaptive O-RAN-based IoT solutions that shrink or scale based on the operating environment requirements is hectic. This is because of the diverging QoS and reliability criteria to be satisfied by the emerging systems. For example, the systems are expected to scale either vertically or horizontally to accommodate the increasing number of connected devices and be equipped with efficient network management mechanisms for handling their dynamic resource allocation based on the demands of IoT applications.

Similarly, as the system complexity grows, the attack surface for potential security threats also increases. Conflicts may also emerge when the IoT devices employ incompatible communication protocols with the O-RAN architecture.

Scalability challenges may also arise when IoT systems need to ensure seamless cross-domain integration with legacy networks, cloud, or data centers. In addition, the vast amount of data generated will require scalable analytics to generate relevant insights that benefit the operating environment. The entire system lifecycle management strategies need to be scalably dynamic and efficient, starting from onboarding, provisioning, and firmware updates. Optimized communication protocols and mechanisms that extend the battery life of these devices will also be required. The system will need to handle a massive variety of new IoT device applications and services to be developed in the future. In other words,

resilient solutions that scale to the operating environment dynamics remain open for the research community to solve.

4.1.3. AI for O-RAN

AI can support the O-RAN network by enhancing its performance, efficiency, and adaptability. On the other hand, AI deployment in O-RAN is not free from challenges. As for the areas of support, with the intervention of the RIC, i.e., rApps/xApps, intelligence could be deployed in O-RAN to yield an efficient network-slicing method. This will dynamically slice the network to meet the needs of different IoT applications, enhance edge intelligence by offloading computation to the edge of the network, improving the performance and reducing the latency of IoT applications. It will also optimize resource allocation in the network (bandwidth, power, etc.), enhancing IoT application performance and reducing costs. Furthermore, it could orchestrate the deployment and operation of IoT applications across the network, ensuring that applications are deployed most efficiently to facilitate effective communication.

The challenges include data quality and availability, as AI models and algorithms require large amounts of data to train and learn. This is a challenge in O-RAN, as the data are distributed across multiple networks and devices. The quality of the data that are used as the input to train AI models and algorithms is essential for the accuracy of the results. The IoT data pipeline, especially for intelligent systems such as smart transportation, healthcare, energy, etc., is critical when integrating IoT with O-RAN. This is because the nature of data pipelines determines the quality of AI/ML model output and data analytic tools. However, the data used in O-RAN networks are sometimes noisy and unreliable. Distributed AI algorithms are primarily complex and computationally expensive to train and run. This can be a challenge for O-RAN-based networks, which are mostly resource-constrained.

Similarly, AI models and algorithms can be challenging to interpret, which makes it much more difficult to understand why they make certain decisions. This can be a challenge for O-RAN operators, who need to be able to trust the decisions made by AI models and algorithms. Finally, AI models and algorithms can be biased, leading to unfair or discriminatory results. These challenges need to be addressed for effective intelligence deployment in O-RAN networks.

4.1.4. Security and Privacy

O-RAN has a core networking infrastructure to support smart IoT systems, but the significance of the security and privacy of the system and its data cannot be overemphasized. There are inherent layer-wise IoT security and O-RAN privacy concerns, which can be transferred to the O-RAN for IoT systems. For instance, by launching denial of service (DoS) attacks on communication channels between the IoT system and O-RAN, adversaries can disrupt the network established by the network protocols and prevent communication between the two systems. Additionally, O-RAN, as a new architecture, opens an additional vulnerability interface, which has left the research community with questions such as the following: *What are the security vulnerabilities to be realized from the emerging system? How do we deal with such vulnerabilities to lead to trustworthy security of O-RAN systems for IoT applications?*

As evident from the previous sections, supporting IoT systems with O-RAN will yield several promising benefits in terms of automation, cost savings, and interoperability while increasing the system's attack surfaces, i.e., exposing the resulting system to several security threats that need to be taken care of to ensure the integrity, confidentiality, and availability of the connected devices and data. Considering the sensing unit, for example, adversaries can spoof the system to gain unauthorized access, thereby corrupting the data generated by the sensing unit with the aid of malicious codes, hardware Trojans, etc., or launch DoS/DDoS attacks by depleting the batteries of the narrow-band IoT sensing devices to make their services unavailable as well as acting as a man in the middle (MITM) between the industrial controllers among others.

The processing unit is responsible for cleaning, filtering, and aggregating the data generated using the networked edge/cloud computing infrastructure that can provision data-driven ML/AI models to assist system security. In this unit, the adversaries can launch attacks that hinder the integrity and availability of the generated data, for example, a jamming attack (damaging the data using irrelevant signals), a hijacking attack that renders the services unavailable, or a social engineering attack by misguiding the unit stakeholders.

The literature has recorded several attacks targeting the protocols, transmission channels, and standards used by the traditional communication unit. However, the O-RAN-based communication unit is exposed to new versions of attacks targeting each layer of the O-RAN setting. The non-RT-RIC guides and orchestrates the RAN using data-driven policies deployed on containerized rApps, while the N-RT-RIC executes the policies with the aid of the containerized xApps. Under openness in the system, adversaries can inject malicious codes into the rApps/xApps as a backdoor or adversarial examples to destabilize the system's operation by compromising the guiding data or the model. The existence of different xApps/rApps, as demonstrated in Figure 4, can result in several conflicts while achieving the interoperability goal. Adversaries can leverage this loophole to misconfigure and disrupt the decisions made by the operating apps or the radio resource management, for example, to degrade the system's performance or even trigger DoS attacks that will shut down the RIC. The disaggregated components (CU, DU, RU) serve as another attack target: network functions deployed on the cloud expose the system to internal and external attacks. On the path to enabling interoperability, the open interfaces expose the system to several threats like MITM, DoS, radio jamming, etc., which are targeted towards the different levels of communication units.

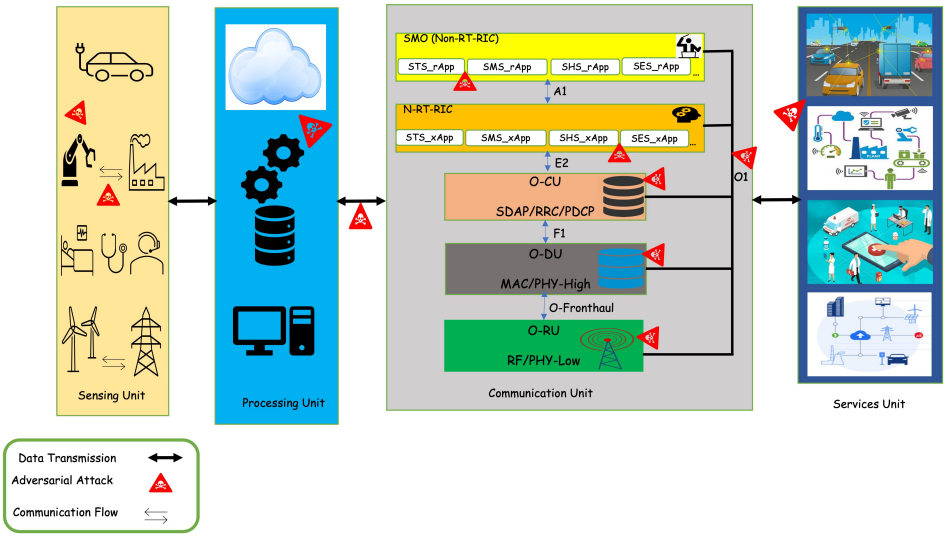

Figure 4. Attack spaces in O-RAN assisted IoT systems.

The services unit integrates the preceding processes from the previous units to yield an effective, efficient operating environment for the users. In this unit, adversaries could inject malicious scripts into the system to launch phishing attacks or even attempt to hijack the control unit's safe operation, rendering the system unavailable.

4.2. Future Research Directions

4.2.1. O-RAN for IoT Applications

Designing O-RAN that supports IoT applications effectively will involve considering scalability, flexibility, resource efficiency, and seamless integration with the diverse IoT devices and use cases, i.e., starting from scalable architectures that support low power, high data rates, and higher-performance devices to dynamic network slicing capabilities implemented in dedicated virtual networks for different IoT use cases where each slice is customized to meet specific IoT application requirements. Traffic models and analysis on

IoT applications can characterize the traffic generated by IoT applications and improve the efficacy of network resource management [88]. QoS differentiation mechanisms can prioritize critical IoT applications to allocate network resources accordingly, as well as robust security by design standards that protect IoT devices and data by enforcing continuous monitoring, authentication, encryption, and threat detection mechanisms tailored to IoT requirements. Seamless integration with edge computing infrastructures can enable real-time data processing and decision-making while reducing latency for time-sensitive IoT applications.

The development of standardized interfaces and protocols can promote interoperability among different devices, vendors, IoT applications, and energy-efficient communication protocols that boost the lifetime of the battery-powered devices, as well as facilitate cross-domain orchestration and communication. Dynamic frequency allocation mechanisms that optimize spectrum usage while minimizing interference among IoT devices will also be required, as will APIs and interfaces that enable third-party developers and IoT solution providers to innovate and integrate with O-RAN.

For O-RAN to remain relevant in supporting the next-generation IoT applications, the O-RAN concept should remain adaptable and evolving to meet the changing dynamics of IoT applications. This can only be achieved with continuous research and development involving collaboration among standardization bodies and industry technocrats to align O-RAN standards with emerging IoT standards to ensure seamless integration and compatibility.

As described in Section 2, O-RAN has defined standardized interfaces (eCPRI, Fronthaul, F1, O1, etc.) to promote flexibility and interoperability among cellular vendors for yielding lower operational and capital expenditures. In this context, with the aid of the network slicing concepts introduced by 5G, these interfaces, if standardized for IoT applications, could promote interoperability within and among IoT systems, just like in the case of the production line of a smart factory as demonstrated in [59] or the traffic steering process as depicted in [57].

Traditionally, IoT communications utilize short-range communication technologies such as BLE, GSM, Wi-Fi, ZigBee, etc. Recently, IoT connectivity has been extended to long-range, low-power WAN (LPWAN), such as LoRaWAN, NB-IoT, Sigfox, and LoRa. Integrating 5G networks with LPWAN technologies based on new architecture such as O-RAN will significantly improve IoT service use cases for industrial automation, smart cities, and other applications [89,90]. Note that how to effectively integrate O-RAN interfaces with IoT applications or implement IoT-specific protocols like the RFID, NB-IoT, LoRAWAN, etc., in O-RAN remain unsolved problems that require further research concerning system modeling, simulation, and empirical evaluations. Even though NB-IoT operates alongside the LTE in the same frequency band, it is evident that the next-generation IoT applications [91] have diverging QoS and reliability requirements that NB-IoT cannot directly satisfy, for instance, live-streaming video surveillance in smart cities or remote surgery in healthcare, which are both high-bandwidth and low-latency applications, or autonomous vehicles, which have stringent latency of 1 ms and high mobility requirements. NB-IoT is only ideal for supporting massive connectivity-intensive applications requiring data rates up to 254 kbps, which does not have mobility [92]. Among the feasible directions for addressing this issue will be dedicating a focus group within the O-RAN Alliance community which will engage both research and standardization communities to develop standards and specifications for enabling O-RAN as a viable network infrastructure to support IoT applications. After that, the yielded specifications could guide the research community's efforts towards developing theoretical foundation and analysis, modeling, and simulation testbeds, etc., until the interoperability and integration vision becomes a reality.

4.2.2. Security and Privacy in O-RAN

Dealing with security and privacy issues in O-RAN will require ongoing strategies involving continuous monitoring, assessment, and adaptation to evolving threats and regulations by implementing various measures and best practices to protect the network, devices, and data.

Starting from end-to-end encryption protocols, access control mechanisms, robust authentication and authorization strategies, network segmentation, intrusion detection, and prevention methods, based on Figure 4, it is clear that individual security and privacy enforcement strategies are ineffective for O-RAN and emerging IoT systems. There is a need for security and privacy by design principles, where security and privacy measures are integrated into the design and development of these systems right from the beginning. In this context, the emerging O-RAN-based IoT systems should integrate security and privacy-preserving features, mechanisms, and best practices throughout the system's entire lifecycle, from its conceptualization and design to its deployment and maintenance.

For example, at the initial stage, the system's threat surface should be identified and modeled to identify the potential security threats and vulnerabilities the system may face to guide the implementation of appropriate security controls. This will catalyze the realization of secured end-to-end architecture in the future that is designed with robust authentication mechanisms, access control strategies, and data encryption protocols to protect sensitive data and prevent unauthorized access. Incorporating secure communication protocols shall ensure data transmitted between IoT devices and the O-RAN network is encrypted and protected from interception. Also, the system should implement continuous monitoring mechanisms to detect and respond to security incidents in real time.

One example of the security and privacy by design principle is the zero-trust architecture (ZTA), where every player is considered an adversary unless verified to be proven otherwise. The approach necessitates the continuous authentication, authorization, and monitoring of every network stakeholder requesting or providing resources to enhance security and reduce the risk of data breaches by minimizing the attack surface and limiting lateral movement within the network [93]. According to some recent research works conducted by [94,95], the ZTA concept has been applied to secure several facets of safety-critical infrastructures. This includes communication networks and O-RAN on the one hand [95–97] and the different IoT domains on the other [98–101]. However, as is obvious from Figure 4, there is a need to develop ZTA to preserve the security and privacy of O-RAN-based IoT systems. Likewise, the open capability of O-RAN interfaces and the heterogeneous nature of IoT provide opportunities for malicious actors [102].

One of the leading security groups, namely, the O-RAN Alliance Security Work Group, is continuously investigating the security challenges and defining O-RAN security solutions [103]. Among the feasible directions for overcoming this is the zero trust architecture (ZTA), which is currently on course for its standardization by the security focus group of the O-RAN Alliance community. To summarize, a body of mechanisms concerning security resilient design, AI-empowered threat detection and recognition, response, and recovery, considering the performance requirements of IoT applications, should be systematically studied. To this end, developing the integrated modeling, analysis, simulation, emulation, and testbed-based evaluation study should be carried out. In this way, systematically understanding the foundational capability and limitation of threats and the ability of defense schemes in the context of O-RAN enable IoT systems should be investigated.

4.2.3. Explainable AI for IoT and O-RAN Integration

One critical problem governing AI models and algorithms in AI-based O-RAN decision making requires transparency. This causes difficulties for network operators in identifying issues and root causes and further controlling the network with desired behaviors. Consequently, incorporating XAI into the O-RAN system management operations process to learn how AI/ML models and algorithms make decisions and find ways to validate them. Thus, to explain their outputs explicitly, running AI-based rApps/xApps

should contain XAI approaches. This would enhance the accuracy and openness of outcomes made by these systems and the network operators optimize the functionalities of networks, leading to efficient network operations and services to IoT applications. For instance, rApps/xApps can be developed with large language model (LLM) capabilities to provide on-demand and real-time feedback to IoT systems.

Developing a naturalistic AI solution for O-RAN will involve integrating natural language understanding and generation capabilities with O-RAN infrastructure to enhance network management, troubleshooting, and communication. This will make it easier for network administrators to interact with complex networking infrastructures using natural language and improve network operations' responsiveness and accuracy. Several factors shall be considered before bringing such solutions to fruition [104].

4.2.4. Standardization Research and Development

Despite the challenges, the reviewed efforts presented in Section 3 can be regarded as preliminary results supporting the feasibility of integrating the O-RAN concept into IoT architecture to support the next-generation IoT systems. However, there is a need for collaborative efforts in this direction from academia, industries, and all the relevant bodies involved in transitioning these visionary ideas into reality. This can be achieved by establishing a collaborative IoT ecosystem housing device manufacturers, solution developers, and focus groups dedicated to IoT within the O-RAN Alliance community to focus on IoT-related standards, use cases, and best practices.

Similarly, research and development should be geared toward simulation tools and testbeds to motivate proof of concept developments and validation before deployments. Some efforts have been recorded in this direction, which led to the development of an *"open-ran gym"* [37] for end-to-end or comprehensive design and testing of data-driven xApps, *"ns-O-RAN"* [105] for simulating O-RAN solutions in ns-3 [106], and *"NS3-O-RAN"* [107] for simulating O-RAN-based AI/ML solutions in ns-3, etc. These efforts primarily focused on the O-RAN concept. There needs to be more effort to develop testing/validation tools for O-RAN-based IoT systems.

Finally, investments in training programs to develop a skilled workforce capable of designing, deploying, and managing O-RAN networks should be encouraged in all facets of teaching and learning. This should include formal and informal training on technical aspects and best practices.

5. Final Remarks

IoT systems consist of physical devices and various objects connected and integrated with monitoring and control capabilities, which can be applied to numerous critical infrastructure systems in energy, transportation, and cities, among others. With the advancement of information communication technology, IoT systems can be enabled by sensors/actuators and other enabling technologies, which support data collection and exchange and derive intelligent decisions to guide their operations based on the collected data via viable data science and machine learning technologies. The advancements in cellular networks, i.e., 5G and beyond, have enabled these systems to achieve their required connectivity. However, their reliability and QoS across various pervasive domains require more effective, economical, and adequate solutions.

In this paper, we have investigated the applications of O-RAN in this context by conducting a literature survey to determine how openness in the RAN, as a critical networking infrastructure, can support the next-generation IoT systems. This research proposes a problem space covering IoT systems: transportation, industry, healthcare, and energy; targets; reliable communication, real-time analytics, fault tolerance, interoperability and integration, and AI/ML; and RL and DNNs. We have outlined several challenges militating against integrating these concepts and future research directions guiding how to design O-RAN for IoT applications and deal with emerging security and privacy issues, natural AI solutions in O-RAN, and finally, the standardization, research, and development efforts required in

the forthcoming years. In the future, we plan to extend this research by investigating the feasible simulation tools, experimental testbeds, and other supporting technologies that could be leveraged to transform the interoperability and integration (Y_4) vision into fruition, as well as the systematical exploration of threats and the design of countermeasures to deal with the security and privacy (Y_3) of the emerging O-RAN-based IoT system.

Funding: This research received no external funding.

Data Availability Statement: Not applicable, the study does not report any data.

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

References

1. Madakam, S. Internet of things: Smart things. *Int. J. Future Comput. Commun.* **2015**, *4*, 250. [CrossRef]
2. Sheth, A. Internet of things to smart iot through semantic, cognitive, and perceptual computing. *IEEE Intell. Syst.* **2016**, *31*, 108–112. [CrossRef]
3. García, L.; Parra, L.; Jimenez, J.M.; Lloret, J.; Lorenz, P. IoT-based smart irrigation systems: An overview on the recent trends on sensors and IoT systems for irrigation in precision agriculture. *Sensors* **2020**, *20*, 1042. [CrossRef]
4. Hussaini, A.; Qian, C.; Guo, Y.; Lu, C.; Yu, W. Digital Twins of Smart Campus: Performance Evaluation Using Machine Learning Analysis. In Proceedings of the 2023 IEEE/ACIS 21st International Conference on Software Engineering Research, Management and Applications (SERA), Orlando, FL, USA, 23–25 May 2023; pp. 132–137.
5. Abdulhamid, A.; Kabir, S.; Ghafir, I.; Lei, C. An Overview of Safety and Security Analysis Frameworks for the Internet of Things. *Electronics* **2023**, *12*, 3086. [CrossRef]
6. Liang, F.; Yu, W.; Liu, X.; Griffith, D.; Golmie, N. Toward Edge-Based Deep Learning in Industrial Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 4329–4341. [CrossRef]
7. Liang, F.; Hatcher, W.G.; Liao, W.; Gao, W.; Yu, W. Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly. *IEEE Access* **2019**, *7*, 158126–158147. [CrossRef]
8. Liu, X.; Qian, C.; Hatcher, W.G.; Xu, H.; Liao, W.; Yu, W. Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities. *IEEE Access* **2019**, *7*, 79523–79544. [CrossRef]
9. Wang, J.; Varshney, N.; Gentile, C.; Blandino, S.; Chuang, J.; Golmie, N. Integrated Sensing and Communication: Enabling Techniques, Applications, Tools and Data Sets, Standardization, and Future Directions. *IEEE Internet Things J.* **2022**, *9*, 23416–23440. [CrossRef]
10. Xu, H.; Liu, X.; Yu, W.; Griffith, D.; Golmie, N. Reinforcement Learning-Based Control and Networking Co-Design for Industrial Internet of Things. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 885–898. [CrossRef]
11. Bui, N.; Castellani, A.P.; Casari, P.; Zorzi, M. The internet of energy: A web-enabled smart grid system. *IEEE Netw.* **2012**, *26*, 39–45. [CrossRef]
12. Xu, G.; Yu, W.; Griffith, D.; Golmie, N.; Moulema, P. Toward Integrating Distributed Energy Resources and Storage Devices in Smart Grid. *IEEE Internet Things J.* **2017**, *4*, 192–204. [CrossRef]
13. Muthuramalingam, S.; Bharathi, A.; Rakesh Kumar, S.; Gayathri, N.; Sathiyaraj, R.; Balamurugan, B. IoT based intelligent transportation system (IoT-ITS) for global perspective: A case study. In *Internet of Things and Big Data Analytics for Smart Generation*; Springer: Cham, Switzerland, 2019; pp. 279–300.
14. Liu, X.; Yu, W.; Qian, C.; Griffith, D.; Golmie, N. Integrated Simulation Platform for Internet of Vehicles. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 2756–2761. [CrossRef]
15. 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] [PubMed]
16. Qian, C.; Yu, W.; Lu, C.; Griffith, D.; Golmie, N. Toward Generative Adversarial Networks for the Industrial Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 19147–19159. [CrossRef]
17. Darshan, K.; Anandakumar, K. A comprehensive review on usage of Internet of Things (IoT) in healthcare system. In Proceedings of the 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, India, 17–19 December 2015; pp. 132–136.
18. 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]
19. Singh, M.; Baranwal, G. Quality of Service (QoS) in Internet of Things. In Proceedings of the 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 23–24 February 2018; pp. 1–6. [CrossRef]
20. Keertikumar, M.; Shubham, M.; Banakar, R. Evolution of IoT in smart vehicles: An overview. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 8–10 October 2015; pp. 804–809.
21. Cano, J.C.; Berrios, V.; Garcia, B.; Toh, C.K. Evolution of IoT: An industry perspective. *IEEE Internet Things Mag.* **2018**, *1*, 12–17. [CrossRef]
22. Pradhan, B.; Bhattacharyya, S.; Pal, K. IoT-based applications in healthcare devices. *J. Healthc. Eng.* **2021**, *2021*, 1–18. [CrossRef]

23. Adhikari, M.; Hazra, A. 6G-enabled ultra-reliable low-latency communication in edge networks. *IEEE Commun. Stand. Mag.* **2022**, *6*, 67–74. [CrossRef]
24. Pongratz, S. Advanced Research Reports on Open RAN. 2023. Available online: https://www.delloro.com/advanced-research-report/openran/ (accessed on 22 April 2023).
25. Alleven, M. Open RAN to reach 15–20% of total market by 2027: Dell'Oro. 2023. Available online: https://www.fiercewireless.com/tech/open-ran-reach-15-20-total-market-2027-delloro (accessed on 24 April 2023).
26. Bonati, L.; Polese, M.; D'Oro, S.; Basagni, S.; Melodia, T. Open, programmable, and virtualized 5G networks: State-of-the-art and the road ahead. *Comput. Netw.* **2020**, *182*, 107516. [CrossRef]
27. Haavisto, J.; Arif, M.; Lovén, L.; Leppänen, T.; Riekki, J. Open-source RANs in Practice: An Over-the-air Deployment for 5G MEC. In Proceedings of the 2019 European Conference on Networks and Communications (EuCNC), Valencia, Spain, 18–21 June 2019; pp. 495–500.
28. Bonati, L.; D'Oro, S.; Polese, M.; Basagni, S.; Melodia, T. Intelligence and learning in O-RAN for data-driven NextG cellular networks. *IEEE Commun. Mag.* **2021**, *59*, 21–27. [CrossRef]
29. Ojaghi, B.; Adelantado, F.; Verikoukis, C. On the benefits of vdu standardization in softwarized ng-ran: Enabling technologies, challenges, and opportunities. *IEEE Commun. Mag.* **2023**, *61*, 92–98. [CrossRef]
30. Barakabitze, A.A.; Ahmad, A.; Mijumbi, R.; Hines, A. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Comput. Netw.* **2020**, *167*, 106984. [CrossRef]
31. Polese, M.; Bonati, L.; D'Oro, S.; Basagni, S.; Melodia, T. Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1376–1411. [CrossRef]
32. RAN. O-RAN Alliance. 2018. Available online: https://www.o-ran.org/ (accessed on 28 July 2023).
33. Singh, S.K.; Singh, R.; Kumbhani, B. The evolution of radio access network towards open-ran: Challenges and opportunities. In Proceedings of the 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Seoul, Rublic of Korea, 6–9 April 2020; pp. 1–6.
34. Abedin, S.F.; Mahmood, A.; Tran, N.H.; Han, Z.; Gidlund, M. Elastic O-RAN slicing for industrial monitoring and control: A distributed matching game and deep reinforcement learning approach. *IEEE Trans. Veh. Technol.* **2022**, *71*, 10808–10822. [CrossRef]
35. Firouzi, R.; Rahmani, R. 5G-Enabled Distributed Intelligence Based on O-RAN for Distributed IoT Systems. *Sensors* **2022**, *23*, 133. [CrossRef] [PubMed]
36. Wang, L.; Zhou, J.; Wang, Y.; Lei, B. Energy Conserved Computation Offloading for O-RAN based IoT systems. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Repulic of Korea, 16–20 May 2022; pp. 4043–4048.
37. Bonati, L.; Polese, M.; D'Oro, S.; Basagni, S.; Melodia, T. OpenRAN Gym: AI/ML development, data collection, and testing for O-RAN on PAWR platforms. *Comput. Netw.* **2023**, *220*, 109502. [CrossRef]
38. Wypiór, D.; Klinkowski, M.; Michalski, I. Open ran—radio access network evolution, benefits and market trends. *Appl. Sci.* **2022**, *12*, 408. [CrossRef]
39. D'Oro, S.; Polese, M.; Bonati, L.; Cheng, H.; Melodia, T. dapps: Distributed applications for real-time inference and control in o-ran. *IEEE Commun. Mag.* **2022**, *60*, 52–58. [CrossRef]
40. Ko, W.H.; Dinesha, U.; Ghosh, U.; Shakkottai, S.; Bharadia, D.; Wu, R. EdgeRIC: Empowering Realtime Intelligent Optimization and Control in NextG Networks. *arXiv* **2023**, arXiv:2304.11199.
41. Hatcher, W.G.; Yu, W. A survey of deep learning: Platforms, applications and emerging research trends. *IEEE Access* **2018**, *6*, 24411–24432. [CrossRef]
42. Wang, J.; Varshney, N.; Zhang, J.; Griffith, D.; Golmie, N. Deep Learning Based Link-Level Abstraction for mmWave Communications. In Proceedings of the 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI), Atlanta, GA, USA, 18–21 October 2021; pp. 391–398. [CrossRef]
43. Liu, X.; Xu, H.; Liao, W.; Yu, W. Reinforcement Learning for Cyber–Physical Systems. In Proceedings of the 2019 IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA, 11–12 November 2019; pp. 318–327. [CrossRef]
44. Li, P.; Thomas, J.; Wang, X.; Khalil, A.; Ahmad, A.; Inacio, R.; Kapoor, S.; Parekh, A.; Doufexi, A.; Shojaeifard, A.; et al. Rlops: Development life-cycle of reinforcement learning aided open ran. *IEEE Access* **2022**, *10*, 113808–113826. [CrossRef]
45. Liang, F.; Qian, C.; Yu, W.; Griffith, D.; Golmie, N. Survey of Graph Neural Networks and Applications. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9261537. [CrossRef]
46. Brik, B.; Boutiba, K.; Ksentini, A. Deep learning for B5G open radio access network: Evolution, survey, case studies, and challenges. *IEEE Open J. Commun. Soc.* **2022**, *3*, 228–250. [CrossRef]
47. Musa, A.A.; Hussaini, A.; Liao, W.; Liang, F.; Yu, W. Deep Neural Networks for Spatial-Temporal Cyber–Physical Systems: A Survey. *Future Internet* **2023**, *15*, 199. [CrossRef]
48. Pham, C.; Fami, F.; Nguyen, K.K.; Cheriet, M. When RAN intelligent controller in O-RAN meets multi-UAV enable wireless network. *IEEE Trans. Cloud Comput.* **2022**, *11*, 2245–2259. [CrossRef]
49. Pham, C.; Nguyen, K.K.; Cheriet, M. Joint optimization of UAV trajectory and task allocation for wireless sensor network based on O-RAN architecture. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 329–334.

50. Riccio, E.L.; Mangipudi, P.K.; McNair, J. O-RAN Signaling Optimizations for Improved IoT Handover Performance in 5G Networks. In Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation, San Antonio, TX, USA, 9–12 May 2023; pp. 454–455.
51. LinI, B.S.P. Toward an AI-enabled O-RAN-based and SDN/NFV-driven 5G& IoT network era. *Netw. Commun. Technol.* **2021**, *6*, 6.
52. Liu, Q.; Han, T.; Ansari, N. Learning-assisted secure end-to-end network slicing for cyber–physical systems. *IEEE Netw.* **2020**, *34*, 37–43. [CrossRef]
53. Kougioumzidis, G.; Vlahov, A.; Poulkov, V.; Zaharis, Z.; Lazaridis, P. QoE-Oriented Open Radio Access Networks for Virtual Reality Applications. In Proceedings of the 2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC), Herning, Denmark, 30 October–2 November 2022; pp. 491–496.
54. Vilà, I.; Sallent, O.; Pérez-Romero, J. On the Design of a Network Digital Twin for the Radio Access Network in 5G and Beyond. *Sensors* **2023**, *23*, 1197. [CrossRef]
55. Masaracchia, A.; Sharma, V.; Fahim, M.; Dobre, O.A.; Duong, T.Q. Digital Twin for Open RAN: Towards Intelligent and Resilient 6G Radio Access Networks. *IEEE Commun. Mag.* **2023**. [CrossRef]
56. Liyanage, M.; Braeken, A.; Shahabuddin, S.; Ranaweera, P. Open RAN security: Challenges and opportunities. *J. Netw. Comput. Appl.* **2023**, *214*, 103621. [CrossRef]
57. Bitton, R.; Avraham, D.; Klevansky, E.; Mimran, D.; Brodt, O.; Lehmann, H.; Elovici, Y.; Shabtai, A. Adversarial machine learning threat analysis in open radio access networks. *arXiv* **2022**, arXiv:2201.06093.
58. Abdalla, A.S.; Upadhyaya, P.S.; Shah, V.K.; Marojevic, V. Toward next generation open radio access networks: What O-RAN can and cannot do! *IEEE Netw.* **2022**, *36*, 206–213. [CrossRef]
59. Wu, Y.; Dai, H.N.; Wang, H.; Xiong, Z.; Guo, S. A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1175–1211. [CrossRef]
60. Linsalata, F.; Moro, E.; Magarini, M.; Spagnolini, U.; Capone, A. Open RAN-empowered V2X Architecture: Challenges, Opportunities, and Research Directions. *arXiv* **2023**, arXiv:2303.06938.
61. Mongay Batalla, J.; Moshin, M.; Mavromoustakis, C.X.; Wesołowski, K.; Mastorakis, G.; Krzykowska-Piotrowska, K. On Deploying the Internet of Energy with 5G Open RAN Technology including Beamforming Mechanism. *Energies* **2022**, *15*, 2429. [CrossRef]
62. de Oliveira, W.; Batista Jr, J.O.R.; Novais, T.; Takashima, S.T.; Stange, L.R.; Martucci Jr, M.; Cugnasca, C.E.; Bressan, G. OpenCare5G: O-RAN in private network for digital health applications. *Sensors* **2023**, *23*, 1047. [CrossRef]
63. Huang, Y.K.; Pang, A.C.; Wu, J.M. An Edge Intelligent Framework for O-RAN based IoV Networks. In Proceedings of the 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Virtual Online, 27 September–28 October 2021; pp. 1–5.
64. Ndikumana, A.; Nguyen, K.K.; Cheriet, M. Age of processing-based data offloading for autonomous vehicles in MultiRATs Open RAN. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 21450–21464. [CrossRef]
65. Hoffmann, M.; Kryszkiewicz, P. Signaling Storm Detection in IIoT Network based on the Open RAN Architecture. *arXiv* **2023** arXiv:2302.08239.
66. Tselikis, C. Automated and Secure Control of Industrial Internet of Things: From WSN to Open RAN Solutions. In Proceedings of the 2023 International Wireless Communications and Mobile Computing (IWCMC), Marrakesh, Morocco, 19–23 June 2023; pp. 556–561.
67. Rahman, T.F.; Zhang, M.; Marojevic, V. O-RAN Perspective on Industrial Internet of Things: A SWOT Analysis. In Proceedings of the 2023 IEEE International Conference on Industrial Technology (ICIT), Orlando, FL, USA, 4–6 April 2023.
68. Moulema, P.; Yu, W.; Xu, G.; Griffith, D.; Golmie, N.; Lu, C.; Su, D. On Simulation Study of Mesh-Based Protocols for Smart Grid Communication Networks. In Proceedings of the 2013 Research in Adaptive and Convergent Systems, Montreal, QC, Canada, 1–4 October 2013; Association for Computing Machinery: New York, NY, USA, 2013; pp. 202–207. [CrossRef]
69. Njoku, J.N.; Nwakanma, C.I.; Amaizu, G.C.; Kim, D.S. Prospects and challenges of Metaverse application in data-driven intelligent transportation systems. *IET Intell. Transp. Syst.* **2023**, *17*, 1–21. [CrossRef]
70. She, C.; Popovski, P.; Bennis, M. *Ultra-Reliable and Low-Latency Communications (URLLC) Theory and Practice*; Wiley: Hoboken, NJ, USA, 2023.
71. Mamane, A.; Fattah, M.; El Ghazi, M.; El Bekkali, M. 5G enhanced mobile broadband multi-criteria scheduler for dense urban scenario. *Telecommun. Syst.* **2022**, *80*, 33–43. [CrossRef]
72. Yang, B.; Wei, F.; She, X.; Jiang, Z.; Zhu, J.; Chen, P.; Wang, J. Intelligent Random Access for Massive–Machine Type Communications in Sliced Mobile Networks. *Electronics* **2023**, *12*, 329. [CrossRef]
73. Gohar, A.; Nencioni, G. The role of 5G technologies in a smart city: The case for intelligent transportation system. *Sustainability* **2021**, *13*, 5188. [CrossRef]
74. Hammami, N.; Nguyen, K.K. Multi-agent actor–critic for cooperative resource allocation in vehicular networks. In Proceedings of the 2022 14th IFIP Wireless and Mobile Networking Conference (WMNC), Sousse, Tunisia, 17–19 October 2022; pp. 93–100.
75. Liu, L.; Zhao, M.; Yu, M.; Jan, M.A.; Lan, D.; Taherkordi, A. Mobility-aware multi-hop task offloading for autonomous driving in vehicular edge computing and networks. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 2169–2182. [CrossRef]
76. Abolhasan, M.; Lipman, J.; Shariati, N.; Ni, W.; Jamalipour, A.; Ashtari, S. Joint Mobile Node Participation and Multihop Routing for Emerging Open Radio-Based Intelligent Transportation System. *IEEE Access* **2022**, *10*, 85228–85242.

77. Zahran, B.; Hussaini, A.; Ali-Gombe, A. IIoT-ARAS: IIoT/ICS Automated risk assessment system for prediction and prevention. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, Virtual, 26–28 April 2021; pp. 305–307.
78. Cheng, J.; Chen, W.; Tao, F.; Lin, C.L. Industrial IoT in 5G environment towards smart manufacturing. *J. Ind. Inf. Integr.* **2018**, *10*, 10–19. [CrossRef]
79. 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]
80. Longo, F.; Padovano, A.; Aiello, G.; Fusto, C.; Certa, A. How 5G-based industrial IoT is transforming human-centered smart factories: A Quality of Experience model for Operator 4.0 applications. *IFAC-PapersOnLine* **2021**, *54*, 255–262. [CrossRef]
81. Lin, S.C.; Lin, C.H.; Chen, W.C. Zero-Touch Network on Industrial IoT: An End-to-End Machine Learning Approach. *arXiv* **2022**, arXiv:2204.12605.
82. Dang, V.A.; Vu Khanh, Q.; Nguyen, V.H.; Nguyen, T.; Nguyen, D.C. Intelligent Healthcare: Integration of Emerging Technologies and Internet of Things for Humanity. *Sensors* **2023**, *23*, 4200. [CrossRef] [PubMed]
83. Trifonov, V.; Atanasov, I.; Pencheva, E. Artificial Intelligence in Open Radio Access Network: Use Case of Internet of Medical Things. In Proceedings of the 2021 International Conference on Biomedical Innovations and Applications (BIA), Varna, Bulgaria, 2–4 June 2022; Volume 1, pp. 5–8.
84. Ghiasi, M.; Wang, Z.; Mehrandezh, M.; Jalilian, S.; Ghadimi, N. Evolution of smart grids towards the Internet of energy: Concept and essential components for deep decarbonisation. *IET Smart Grid* **2023**, *6*, 86–102. [CrossRef]
85. Kundacina, O.; Forcan, M.; Cosovic, M.; Raca, D.; Dzaferagic, M.; Miskovic, D.; Maksimovic, M.; Vukobratovic, D. Near Real-Time Distributed State Estimation via AI/ML-Empowered 5G Networks. In Proceedings of the 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Singapore, 25–28 October 2022; pp. 284–289.
86. Wang, L.; Zhou, J.; Ma, M.; Niu, X. Minimizing energy consumption of IoT devices for O-RAN based IoT systems. *Energy Rep.* **2023**, *9*, 379–388. [CrossRef]
87. RAN. O-RAN Alliance. 2023. Available online: https://www.o-ran.org/about#technical-workgroup/ (accessed on 4 September 2023)
88. Wu, Y.; Cui, Y.; Yu, W.; Lu, C.; Zhao, W. Modeling and Forecasting of Timescale Network Traffic Dynamics in M2M Communications. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–9 July 2019; pp. 711–721. [CrossRef]
89. Ogbodo, E.U.; Abu-Mahfouz, A.M.; Kurien, A.M. A survey on 5G and LPWAN-IoT for improved smart cities and remote area applications: From the aspect of architecture and security. *Sensors* **2022**, *22*, 6313. [CrossRef] [PubMed]
90. Muteba, K.; Djouani, K.; Olwal, T. 5G NB-IoT: Design, considerations, solutions and challenges. *Procedia Comput. Sci.* **2022**, *198*, 86–93. [CrossRef]
91. Qadir, Z.; Le, K.N.; Saeed, N.; Munawar, H.S. Towards 6G Internet of Things: Recent advances, use cases, and open challenges. *ICT Express* **2023**, *9*, 296–312. [CrossRef]
92. Moges, T.H.; Lakew, D.S.; Nguyen, N.P.; Dao, N.N.; Cho, S. Cellular Internet of Things: Use cases, technologies, and future work. *Internet Things* **2023**, *24*, 100910. [CrossRef]
93. Stafford, V. Zero trust architecture. *NIST Spec. Publ.* **2020**, *800*, 207.
94. Aryal, N.; Bertin, E.; Crespi, N. Open Radio Access Network challenges for Next Generation Mobile Network. In Proceedings of the 2023 26th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 6–9 March 2023; pp. 90–94.
95. Groen, J.; DOro, S.; Demir, U.; Bonati, L.; Polese, M.; Melodia, T.; Chowdhury, K. Implementing and Evaluating Security in O-RAN: Interfaces, Intelligence, and Platforms. *arXiv* **2023**, arXiv:2304.11125.
96. Ramezanpour, K.; Jagannath, J. Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Comput. Netw.* **2022**, *217*, 109358. [CrossRef]
97. Sedjelmaci, H.; Tourki, K. A Distributed Zero Trust Framework for 6G RAN. In Proceedings of the NOMS 2023–2023 IEEE/IFIP Network Operations and Management Symposium, Paris, France, 7–9 March 2023; pp. 1–5.
98. Kondaveety, V.B.; Lamkuche, H.; Prasad, S. A zero trust architecture for next generation automobiles. In *AIP Conference Proceedings*; AIP Publishing: College Park, ML, USA, 2022; Volume 2519.
99. Federici, F.; Martintoni, D.; Senni, V. A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. *Electronics* **2023**, *12*, 566. [CrossRef]
100. Wu, K.; Cheng, R.; Xu, H.; Tong, J. Design and Implementation of the Zero Trust Model in the Power Internet of Things. *Int. Trans. Electr. Energy Syst.* **2023**, *2023*, 6545323. [CrossRef]
101. Tyler, D.; Viana, T. Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. *Appl. Sci.* **2021**, *11*, 7499. [CrossRef]
102. Arnaz, A.; Lipman, J.; Abolhasan, M.; Hiltunen, M. Towards integrating intelligence and programmability in open radio access networks: A comprehensive survey. *IEEE Access* **2022**. [CrossRef]

103. Amy, Z.; Sébastien, J. The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components. 2023. Available online: https://www.o-ran.org/blog/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components/ (accessed on 6 November 2023).
104. Brik, B.; Chergui, H.; Zanzi, L.; Devoti, F.; Ksentini, A.; Siddiqui, M.S.; Costa-Pérez, X.; Verikoukis, C. A survey on explainable AI for 6G O-RAN: Architecture, use cases, challenges and research directions. *arXiv* **2023**, arXiv:2307.00319.
105. Lacava, A.; Bordin, M.; Polese, M.; Sivaraj, R.; Zugno, T.; Cuomo, F.; Melodia, T. ns-O-RAN: Simulating O-RAN 5G Systems in ns-3. *arXiv* **2023**, arXiv:2305.06906.
106. Riley, G.F.; Henderson, T.R. The ns-3 network simulator. In *Modeling and Tools for Network Simulation*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 15–34.
107. Garey, W.; Ropitault, T.; Rouil, R.; Black, E.; Gao, W. O-RAN with Machine Learning in ns-3. In Proceedings of the 2023 Workshop on ns-3, Washington, DC, USA, 28–29 June 2023; pp. 60–68.