Computers and Electrical Engineering 81 (2020) 106522

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Industrial internet of things: Recent advances, enabling technologies and open challenges☆

W.Z. Khan[a,*], M.H. Rehman[b], H.M. Zangoti[c], M.K. Afzal[d], N. Armi[a], K. Salah[e]

[a] Farasan Networking Research Laboratory, Faculty of CS & IS, Jazan University, Saudi Arabia
[b] Department of CS, FAST-NUCES, Lahore, Pakistan
[c] Department of Computing and Information Science, Florida International University, USA
[d] Department of Computer Science at COMSATS University Islamabad, Pakistan
[e] Department of Electrical Engineering & and Computer Science, Khalifa University, UAE

ARTICLE INFO

Article history:
Received 16 November 2018
Revised 30 October 2019
Accepted 25 November 2019

Keywords:
Industrial internet of things
Industry 4.0
Cyber physical systems
Cloud computing
Blockchain
Artificial intelligence
Virtual reality

ABSTRACT

The adoption of emerging technological trends and applications of the Internet of Things (IoT) in the industrial systems is leading towards the development of Industrial IoT (IIoT). IIoT serves as a new vision of IoT in the industrial sector by automating smart objects for sensing, collecting, processing and communicating the real-time events in industrial systems. The major objective of IIoT is to achieve high operational efficiency, increased productivity, and better management of industrial assets and processes through product customization, intelligent monitoring applications for production floor shops and machine health, and predictive and preventive maintenance of industrial equipment. In this paper, we present a new and clear definition of IIoT, which can help the readers to understand the concept of IIoT. We have described the state-of-the-art research efforts in IIoT. Finally, we have highlighted the enabling technologies for IIoT and recent challenges faced by IIoT.

1. Introduction

The development of wireless technologies during the past decades has led to a novel paradigm called the Internet of Things termed as IoT. The IoT paradigm was firstly introduced by Kevin Ashton in 1998 as a concept for connecting things or objects to the Internet. Although IoT is believed to have a wide range of benefits in many IoT applications such as smart homes, healthcare, transportation and environment, it is also believed to have a significant impact in the industry by achieving more efficient, optimized monitoring and controlling with reduce cost. IoT is expected to bring innovations and benefits to the industry leading to the concept of IIoT. The IIoT system allows the industry to collect and analyze a large amount of data that can be used to improve the overall performance of industrial systems, providing various types of services. The IIoT system is also believed to bring cost reduction in Capital Expenditures (CAPEX) and Operating Expenses (OPEX).

Many similar terms are coined to describe the concept of IoT into Industry, for example, Industry 4.0, Industrial IoT and Smart Manufacturing etc. The core concept behind all these terms is the use of advanced technologies and applications (e.g.

☆ This paper is for CAEE special section SI-bciot. Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. Shaohua Wan.

* Corresponding author.
E-mail addresses: wazirzadakhan@jazanu.edu.sa (W.Z. Khan), mhrehman@ieee.org (M.H. Rehman), hzang001@fiu.edu (H.M. Zangoti), khaled.salah@ku.ac.ae (K. Salah).

https://doi.org/10.1016/j.compeleceng.2019.106522
0045-7906/

Table 1
Operational difference between IoT and IIoT systems.

Concentration	IIoT	IoT
Area of Focus	Industrial Applications	General Applications
Focus Development	Industrial Systems	Smart Devices
Security and Risk Measures	Advanced and Robust	Utility-centric
Interoperability	CPS-Integrated	Autonomous
Scalability	Large-scale Networks	Low-scale Network
Precision and Accuracy	Synchronized with milliseconds	Critically Monitored
Programmablity	Remote on-site programming	Easy Off-site programming
Output	Operational Efficiency	Convenience and Utilization
Resilience	High Fault Tolerance Required	Not Required
Maintenance	Scheduled and Planned	Consumer Preferred

Table 2
Existing related works on IIoT systems.

Reference	Theme of the survey
[1]	The magazine article focuses on general understanding of trust based communications in IIoT.
[2]	The magazine article discusses the massive adoption of IoT technologies and gives a road map on how to address wireless connectivity challenges in IIoT systems.
[3]	The article discusses energy-aware routing issues in IIoTs
[4]	The article presents review of IIoTs in CPS perspectives.
[5]	The article presents a reveiw of application deployment strategies using edge computing systems in IIoT
[6]	The article presents a survey of IoT technologies and big data systems in the domain of Industry 4.0 systems.
[7]	The article presents the review of IIoTs in monetization and commercialization perspectives.
[8]	The article presents an initial study on IIoT and its relationship with industry 4.0. In addition, the article presents the opportunities and challenges in terms of energy efficiency, performance, interoperability, security, and privacy,
[9]	The book chapter introduces IIoT for cyber manufacturing systems and discusses its enabling technologies and economic impact, IIoT infrastructure, and architectural pattern.
[10]	The article presents a systematic literature review of key contributions related to IIoT systems.

IoT, 5G, Cloud computing, Edge/Fog computing, Machine learning etc.) specially optimized for industrial processes. In 2011, an initiative led by the German government, called “Industry4.0” or sometimes refer as “Industrie4.0”, was introduced in order to improve the efficiency of manufacturing in industry. It aims to exchange and collect information during the whole lifecycle of any product.

We define the IIoT as: *Industrial IoT (IIoT) is the network of intelligent and highly connected industrial components that are deployed to achieve high production rate with reduced operational costs through real-time monitoring, efficient management and controlling of industrial processes, assets and operational time.*

IIoT is a subset of IoT which requires higher levels of safety, security and reliable communication without the disruption of real-time industrial operations due to mission-critical industrial environments. The focus of IIoT is efficient management of industrial assets and operations along with predictive maintenance. Table 1 outlines the key differences among IoT and IIoT systems. On the other hand, Industry 4.0 is a subset of IIoT which focuses on safety and efficiency in manufacturing. The evolution of IIoT is expected widely in future industrial networks as well. The IIoT will enable Industry 5.0 systems to narrow the gap between human and machines and it will help to achieve massive personalization vision of Industry 6.0. However, considering currency technology ecosystem, we limited our discussions to IIoT in relation with Industry 4.0 vision. The recent estimation shows the noteworthy progression in the field of IoT and IIoT, according to these estimations there will be 70 billion Internet connected devices by 2025 and in 2023 the share of IIoT in the global market will be approximately 14.2 trillion US dollars.

We studied and compared the existing published reviews closely related to IIoTs (See Table 2 for further understanding). Current research works present either the early studies on IIoT systems as presented in [1–3]. For example, researchers in [1] studied trustworthy communication related research challenges in IIoT and researchers in [2] discussed the road map to resolve the connectivity issues in wireless IIoTs. Alternately, researchers presented comprehensive review of IIoT in some specific perspectives such as Cyber Physical Systems (CPS) for IIoTs [4], energy-aware data routing in IIoTs [3], application deployment strategies in edge-computing enabled IIoT systems [5], big data [6], and commercialization of IIoT systems [7]. However, to the best of our knowledge, we have provided an up-to-date overview of three important areas in IIoT such as IIoT architectures and frameworks, communication protocols and data management techniques. We have covered the most recent literature from 2015 to 2018. We have also proposed a clearer, easy to understand the definition of IIoT and highlighted more recent challenges faced by the IIoT system. Most recent enabling technologies which can play an important role in the success of IIoT systems are also presented. This study also highlighted the gap and focus areas of machine learning in manufacturing. The paper structure is presented in Fig. 1 and key abbreviations are presented Table 3.

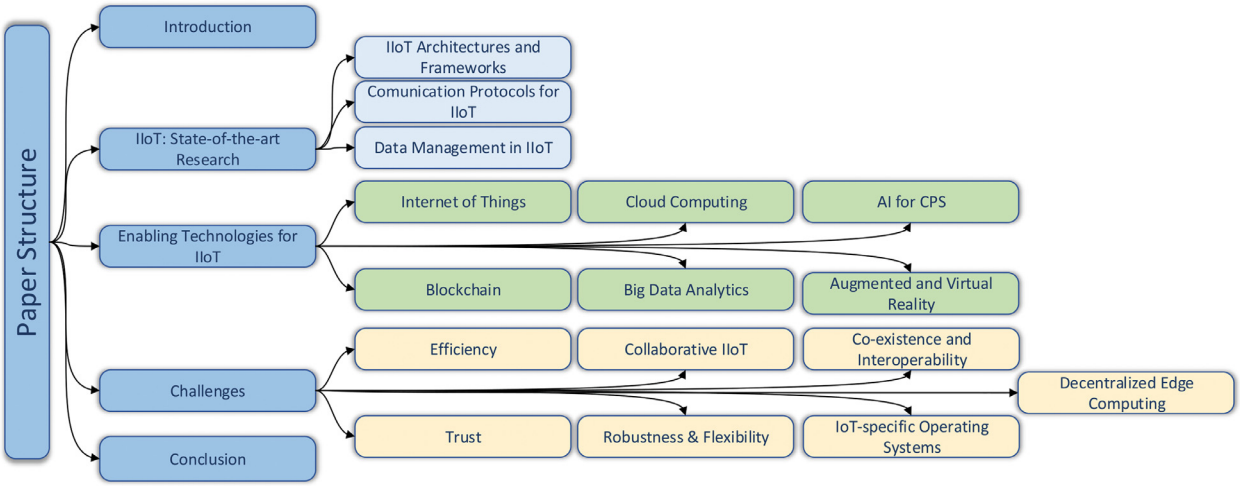

Fig. 1. Paper structure.

Table 3
Abbreviations used in this study.

IIoT	Industrial internet of things
CPS	Cyber Physcial Systems
IAM	Identification and Access Management
PMR	Physical Manufacturing Resource
CoAP	Constrained Application Protocol
LPS	Local Pool Service
ASN	Absolute Slot Number
TT	Timeslot Template
MQTT	Message Queue Telemetry Transport
RTT	Round Trip Time
DML	Data Management Layer
LM	Local Manager
CCM	Concentric Computing Model
H2M	Humane-to-Machine
M2M	Machine-to-Machine
TPSN	Timing-sync Protocol for Sensor Networks
GPA	Groupwise Pair selection Algorithm
STETS	Spanning Tree-based Energy-efficient Time Synchronization
PCA	Prioritized Contention Access
CSMA/CA	Carrier-sense Multiple Access with Collision Avoidance

In this paper we contribute to the following:

- A new definition for IIoT is devised.
- The state-of-the-art research efforts are reviewed that are specifically done in the areas of architectures and frameworks for IIoT, communication protocols and data management schemes.
- Various enabling technologies related to IIoT are highlighted.
- Finally, open research challenges in the field of IIoT are highlighted.

The rest of the paper is organized as follows: Section 2 presents the state-of-the-art research efforts in IIoT. Section 3 describes the enabling technologies for IIoT. Section 4 presents the related challenges and issues in detail. Section 5 finally concludes the paper.

2. IIoT: State-of-the-art research efforts

In this Section, we have highlighted state-of-the-art research efforts in IIoT. The focus of this section is the latest research efforts done in the area of IIoT architectures and frameworks, communication protocols and data management techniques.

2.1. IIoT architectures and frameworks

A generic architecture of IIoT systems was discussed by industrial internet consortium [11] which is presented in Fig. 2 where by IIoT devices and industrial data sources generate continuous data streams at Layer-1 while the edge servers and

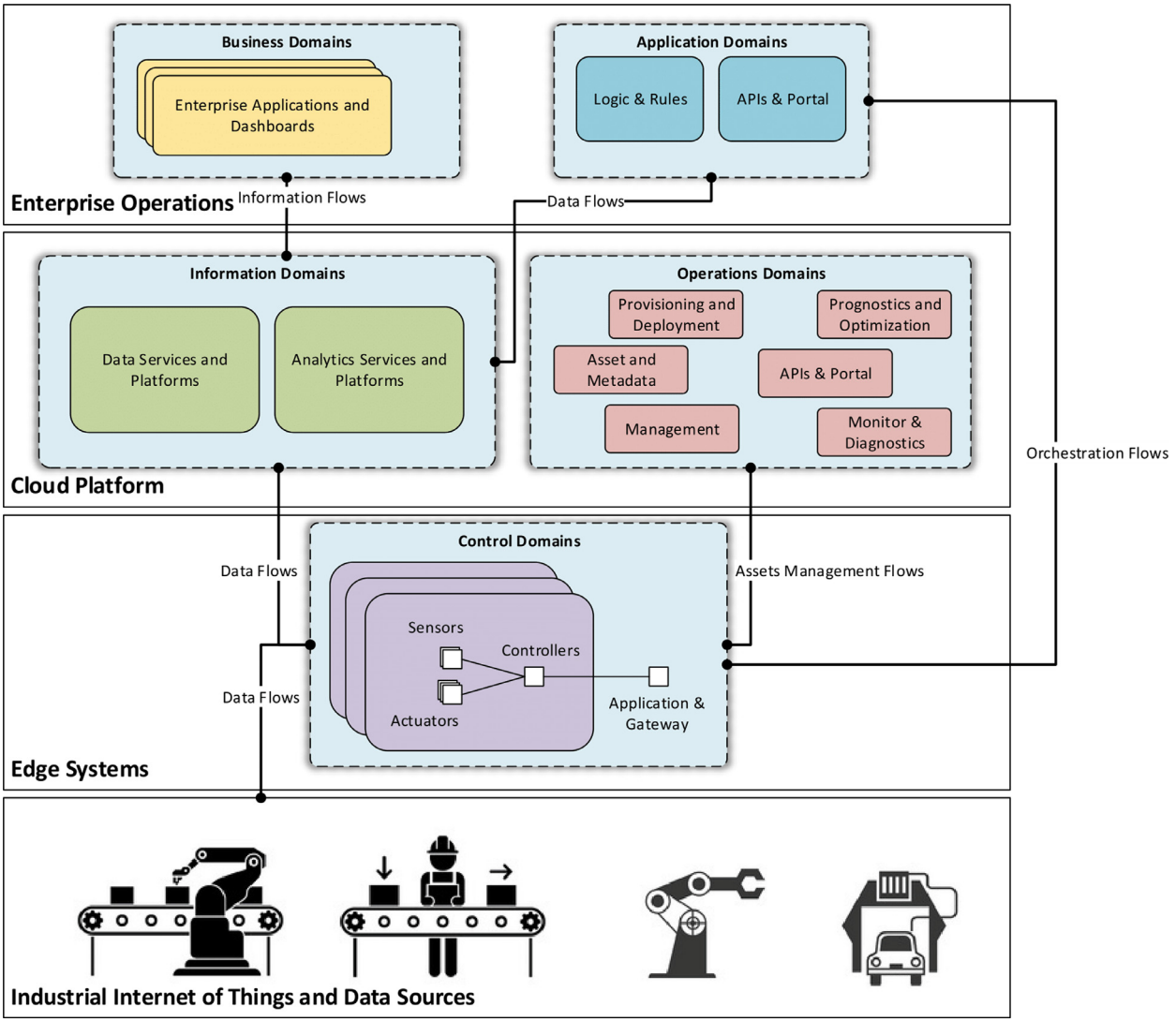

Fig. 2. A general architecture for IIoT systems.

cloud computing systems empower IIoT applications at Layer-2 and Layer-3, respectively. The enterprise applications are depicted at Layer-4. Fig. 2 also shows the flow of data and information among different layers as well as it exhibits the orchestration flow for resource management and operational flow for managing assets in the industrial networks. However, different researchers perceive these architectures differently considering design variations in terms of location awareness, communication paradigms, computational assignments, execution paradigms, resource management schemes, safety, security, privacy, addressibility, and resilience, to name a few. Table 4 shows the main features of IIoT architectures. The details of these architectures is given as follow.

Campobello et al. [12] have proposed a solution for IIoT named Wireless EVolution for Automation (WEVA) that is based on open source software and communication protocols. Its architecture consists of sensors, actuator boards, motes and operating system, protocols, access gateway, services, and applications. Moreover, WEVA uses Easy WSN as a graphical management tool. The authors suggest that IPv6 is a requirement for IIoT in terms of flexibility. However, incorporating these network technologies is not an easy job in order to achieve a high-performance IIoT in terms of (latency, security etc.). Many researchers have proposed solutions however, they address a specific performance issue and ignore the integration of Wireless Sensors Network (WSN) which plays important role in industrial applications.

Lee et al. [13] have proposed an IIoT suite to achieve re-industrialization for Hong Kong by addressing various challenges like objects identification in real-time and their locations throughout the manufacturing processes, establish a network system that allows objects to communicate between the network and other objects in real time etc. The main components of the IIoT suite architecture include a smart hub and a cloud platform. The smart hub works as a gateway for IoT devices and

Table 4
Main features of IIoT architectures.

Study	Industry	Deign type	Protocol	Hardware	Software	Main features
WEVA [12]	General Industry	Practical Design	IEEE 802.15.4, IPv6, CoAP, Chinese Remainder Theorem (CRT)	IRIS, TelosB, TP-Link MR3020	TinyOS, EasyWSN, OpenWrt	The proposed architecture is consisting of open source software and communication protocols are used. The network set-up and maintenance is done through a GUI.
Lee et al. [13]	Manufacturing Industry	Conceptual Design	MQTT/ CoAP, Wi-Fi, Bluetooth/BLE, ZigBee and Z-Wave	Smart Hub	XML/ JSON, RESTful Web Service	The proposed IIoT suite a smart hub and a cloud platform for re-industrialization in Hong Kong. The proposed IIoT suite helps in up-gradation and achieving high production in manufacturing industry.
Khan et al. [14]	Oil and Gas Industry	Conceptual Design	Wi-Fi, Bluetooth, ZigBee	Smart Objects, Smart Gateway	Cloud based Servers	The proposed architecture can be applied to the operations of all three sectors (i.e. downstream, midstream and upstream) of oil and gas industry.
IIHub [15]	Manufacturing Industry	Test-Bed	Wi-Fi, ZigBee, CoAP	RFID labels, Modbus-RTU, IIHub controller	XML, UML	The IIHub is proposed to slove the issue of deployment, configuration, and interaction between heterogeneous IIoT devices.
I3Mote [16]	General Industry	Prototyping Development	IEEE 802.15.4, 6LoWPAN, Bluetooth and BLE	ARM - MSP432, CC2650, HART	Code Composer Studio V.7, GNU ARM GCC compiler, TI-RTOS	The I3Mote is an open Industrial hardware platform for prototyping and final product development of IIoT.
Kaleem et al. [17]	General Communication Architectur	Conceptual Design	OpenFlow and 3GPP protocols	UAV, eNodeB, LTE, home eNBs (HeNB), remote radio head (RRH)	Cloudlet based services	The proposed architectures could be used in IIoT environment to provide efficient, low-cost data processing and data communication services for public safety in emergency/disaster situations.

manages IoT devices at different locations. The smart hub intends to accomplish three tasks. First, it facilitates the communication, data exchange and data processing between IoT devices. Second, it provides convenient solutions when scaling the system with new IoT devices. Finally, it provides a secure connection channel between IoT devices and the cloud platform by performing data collection, filtering, aggression, and formatting. The cloud platform of IIoT acts like the brain of the IIoT suite, and is responsible for performing Identification and Access Management (IAM), load balancing, device discovery/configuration, routing algorithm, monitoring and controlling IoT devices.

Khan et al. [14] have proposed an IoT based architecture for controlling and monitoring of oil and gas industry operations. The proposed architecture can be applied to the operations of all three sectors (i.e. downstream, midstream and upstream) of oil and gas industry. The architecture comprises of three modules including a smart object, gateway, and control center. Each module performs special functionality and is consisting of three layers which include an application layer, network layer and a sensing layer. Smart objects are installed on different oil and gas equipment (e.g. pipelines, storage tanks, pumps and wellheads etc.). These smart objects are equipped with different types of sensors (flow, pressure, temperature and acoustic etc.) to detect different events like leaks, fire and fluid level etc. Smart objects send their sensed data directly or through gateway to the control center. Smart objects and gateways are also equipped with radio transceiver (short and long range). The control center consists of databases for data storage, management applications, smart object interfaces, data analysis and data visualization tools.

The deployment, configuration, and interaction between heterogeneous IIoT devices are an important issue. To cope with these issues, Tao et al. [15] have proposed an IIoT based hub called IIHub. The IIHub consists of three modules. The first module is called Customized Access Module (CA-Module) which is responsible for connecting heterogeneous devices called PMRs (Physical Manufacturing Resources) through a group of communication protocols. The second module is called A-Hub (Access Hub) which works as a bridge between factory worker, smart terminals and CA-Module through Wifi or Ethernet in-

terfaces and Constrained Application Protocol (CoAP) protocol. The third and most important module is called LPS (Local Pool Service) or smart terminals. LPS perform their different functions and are responsible for data collection, processing, smart decision making and storing. Based on data generated by PMRs, LPS perform real-time data processing and predict expected production rate, total energy consumption and PMRs predicted maintenance. Each IIHub module is embedded with special purpose libraries. CA-Module has a group of communication protocols which interact with each other using a library called CPPLib (Communication Protocol Package Library). A-Hub has an embedded library called MDIMLib (Multi-dimensional information models library) which help in connectivity. LPS has an embedded library called DPALib (Data Processing Algorithm Library) which perform data processing, analysis, and decision making.

Martinez et al. [16] have proposed an open Industrial hardware platform for sensing and connectivity called I3Mote. The main components of I3Mote include different type of sensors, processor (MSP432), wireless radio interface (CC2650) and multi-source power support (battery, solar and thermoelectric etc.). I3Mote is basically a prototyping hardware which aims to provide all sensing and connectivity features required for IIoT and leads to final product. For fast development of industrial applications I3Mote platform also provide suite of software packages. The software tools can help in data actuation, processing, analysis and fast application development. I3Mote also provide a unique feature of simple application development by providing two separate processors for communication (CC2650) and applications (MSP432). The open hardware and software support of I3Mote makes it suitable for fast automation and adoption in Industrial sector.

Kaleem et al. [17] have proposed a three-layer architecture for Public Safety based on LTE (Long Term Evolution) called DR-PSLTE. In the proposed architecture the authors have employed various recent technologies (e.g. SDN (Software Defined Network), UAV (Unmanned Air Vehicle) as cloudlet, RAN (radio access network) to achieve the resilience against disaster and lower communication delay. The proposed architecture consists of three layers. The first layer is based on SDN whereby the SDN controller is responsible for the management of network synchronizations, control signals, and resources. The second layer is based on UAV which serves as cloudlet. These UAVs provide two basic services in disaster or emergency situations i.e., data processing and data communication. Finally, the third layer is based on a RAN which is responsible for radio access services to the end users. The proposed architectures could be used in IIoT environment to provide efficient, low-cost data processing and data communication services for public safety in emergency/disaster situations. However, power consumption, issues related to network management, placement, trajectory, and altitude prediction of UAVs are challenges faced by these proposed architectures.

2.2. Communication protocols for IIoT

In this section, we devise a taxonomy demonstrating the working of various communication protocols of IIoT and Table 5 shows the comparative analysis of communication protocols for IIoT.

Meng et al. [18] have proposed a ZMQ messaging design model which represents a generic and flexible Machine-to-Machine (M2M) messaging mechanism between the machines for event and command notification and data sharing. The experimentation using a case study of Quality inspection microwave sensor of food manufacturing production concludes that the proposed ZMQ technique is promising tool to deal with machine connectivity, machine presence and discovery, and messaging to allow ubiquitous data access and data interaction for rich sensing IoT application. The proposed technique solves the complex structure and heterogeneity problems of IIoT applications and contributes to cross-platform capability that allows the implementation on various powerful computers and light-weight devices.

Yang et al. [19] have first proposed two types of time synchronization attacks in IIoT called Absolute Slot Number (ASN) attack and Timeslot Template (TT) attack and then two algorithms called Sec_ASN algorithm and Threshold Filter (TOF) have been proposed to counter the proposed two attacks using IEEE802.15.4e-based IIoT protocol stack. When new nodes join the network, they can receive incorrect values of ASN, under ASN attack. On the other hand in TT attack the malicious node misguide the legitimate node for calculating the error clock offset. The Sec_ASN is the combination of authentication and a method called 2s + 1. The authentication is achieved through two steps, first verifying the information about the sender and then checking the sent information for tampering during communication. For the method 2s + 1, one node is selected from neighboring nodes as time parent node for synchronizations. TOF algorithm is proposed for clock offset estimation using least squares method through the difference between normal node times and sending time of the node.

Qiu et al. [20] have proposed a robust time synchronization scheme known as R-Sync which eliminates the isolated nodes to makes all nodes synchronized and also reduces energy consumption on entire synchronization process. Two timers are adopted to pull isolated nodes to join the synchronized networks. One timer is for time synchronization using two-way message exchanges and another timer at the beginning of the synchronization process. The authors have also introduced a root node selection algorithm to balance energy consumption among sensor nodes and extend the lifetime of sensor networks. The proposed algorithm is compared with three existing time synchronization algorithms, Timing-sync Protocol for Sensor Networks (TPSN), Groupwise Pair selection Algorithm (GPA), and Spanning Tree-based Energy-efficient Time Synchronization (STETS) and through experimentation it is shown that the proposed R-Sync algorithms has lower energy consumption than GPA, TPSN and STETS algorithms, especially in densely connected and large scale networks.

Katsikeas et al. [21] studied the security implementation of MQTT (Message Queue Telemetry Transport) protocol using payload encryption (with AES, AES-CBC, AES-OCB) and link layer (with encryption with AES-CCM) in industrial domain. The authors evaluated and compared the secure and lightweight MQTT implementation using WSN testbed (Raspberry Pi) and through simulator. Two nodes are used during evaluation process, Publisher to emulate IIoT sensors and encrypt the data,

Table 5
Comparative analysis of communication protocols for IIoT.

Scheme	Protocol	Topology	Latency	Hardware	Remarks
Meng et al. [18]	ZMQ messaging protocol based on low level TCP/UDP	Distributed	High latency	Matlab, Visual C	Messaging mechanism for event and command notification and data sharing between the machines is evaluated.
Yang et al. [19]	IEEE802.15.4e time synchronization protocol	Distributed	-	OpenWSN Platform with OpenSim simulator	Mitigation of ASN and timeslot template attacks.
Qiu et al. [20]	R-Sync time synchronization protocol	Distributed	-	NS-2, sensor modules based on ARM Cortex-M3 (88MZ100) with 32MHz crystal oscillator	The scheme achieves high accuracy and low energy consumption as compared to TPSN, GPA, STETS.
Katsikeas et al. [21]	MQTT 3.1.1,OASIS, ISO/IEC, TLS, IPSec	Distributed star	Optimized high latency	Zolertia Z1 Motes (Test-bed), Mosquito, 6lbr as Border Router, Raspberry Pi, Four wind turbines.	Evaluation of different security mechanisms protecting the MQTT-enabled interactions on a test-bed.
Ferrari et al. [22]	MQTT 3.1 and 3.1.1	Distributed	Varying Latency	IOT2040-Siemens, Intel Quark x1020, Yocto Linux (kernel release 2.2.1), Intel i3-5000, Windows 7, Mosquito	Authors experimentally investigate the data transfer latency in IIoT devices deployed in a worldwide scale.
Kiran et al. [23]	Markov-Chain based Slotted/ Unslotted CSMA/CA and PCA based Model	Distributed star	High	IITH motes, Contiki 3.0	Slotted PCA reduces delay and power consumption compared with slotted CSMA/CA. Unslotted PCA also reduce delay and power consumption compared to unslotted CSMA/CA.

and Subscriber to emulate IIoT actuators and decrypt the data. For comparison, latency, memory usage and energy consumption are considered. It is observed that MQTT implantation payload encryption (with AES, AES-CBC, AES-OCB) required more memory, energy and high latency as compare to MQTT implantation with link layer (with encryption with AES-CCM). However, if payload size is limiting factor, AES-CBC could be a better option.

Ferrari et al. [22] have investigated the latency of MQTT protocol for IIoT by observing the round trip time (RTT) through transferring data from the field to the Clouds and back. The authors have used embedded device IoT2040 from Siemens, energy saving Intel Quark x1020 (+secure boot), 1 GB RAM, 2 ethernet ports, 2xRS232/485 interfaces, battery backed RTC, Yocto Linux and industrial PC Intel i3-5000 with Windows 7 for the experimentation. The experimental works conclude that intercontinental roundtrip latency is less than 300ms, while local roundtrip latency is achieved at less than 50ms. The roundtrip delay is caused by the free Clouds used, internet connection, and the used hardware. However, implementation of filter reduces the values effectively.

Kiran et al. [23] have proposed a novel Markov chain based analytical/theoretical model to analyze the performance of unslotted Prioritized Contention Access (PCA) and Carrier-sense Multiple Access with Collision Avoidance (CSMA/CA) in nonbeacon-enabled PAN and slotted PCA and CSMA/CA in beacon enabled Personal Area Network (PAN). The reliability and the performance of the proposed model with less than 5% error is validated using Monte Carlo simulation and real-time test bed. The achieved results of slotted PCA claim that the reduction of 63.3% and 97% in delay and power consumption respectively compared with the slotted CSMA/CA, whereas unslotted PCA achieves reduction of 53.3% and 96% for delay and power consumption, respectively compared with unslotted CSMA/CA without significant loss of reliability.

2.3. Data management in IIoT

In this section, we describe the available data management techniques for IIoT. Theofanis Raptis et al. [24] have proposed a distributed Data Management Layer (DML) for data storage in IIoT. The proposed DML interact with network layer to help in identifying the network nodes for generating, storing and requesting and the data. To reduce the latency and improve the network performance the DML works independently from the routing operations. The data is transferred between data generating nodes (source) and data requesting nodes (destination) through intermediate nodes called proxy nodes. All these nodes work through cooperation algorithm. The proxy nodes also work as caching node for efficient and fast data transfer between data generating and requesting nodes. The core idea behind DML is separating the network management from data

management. DML provide two functionalities; selection and identifications of intermediate nodes (proxies) and through efficient mechanism deliver and distribute data.

Lucas-Estan et al. [25] have proposed software defined hierarchical and multi-tier architecture for network connectivity and data management for Industry 4.0. The proposed architecture enables data distribution and network connectivity through different available heterogeneous licensed and unlicensed wireless technologies. The heterogeneous technologies include 5G, 5G-PPP, LTE, IEEE802.15.4e, ISA100.11a and WirelessHART. The main idea behind enabling these heterogeneous wireless technologies is to operate them together without any interference using RAN Slicing and Cloud RAN. The idea is achieved through the concept of cell or subnetworks. Each cell or subnetworks use different set of wireless technology. For example for normal or local communication within the cell, unlicensed technology can be used (e.g. WirelessHART) and for time-critical or centralized (among cells) communication licensed technology (e.g 5G) can be utilized. Through hybrid management, the data management and radio resources inside the cell are manage through local entity also called Local Manager (LM) and between the cells through central management entity also called Orchestrator. Orchestrator is responsible for all data related process and functions like data storage, distributions, replication and management.

Rao et al. [26] have proposed a data aggregation scheme through device to device association in IIoT. In the proposed scheme, each IoT device is connected to Base Station (BS) through intermediate devices called User Equipments (UEs). The IoT devices send their sensed data to associated UEs. UEs aggregate the receive data from IoT devices and forward it to BS. BS uploads the received aggregated data from UEs for further processing and storage to cloud servers. Each IoT device is associated with UEs. The association is based on three different schemes i.e. random, fixed and greedy. In all three association scheme, the IoT devices are linked with UEs; when they have data to transmit called random, at system deployment and instillations phase is called fixed and based on the number of devices a UEs can support is called greedy scheme.

Theofanis Raptis et al. [27] have proposed Edge computing based data distribution scheme for prolonging the lifetime of IIoT network. To minimize the access latency and energy consumption of IoT devices, the authors have introduced intermediate nodes called proxies or Edge nodes for data storage. These Edge nodes receive the data from resource limited IoT devices and store the received data and as serve as cache points for the consumers nodes (data requesting nodes). The authors have also proposed heuristic based centralized algorithm for the selection and searching of these distributed Edge nodes who store the data. The algorithm learns the data request patterns from consumer nodes requests and locations of Edge nodes for the follow of data. The proposed scheme is implemented using testbed develop by FIT IoT-LAB. The testbed consist of 30 WSN nodes, these nodes support IEEE 802.15.4.

Conventional IoT- cloud systems enable centralized data processing for big data analytics applications. This approach results in massive data transfer from IoT end to cloud systems therefore it increases cost of data transfer, bandwidth utilization, potential privacy and security threats, and incremental cost of processing large and duplicated data in cloud systems. Concentric Computing model (CCM) was proposed as an alternate approach in order to run big data applications in multi-layer data processing environments whereby devices and systems with different granularities and processing power perform collaborated data processing by considering overall application objectives [28]. The essence of CCM model lies in early data processing i.e. big data streams should be processed as early as it was produced in order to minimize the issues created in conventional IoT-cloud environments. The CCM model caters the devices and systems at five different layers namely, (1) sensing systems (i.e., IWSNs, IoT devices, machines' and peoples' data); (2) outer gateway processors (i.e., smart routers, application servers, smart switches); (3) inner gateway processors (i.e., cloudlets, micro-clouds); (4) outer central processors (i.e., virtual servers, VPN servers, cloud controllers); (5) inner central processors (i.e., WAN servers, cloud data centers). However, the design of CCM should be flexible enough to enable same type of algorithms at all layers in order to easily switch the application processing by considering the available computational and energy resources at one end and the computational complexities and data processing requirements at the other end. The advancements on CCM are still at its earlier stages but it is perceived to have great potential in future research applications for IIoT systems.

3. Enabling technologies for IIoT

The backbone of IIoT is established by enabling a large plethora of technologies including IoT, cloud computing, big data analytics, artificial intelligence, cyber physical systems, augmented reality, virtual reality, Humane-to-Machine (H2M), and M2M communication.

3.1. Internet of things

Considering the connected factory scenario, IoT devices assist in real-time data collection and actuation. Being the primary component in IIoT, these devices track the factory assets across the globe. The whole process which is starting from raw material and ends with finish products is monitored using IoT devices in order to achieve significant reduction in labor cost and manual system management. The IoT devices in a fully connected IIoT system are deployed across all the factory facilities ranging from warehouses to production facilities and distribution centers. However, the configuration, deployment, monitoring, and maintenance of these devices is a challenging task and require highly qualified technical staff.

3.2. Blockchain technology

The blockchain is among the most important technologies that will play a key role to bring the dream of IIoT into reality [29]. Currently, an intensive research is carried by academia and industry on blockchain technology in various fields such as finance, healthcare, supply chain, car insurance. The IoT enabled devices used in smart industry generate a huge amount of data. The data generated by these IoT devices is multipurpose, the data is analyzed and processed for performance monitoring of devices, anomaly detection, diagnosis, predictive maintenance, asset monitoring, tracking of the complete product lifecycle from raw material to finishing goods and delivery to end consumers. However, sharing this important data with all entities involved in the IIoT system in a secure manner is a very challenging task. The unique characteristics of blockchain technology like distributed nature, traceability, survivability, trust, tamper resistance, security, and inherent data provenance make it suitable for IIoT. More recently blockchain technology is utilized for IoT devices firmware updates and access control.

3.3. Cloud computing

The massive growth of data in IIoT requires highly distributed high performance computing systems in order to manage, process, analyze, and store the data. Cloud computing technologies provide compute, network, and storage services across all the facilities in an IIoT system. All connected devices and applications are directly interfaced with backend clouds. The cloud service models are designed as private (solely owned and managed by IIoT staff), public (solely owned and managed by third-party cloud vendors), or hybrid (whereby a mix of both service models is used). Since the establishment of data centers and recruitment of technical staff require high spending therefore private cloud service models are not a viable option for newly entrants and/or small and medium level enterprises. However, large and well-established multinational enterprises prefer the deployment of private clouds in order to ensure the safety, security, and privacy and cope with industrial espionage for competitive advantage.

3.4. Big data analytics

The devices and systems in IIoT generate massive amount of data streams resulting the requirement of highly sophisticated high performance computing systems for big data processing and analytics. However, it is quite challenging to specify when, how, and where to process and analyze the big data considering latency and real-timeliness in IIoT systems. In order to fully orchestrate the big data analytics services, IIoT systems enable different technologies for big data collection, storage, management, processing, analyzing, and actuation. The data collection technologies provide connectors to a large plethora of data sources including sensors, smart devices, onboard data collectors, web-enable data sources, and humane-machine movements in IIoT systems, to name a few. Similarly big data storage technologies facilitate in onboard, on premise, in-network, and remote data storage in cloud environments. The data management and processing technologies enable to handle big data near the sensors, in edge servers, and in cloud data centers. The data analysis technologies provide different tools for data mining, machine learning, deep learning, and statistical data analysis at different layers in IIoT systems. The actucation technologies enable interactions between IIoT devices and their ambient environments. Despite complexity, big data processing and analytics technologies play a primary role in next-generation IIoT systems.

3.5. Artificial intelligence and cyber physical systems

AI technologies ensure that IIoT system should run autonomously and intelligently to minimize the humane-interventions and improve efficiency. The AI technologies make IIoT autonomous by using complex AI technologies such as multi-agent systems and conversational AI. In addition, the intelligence is embedded at layers in IIoT systems from sensors to devices to edge servers and cloud data centers by enabling different search, optimization, and prediction algorithms. In order to minimize the human efforts and interventions, IIoT systems empower different cyber-physical systems such as manufacturing systems and industrial robots. The essence of CPS lies in onboard embedded IoT devices which enable different sensors and actuators to operate in the industrial environments. These onboard embedded IoT devices also facilitate in intelligent data processing for autonomous operations and enhance efficiency in IIoT systems. These efficiencies range from different operational efficiencies in industrial environments to system-wide efficiencies in CPS and IIoT systems.

3.6. Augmented and virtual reality

The Augmented Reality (AR) technologies help in aiding the industrial workers during complex operations such as assembling/de-assembling the machineries, complex industrial products, and mission critical systems. The AR technologies enable to monitor the workers and machines during operations and immediately generate alters or notifications in order to minimize the errors. The Virtual Reality (VR) technologies facilitate in visualizing the configurations and re-configurations of industrial functions and modules before actual implementations in IIoT systems. The use of VR enables to reduce the (re-)configuration times and cuts off the shut down time of industrial plants and machines. The VR simulations are designed by considering open standards which are designed by considering heterogeneity in CPS and IIoT systems.

4. Challenges

The heterogeneous and complex nature of IIoT systems has brought together many technical challenges, such as interoperability, security and privacy, scalability, heterogeneity, reliability and resource management. However, there are some important challenges that are still needed to be resolved. Herein, we discuss these challenges.

4.1. Efficient data management schemes

The vast adaptation of heterogeneous IIoT devices results leads to a radical increase in data volume. Sensors and actuators integrated with industrial devices generate an increased amount of sensed data streams with high velocity. The sensed data is stored on these heterogeneous IIoT devices, local gateway/edge servers and cloud servers are used for real-time and future decision making. Processing, transmission, availability, and storage of sensed data is a challenging task and require big efforts. To cup with these challenges, efficient data management models are required. These data management models should be capable of efficiently handling the huge amount of raw data generated by heterogeneous IIoT devices in an effective way. These models should also provide the data management services with high-speed data processing, reliable and secure data storage, retrieval and fast data flow.

4.2. Collaborations between heterogeneous IIoT systems

The suite of IIoT system is a collection of different heterogeneous and multi-vendor technologies such as industrial machine, robotics, IoT devices, sensors, actuators, gateways, edge nodes, edge/cloud data servers (data centers), different wired/wireless communication and cellular networks (WiFi, 5G). Integration and collaboration between these heterogeneous and multi-vendor technologies based IIoT system are a challenging issue. Different factors like synchronization, resource sharing, data sharing, interoperability, and data privacy enable the integration and collaboration more challenging. More research and development efforts are still required for flexible and efficient techniques for collaboration and interoperability.

4.3. Robust and flexible big data analytic technologies

For achieving the vision of IIoT and getting full benefits from the high volume of data generated by IIoT devices, there is a high demand for robust and flexible big data analytics technologies. The conventional database management systems are unable to produce the desired results as these systems are unable to process and analyze the high magnitude of data efficiently. Processing the IIoT data in real time a critical task as this data is used for critical real-time industrial automation operations such as predict a malfunction, predictive maintenance, increase production, reduce down-times and anomaly detection. Thus, to meet the varying demands of IIoT applications (i.e. data rates, latency and reliability etc.) there is a need for efficient and real-time big data analytics technologies for robust and efficient processing of data generated by IIoT devices. These data analytics technologies also provide processing and visualizations of data to support the whole product life-cycle (e.g. production, testing, customer feed-backs and after sale services etc.) for getting a full insight of business.

4.4. Trust on IIoT systems

Consumer acceptance and adaptation is directly connected to the success of any technology and is highly influenced by consumer Trust on these technologies. The successful deployment of IIoT based systems by the commercial customers (e.g. owners of the particular industry) is also affected by the trust on these IIoT systems. IIoT systems are in their infancy and most of the recent research literature highlighted security and privacy as a major challenge faced by these systems. Security and privacy of technology are strongly linked with the trust of their customers, thus, weak security and privacy of IIoT systems will discourage the customers from adoptions of these IIoT systems. Therefore, for successful deployment and adaptation of IIoT systems in the industry, customer trust must be deal properly with effective customer trust models. Hence, more research in the area of customer trust models is required for the successful acceptance of IIoT systems.

4.5. Coexistence of wireless technologies and protocols in IIoT

Recently, the IIoT is attracting growing attention from both academia and industry. Communication in IIoT is mandatory for the exchange of information. Therefore, communication in IIoT must be able to connect a large number of heterogeneous devices, provide enough bandwidth to transfer data and offer a deterministic behavior with low latency. In addition, some industrial applications have some restrict timing, reliability, availability, and security requirements. Many communication technologies, protocols, and standards are in used in IIoT. Recently, wireless system (WLAN, IEEE 802.15 (WSN)) and wireless devices is gaining much attention in contrast to the past wired communication. Wireless communication also imposes many challenges. Coexistence of different wireless system and protocols is a major challenge in IIoT. As there are many communication technologies and protocols. The question is which communication technology and protocol is the best for my application. One wireless technology or protocol cannot offer all the features and strengths that fit the various application requirements in IIoT. Therefore, selection of communication technology and communication protocol is a big challenge.

4.6. Enabling decentralization on the edge

The heterogeneity in data sources and massive production of continuous data streams require the availability of compute, network, and storage services on the edge of the Internet. Edge computing enables to enrich the end-nodes, however, the edge services as well as data management on the edge is fully orchestrated via centralized cloud controllers. This dependency not only increases the requirements of highly available communication channels but also leads towards single-point of failure in industrial system. The decentralization of edge-cloud services can help in addressing above-mentioned issues. The edge servers coupled with blockchain technologies can keep immutable traces of resource requirements from end-point devices and applications. In addition, the servers can enable decentralized resource provisioning and service orchestration without depending upon the centralized controllers.

4.7. Emergence of IoT specific operating systems

An IoT Operating System (OS) is designed to perform within the constraints that are particular to IoT devices, including restrictions on memory, size, power and processing capacity. Popular IoT OS in term of memory usage, programming language support, scheduler, and architecture are discussed in [30]. TinyOS and Contiki are mostly used IoT OSs by the research community as they fulfill most of the requirements of the application. The key requirements for the IoT OS can be a small memory footprint, real-time, energy efficiency, hardware agnostic operations, security, networking, protocols support, data storage, reliable communication, and end device management. In contrast to IoT applications such as smart home, smart grid, smart traffic, and smart health, applications in IIoT require very stringent QoS requirements. Security and privacy, reliable communication, power consumption, interoperability, heterogeneous devices support, and bandwidth consumption are the key challenges in IIoT. In [31], authors provide a comprehensive survey of the most relevant key features of an OS for IoT and its applications. Further, they discussed IoT OS according to their implemented technologies for communication, challenges, and case studies.

4.8. Public safety in IIoT

Public safety in case of emergency situations and catastrophe in IIoT should be highly prioritized. In case of disaster, the safety of industrial workers and equipment depends upon the timely detection of events, alert generation, site-localization and notification of alerts to emergency response service providers such as fire department, ambulance, disaster management units, traffic police, and other law enforcement agencies. However, the absence or malfunctioning of communication infrastructures in disaster areas becomes a major issue. In addition, collaboration and communication between various IIoT devices and other communication systems are challenging issues. Many recent studies have proposed network architectures based on public safety communications for IoT and future smart cities by utilizing UAVs, SDN, Edge computing and other advanced communication technologies e.g., LTE, 4G/5G, etc. However, research efforts are needed to design disaster-resilient, autonomous architectures which should enable highly efficient communication in normal circumstances. In addition, these architectures are perceived to ensure disaster recovery mechanisms for public safety in case of emergency situations.

5. Conclusion

The Industrial IoT (IIoT) system allows the industry to collect and analyze a large amount of data, that can be used, monetized and improve the overall performance of the systems for providing new types of services. In this paper, we have highlighted the latest state-of-the-art research efforts in IIoT. Particularly, three areas of research including IIoT architectures and frameworks, communication protocols and data management techniques are explored in detail. We presented various enabling technologies related to IIoT. Moreover, major open research challenges are identified for the successful deployment of IIoT.

This study concludes that the success of IIoT is hindered by a number of challenges highlighted in this study which include efficient data management schemes, collaborations between heterogeneous IIoT systems, robust and flexible big data analytic technologies, trust on IIoT systems, coexistence of wireless technologies and protocols in IIoT, enabling decentralization on the Edge, specific operating systems and public safety in IIoT. These challenges can be overcome by proposing appropriate solutions. This study can be utilized as a guideline to address some of the unresolved challenges in the field of IIoT. Our future research aims to explore the research trends in enabling personalized manufacturing in IIoT systems.

Declaration of Competing Interest

The authors declare no conflict of interest.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.compeleceng.2019.106522

References

[1] Zhu C, Rodrigues JJPC, Leung VCM, Shu L, Yang LT. Trust-based communication for the industrial internet of things. IEEE Commun Mag 2018;56(2):16–22. doi:10.1109/MCOM.2018.1700592.
[2] Mumtaz S, Alsohaily A, Pang Z, Rayes A, Tsang KF, Rodriguez J. Massive internet of things for industrial applications: addressing wireless IIoT connectivity challenges and ecosystem fragmentation. IEEE Ind Electron Mag 2017;11(1):28–33.
[3] Long NB, Tran-Dang H, Kim D. Energy-aware real-time routing for large-scale industrial internet of things. IEEE Internet Things J 2018;5(3):2190–9. doi:10.1109/JIOT.2018.2827050.
[4] Xu H, Yu W, Griffith D, Golmie N. A survey on industrial internet of things: a cyber-physical systems perspective. IEEE Access 2018;6:78238–59. doi:10.1109/ACCESS.2018.2884906.
[5] Aazam M, Zeadally S, Harras KA. Deploying fog computing in industrial internet of things and industry 4.0. IEEE Trans Ind Inf 2018;14(10):4674–82. doi:10.1109/TII.2018.2855198.
[6] Al-Gumaei K, Schuba K, Friesen A, Heymann S, Pieper C, Pethig F, et al. A survey of internet of things and big data integrated solutions for industrie 4.0. In: 2018 IEEE 23rd international conference on emerging technologies and factory automation (ETFA), 1. IEEE; 2018. p. 1417–24.
[7] Perera C, Liu CH, Jayawardena S. The emerging internet of things marketplace from an industrial perspective: a survey. IEEE Trans Emerg Top Comput 2015;3(4):585–98. doi:10.1109/TETC.2015.2390034.
[8] Sisinni E, Saifullah A, Han S, Jennehag U, Gidlund M. Industrial internet of things: challenges, opportunities, and directions. IEEE Trans Ind Inf 2018;14(11):4724–34. doi:10.1109/TII.2018.2852491.
[9] Jeschke S, Brecher C, Meisen T, Özdemir D, Eschert T. Industrial internet of things and cyber manufacturing systems. In: Industrial internet of things. Springer; 2017. p. 3–19.
[10] Liao Y, de Freitas Rocha Loures E, Deschamps F. Industrial internet of things: a systematic literature review and insights. IEEE Internet Things J 2018;5(6):4515–25. doi:10.1109/JIOT.2018.2834151.
[11] Lin SW, Miller B, Durand J, Bleakley G, Chigani A, Martin R, Murphy B, Crawford M. The industrial internet of things volume G1: reference architecture. Ind Internet Consort 2017;1:10–46.
[12] Campobello G, Castano M, Fucile A, Segreto A. Weva: a complete solution for industrial internet of things. In: International conference on ad-hoc networks and wireless. Springer; 2017. p. 231–8.
[13] Lee CKM, Zhang SZ, Ng KKH. Development of an industrial internet of things suite for smart factory towards re-industrialization. Adv Manuf 2017;5(4):335–43. doi:10.1007/s40436-017-0197-2.
[14] Khan WZ, Aalsalem MY, Khan MK, Hossain MS, Atiquzzaman M. A reliable internet of things based architecture for oil and gas industry. In: Advanced communication technology (ICACT), 2017 19th international conference on. IEEE; 2017. p. 705–10.
[15] Tao F, Cheng J, Qi Q. IIHub: an industrial internet-of-things hub toward smart manufacturing based on cyber-physical system. IEEE Trans Ind Inf 2018;14(5):2271–80. doi:10.1109/tii.2017.2759178.
[16] Martinez B, Vilajosana X, Kim I, Zhou J, Tuset-Peiró P, Xhafa A, Poissonnier D, Lu X. I3mote: an open development platform for the intelligent industrial internet. Sensors 2017;17(5):986. doi:10.3390/s17050986.
[17] Kaleem Z, Yousaf M, Qamar A, Ahmad A, Duong TQ, Choi W, Jamalipour A. Uav-empowered disaster-resilient edge architecture for delay-sensitive communication. IEEE Netw 2019:1–9. doi:10.1109/MNET.2019.1800431.
[18] Meng Z, Wu Z, Muvianto C, Gray J. A data-oriented M2M messaging mechanism for industrial IoT applications. IEEE Internet Things J 2017;4(1):236–46.
[19] Yang W, Wan Y, Wang Q. Enhanced secure time synchronisation protocol for IEEE802. 15.4 e-based industrial internet of things. IET Inf Secur 2017;11(6):369–76.
[20] Qiu T, Zhang Y, Qiao D, Zhang X, Wymore ML, Sangaiah AK. A robust time synchronization scheme for industrial internet of things. IEEE Trans Ind Inf 2017;14(8):3570–80.
[21] Katsikeas S, Fysarakis K, Miaoudakis A, Van Bemten A, Askoxylakis I, Papaefstathiou I, Plemenos A. Lightweight & secure industrial IoT communications via the MQ telemetry transport protocol. In: Computers and communications (ISCC), 2017 IEEE symposium on. IEEE; 2017. p. 1193–200.
[22] Ferrari P, Sisinni E, Brandão D, Rocha M. Evaluation of communication latency in industrial IoT applications. In: Measurement and networking (M&N), 2017 IEEE international workshop on. IEEE; 2017. p. 1–6.
[23] Kiran M, Rajalakshmi P. Performance analysis of CSMA/CA and PCA for time critical industrial IoT applications. IEEE Trans Ind Inf 2018;14(5):2281–93.
[24] Raptis TP, Passarella A. A distributed data management scheme for industrial IoT environments. In: Wireless and mobile computing, networking and communications (WiMob). IEEE; 2017. p. 196–203.
[25] Lucas-Estañ MC, Raptis TP, Sepulcre M, Passarella A, Regueiro C, Lazaro O. A software defined hierarchical communication and data management architecture for industry 4.0. In: Wireless on-demand network systems and services (WONS), 2018 14th annual conference on. IEEE; 2018. p. 37–44.
[26] Rao S, Shorey R. Efficient device-to-device association and data aggregation in industrial IoT systems. In: Communication systems and networks (COMSNETS), 2017 9th international conference on. IEEE; 2017. p. 314–21.
[27] Raptis T.P., Passarella A., Conti M.. Maximizing industrial IoT network lifetime under latency constraints through edge data distribution. In: 1st IEEE international conference on industrial cyber-physical systems, (ICPS)(May 2018), available at http://cnd.iit.cnr.it/traptis/2018-raptis-icps.pdf.
[28] ur Rehman MH, Yaqoob I, Salah K, Imran M, Jayaraman PP, Perera C. The role of big data analytics in industrial internet of things. Future Gener Comput Syst 2019;99:247–59. doi:10.1016/j.future.2019.04.020.
[29] Miller D. Blockchain and the internet of things in the industrial sector. IT Prof 2018;20(3):15–18.
[30] Javed F, Afzal MK, Sharif M, Kim B-S. Internet of things (IoT) operating systems support, networking technologies, applications, and challenges: a comparative review. IEEE Commun Surv Tutor 2018;20(3):2062–100.
[31] Zikria YB, Kim SW, Hahm O, Afzal MK, Aalsalem MY. Internet of things (IoT) operating systems management: opportunities, challenges, and solution. Sensors 2019;19:1–10.

W. Z. Khan is currently with Faculty of Computer Science and Information System, Jazan University, Saudi Arabia. He received his Ph.D. from Electrical and Electronic Engineering Department, Universiti Teknologi Petronas, Malaysia. His research interests include Security, Privacy, IoT, IIoT, and WSNs. He is SMIEEE.

M. H. Rehman is an Assistant Professor with the National University of Computer and Emerging Sciences, Lahore, Pakistan, where he works on data stream mining systems for the Internet of things. His research covers a wide spectrum of application areas, including smart cities, mobile social networks, blockchain and Industry 4.0.

H. M. Zangoti received his BS, MS degrees in Computer Science from Jazan University, and Monmouth University, respectively. Currently, he is pursuing his Ph.D. in Computer Science at Florida International University. His research interests include IoT, SIoT, networking, security, and social networks.

M. K. Afzal is currently working as Assistant Professor in Department of Computer Science at COMSATS, Wah Cantt Pakistan. He received his Ph.D. Degree from Department of Information and Communication Engineering, Yeungnam University, South Korea, in December 2014. His research interest includes wireless sensor networks, ad hoc networks, Smart Cities, 5G, and IoT.

N. Armi is a Researcher from Indonesian Institute of Sciences. He was an Assistant Professor in Jazan University, Kingdom of Saudi Arabia from 2016 to 2018. He received his Ph.D. degree from Universiti Teknologi Petronas, Malaysia in 2013. His research interests includes Signal Processing, Wireless Communication & Networks.

K. Salah is a Full Professor with the Department of Electrical and Computer Engineering, Khalifa University, UAE. His research interests include cloud and fog computing, IoT, blockchain, and cybersecurity. He received the Ph.D. degree in computer science from the Illinois Institute of Technology, USA, in 2000.