Review

Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review

Akseer Ali Mirani [1,2]*, Gustavo Velasco-Hernandez [1,3]*, Anshul Awasthi [1,2] and Joseph Walsh [1,2,3]

[1] IMaR Research Centre, Munster Technological University, Tralee, Ireland, V92 CX88
[2] CONFIRM Research Centre, Unit 2 Park Point, Dublin Road, Castletroy, Limerick, Ireland, V94 C928
[3] Lero, The Irish Software Research Centre, Tierney Building, University of Limerick, Ireland, V94 NYD3
* Correspondence: akseer.ali.mirani@research.ittralee.ie (A.M.), gustavo.velascohernandez@mtu.ie (G.V.)

Abstract: The Industrial Internet of Things (IIoT) is bringing evolution with remote monitoring, intelligent analytics, and control of industrial processes. A reference architecture provides the general layout information for the flexible integration of IIoT systems; however, as the industrial world is currently in its initial stage of adopting the full-stack development solutions with IIoT, some challenges need to be addressed. To cope with the rising challenges and provide the blueprint guidelines to develop and implement IIoT in real-time, researchers around the globe have proposed IIoT architectures based on different architectural layers and emerging technologies. In this paper, we first review and compare some widely accepted IIoT reference architectures and present a state-of-the-art review of conceptual and experimental IIoT architectures in literature. We highlight scalability, interoperability, security, privacy, reliability, and low latency as the main IIoT architectural requirements and compare how the current architectures address these challenges. We also highlight the role of emerging technologies in current IIoT architectures to address these requirements and present the literature gap for future research work to address the challenges.

Keywords: blockchain; Edge/Fog computing; IIoT architectures; Industry 4.0; interoperability; low latency; reliability; scalability; security; Software-Defined Networking

1. Introduction

Internet of Things (IoT) has brought a revolution in the current century by enabling ubiquitous and exponential connectivity of billions of devices and accessing them from any place at any time [1]. The initial concept of IoT to be the connection between people and things, between things, or between unforeseen things, was given by International Telecommunication Union (ITU) in its report in 2005 [2]. As the IoT's ability to connect real-world applications is achieving smart objectives without human involvement [3], Industrial IoT is further bringing the evolution in the manufacturing process by withstanding the mission-critical requirements [4]. IIoT is helping the industries by increasing operational efficiency with the convergence of Information Technology (IT) and Operational Technology (OT) [5]. The new era of the Fourth Industrial Revolution (Industry 4.0) is further bringing paradigm shifts with the integration of IIoT and Cyber-Physical Systems (CPS) to provide insights for the collaborative work of intelligent devices [6]. While Industry 4.0 applies to any industry to provide self-optimization, better decisions from advanced sensors, production quality, and predictive maintenance for minimizing the system downtime [7], CPS integrates the networking, sensing, and computational features with physical systems to learn and adapt themselves [8]. The convergence of IoT, IIoT, and CPS forms the Industry 4.0 component as shown in figure 1.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2022 doi:10.20944/preprints202207.0022.v1

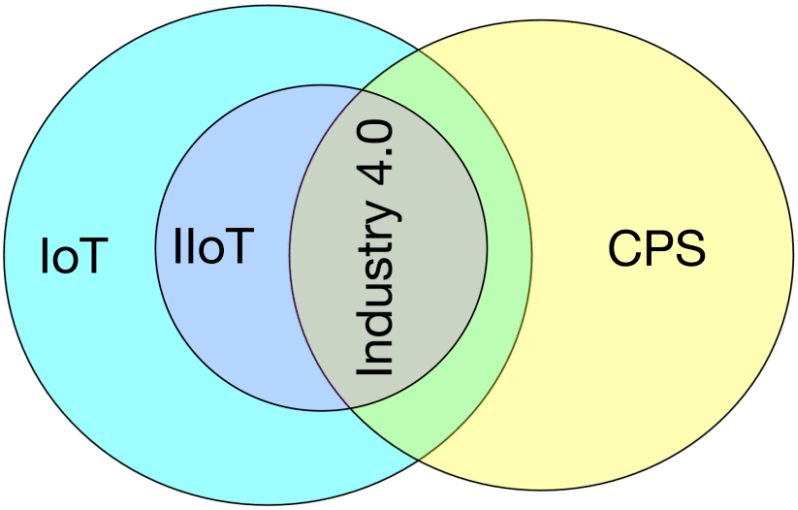

Figure 1. Relation between IoT, IIoT, CPS, and Industry 4.0 (adapted from [9])

As with the rapid technological advancements and higher expectations from IIoT than IoT, IIoT is dealing with challenges in its end-to-end development [9,10]. IoT is a revolution, but IIoT is an evolution in the modern world with machine-oriented features and stringent requirements of reliability, scalability, interoperability, and security than IoT. Table 1 shows the difference between IoT and IIoT. For the end-to-end development of IIoT systems, different reference architectures such as Reference Architectural Model Industrie 4.0 (RAMI 4.0) [11], Industrial Internet Reference Architecture (IIRA) [12], and OpenFog Reference Architecture [13] provide the blueprint guidelines containing the set of architectural layers from sensors to the enterprise management features. Moreover, IIoT architectures composed of different layers are present in the literature to address the challenges and for the flexible integration, management, and control of collaborative services [14]. While the reference architectures provide the general layout for the development process without any fixed support of protocols and standards [13], the IIoT architectures present in the literature address the specific challenges, either in a particular use case in industry or the general-purpose industrial use. The proposed solutions in the literature share some attributes of using emergent technologies to develop layered architectures.

Table 1. Main differences between IoT and IIoT [4,9,15]

Features	IoT	IIoT
Impact	Revolution	Evolution
Service Model	Human-oriented	Machine Specific
Status	Focused on new standards	Utilization of existing standards
Network Connectivity	Ad-Hoc	Structured
Data Generation	Data handling from medium to high	Very high volume of data
Area of Interest	General Applications e.g. wearables	Industrial Applications e.g. production, manufacturing, maintenance
Scalability	Low scalability	High Scalability
Interoperability	Independent	Highly required
Security	Less critical except few applications	Very critical
Life-cycle	Shorter product life-cycle	Longer product life-cycle
Reliability	Less reliable	High reliability
Programming	Off-site programming	Remote on-site programming

In this paper, we provide a state-of-the-art review on IIoT architectures, comparing some widely accepted IIoT reference architectures and detailing on proposed architectures

 doi:10.20944/preprints202207.0022.v1

in literature, the key challenges in their adoption and the role of emergent technologies in addressing these challenges. The rest of the paper is structured as follows: Section 2 presents the review and comparison of RAMI 4.0, IIRA, and OpenFog reference architectures. In Section 3, we identify the main IIoT requirements for its end-to-end development from the factory floor to the enterprise services, the emerging technologies used in IIoT architectural papers for presenting the solutions and addressing the challenges, and current research on IIoT architectures. Section 4 identifies how the conceptual and experimental architectures address these challenges, the relation of emerging technologies to IIoT requirements, and the scope of literature in addressing these requirements and using the emerging technologies. In Section 5, we summarise the findings and identify the potential research directions to address the challenges.

2. Industrial IoT Reference Architectures

A reference architecture provides the minimum functional requirements for a common ground to develop and analyze the systems [16]. The reference architectures in IIoT are independent of specific technologies and standards [13]. It provides the structural guidelines for the multiple aspects of a system, including the standard networking model for the interaction with devices and sensors. It also provides the cloud architecture services for the remote monitoring and management features and the information on what hardware components the architecture support [17]. Experts from different organizations have proposed reference architectures to provide the necessary structure and transform the manufacturing process in industries based on the available technologies [18]. Three of the main IIoT reference architectures are RAMI 4.0, IIRA, and OpenFog RA, which are detailed below.

2.1. Reference Architectural Model Industrie 4.0 (RAMI 4.0)

Reference Architecture Model for Industrie 4.0 (RAMI 4.0) was developed in Germany to modernize the manufacturing process and industrial automation with the standardization of DIN SPEC 91345:2016 and IEC/PAS 63088:2017 [19]. In Industry 3.0, the products are isolated from each other, functions are bound to hardware, and system components interact across hierarchy levels. According to RAMI 4.0 RA information for Industry 4.0, the products are part of the network, functions are distributed throughout the network structure, and the participants can communicate with each other irrespective of the system hierarchy [20]. Figure 2 highlights how the RAMI 4.0 distinguishes Industry 4.0 from Industry 3.0.

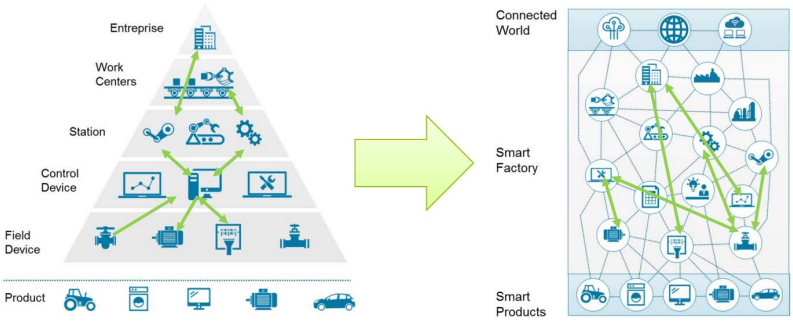

Figure 2. Industry 3.0 vs Industry 4.0 (adapted from [21])

In RAMI 4.0, the international standards for electronics, electrical, mechanics, and Information Technology (IT) participate in interdisciplinary ways to deploy the technology. It's based on Service-Oriented Architecture (SOA) for provisioning services between system components through network protocols and converting the complex tasks into easy processes based on independent technologies and products [22]. Figure 3 shows the three-dimensional RAMI 4.0 RA model that provides insights into the framework where all the industrial partners can interact and understand each other and know how to adopt industry 4.0 in a structured way.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2022 doi:10.20944/preprints202207.0022.v1

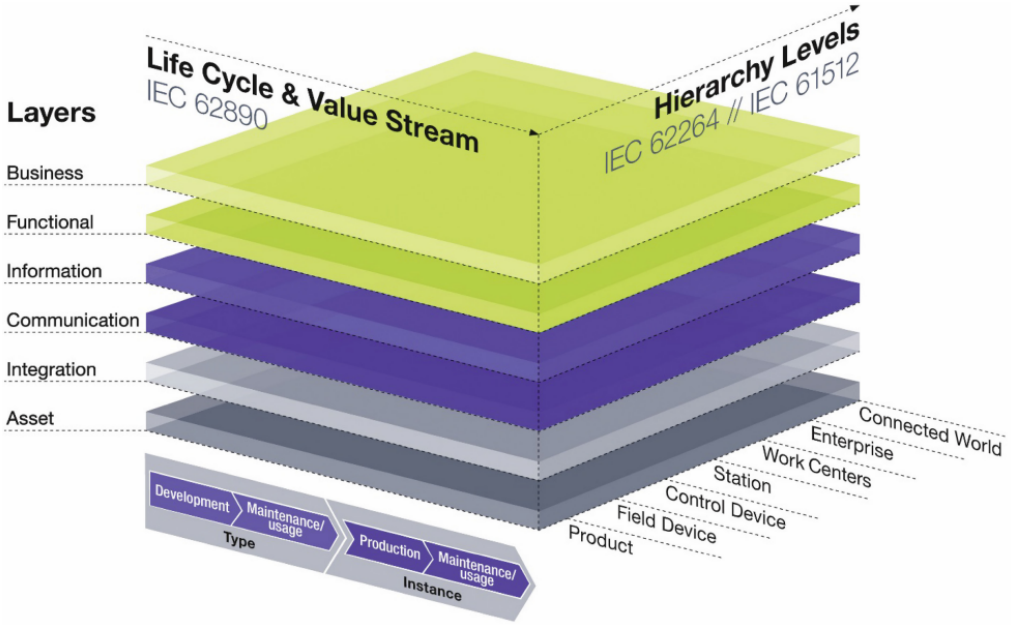

Figure 3. RAMI 4.0 Architecture Model (adapted from [11])

2.1.1. Hierarchy Levels axis

The hierarchy levels on the right horizontal axis of the model are on the IEC 62264 and IEC 61512 international standards for Information Technology (IT) and Control Systems (CS). The terms Station, Work Centers, Enterprise, and Connected World are included in the hierarchy axis from these standards for the common ground of current factory automation and process industry sectors [11]. Based on [23,24], following are the seven levels in the hierarchy axis of the RAMI 4.0 model:

- **Product:** The product is the final outcome of manufacturing in industry.
- **Field Device:** These are the hardware components such as sensors and actuators which collect the environment values.
- **Control device:** Controlling devices such as PLCs and DCs take the readings from sensors and send the controlling commands to operate the system.
- **Station:** It's the place where the user with administrative rights monitors the industrial activity and takes care of processes and events. e.g. SCADA.
- **Work Centers** It provides the data storage, information, and analysis (MES) based on the historical insights.
- **Enterprise:** The enterprise level follows (ERP) to manage all information and carry-out business profitable decisions. It keeps track of production vs orders, expenses vs revenue, and manage the manufacturing planning.
- **Connected World:** The system is connected to the internet to remain connected with the supply-chain process with external industries.

2.1.2. Life Cycle Value Stream

The life cycle process standards used in Industrial automation, control, and measurement systems are on the left horizontal axis of the RAMI 4.0 model. The process shows the information of manufacturing components from the designing stage to the complete product. The Type field is related to the Design and Prototype level of manufacturing, while the Instance field is related to when the product is finally manufactured [11,25].

2.1.3. Architecture layers of RAMI 4.0 model

The vertical layers are also called interoperability layers which cover all the industrial process from the physical devices and assets to the integration of humans, technology, and protocols along with the functional properties of system components and their Business

 doi:10.20944/preprints202207.0022.v1

processes [22,25]. The researchers in [23,26–28] explain the following architectural layers of RAMI 4.0 model:

- **Asset:** This is the lowest layer which contains all the physical components including the devices and peripherals.
- **Integration:** This layer provides the information generating from assets to the upper layers, enables the command and control of assets to the application and functional layer, and contains the IT elements such as RFID, HMI, and actuators.
- **Communication:** This layer is responsible for maintaining the communication between networks using the standards and protocols and enables the interaction of Asset and Integration layers with the upper layers.
- **Information:** This layer provides the pre-processing of information for different events as well as makes sure the integrity and quality of data received from the lower layers and then present the structured data to the Functional and, Business layers.
- **Functional:** The functional layer receives the data from Assets layer and carry out the decisions based on data analytics.
- **Business:** This layer covers the enterprise business models and legal frameworks along with the industrial real-time monitoring services using the dashboards and user interaction applications.

2.2. Industrial Internet Reference Architecture (IIRA)

International Industrial Consortium (IIC) provides a common framework architectural model IIRA to address the support of diverse applications and standards for developing IIoT solutions. The IIRA is adapted based on the ISO/IEEE/IEC 42010 standards, and it can address the change in industrial control systems in the following ways [12]:

- **Increasing local collaborative autonomy:** It includes the provision of new technologies, computational power, and improved sensing, which will provide enhanced data accuracy and further assist in creating autonomous systems.
- **Increasing system optimization through global orchestration:** It includes data analytics using machine learning on collected sensor data to provide insights about the deployed system for system optimization and enhanced control systems.

IIRA is a three-tier system architecture containing Edge Tier, Platform Tier, and Enterprise Tier. Different nodes, devices, sensors, control systems, and assets connected to the Edge Gateway via wireless and wired connections forms a Proximity Network. The Edge Gateway performs the Device Management and Aggregation, then send the relevant data to the Platform Tier via the Access Network. The Platform Tier performs the data transformation, operations, and analytics; and then sends the information to the Enterprise Tier via the Service Network. On Enterprise Tier, the user performs the monitoring and controlling under the Domain Applications and sends the controlling commands back to the Platform Tier through the Control Flow process. The Platform Tier then sends this information to the Edge Tier to perform the relevant tasks. Figure 4 shows the three-tier IIoT architecture given by IIC.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2022 doi:10.20944/preprints202207.0022.v1

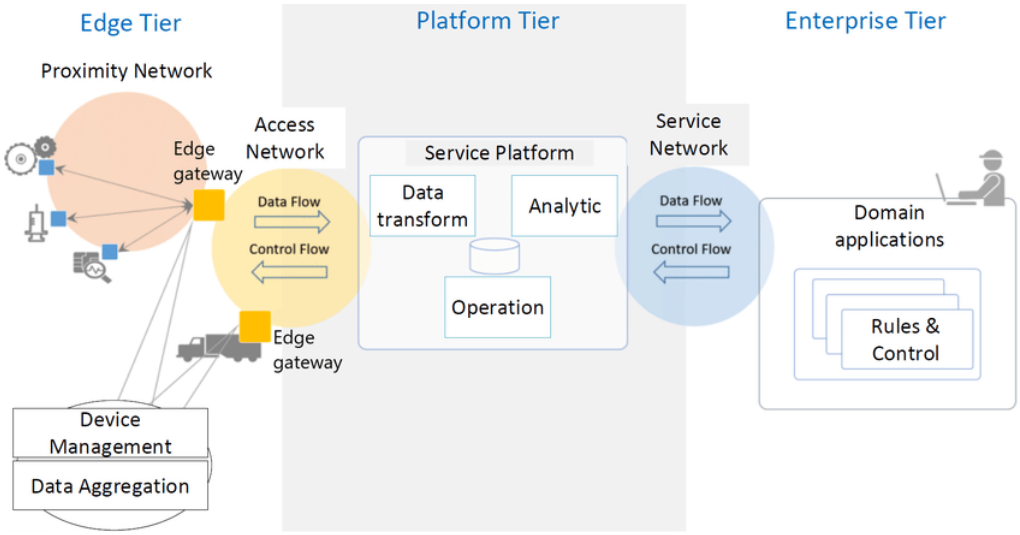

Figure 4. Three-Tier IIoT System Architecture of IIRA (adapted from [29])

2.2.1. Functional Domains and Functional Viewpoints

IIRA contains two important functional parts in its architecture, the Functional Viewpoint, and Functional Domain. The Functional Viewpoint is the overall architectural view of system components and their structure. The Functional Domain contains five distinct domains, which are the building blocks of the system architecture. Figure 5 highlights the information process between the functional domains of the IIRA model. The green arrows show the Data/Information Flows, the grey/white arrows show the Decision Flows, and the red arrows show Command/Request Flows.

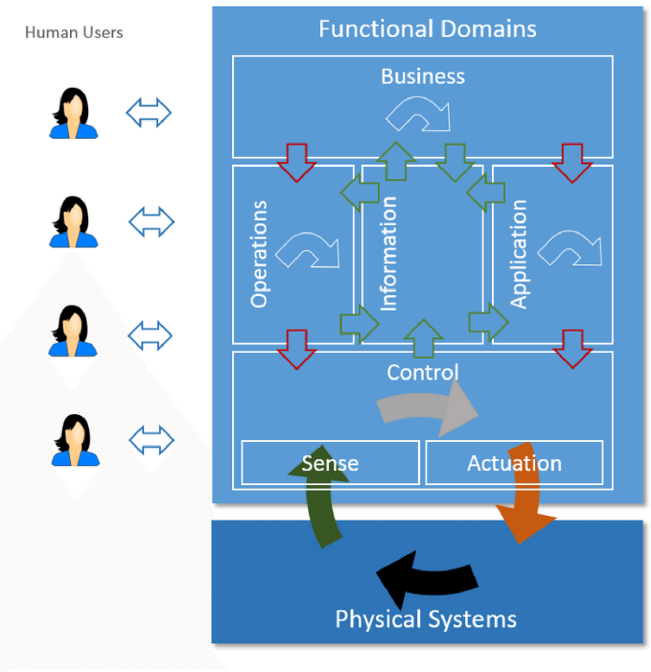

Figure 5. IIRA Domains (adapted from [30])

2.2.2. Functional Domains

1. **Control Domain:** It contains the functions for implementing the control systems in industries. It includes the sensing and actuation functions which read the data from sensors and carry out the controlling signals for the actuators. It also contains the communication function that enables the information exchange between the system

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2022 doi:10.20944/preprints202207.0022.v1

components and technologies using different features such as APIs. The control domain also interprets the system behavior and conditions by using modeling on the sensors' data.

2. **Operations Domain:** It carries outs the management and operation tasks for the control domain. It also provides the Provisioning and Deployment functions to access the assets remotely at a large scale and track, add, modify, or remove them regardless of the harsh industrial environment.
3. **Information Domain:** This functional domain handles the data processing and collection from system components and performs the data analytics to acquire information about the system parameters and optimize the system through the decision-making steps.
4. **Application Domain:** The Application Domain contains functions for implementing the application logic and rules for high-level optimization. It also includes the APIs and UI by which the relevant information is available for human interactions or different applications for processing.
5. **Business Domain:** It contains different functionalities to support the business activities and processes and integrate them into the IIoT systems. Examples of the business functionalities are ERP, MES, Payments, Billings, etc.

2.3. OpenFog Reference Architecture

This architecture facilitates the researchers, developers, designers, and industries to make needed components for fog computing. OpenFog provides the Fog as a Service (FaaS) based architectural model to address industrial implementation issues through its compatibility with SaaS, PaaS, and IaaS. The OpenFog RA has many applications in industries, including, Smart vehicles and Traffic control systems, Smart Cities, Smart Buildings, etc. It aims to provide security, cognition, agility, low latency, and efficiency. Moreover, the OpenFog RA is formed based on eight main pillars representing the overall system model attributes for the real-time deployments. The Perspective highlights the cross-cutting features of RA, while the View represents the structural aspects of the layered architecture. The View component contains three stakeholder views in the RA as Software View, System View, and Node View [13]. Figure 6 shows the OpenFog RA model. The light green colored vertical layers are the perspectives of RA, the light yellow and blue colored layers highlight the Node View and Software Architecture View, and the layers under the red border line show the System Architecture View.

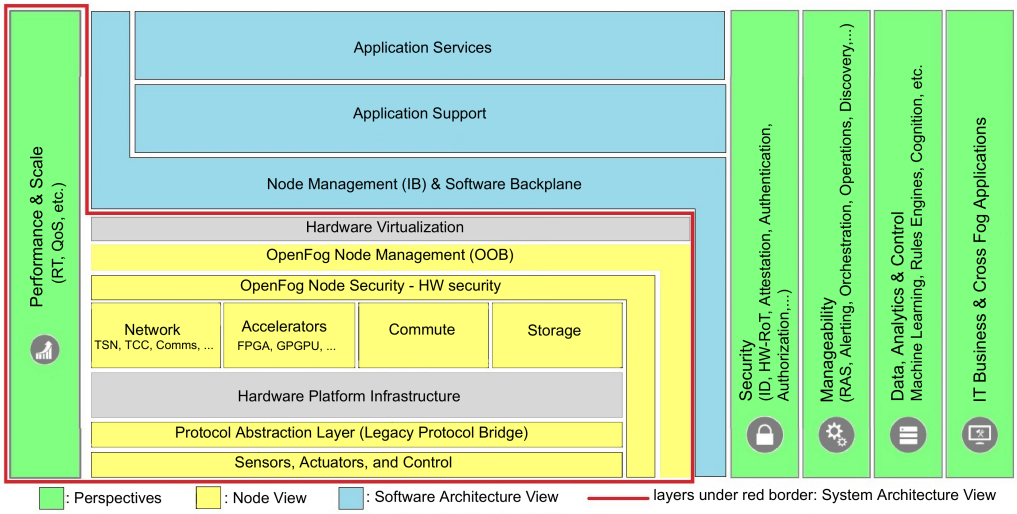

Figure 6. OpenFog Reference Architecture (adapted from [31])

 doi:10.20944/preprints202207.0022.v1

2.3.1. Eight pillars of Fog Computing architecture

The OpenFog RA is formed based on the core principles of eight pillars. These pillars represent the main attributes deployed systems manifest as per given layered RA and fog computing technology.

1. **Security Pillar:** The security of OpenFog architecture is not just limited to the specific standards; it also contains all the mechanisms for security from the hardware component to the software-based application level. The security attributes presented in the OpenFog RA are data privacy and integrity, anonymity, attestation, measurement, trust, and user and device verifications. The OpenFog model provides end-to-end security. Moreover, the network link is provided between the nodes after information attestation is completed, followed by the verification process.
2. **Scalability pillar:** This model provides the features where the individual fog nodes, storage services, and networks can scale based on the users' requirements. There are the following scalability types in the OpenFog RA:
    - Scalable performance: It includes improved fog performance as per the application demands by reducing the latencies in the system.
    - Scalable capacity: It helps increasing the network, system, applications, and users capacity.
    - Scalable reliability: Scalable reliability is ensured by adopting the redundant fogs when there is a network fault or overload of information or processing.
    - Scalable security: It includes the additional software and hardware security features such as access provision and crypto based information processing when the security is becoming stringent.
    - Scalable hardware: It enables the provision of additional hardware components upon requirement between the fogs in network and their internal systems, such as data storage, scale of wired and wireless networks, and the scaling of computational processes.
3. **Openness pillar:** This pillar supports the diverse environment where the fog nodes and devices form an interoperable network by removing the negative impacts such as the quality and cost of a single vendor. It enables the open communication between the components with the location transparency and interoperability.
4. **Autonomy pillar:** The autonomous structure avoids centralized processing by providing the decision-making facility near the devices for efficient operations, security, and cost. It enables the network discovery option, which allows the devices to keep alive if there is an uplink connection problem.
5. **Programmability pillar:** The programming of the deployed nodes and system is available at the hardware and software layers with the ability to re-tasking the fog node. The programmability provides the optimized security with the automatic security patch updates, along with adaptable infrastructure and multi-tenancy.
6. **Reliability, Availability, and Serviceability (RAS) pillar:** While reliability ensures the fog nodes and overall system components are working to deliver their functionalities under the given conditions, the availability functionality refers to the continuous management and back-end support, including the redundant and secure access from devices and redundant configurations. The serviceability enables the automated installation, up-gradation, and maintenance of fog nodes by supporting easily swappable hardware components.
7. **Agility pillar:** This pillar is responsible for dealing with the changes occurring in the system and providing the analytical insights from the extensive data received from the sensors to carry out efficient business decisions.
8. **Hierarchy pillar:** Although in OpenFog RA, not all the systems are hierarchy-based, this pillar provides complementary and traditional hierarchy-based information for the enterprise systems.

 doi:10.20944/preprints202207.0022.v1

2.3.2. Perspectives

The Perspectives shown in the vertical green columns in Figure 6 are described below:

- **Performance and Scale:** The performance of deployed systems is under continuous care for the Quality of Service (QoS) and low latency by using time-sensitive networking and critical computing. The measurement of throughput and latency of a fog node defines the performance of fog computing that can be improved by bringing the fog computing closer to the edge. The new virtualization and containerization technologies in fog computing further improves the nodes' scalability and isolation. These technologies can also carry out priority based network traffic and resource allocation.
- **Security:** The fog architecture is not secured until trustworthiness is absent between the system components. The fog node hardware is secured with appropriate measures, and the complete data security and integrity are ensured from the low-level hardware to the software level with end-to-end security encryption. The security perspective also contains threat detection and privacy preservation features.
- **Manageability:** The manageability perspective provides the capability of responding and making the decisions like humans with the help of machine algorithms. It enables efficient manageability functions for a wide range of actions compared to the traditional IT and OT systems. Furthermore, it takes care of all the management functions, including the system alerting, operation and maintenance, the discovery of devices and nodes, etc.
- **Data, Analytics, and Control:** As the industries are generating high data for performing the analytics to make decisions, the traditional analytics approach is suitable for the increasing demands. Moreover, as the companies are moving forward to predictive maintenance from monitoring the system parameters, it's difficult to face the stringent requirements. Fog computing helps achieve these objectives by performing the data analytics at the edge closer to the source for specific analysis and sending the relevant information to the cloud services for business operations and business-related processing.
- **IT Business and Cross Fog Applications:** It highlights that fog applications need to operate at any hierarchy level and share the data to other nodes ensuring the data interoperability to maximize the values from IT Business perspectives in a multi-vendor nature.

2.3.3. Node View

It's the lowest level view used in the OpenFog RA. The light yellow colored layers in Figure 6 highlights the Node View aspects in architecture. These are necessary aspects to address before adding a node into fog computing network.

- **Node Security:** The Node Security represents both the vertical security perspectives and horizontal layer requirements as system security is critical from the silicon to the software level.
- **Node Management:** It supports the system management process by enabling management interfaces from the nodes. These interfaces support the monitoring and controlling of low-level nodes from high-level management systems.
- **Network:** The network part enables the nodes to communicate and share the information within the network based on the time-sensitive and time-aware networking.
- **Accelerators** The accelerators used in fog applications improve the power and communication latency depending on the network scenario.
- **Compute:** The fog nodes run the open-source software at their node level for the basic computation and the interoperability between other nodes and system components.
- **Storage:** As it is necessary for a node to store data before learning or performing analysis, it requires a reliable storage device that should perform well with data integrity requirements and inform the storage device's health condition.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2022 doi:10.20944/preprints202207.0022.v1

- **Sensors, Actuators, and Control:** These are the lowest level architectural elements of an IoT system. While some of these devices have processing capabilities, some are dumb and can't process the data. These elements are connected to the system by using the wired or wireless connection.
- **Protocol Abstraction Layer:** This layer is responsible for interfacing the sensors and actuators with the fog node for performing the data analytics. It also makes sure interoperability between the multi-vendor products for cross-layer data optimization.

2.3.4. System Architecture View

The system architecture view contains multiple node views for the scalable fog deployments. It addresses the issues of technical teams, manufacturers, and system architects. The Performance & Scale vertical layer and some horizontal layers covered under the red border line in Figure 6 highlight the system architecture view of OpenFog RA.

- **Hardware Platform Infrastructure:** It highlights the fog platform requirements for ensuring the safety of people and hardware from any harm, protection of the system from the environment, and mechanical support of overall hardware infrastructure. The deployed system should also follow compliance and regulation standards.
- **Hardware Virtualization and Containers:** The hardware virtualization enables multiple entities to share the same physical machine and ensure system security by limiting specific system components from virtual machines (VMs). The use of containers decreases the overheads and provides lightweight mechanisms in the fog computing environment.

2.3.5. Software Architecture View

It contains the architecture view of software running on a platform. The platform is formed with the combination of node views for addressing specific deployment scenarios. The fog node software is further separated into three layers as shown in light blue colored layers in Figure 6.

- **Application Services:** This layer provides the services with the help of other layers to accomplish the use case and specific requirements.
- **Application Support:** This infrastructure software part does not perform any new services but supports other applications in carrying out specific tasks.
- **Node Management and Software Backplane:** It performs node management and enables communication between nodes.

2.4. Comparison of RAMI 4.0, IIRA, and OpenFog reference architectures

The reference architectures given by different organizations have different approaches for the development and implementation of Industrial IoT. While RAMI 4.0 is mainly about the manufacturing process from the Production level to the Enterprise level, IIRA is about the industrial process with the established communication between deployed systems. The Platform Industrie 4.0 and IIC are currently collaborating to provide a common reference architecture by mapping the RAMI 4.0 and IIRA together [32]. While the RAMI 4.0 establishes the communication between the hardware and software by using a gateway, the IIRA provides the Edge Tier for the computation and storage of data. The OpenFog RA is about the high data generating and processing use cases in industrial applications. OpenFog is designed to be implemented in any vertical integration application in the industry [13]. The selection of a particular reference architecture depends on the requirements of the deploying system. Table 2 shows the comparison of IIoT reference architectures.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2022 doi:10.20944/preprints202207.0022.v1

Table 2. Comparison of Industrial IoT reference architectures

Category	RAMI 4.0	IIRA	OpenFog	Refs
Organization	German Electrical and Electronic Manufacturers' Association (ZVEI)	Industrial Internet Consortium (IIC)	OpenFog Architecture Workgroup	[22], [12], [13]
Layers	Business, Functional, Information, Communication, Integration, and Asset.	Business, Usage, Function, and Implementation.	Included but not limited to Functional and Deployment viewpoints.	[13], [32], [33]
Hierarchy	Product, Field, Device, Control Device, Station, Work Centers, and Enterprise.	Not hierarchy-based	Devices, Monitoring and Controlling, Operational Support, Business Support, Enterprise Systems.	[13], [32]
Connectivity	Whitepaper	Framework	Framework	[13], [32]
Difference in Industry applications	Focused on manufacturing the things smartly through Product Life-Cycle process.	Covers manufacturing process but not complete product life cycle. Enables the things to work smartly with the interaction of large deployed systems.	Focused on generic platform for applicability with any vertical market use case studies. e.g. Agriculture, Smart cities, Transportation, etc.	[13], [32]
Gateway, Edge/Fog	Analyse the data and connects the hardware and cloud at the gateway.	Computing, processing, and storage at edge.	Storage, Processing, Computing, Accelerators, and Network capabilities for vertical application at each fog hierarchy.	[13], [28]

3. Key IIoT requirements, Emerging Technologies, and literature review of IIoT architectures

As the IIoT is itself emerging due to the integration of Information Technology (IT) and Operational Technology (OT) [34], the problems due to its arising issues have to be addressed with the help of emerging technologies as well. The RAs such as RAMI 4.0, IIRA, and OpenFog provide the basic layout guidelines for the IIoT applications; however, due to the problems arising from heterogeneous technologies and diverse industrial usage, it is difficult to address the arising challenges just by following the reference architectures. In this regard, we have reviewed the IIoT architectural research papers to highlight the main IIoT requirements addressed in the current literature. The literature is solving the challenges for the full integration of Industrial IoT by using the various emerging technologies such as Edge/Fog computing, Software-Defined Networks (SDN), Blockchain, 5G, Machine Learning, WSN, and Machine Learning, along with the support of reference architectures, cloud services, protocols, and standards. Before discussing the literature review of IIoT architectures in detail, we highlight the key IIoT requirements and the emerging technologies used to address these challenges in the IIoT architectures.

3.1. Key IIoT requirements

As the overlapping of Industrial IoT, Industry 4.0, and IoT is improving the production efficiency in industries, some challenges need to be addressed [9]. According to the RAMI 4.0 model, physical and virtual components of a deployed system can directly communicate with each other irrespective of the network hierarchy [11]; however, the system will require the interoperability ability for the system elements to communicate with each other. Due to the exponential growth of heterogeneous technologies, IIoT is facing many challenges in interoperability, latency, security, privacy, and scalability [35]. According to IIC in [36]

 doi:10.20944/preprints202207.0022.v1

and authors in [37], security, privacy, and reliability are among the system characteristics and challenges in Industrial IoT systems. ITU has also defined latency, scalability, security, and privacy as the key requirements in IIoT networks [38]. Anitha et al. in [4] emphasized that IIoT requires high scalability compared to the IoT and highlighted the need for low network latency, interoperability, reliability, security, and privacy in IIoT in their research. Based on the challenges and information available in the literature, we have grouped the following key Industrial IoT requirements, which are critical for its full-stack development and integration in real-time.

- **Interoperability:** Interoperability is the ability to share meaningful information between the two or more communication components [39]. In [40], the authors have highlighted the need for interoperability to guarantee the complete integration of industry 4.0 technology. Due to the increasing use of heterogeneous devices, technologies, and standards in industry 4.0, interoperability has become the major challenge for the industrial ecosystem [41]. The authors in [42] have further emphasized addressing the interoperability in IIoT for enabling the communication between the systems from individual vendors.
- **Scalability:** Scalability is the ability of a system to handle the increasing amount of work due to the growth of components throughout the system operation without affecting its performance [43,44]. According to [45], it is necessary to address the scalability solutions to deal with the exponential growth of devices and data generating in IIoT. The authors in [46] further highlight the need of scalability in IIoT and main issues which affect it, for example, the diversity of networks, heterogeneity of devices, and massive data generating in IIoT systems.
- **Security:** As the IIoT is developing with the integration of both Information Technology (IT) and Operational Technology (OT), the current development of IIoT systems bring the new security challenges which can't be addressed by using the traditional IoT security mechanisms [45]. According to Jamai et al. in [47], most of the security attacks in IIoT are focused on industrial devices, control systems, and networks. The authors in [48] have further classified the attacks on IIoT connectivity protocols into five threads: DoS/DDoS attacks, Information Gathering, Man in the Middle attacks, Injection attacks, and Malware Attacks.
- **Privacy:** "Privacy is the right of an individual or group to control or influence what information related to them may be collected, processed, and stored and by whom, and to whom that information may be disclosed" [36]. With the growing number of heterogeneous devices, it is essential to focus on data privacy issues in IoT and IIoT [49,50]. Different remedial frameworks are present in the literature to address the security and privacy issues in IIoT. According to [51], Fog Computing addresses the security and privacy issues in the IIoT, while the authors in [52] highlight the features of blockchain for solving the security and privacy issues.
- **Reliability:** Reliability in IIoT is the performance indicator that highlights the system working ability as per the design and for the specified time duration in industrial environment [36,53]. ITU has defined reliability as the essential ability for IIoT networks to avoid the risks and production interruptions [38]. The authors in [54] have presented the detailed literature review on the challenges of reliability in Devices, Networks, Applications, and Systems in IoT applications. A system is reliable if all of its components satisfy the reliability conditions.
- **Low latency:** According to ITU, network latency is the duration of time an information packet takes to reach from the source to the destination [55]. According to the authors in [56,57], IIoT services are suffering critically from latency issues due to the generation of a huge volume of data. To address the latency issues, researchers are proposing solutions using different technologies such as 5G [58] and Edge/Fog computing [59].

3.2. Emerging Technologies used in Industrial IoT architectures

In the literature review, we have found some similarities between the Industrial IoT architectures. The architectural solutions are developed by using some emerging technologies for the flexible integration and better performance of IIoT systems. We have grouped the widely used emerging technologies in the literature and focused on evaluating the scope of each technology in addressing the main IIoT requirements in those architectures. Following are some of the emerging technologies we have observed in developing the IIoT layered architectures:

- **Edge/Fog Computing:** Fog computing brings the cloud services closer to the ground mobile devices to off-load the processing burden, improve the Quality of Service (QoS) of a system, and save resources [60]. Based on the information given by National Institute of Standards and Technology (NIST), the fog computing should have the main characteristics of supporting the geographical distribution, low latency, interoperability features, scalability, and real-time interactions rather than batch processing [61]. The size of fog computing is smaller than the traditional cloud computing; however, the number of nodes can be combined to make it a large fog system [62].
  With the generation of an exponential volume of data from the sensors, it's difficult to process information locally due to the limitations of hardware devices. Edge computing provides the features to process the data at the edge device and reduce the required network resources for cloud computing by only sending the required data to the cloud for further processing [63]. Edge computing provides the data storage service at the edge, performs the tasks in the absence of cloud computing, and improves the network latency [64].
- **Software-Defined Networking (SDN):** Software-Defined Networking (SDN) helps in making the static and dedicated networking infrastructure agile and centrally controlled by using the software applications [65]. According to IBM, SDN provides the dynamic load-balancing in network traffic and vendor-independent support with the ease of central programmability and configuration features [66]. SDN is based on three-layer architecture: Infrastructure layer (Data Plane), Control layer (Control Plane), and Application layer [67].
- **Blockchain:** Blockchain technology is based on decentralized and distributed nodes where all the transactions are processed after validation from the participants. In the blockchain, there is no third-party organization to control the transactions process, and the transactions from each participant are locally available to all the participants in the distributed ledger network forming the data transparency [68]. According to [69], transparency and trust, decentralized networking, immutable data, and security are the main advantages of blockchain technology.
- **Machine Learning (ML):** Machine Learning (ML) is a subset of Artificial Intelligence (AI) that imitates intelligent human behavior based on accuracy with the help of data and algorithms [70,71]. ML has many applications, including prediction, semantic analysis, natural language processing, information retrieval, and computer vision [72]. According to research in [73], ML provides some necessary features in Industry 4.0, such as fault detection, predictive maintenance, security and threat detection, and human-machine interaction.
- **5G:** According to ITU, 5G is the evolution of previous mobile technologies (2G, 3G, and 4G) to deliver more speed for processing the high volume of data transfer with minimal latencies while also providing the large-scale connectivity for the exponential growth of devices and services [74]. As per the ITU's recommendations for the International Mobile Telecommunications (IMT) for 2020, 5G technology has the three main usage scenarios, 1) Enhanced Mobile Broadband (eMBB), 2) Massive Machine-type Communications (mMTC), and 3) Ultra-reliable and Low Latency Communications (URLLC) [75]. According to ETSI, 5G is facilitating the new services in different domains but not limited to Industry 4.0, Education, Agriculture, and Publication Safety [76].

 doi:10.20944/preprints202207.0022.v1

- **Wireless Sensor Networks (WSN):** According to the International Electrotechnical Commission (IEC), Wireless Sensor Networks (WSN) is the key IoT technology containing a large group of sensor nodes that detect the properties of physical phenomena such as temperature, humidity, light, pressure, etc., with the easy, reliable, and rapid deployment of systems [77]. In WSN, the nodes interact to form a cluster to utilize resources, providing network scalability, and transmitting the collected data until it has arrived at the base station [78].

3.3. Current research on IIoT architectures

In IIoT architectures, we found some common topics in terms of challenges and emerging technologies. Each layered architecture addresses some of the key requirements and uses one or more emerging technologies for the end-to-end development of IIoT systems. We present a state-of-the-art review on how the layered architectures address these requirements by grouping them based on Edge/Fog Computing, Blockchain, SDN, 5G, Machine Learning, and Wireless Sensor Networks (WSN) technologies. Moreover, in references covering more than one technology, we grouped it with the more emphasized technology according to the paper.

3.3.1. Edge/Fog Computing

Due to the massive and diverse data generation in manufacturing industries, cloud services are unable to take care of large-scale data processing. Furthermore, the delay-sensitive information is vulnerable due to the semi-secure nature of cloud services. In this regard, Sengupta et al. have proposed an Industrial IoT architecture based on fog computing technology. The proposed solution is based on four layers perception layer, fog nodes layer, cloud layer, and application layer. To process the data and reduce the workload from cloud computing, the authors have included the fog nodes layer with semi-secure cloud computing features where a node can be a PC, a Raspberry Pi device, or a virtual operating system (OS). The authors have carried out the experiments in simulations as well as by developing a hardware testbed; however, the proposed solution does not address the reliability as per the harsh industrial environments and interoperability for accommodating the heterogeneous field devices [79].

In [80], the authors have addressed the system reliability shortcoming by presenting a fault-tolerant IIoT architecture using an edge gateway that also provides the low-latency, scalability, and security based on the industrial requirements. In the practical example, the authors have developed the system for machine operative status detection using the raspberry pi as an edge device that stores the information in the local database. The edge device uses this data with algorithms to predict the machine status and display the monitoring parameters such as current, power consumption, and vibration. With edge computing, the proposed system avoids the congestion of bandwidth, unnecessary network lags during the data transfer, and securing the information by bringing it closer to the edge.

The authors in [59] present a conceptual architecture intending to integrate versatile fieldbuses and solve interoperability issues. The proposed model ensures data security by bringing the data processing closer to the edge/fog nodes. Furthermore, the ability of distributed edge/fog nodes in different domains provides high network scalability. The proposed model also addresses the reliability and low latency of the communication process. The proposed model contains four Layers, Sensing Layer, Data Provider Layer, Fog/Edge Computing Layer, and Application/Services Layer. The Sensing layer contains peripherals and devices connected to specific fieldbuses such as Modbus and Ethernet. The Data Provider layer stores the bidirectional data from fieldbuses and upper layers in buffer memory while the Fog/Edge computing layer performs the data processing. The Applications/Services layer provides developed applications for remote monitoring and controlling. The authors have emphasized interoperability for M2M communication between the network elements; however, this conceptual model does not address the data privacy concerns.

 doi:10.20944/preprints202207.0022.v1

The function of distributed automation systems in industries with heterogeneous technologies, protocols, and devices from different vendors is the future of industrial processes; however, the high number of connected devices in current systems are having privacy and interoperability problems for exchanging the information efficiently. In this regard, Dobaj et al. have proposed a state-of-the-art light weight, flexible, and secure Industrial IoT theoritical architecture with the continuous system integration and development (CI/CD) process under the containerized environment. The use of distributed Edge/Fog nodes allow minimum latency and network scalability. Furthermore, the proposed microservices-based architecture ensures network reliability with the support of fault-tolerant network protocols such as OPC-UA, and DDS. The data privacy is ensured by keeping the data at the respective microservice unit and can only be accessed by using its API [81]. The authors have addressed all the IIoT challenges we have highlighted in our paper; however, they have proposed the architecture based on theoritical approach, not by performing the hardware or simulations based experiments.

3.3.2. Software-Defined Networking (SDN)

According to the ref. [82] the performance of the IIoT depends on the deployed systems and the set of communication protocols. Furthermore, the efficiency and reliability in the existing IIoT architectural solutions are compromised due to the lack of testing and usage of new protocols. This problem has resulted in integration of SDN technology with the IIoT architectures. Moreover, as the IIoT devices are generating high data, the transmission of information is facing delays and causing the computation offloading issues. In this regard, Chandramohan et al. in [83] have used Software-Defined Networking (SDN) emerging technology in their proposed architectural solution for the efficient Quality of Service (QoS) based communication. SDN provides the priority-based transmission control with low processing time performed at the edge device. The edge allows the features of adaptive computing and network scalability. In the proposed architecture, the physical layer contains various nodes with a single cluster head as the main device which interacts with the control layer. The centralized SDN controller manages the network flow routing and provides access to the user application. The proposed model is simulated in MATLAB, and the results showed the advantages of network reliability, higher throughput, and lower latencies compared to the present solutions.

The OPC-UA network protocol in client-server communication provides the Machine-to-Machine (M2M) information exchangeability; however, the traditional devices don't support this protocol. To solve the interoperability issues and provide reliable and low latency-based communication, the authors in [84] have proposed OPC-UA gateways and Time Sensitive Software-Defined Networking (TSSDN) based Industrial IoT architecture. The network elements send the information to the OPC-UA-based edge gateway that handles the heterogeneous data and enables the communication between the vendor-specific devices. The TSSDN switch enables reliable and low latency-based communication by controlling the network resources. The proposed architecture showed efficient results of information exchange between the network components; however, the authors have not addressed security, privacy, and scalability requirements in the given architecture.

Bedhief et al. in [85] have proposed a software-based architecture for IIoT based on SDN and Edge/Fog computing technology. While SDN provides flexibility and scalability, Fog/Edge Computing enables low latency and interoperability. The central programmability approach of SDN in the proposed solution allows the flexibility to use the heterogeneous network technologies, which can be deployed and changed independently. However, the authors have not addressed the security and privacy features in the proposed architecture.

The security and privacy shortcoming is improved by Friha et al. in [86] by using SDN technology with Blockchain's Hyperledger Sawtooth and Fog Computing. The proposed robust framework contains four layers specifically for the secure Agricultural IoT. (1) The Agricultural layer contains the peripherals for sensing and controlling, (2) the Fog layer contains various nodes that provide the storage, data processing, and computations in

 doi:10.20944/preprints202207.0022.v1

containerized docker environment near the end devices, (3) the SDN Controller Network layer contains the central controller and all network acts as a single Network Operation System (NOS), and (4) Blockchain Network layer, which validates all the information and enforces the transactions in the system. However, the proposed architecture does not address interoperability.

The future of industries is to be accompanied by the constellation of thousands of sensors and devices. Without the interoperability between heterogeneous devices, the deployed systems will be handled by various vendor-specific solutions that will create the problems of not utilizing the performance of system elements collectively. In this regard, the authors in [87] have proposed an open-source Software-Defined Networking (SDN) based IIoT architecture with the OpenDaylight (ODL) SDN controller. The proposed architecture contains three layers: Data Plane, Control Plane, and Application Plane. The data plane layer is composed of switches, routers, and other network devices forming the SDN and WSN network, and it handles the traffic flow based on Quality of Service (QoS) and takes care of the data routing. The Control Plane sends the information to the Application Plane that manages the SDN operations and provides the cloud services and controlling features. While WSN provides scalability, ODL further ensures the fault-tolerance and scalable network with the central control of a group of controllers. The given IIoT architecture also provides network reliability and fault tolerance by monitoring and providing the redundant ODL controller features.

3.3.3. Blockchain

In [88], the researchers suggest blockchain technology to make the processing chain in Industrial IoT secure, traceable and transparent. Teslya et al. have proposed a conceptual blockchain-based model for security and reliability; however, the proposed model doesn't address the interoperability and has its drawbacks of the durability of information in Semantic Information Broker (SIB), and non-matching of data between the different participants [89].

The authors in [90] have addressed security and privacy challenges in their theoretical blockchain-based IIoT architecture. The proposed model ensures the addressed shortcomings by establishing trust between the components. The message transactions in this solution are secured by using the gossip protocol-based private/public key exchange between the communication nodes.

In industries, sensors lack the capabilities to process, compute, and detect security vulnerabilities. Furthermore, the current solutions lack authentication, integrity, and identification ability. In this regard, the authors in [91] have presented a practical distributed ledger-based authentication framework. The proposed framework utilizes the combination of Secure Multi-Party Computation (SMPC) and Distributed Ledger Technology (DLT) to detect attacks and malicious sensors in Industrial IoT. The distributed ledger technology solves the aforementioned issues in a decentralized way; however, the theoretical and practical models presented in [90] and [91] have a shortcoming in terms of handling the large-scale devices, which will create scalability problems.

Lin et al. in [92] have addressed this shortcoming by combining the Oracle software features with Blockchain technology. Blockchain technology in literature provides trust and ensures security; however, the current blockchain-based decentralized architectures can't obtain complex real-time and isolated data with low processing time. In this regard, the authors have used Federated Learning (FL) with Oracle and Blockchain to propose IIoT digital twin architecture that provides a low processing time and high network traffic stability. The oracle-based fast computing mechanism allows the exchange of trusted data between the physical and digital machines in a decentralized network.

Ghajar et al. in [93] have further addressed the interoperability along with security and privacy features by proposing Schloss, a blockchain-based IIoT architecture. The proposed architecture authenticates the network nodes based on the application-level authentication process in the distributed blockchain management system. The model

 doi:10.20944/preprints202207.0022.v1

ensures the nodes' privacy, whereas the authority of each node is decided based on its behavior. The architecture contains the feature to decrease the node power based on the proof of work (PoW) between the nodes. The proposed model ensures network security and establishes trust between business partners. The devices connected to the network are dynamically identified and controlled by using the multi-signature intelligent contract mechanism while maintaining data privacy.

In [94], the authors have addressed the scalability and latency along with security and privacy challenges by proposing Fog Computing and Blockchain-based security architecture for IIoT enabled Cloud Manufacturing (CM). The authors have focused on addressing three main things which are lacking in the security of CM in current literature, (1) trust in manufacturing/monitoring equipment to ensure the authenticity, (2) privacy of CM data over the internet, (3) scalability requirement of security services to deal with future expansions.

The use of heterogeneous technologies is resulting in privacy and security issues between the network components, and that is also causing a lack of trust among the participants. To address these challenges together with scalability, low latency, and network reliability, Ceccarelli et al. in [95] propose an Industrial IoT architecture, specifically for the real-time railway systems, by combining Blockchain, Fog Computing, and SDN emerging technologies. The computing nodes in the proposed FUSION model are reconfigurable to act as Fog/Edge, SDN, or End Devices based on the system requirement. The blockchain ensures the information exchange between the decentralized network components in a secured and trusted environment. The SDN technology in the given architecture allows the network resources management and reconfiguration of system operations. Furthermore, Edge/Fog computing ensures low network latency and provides information processing and storage closer to the devices. While the blockchain enables secure and privacy-preserved communication, the decentralized control of system architecture with SDN ensures the network scalability.

3.3.4. Machine Learning (ML)

The Android operating system (OS) is recently facing a lot of malware attacks due to its integration with heterogeneous IIoT devices. There are various ML-based solutions to provide the security; however, the models in the literature lack to address data privacy. Since the algorithms are trained in a centralized way where all the network nodes have to share their data, it's causing privacy issues. In this regard, Taheri et al. have proposed a Federated Learning (FL) based decentralized privacy protection architecture for Industrial IoT. The network nodes don't have to share private information with the FL approach and train the algorithms locally using the global training model. The authors have also addressed the vulnerabilities of traditional FL-based solutions in current literature that are susceptible to security attacks from the participants' side while they are in the learning phase. To address the shortcomings of FL in literature and evaluate the efficiency of the proposed architecture, the authors have proposed architecture in two parts first part contains the poisoning attacks based on the Generative Adversarial Networks (GAN) and Federated GAN. For the counter-measure solution, the authors have utilized Byzantine Median (BM) and Byzantine Krum (BK) to detect these malware attacks and to ensure network reliability at the server-side. The proposed architecture provides 8% more accuracy than the existing architectural solutions [96].

As the IIoT is growing due to high scale data sensing, processing, and storage, many adversarial attacks are breaking the security barriers to access the user data, steal it, and inject different malware and other malicious codes. Some of the increasing attacks are DoS, DDoS, Advanced Persistent Threat (APT), and modern botnets. To solve these issues, the authors in [97] have proposed a Convolutional Neural Networks (CNN) based botnet and malware detection architecture to ensure security and privacy while also addressing the interoperability and scalability at the network layer. The proposed architecture uses the

 doi:10.20944/preprints202207.0022.v1

hybrid Long short-term memory and CNN-based DL approach by utilizing the publicly available datasets. It provides efficient results in terms of accuracy and speed.

3.3.5. 5G Technology

Ludwig et al. have proposed a 5G architecture based on the 5G use cases in various industries such as Smart Production, Condition Monitoring, Distributed Sensing, and Automated Guided Driving. The proposed architecture consists of different edge devices connected to the public and private base stations via eMBB, uRLLC, and mMTC wireless mechanisms of 5G. The authors have also included the Software-Defined Networking (SDN) in their architecture for the reliable communication using effective management of network resources [98].

The authors in [99] have further addressed the network scalability in their proposed solution. Due to the high number of IIoT devices, the existing architectures are not providing low latency and reliable communication with high scalability. This issue has resulted in the creation of Mobile Edge Computing (MEC); however, the MEC-based architectures present in the literature face diverse nature of components and technologies, complex development of IIoT systems, lack of flexibility, and poor mobility. In this regard, the authors have proposed the MEC architecture by combining the docker container technology. The runtime instances of the Docker images run independently, and the containers map the physical components with the virtual environment. While the 5G provides low latency and reliable communication, the docker containerization makes the mobility of the proposed architecture efficient and ensures high scalability.

The authors in [100] have addressed more key IIoT requirements in their proposed conceptual architecture by addressing the security and privacy features along with low latency, scalability, and reliable communication. The proposed framework architecture for Smart Manufacturing addresses the IIoT requirements based on its six architectural layers.

Wang et al. in [101] propose an experimental Quality of Service (QoS) and secure privacy preserved Industrial IoT architecture based on 5G technology and Federated Learning. The 5G brings reliability and low latency, while the FL further improves the latency and deals with load-balancing and privacy leakage issues. The minimum possible routing paths are selected in the model to attain the minimum latencies. Like [100], this proposed solution addresses many requirements; however, it doesn't address the interoperability features for the reusability of data and machine to machine communication in IIoT systems.

According to Jiang et al. in [102], the communication among the network elements is not secured until the trustworthiness of all partners is not ensured. In this regard, the authors in [103] have combined a trust and authentication method in their proposed 5G technology-based architecture for the network components to cope with security and privacy issues due to the exponential growth of data. The proposed solution uses Advanced Encryption Standard (AES) based encryption method to ensure the secure data transfer between the participants. Furthermore, the Dempster Shafer Theory (DST) method in the architecture allows the reliability and trustworthiness of the collected data from sensors. While 5G technology provides the high bandwidth for low latency, the network scalability is achieved by using the gateway with the help of a cloud server.

In [58], the authors have proposed a 5G enabled IIoT architecture named Smart Networks for Industry (SN4I) to address the increasing use of Industry 4.0 in industrial manufacturing. The proposed architecture addresses the interoperability and heterogeneity issues such as lack of dynamicity due to the static utilization of components for a fixed solution. By enabling network interoperability, this architecture ensures the reusability of resources. It secures Wireless Sensor Networks (WSN) by blocking unauthorized access within the network using the Hidra Server access control protocol mechanism. The SDN and NFV technologies in the proposed solution ensure the interoperability and scalability of the system. Moreover, Wireless Sensor Networks (WSN) technology is also used to further improve network scalability.

 doi:10.20944/preprints202207.0022.v1

3.3.6. Wireless Sensor Networks (WSN)

In [104], the authors have proposed a general-purpose two-tier wireless architecture for the reliable and ease of implementation efforts of Industrial IoT. The upper tier in the proposed model is responsible for the information exchange between the network nodes based on wireless and wired communication. The QoS configuration of the switch allows the control of communication and bandwidth quality, whereas the communication is possible with the help of TCP/IP/UDP protocols. The architecture is suitable for the MODBUS and OPC-UA-based communication between the machines. The lower tier contains the Head Devices (HD), which interact with the controllers such as PLCs. Low power and reliable communication are achieved by employing the 6TiSCH-based frequency hopping technique with the ubiquitous connectivity based on IPv6 with Wireless Sensor Networks. The authors have tested the proposed architecture by using Raspberry Pi as the Head Device (HD) connected to the remote I/O terminals using the M2M protocols.

4. Observations and Discussion

4.1. Experimental vs Conceptual architectures

Aside from reference architectures, we have reviewed the proposed IIoT architectures by dividing them into two categories of Experimental and Conceptual. The researchers have proposed technical architectural hierarchy levels in their solutions. In experimental architectures, the authors have performed real-time experiments on their proposed models either by testing and evaluating the hardware-based prototypes or by testing the simulations in the virtual environment. The conceptual architectures are based on theoretical knowledge without performing any experiments. Figure 7 shows the research trend in presenting the architectures from 2015 to 2022. The reference architectures have laid the foundation of proposed architectures in the literature, and the focus on providing experiment-based architectures is increasing over time.

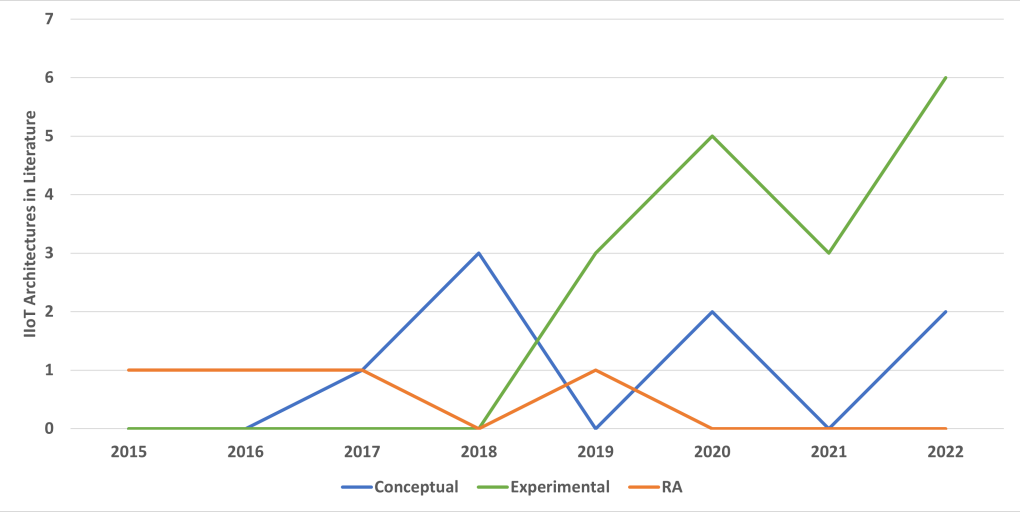

Figure 7. Conceptual and Experimental architectures in literature

4.2. Comparison of proposed architectures in literature

Researchers in literature have proposed various architectures to address the main IIoT challenges and requirements. Table 3 highlights the work of each architecture in the literature reviewed in addressing the features of Scalability, Interoperability, Security, Privacy, Reliability, and Low latency for Industrial IoT. Based on the literature reviewed in this paper, there is a research gap in addressing all these requirements collectively. Although the IIoT architecture in [81] addresses all the features, the authors have presented this architecture based on the theoretical approach, not the practical.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2022 doi:10.20944/preprints202207.0022.v1

Table 3. Comparison of IIoT architectures in literature

Refs	Arch. Type	Low Latency	Security	Scalability	Reliability	Privacy	Interoperability
[90]	Conceptual		✓			✓	
[98]	Conceptual	✓			✓		
[89]	Conceptual	✓	✓		✓		
[93]	Conceptual		✓		✓	✓	✓
[59]	Conceptual	✓	✓	✓	✓		✓
[87]	Conceptual	✓	✓	✓	✓		✓
[100]	Conceptual	✓	✓	✓	✓	✓	
[81]	Conceptual	✓	✓	✓	✓	✓	✓
[91]	Experimental		✓			✓	
[96]	Experimental		✓			✓	
[83]	Experimental	✓		✓	✓		
[84]	Experimental	✓			✓		✓
[92]	Experimental	✓	✓	✓			
[99]	Experimental	✓		✓	✓		
[104]	Experimental	✓		✓	✓		
[79]	Experimental	✓	✓	✓		✓	
[85]	Experimental	✓		✓	✓		✓
[94]	Experimental	✓	✓	✓		✓	
[97]	Experimental		✓	✓		✓	✓
[58]	Experimental	✓	✓	✓		✓	✓
[80]	Experimental	✓	✓	✓	✓	✓	
[86]	Experimental	✓	✓	✓	✓	✓	
[95]	Experimental	✓	✓	✓	✓	✓	
[101]	Experimental	✓	✓	✓	✓	✓	
[103]	Experimental	✓	✓	✓	✓	✓	

Figure 8 shows the focus of current IIoT architectures on addressing the Industrial IoT requirements in order, low latency, security, scalability, reliability, privacy, and interoperability. As Industry 4.0 is currently in its initial phase of development with the integration of Industrial IoT, the current literature needs to focus on interoperability for the efficient utilization of resources through machine-to-machine (M2M) communication.

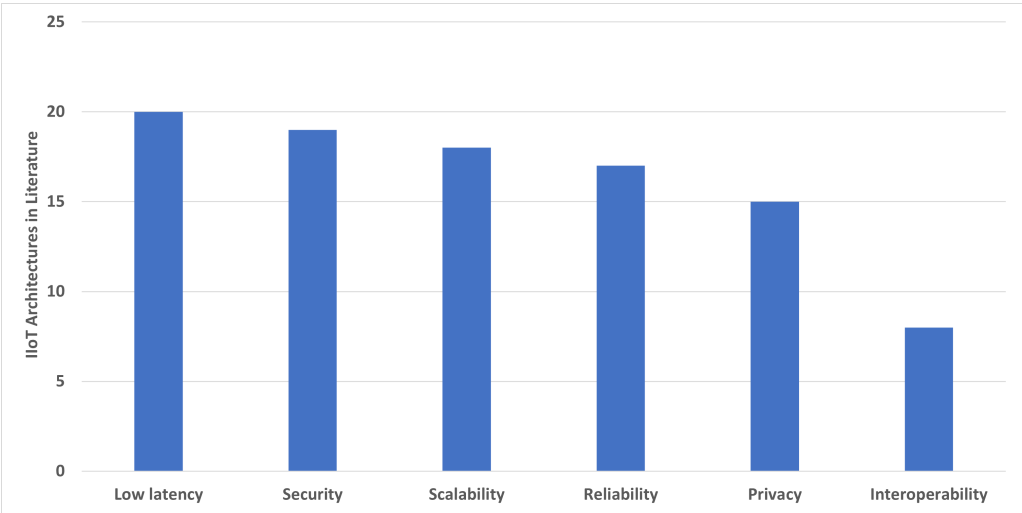

Figure 8. Literature focus on key IIoT requirements

4.3. Relation of emerging technologies to key requirements

We have extracted the research papers on Industrial IoT architectures with the general keywords to avoid a biased literature review. Based on the literature reviewed in this paper, table 4 shows the use of emerging technologies to address the main IIoT requirements in the literature. While some researchers have used only a single emerging technology along

 doi:10.20944/preprints202207.0022.v1

with standards and protocols to propose a solution, some have utilized more than one emerging technology in their proposed architectures.

Table 4. Emerging Technologies in literature

Refs	Edge/Fog	Blockchain	SDN	5G	ML	WSN
[90]		✓				
[98]			✓	✓		
[89]		✓				
[93]		✓				
[59]	✓					
[87]			✓			✓
[100]	✓			✓		
[81]	✓					
[91]		✓				
[96]					✓	
[83]	✓		✓			
[84]			✓			
[92]		✓			✓	
[99]	✓			✓		
[104]						✓
[79]	✓					
[85]	✓		✓			
[94]	✓	✓		✓		
[97]					✓	
[58]			✓	✓		✓
[80]	✓					
[86]	✓	✓	✓			
[95]	✓	✓	✓			
[101]				✓	✓	✓
[103]				✓		

Apart from the relation between key IIoT requirements and emerging technologies, we also highlight the trend of these technologies in IIoT architectures. Figure 9 shows the use of emerging technologies in presenting architectural solutions. The current literature is heavily focused on utilizing the processing and storage characteristics of Edge/Fog Computing to provide IIoT architectures. Furthermore, the literature is least focused on presenting the architectures based on Wireless Sensor Networks (WSN) and Machine Learning. Researchers are using machine learning to address many specific solutions in Industrial IoT; however, the literature is less focused on providing the architectural models. The Wireless Sensor Networks (WSN) technology is the core part of many Internet of Things (IoT) architectural applications, but it's less utilized in proposing the IIoT architectures.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2022 doi:10.20944/preprints202207.0022.v1

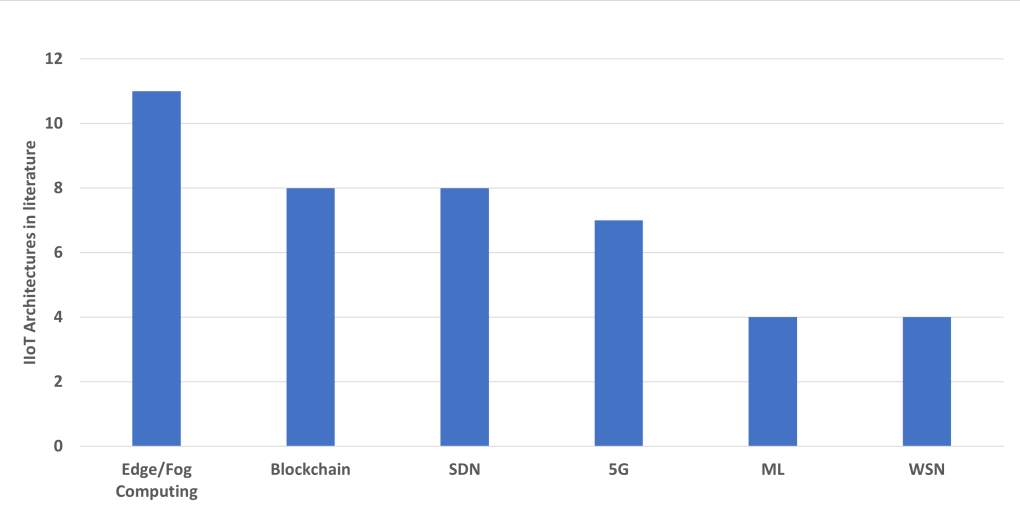

Figure 9. Focus on Emerging Technologies in literature

The scope and characteristics of each emerging technology are unique in terms of addressing the challenges in IIoT architectures in literature. Figure 10 highlights the scope of each emerging technology in IIoT architectures. Researchers are using the edge and fog computing to solve the main IIoT requirements; however, current literature has not utilized this technology to address all the challenges collectively in an IIoT architecture. Blockchain technology highly addresses the security and privacy issues in IIoT architectures, while some literature also focuses on a few other challenges of scalability, reliability, and interoperability. The information from table 4 highlights that SDN technology is mostly used in combination with other emerging technologies for the reliability and scalability in IIoT architectures. The central network controlling characteristics of SDN enables it to provide Low latency, while some literature has also used SDN for addressing the interoperability issues. The adoption of 5G technology in IIoT architectures provides high-speed features with minimal latency compared to the other technologies. 5G also addresses the scalability and reliability challenges in IIoT architectures. The use of machine learning (ML) in IIoT architectures preserves data privacy from unauthorized access and ensures network security. The integration of Wireless Sensor Networks (WSN) technology in IIoT architectural solutions is addressing three challenges, low latency, reliability, and scalability. WSN extensively addresses the scalability requirements as compared to other features.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 July 2022 doi:10.20944/preprints202207.0022.v1

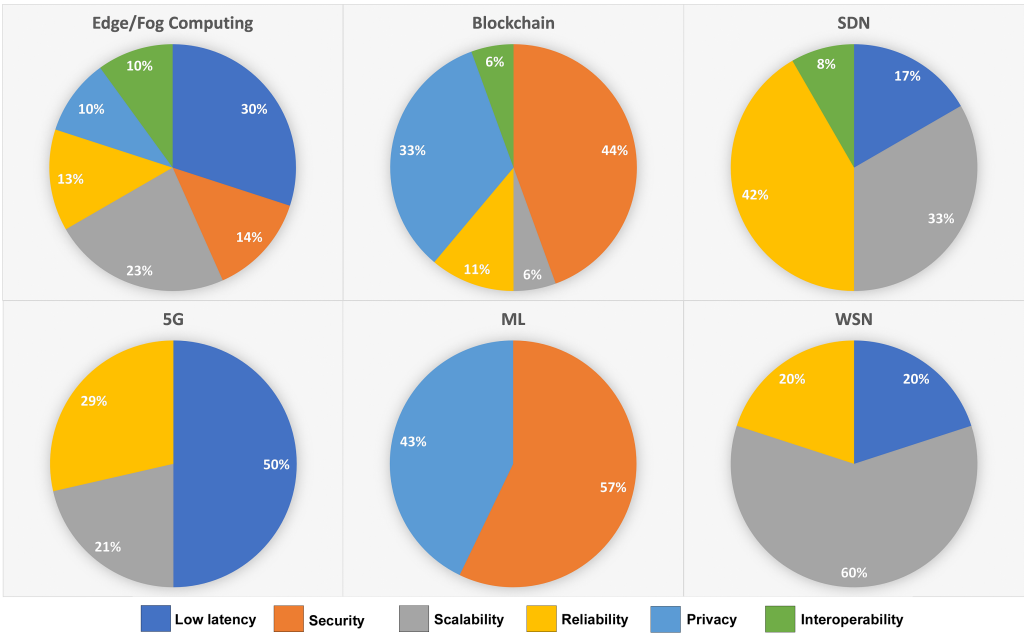

Figure 10. Scope of Emerging Technologies in IIoT architectures

5. Conclusions and Future Work

In this paper, we presented a state-of-the-art review on IIoT reference architectures from organizations and proposed architectures in literature, the main IIoT requirements for the end-to-end implementation, and the emerging technologies used in architectural solutions to address these requirements and challenges. Each reference architecture has specific characteristics of industrial use case applications, system topology, services, data processing, storage, and computation abilities. The selection of particular reference architecture depends on the required full-stack IIoT solution under specific industrial scenarios. We identified that the main IIoT issues addressed in various research papers are scalability, interoperability, security, privacy, reliability, and low latency. These are the main requirements that affect the deployment of Industrial IoT in real-time. We also identified the use of Edge/Fog Computing, Blockchain, SDN, 5G, Machine Learning, and WSN technologies in developing the architectural solutions and their unique characteristics in addressing the challenges. Each research paper uses one or more emerging technologies for layered architecture. We also highlighted the literature focus on utilizing these technologies and addressing the challenges.

On the other hand, each IIoT architecture addresses at least two main requirements, either with a conceptual approach or with simulations/hardware-based experimental approach. The authors in [81] have addressed all the mentioned requirements based on the theoretical model, not the practical solution. Meanwhile, the literature is trending towards presenting more experimental architectures over the time. We have described the prospectice research directions which can contribute to the flexible deployments of IIoT systems. There is a need to present a common IIoT architectural framework that addresses all the applications in IIoT under harsh industrial conditions and provides secure and reliable integration from the factory floor up to the enterprise level.

Author Contributions: Conceptualization, A.M. and G.V.; methodology, A.M. and G.V.; investigation, A.M.; writing—original draft preparation, A.M.; writing—review and editing, A.M. and G.V.; visualization, A.M.; supervision, A.A. and J.W.; project administration, G.V. and A.A.; funding acquisition, A.A. and J.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported, in part, by Science Foundation Ireland grants 16/RC/3918 (Confirm, the Smart Manufacturing Research Centre) and 13/RC/2094_P2 (Lero - the Science Foundation Ireland Research Centre for Software (www.lero.ie))

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 754489

Data Availability Statement: Not applicable.

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

References

1. Srinadh, V.; Srinivasa Rao, M.; Ranjan Sahoo, M.; Rameshchandra, K. An analytical study on security and future research of Internet of Things. *Materials Today: Proceedings* **2021**. https://doi.org/https://doi.org/10.1016/j.matpr.2020.12.342.
2. International Telecommunication Union. ITU Internet techreports 2005: The Internet of Things. Technical report.
3. Farhan, L.; Kharel, R.; Kaiwartya, O.; Quiroz-Castellanos, M.; Alissa, A.; Abdulsalam, M. A Concise Review on Internet of Things (IoT) -Problems, Challenges and Opportunities. In Proceedings of the 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2018, pp. 1–6. https://doi.org/10.1109/CSNDSP.2018.8471762.
4. Anitha, T.; Manimurugan, S.; Sridhar, S.; Mathupriya, S.; Latha, G.C.P. A Review on Communication Protocols of Industrial Internet of Things. *Proceedings of 2022 2nd International Conference on Computing and Information Technology, ICCIT 2022* **2022**, pp. 418–423. https://doi.org/10.1109/ICCIT52419.2022.9711544.
5. Kebande, V.R. Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0. *Forensic Science International: techreports* **2022**, *5*, 100257. https://doi.org/10.1016/j.fsir.2022.100257.
6. Govender, E.; Telukdarie, A.; Sishi, M. Approach for Implementing Industry 4.0 Framework in the Steel Industry. In Proceedings of the 2019 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), 2019, pp. 1314–1318. https://doi.org/10.1109/IEEM44572.2019.8978492.
7. IBM. How Industry 4.0 technologies are changing manufacturing. https://www.ibm.com/topics/industry-4-0.
8. Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. *Computers in Industry* **2018**, *100*, 212–223. https://doi.org/10.1016/j.compind.2018.04.017.
9. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Transactions on Industrial Informatics* **2018**, *14*, 4724–4734. https://doi.org/10.1109/TII.2018.2852491.
10. Jain, S.; Chandrasekaran, K. Industrial Automation Using Internet of Things. In *Research Anthology on Cross-Disciplinary Designs and Applications of Automation*; IGI Global, 2022; pp. 355–383. https://doi.org/10.4018/978-1-6684-3694-3.ch019.
11. Adolphs, P.; Berlik, S.; Dorst, W.; Friedrich, J.; Gericke, C.; Hankel, M.; Heidel, R.; Hoffmeister, M.; Mosch, C.; Pichler, R.; et al. DIN SPEC 91345:2016 - Reference Architecture Model Industrie 4.0 (RAMI4.0). Technical Report ICS 03.100.01; 25.040.01; 35.240.50, 2016.
12. Lin, S.W.; Miller, B.; Durand, J.; Bleakley, G.; Chigani, A.; Martin, R.; Murphy, B.; Crawford, M. The Industrial Internet Reference Architecture, 2019.
13. OpenFog Consortium. OpenFog Reference Architecture for Fog Computing **2017**.
14. Tan, S.F.; Samsudin, A. Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey. *Sensors* **2021**, *21*. https://doi.org/10.3390/s21196647.
15. Mulchandani, D. Difference between IIOT and IOT - GeeksforGeeks, 2020.
16. Bassi, A.; Bauer, M.; Fiedler, M.; Kramp, T.; van Kranenburg, R.; Lange, S.; Meissner, S., Eds. *Enabling Things to Talk*; Springer Berlin Heidelberg, 2013. https://doi.org/10.1007/978-3-642-40403-0.
17. Fremantle, P. A Reference Architecture for the Internet of Things, 2015.
18. Bader, S.R.; Maleshkova, M.; Lohmann, S. Structuring reference architectures for the industrial Internet of Things. *Future Internet* **2019**, *11*. https://doi.org/10.3390/FI11070151.
19. Megow, J. REFERENCE ARCHITECTURE MODELS FOR INDUSTRY 4.0, SMART MANUFACTURING AND IOT AN INTRODUCTION. Technical report, 2020.

20. Schweichhart, K. Reference Architectural Model Industrie 4.0 (RAMI 4.0). https://ec.europa.eu/futurium/en/system/files/ged/a2-schweichhart-reference_architectural_model_industrie_4.0_rami_4.0.pdf.
21. Moldehn, A. Industrie 4.0 - Intelligent production of tomorrow. https://dam-mdc.phoenixcontact.com/asset/156443151564/d90d65eff0734c9a49d76134aa1061e1/Digital_Tranformation_at_Phoenix_Contact.pdf.
22. Lydon, B. RAMI 4.0 - ISA. https://www.isa.org/intech-home/2019/march-april/features/rami-4-0-reference-architectural-model-for-industr.
23. Melo, P.F.S.; Godoy, E.P.; Ferrari, P.; Sisinni, E. Open Source Control Device for Industry 4.0 Based on RAMI 4.0. *Electronics* **2021**, *10*. https://doi.org/10.3390/electronics10070869.
24. Kapoor, V. RAMI 4.0 for pizza lovers – Part 3 | SAP Blogs. https://blogs.sap.com/2017/08/27/rami-4.0-for-pizza-lovers-part-3/.
25. Collins, D. What are RAMI 4.0 and asset administration shells? https://www.motioncontroltips.com/what-are-rami40-and-asset-administration-shells-in-the-context-of-industry40/.
26. Zezulka, F.; Marcon, P.; Vesely, I.; Sajdl, O. Industry 4.0 – An Introduction in the phenomenon. *IFAC-PapersOnLine* **2016**, *49*, 8–12. 14th IFAC Conference on Programmable Devices and Embedded Systems PDES 2016, https://doi.org/https://doi.org/10.1016/j.ifacol.2016.12.002.
27. Wang, Y.; Towara, T.; Anderl, R. Topological Approach for Mapping Technologies in Reference Architectural Model Industrie 4.0 (RAMI 4.0). 2017.
28. Kaviraju. RAMI 4.0 (Reference Architectural Model Industry 4.0): Explained with example - KR Knowledge World. https://industry40.co.in/rami-reference-architecture-model-industry-4-0/.
29. Lin, S.W.; Miller, B.; Durand, J.; Bleakley, G.; Chigani, A.; Martin, R.; Murphy, B.; Crawford, M. The Industrial Internet Reference Architecture. Technical Report IIC:PUB:G1:V1.07:PB:20150601, 2019.
30. Usländer, T.; Batz, T. Co-Design of Requirements and Architectural Artefacts for Industrial Internet Applications. 2016.
31. OpenFog Concortium. The OpenFog Consortium Reference Architecture: Executive Summary. Technical report, 2017.
32. Lin, S.W.; Murphy, B.; Clauer, E.; Loewen, U.; Neubert, R.; Bachmann, G.; Pai, M.; Hankel, M. Architecture Alignment and Interoperability: An Industrial Internet Consortium and Plattform Industrie 4.0 Joint Whitepaper. Technical Report IIC:WHT:IN3:V1.0:PB:20171205, 2017.
33. The Open Group. Reference Architectures and Open Group Standards for the Internet of Things – Four Internet of Things Reference Architectures. http://www.opengroup.org/iot/wp-refarchs/p3.htm.
34. Shakya, S.R.; Jha, S. Challenges in Industrial Internet of Things (IIoT). *Industrial Internet of Things* **2022**, pp. 19–39. https://doi.org/10.1201/9781003102267-2.
35. Younan, M.; Houssein, E.H.; Elhoseny, M.; Ali, A.A. Challenges and recommended technologies for the industrial internet of things: A comprehensive review. *Measurement* **2020**, *151*, 107198. https://doi.org/https://doi.org/10.1016/j.measurement.2019.107198.
36. Industrial Internet Consortium. Industrial Internet of Things Volume G4: Security Framework IIC. Technical Report IIC:PUB:G4:V1.0:PB:20160926, 2016.
37. Jaidka, H.; Sharma, N.; Singh, R. Evolution of IoT to IIoT: Applications & Challenges. *Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020* **2020**.
38. International Telecommunication Union. FG-NET2030 – Focus Group on Technologies for Network 2030. Technical report, 2020.
39. Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mobile Networks and Applications* **2019**, *24*, 796–809. https://doi.org/10.1007/S11036-018-1089-9/FIGURES/5.
40. da Rocha, H.; Abrishambaf, R.; Pereira, J.; Espirito Santo, A. Integrating the IEEE 1451 and IEC 61499 Standards with the Industrial Internet Reference Architecture. *Sensors* **2022**, *22*. https://doi.org/10.3390/s22041495.
41. Paniagua, C.; Eliasson, J.; Delsing, J. Interoperability Mismatch Challenges in Heterogeneous SOA-based Systems. In Proceedings of the 2019 IEEE International Conference on Industrial Technology (ICIT), 2019, pp. 788–793. https://doi.org/10.1109/ICIT.2019.8754991.
42. Derhamy, H.; Eliasson, J.; Delsing, J. IoT Interoperability—On-Demand and Low Latency Transparent Multiprotocol Translator. *IEEE Internet of Things Journal* **2017**, *4*, 1754–1763. https://doi.org/10.1109/JIOT.2017.2697718.
43. Hassan, Z.; Ali, H.; Badawy, M. Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions. *International Journal of Computer Applications* **2015**, *128*, 975–8887.

44. Gupta, A.; Christie, R.; Manjula, R. Scalability in Internet of Things: Features, Techniques and Research Challenges. *International Journal of Computational Intelligence Research* **2017**, *13*, 1617–1627.
45. Yu, X.; Guo, H. A Survey on IIoT Security. In Proceedings of the 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), 2019, pp. 1–5. https://doi.org/10.1109/VTS-APWCS.2019.8851679.
46. Wu, Y.; Dai, H.N.; Wang, H. Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0. *IEEE Internet of Things Journal* **2021**, *8*, 2300–2317. https://doi.org/10.1109/JIOT.2020.3025916.
47. Jamai, I.; Ben Azzouz, L.; Saïdane, L.A. Security issues in Industry 4.0. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, pp. 481–488. https://doi.org/10.1109/IWCMC48107.2020.9148447.
48. Ferrag, M.A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning **2022**. https://doi.org/10.36227/TECHRXIV.18857336.V1.
49. Zhou, L.; Yeh, K.H.; Hancke, G.; Liu, Z.; Su, C. Security and Privacy for the Industrial Internet of Things: An Overview of Approaches to Safeguarding Endpoints. *IEEE Signal Processing Magazine* **2018**, *35*, 76–87. https://doi.org/10.1109/msp.2018.2846297.
50. Rondanini, C.; Carminati, B.; Ferrari, E. Confidential Discovery of IoT Devices through Blockchain. In Proceedings of the 2019 IEEE International Congress on Internet of Things (ICIOT), 2019, pp. 1–8. https://doi.org/10.1109/ICIOT.2019.00014.
51. Tange, K.; Donno, M.D.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Communications Surveys & Tutorials* **2020**, *22*, 2489–2520. Tan K et al discusses the security concerns in IoT 4.0 by overviewing the current literature work and suggests the use of god f, https://doi.org/10.1109/COMST.2020.3011208.
52. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet of Things* **2020**, *10*, 100081. Special Issue of the Elsevier IoT Journal on Blockchain Applications in IoT Environments, https://doi.org/https://doi.org/10.1016/j.iot.2019.100081.
53. Kim, D.S.; Hoa, T.D.; Thien, H.T. On the Reliability of Industrial Internet of Things from Systematic Perspectives: Evaluation Approaches, Challenges, and Open Issues. *IETE Technical Review* **2022**, *0*, 1–32, [https://doi.org/10.1080/02564602.2022.2028586]. https://doi.org/10.1080/02564602.2022.2028586.
54. Moore, S.; Nugent, C.; Zhang, S.; Cleland, I. IoT reliability: a review leading to 5 key research directions. *CCF Transactions on Pervasive Computing and Interaction* **2020**, *2*. https://doi.org/10.1007/s42486-020-00037-z.
55. International Organization for Standardization. Pulps — Laboratory wet disintegration — Part 3: Disintegration of mechanical pulps at > 85 degrees C. https://www.iso.org/obp/ui/#iso:std:iso:5263:-3:ed-1:v1:en.
56. Ma, J.; Shang, B.; Song, H.; Huang, Y.; Fan, P. Reliability Versus Latency in IIoT Visual Applications: A Scalable Task Offloading Framework. *IEEE Internet of Things Journal* **2022**. https://doi.org/10.1109/JIOT.2022.3148115.
57. Shi, C.; Ren, Z.; Yang, K.; Chen, C.; Zhang, H.; Xiao, Y.; Hou, X. Ultra-low latency cloud-fog computing for industrial Internet of Things. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1–6. https://doi.org/10.1109/WCNC.2018.8377192.
58. Sasiain, J.; Sanz, A.; Astorga, J.; Jacob, E. Towards Flexible Integration of 5G and IIoT Technologies in Industry 4.0: A Practical Use Case. *Applied Sciences 2020, Vol. 10, Page 7670* **2020**, *10*, 7670. https://doi.org/10.3390/APP10217670.
59. Ungurean, I.; Gaitan, N.C. A Software Architecture for the Industrial Internet of Things—A Conceptual Model. *Sensors 2020, Vol. 20, Page 5603* **2020**, *20*, 5603. https://doi.org/10.3390/S20195603.
60. Mas, L.; Vilaplana, J.; Mateo, J.; Solsona, F. A queuing theory model for fog computing. *The Journal of Supercomputing* **2022**, *78*, 11138–11155. https://doi.org/10.1007/s11227-022-04328-3.
61. Iorga, M.; Feldman, L.; Barton, R.; Martin, M.J.; Goren, N.; Mahmoudi, C. Fog computing conceptual model. Technical report, 2018. https://doi.org/10.6028/nist.sp.500-325.
62. Mukherjee, M.; Shu, L.; Wang, D. Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges. *IEEE Communications Surveys Tutorials* **2018**, *20*, 1826–1857. https://doi.org/10.1109/COMST.2018.2814571.

63. Wu, Y.; Guo, H.; Chakraborty, C.; Khosravi, M.; Berretti, S.; Wan, S. Edge Computing Driven Low-Light Image Dynamic Enhancement for Object Detection. *IEEE Transactions on Network Science and Engineering* **2022**, pp. 1–1. https://doi.org/10.1109/TNSE.2022.3151502.
64. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A Survey on the Edge Computing for the Internet of Things. *IEEE Access* **2018**, *6*, 6900–6919. https://doi.org/10.1109/ACCESS.2017.2778504.
65. Ciena. What is SDN? https://www.ciena.com/insights/what-is/What-Is-SDN.html.
66. IBM Cloud Education. What is Software-Defined Networking (SDN)? https://www.ibm.com/cloud/blog/software-defined-networking.
67. Braun, W.; Menth, M. Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices. *Future Internet* **2014**, *6*, 302–336. https://doi.org/10.3390/fi6020302.
68. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLOS ONE* **2016**, *11*, e0163477. https://doi.org/10.1371/journal.pone.0163477.
69. Golosova, J.; Romanovs, A. The Advantages and Disadvantages of the Blockchain Technology. In Proceedings of the 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018, pp. 1–6. https://doi.org/10.1109/AIEEE.2018.8592253.
70. Brown, S. Machine learning, explained. https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained.
71. IBM Cloud Education. Machine Learning. https://www.ibm.com/cloud/learn/machine-learning.
72. Shinde, P.P.; Shah, S. A Review of Machine Learning and Deep Learning Applications. In Proceedings of the 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018, pp. 1–6. https://doi.org/10.1109/ICCUBEA.2018.8697857.
73. Angelopoulos, A.; Michailidis, E.T.; Nomikos, N.; Trakadas, P.; Hatziefremidis, A.; Voliotis, S.; Zahariadis, T. Tackling Faults in the Industry 4.0 Era—A Survey of Machine-Learning Solutions and Key Aspects. *Sensors* **2020**, *20*.
74. International Telecommunication Union. 5G - Fifth generation of mobile technologies. https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx.
75. International Telecommunication Union. IMT Vision-Framework and overall objectives of the future development of IMT for 2020 and beyond. Technical report, 2015.
76. European Telecommunications Standards Institute. ETSI - 5g Standards - 5g Mobile Technologies. https://www.etsi.org/technologies/mobile/5g.
77. Yinbiao, S.; Lee, K.; Lanctot, P.; Jianbin, F.; Hao, H.; Chow, B.; Desbenoit, J.P.; Stephan, G.; Hui, L.; Guodong, X.; et al. Internet of Things: Wireless Sensor Networks. Technical report, 2014.
78. Khalaf, O.I.; Romero, C.A.T.; Hassan, S.; Iqbal, M.T. Mitigating Hotspot Issues in Heterogeneous Wireless Sensor Networks. *Journal of Sensors* **2022**, *2022*, 1–14. https://doi.org/10.1155/2022/7909472.
79. Sengupta, J.; Ruj, S.; Bit, S.D. A Secure Fog-Based Architecture for Industrial Internet of Things and Industry 4.0. *IEEE Transactions on Industrial Informatics* **2021**, *17*, 2316–2324. https://doi.org/10.1109/TII.2020.2998105.
80. Ghosh, A.; Mukherjee, A.; Misra, S. SEGA: Secured Edge Gateway Microservices Architecture for IIoT-Based Machine Monitoring. *IEEE Transactions on Industrial Informatics* **2022**, *18*, 1949–1956. https://doi.org/10.1109/TII.2021.3102158.
81. Dobaj, J.; Iber, J.; Krisper, M.; Kreiner, C. A Microservice Architecture for the Industrial Internet-Of-Things. In Proceedings of the Proceedings of the 23rd European Conference on Pattern Languages of Programs; Association for Computing Machinery: New York, NY, USA, 2018; EuroPLoP '18. https://doi.org/10.1145/3282308.3282320.
82. Desai, P.R.; Mini, S.; Tosh, D.K. Edge-based Optimal Routing in SDN-enabled Industrial Internet of Things. *IEEE Internet of Things Journal* **2022**, pp. 1–1. https://doi.org/10.1109/JIOT.2022.3163228.
83. Chandramohan, S.; Senthilkumaran, M.; Sivakumar, M. Adaptive Computing Optimization for Industrial IoT using SDN with Edge Computing. In Proceedings of the 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), 2022, pp. 360–365. https://doi.org/10.1109/ICCMC53470.2022.9754048.
84. Wang, R.; Ji, L.; Ren, T.; He, S.; Shi, Z. A Low-latency and Interoperable Industrial Internet of Things Architecture for Manufacturing Systems. In Proceedings of the 2020 IEEE 18th

International Conference on Industrial Informatics (INDIN), 2020, Vol. 1, pp. 859–864. https://doi.org/10.1109/INDIN45582.2020.9442203.

85. Bedhief, I.; Foschini, L.; Bellavista, P.; Kassar, M.; Aguili, T. Toward Self-Adaptive Software Defined Fog Networking Architecture for IIoT and Industry 4.0. IEEE, 2019, Vol. 2019-September, pp. 1–5. https://doi.org/10.1109/CAMAD.2019.8858499.
86. Friha, O.; Ferrag, M.A.; Shu, L.; Nafa, M. A Robust Security Framework based on Blockchain and SDN for Fog Computing enabled Agricultural Internet of Things. *2020 International Conference on Internet of Things and Intelligent Applications, ITIA 2020* **2020**. https://doi.org/10.1109/ITIA50152.2020.9312286.
87. Romero-Gázquez, J.L.; Bueno-Delgado, M.V. Software Architecture Solution Based on SDN for an Industrial IoT Scenario. *Wireless Communications and Mobile Computing* **2018**, *2018*, 1–12. https://doi.org/10.1155/2018/2946575.
88. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access* **2020**, *8*, 32031–32053. https://doi.org/10.1109/ACCESS.2020.2973178.
89. Teslya, N.; Ryabchikov, I. Blockchain-Based Platform Architecture for Industrial IoT.
90. Puri, V.; Priyadarshini, I.; Kumar, R.; Kim, L.C. Blockchain meets IIoT: An architecture for privacy preservation and security in IIoT. *2020 International Conference on Computer Science, Engineering and Applications, ICCSEA 2020* **2020**. https://doi.org/10.1109/ICCSEA49143.2020.9132860.
91. Lupascu, C.; Lupascu, A.; Bica, I. DLT Based Authentication Framework for Industrial IoT Devices. *Sensors* **2020**, *20*. https://doi.org/10.3390/s20092621.
92. Lin, Y.; Gao, Z.; Shi, W.; Wang, Q.; Li, H.; Wang, M.; Yang, Y.; Rui, L. A Novel Architecture Combining Oracle with Decentralized Learning for IIoT. *IEEE Internet of Things Journal* **2022**, pp. 1–1. https://doi.org/10.1109/JIOT.2022.3150789.
93. Ghovanlooy Ghajar, F.; Sikora, A.; Welte, D. Schloss: Blockchain-Based System Architecture for Secure Industrial IoT. *Electronics* **2022**, *11*. https://doi.org/10.3390/electronics11101629.
94. Hewa, T.M.; Braeken, A.; Liyanage, M.; Ylianttila, M. Fog Computing and Blockchain based Security Service Architecture for 5G Industrial IoT enabled Cloud Manufacturing. *IEEE Transactions on Industrial Informatics* **2022**. https://doi.org/10.1109/TII.2022.3140792.
95. Ceccarelli, A.; Cinque, M.; Esposito, C.; Foschini, L.; Giannelli, C.; Lollini, P. FUSION—Fog Computing and Blockchain for Trusted Industrial Internet of Things. *IEEE Transactions on Engineering Management* **2020**, pp. 1–15. https://doi.org/10.1109/TEM.2020.3024105.
96. Taheri, R.; Shojafar, M.; Alazab, M.; Tafazolli, R. Fed-IIoT: A Robust Federated Malware Detection Architecture in Industrial IoT. *IEEE Transactions on Industrial Informatics* **2021**, *17*, 8442–8452. https://doi.org/10.1109/TII.2020.3043458.
97. Hussain, Z.; Akhunzada, A.; Iqbal, J.; Bibi, I.; Gani, A. Secure IIoT-Enabled Industry 4.0. *Sustainability 2021, Vol. 13, Page 12384* **2021**, *13*, 12384. https://doi.org/10.3390/SU132212384.
98. Ludwig, S.; Karrenbauer, M.; Fellan, A.; Schotten, H.D.; Buhr, H.; Seetaraman, S.; Niebert, N.; Bernardy, A.; Seelmann, V.; Stich, V.; et al. A5G Architecture for the Factory of the Future. In Proceedings of the 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), 2018, Vol. 1, pp. 1409–1416. https://doi.org/10.1109/ETFA.2018.8502642.
99. Hou, X.; Ren, Z.; Yang, K.; Chen, C.; Zhang, H.; Xiao, Y. IIoT-MEC: A Novel Mobile Edge Computing Framework for 5G-enabled IIoT. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), 2019, pp. 1–7. https://doi.org/10.1109/WCNC.2019.8885703.
100. Mahiri, F.; Najoua, A.; Souda, S.B. 5G-Enabled IIoT Framework Architecture Towards Sustainable Smart Manufacturing. *International Journal of Online and Biomedical Engineering (iJOE)* **2022**, *18*, 4–20. https://doi.org/10.3991/ijoe.v18i04.27753.
101. Wang, X.; Hu, J.; Lin, H.; Garg, S.; Kaddoum, G.; Piran, M.J.; Hossain, M.S. QoS and Privacy-Aware Routing for 5G-Enabled Industrial Internet of Things: A Federated Reinforcement Learning Approach. *IEEE Transactions on Industrial Informatics* **2022**, *18*, 4189–4197. https://doi.org/10.1109/TII.2021.3124848.
102. Jiang, J.; Han, G.; Wang, F.; Shu, L.; Guizani, M. An Efficient Distributed Trust Model for Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems* **2015**, *26*, 1228–1237. https://doi.org/10.1109/TPDS.2014.2320505.

103. Soleymani, S.A.; Goudarzi, S.; Anisi, M.H.; Cruickshank, H.; Jindal, A.; Kama, N. TRUTH: Trust and Authentication Scheme in 5G-IIoT. *IEEE Transactions on Industrial Informatics* **2022**, pp. 1–1. https://doi.org/10.1109/TII.2022.3174718.
104. Cena, G.; Scanzio, S.; Valenzano, A.; Zunino, C. A Full-Wireless Network Architecture Based on the Industrial Internet of Things Paradigm. In Proceedings of the 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp. 1301–1304. https://doi.org/10.1109/ETFA.2019.8869005.