Industrial Internet of Things: A Review of Improvements Over Traditional SCADA Systems for Industrial Automation

Bilal Babayigit and Mohammed Abubaker

***Abstract*—This review article provides an overview of the potential of the Industrial Internet of Things (IIoT) to revolutionize industrial automation. The IIoT is the Internet of Things (IoT) but in an industrial context, i.e., IIoT is used more to connect machines and devices in industrial environments. The IIoT has the potential to benefit from advances in artificial intelligence, particularly machine learning and deep learning, to increase efficiency and productivity and reduce overhead costs. We provide an overview of the supervisory control and data acquisition system, a definition of IIoT, and how IIoT can offer industry greater potential for system integration to improve automation and optimization. In addition, five of the major IIoT protocols are discussed, namely, message queue telemetry transport, advanced messaging queuing protocol, constrained application protocol, data distribution service, and open platform communication unified architecture. We then identified key IIoT improvements for industrial automation. These are; efficient and low-cost systems, digital twin, machine failure prediction, real-time remote monitoring, and security. We then discussed the key research in the literature for each category. We presented some public IIoT datasets so that researchers can use them to develop new learning models to improve the security of IIoT systems. Finally, we discussed some of the limitations, recommendations, and future perspectives for developing IIoT-enabled systems.**

***Index Terms*—Deep learning (DL), digital twin (DT), industrial Internet of Things (IIoT), IIoT protocols, Internet of Things (IoT), machine learning (ML), supervisory control and data acquisition (SCADA), security.**

I. Introduction

THE Industrial Internet of Things (IIoT) industry was valued at USD 76.7 billion in 2021 and is expected to grow to USD 106.1 billion by 2026, at a compound annual growth rate of 6.7% [1]. IIoT refers to the use of the Internet of Things (IoT) in industrial contexts [2], [3], [4], [5], [6], [7], [8], [9]. It is the mainstay of the fourth industrial revolution known as Industry 4.0, while supervisory control and data acquisition (SCADA) was the distinguishable component of Industry 3.0. IIoT helps making smart decisions from real-time data received by intelligently interconnected devices. Many industries, such as transportation [10], agriculture [11], smart cities [12], power system [13], oil and gas [14], healthcare [15], and smart factories [16] are seeking to benefit from the adoption of IIoT-enabled systems as a means for digital transformation. This helps to increase the efficiency and productivity of these various sectors. Through meaningful automation with the help of IIoT and its supporting technologies such as artificial intelligence (AI), machine learning (ML), deep learning (DL), sensors, cybersecurity, web technologies, networks, cloud computing, edge computing [17], [18], [19], [20], [21], [22], [23], [24], many industrial sectors could improve their performance and increase production rates in high quality, increasing their opportunities to enter new markets.

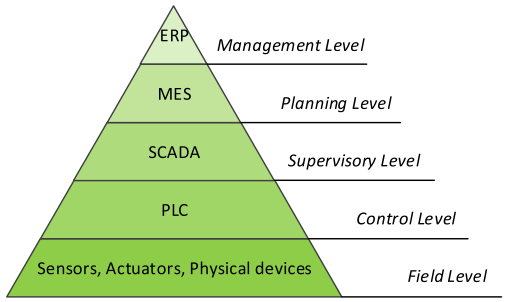

Fig. 1. Abstract view of the automation pyramid.

The main difference between the IoT and IIoT is that the IoT is usually used for individual usage such as in smart home devices, which are usually low-risk, while the IIoT is more used to connect machines and devices in industrial environments, focusing on machine-to-machine (M2M) communication, and any failure can lead to high-risk losses. In IIoT for factory usage, the data generated by the industrial sensors are generally input to the programmable logic controller (PLC) [5], [25].

To help the business become more efficient, it is important to understand the automation pyramid for industrial automation. The automation pyramid is a graphical representation of various technologically integrated levels of automation in the manufacturing industry [26], [27], [28], [29]. It is logically divided into five levels, as shown in Fig. 1. The bottom level, known as the field level, consists of physical devices such as sensors and actuators that generate the raw data and handle the physical works of the industrial facility. The second level is the control level, which may contain many PLCs that control and operate the devices in the field level. They receive data from the sensors in the field level to make decisions about

Manuscript received 8 November 2022; revised 3 March 2023; accepted 20 April 2023. Date of publication 10 May 2023; date of current version 15 March 2024. This work was supported by Erciyes University Scientific Research Projects Coordination Unit (ERU/BAP) under Grant FDK-2023-12860. *(Corresponding author: Mohammed Abubaker.)*

Bilal Babayigit is with the Department of Computer Engineering, Erciyes University, 38039 Melikgazi, Turkey (e-mail: bilalb@erciyes.edu.tr).

Mohammed Abubaker is with the Department of Computer Engineering, Erciyes University, 38039 Melikgazi, Turkey, and also with the Palestine Technical College, P920 Gaza, Palestine (e-mail: mabubaker@ptcdb.edu.ps).

Digital Object Identifier 10.1109/JSYST.2023.3270620

TABLE I
COMPARISON WITH EXISTING REVIEW ARTICLES ON IIOT

Ref.	IIoT structure	SCADA	IIoT sensors	IIoT Protocols					Improvement for Industrial Automation					ML/DL	Datasets
				MQTT	AMQP	CoAP	DDS	OPC UA	1.	2.	3.	4.	5.		
[2]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
[4]	●	○	◑	○	○	○	○	○	○	○	○	○	○	○	○
[5]	●	◑	○	○	○	○	○	○	○	○	◑	○	◑	○	○
[7]	●	○	○	◑	○	○	○	○	○	○	○	○	○	○	○
[8]	●	○	○	○	○	○	○	○	○	○	○	○	●	○	○
[9]	●	◑	○	○	○	○	○	○	○	○	○	○	◑	○	○
[17]	●	○	○	○	○	○	○	○	○	○	○	○	●	○	○
[18]	●	○	○	○	○	○	○	○	○	○	●	○	○	●	○
[30]	○	○	○	●	◑	●	○	○	○	○	○	○	○	○	○
[31]	●	○	○	●	●	●	●	○	○	○	○	○	○	○	○
This study	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

● Fully addressed, ◑ Partially addressed, ○ Not addressed.
1. Efficient and Low-cost systems, 2. DT, 3. Prediction of machines failures, 4. Real-Time Remote monitoring, 5. Security

what actions should be taken by the actuators in the field level. The SCADA system operates at the supervisory level, which is essentially a collection of hardware and software components used to monitor and control systems from a single location, with functions typically controlled remotely by visualizing data in a graphical user interface (GUI). The planning level uses a computerized system called a manufacturing execution system to help monitor the entire manufacturing process from raw material usage to on-time product delivery. At the top of the automation pyramid is the management level, which uses a software-integrated management system known as an enterprise resource planning system to manage and integrate all of the factory's business processes.

The main drawback of the automation pyramid is that data are exchanged between adjacent levels and integration of multiple vendors is not supported. Therefore, the levels of this model are not fully connected and integrated, resulting in lack of efficiency and poor decisions. On the other hand, IIoT is about taking decisions based on real-time information rather than relying on outdated data in paper reports from the previous day.

There are some previous surveys on IIoT; however, they typically focus on some aspects related to IIoT and they did not give the reader the whole knowledge needed in the field of IIoT. Table I lists a comparison of this article with existing review articles on IIoT. And Table II lists the key abbreviations used in this article with their definitions.

This review article provides a roadmap for the wide variety of potentials of IIoT-enabled systems to revolutionize industrial automation, as summarized in Fig. 2. The main contribution of this work is to comprehensively reviewed the IIoT including the development trend, the potential values, the important products, the major protocols, the key issues to improve the industrial automation, and the role of ML/DL in IIoT applications. Thus, the reader can easily get the main information about IIoT, which is not available before.

The rest of this article is organized as follows. Section II presents an overview of the SCADA system. The IIoT definition, sensors, and protocols are explained in Section III. Section IV provides a comprehensive review of the major improvements in IIoT-enabled industrial automation systems. Section V lists the publicly available IIoT datasets. Section VI discusses limitations and recommendations and future perspectives for developing IIoT-enabled systems, while conclusions are given in Section VII.

II. SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM

A. SCADA Definition and Components

SCADA is an acronym for Supervisory Control And Data Acquisition [32], [33], [34]. It has the ability to remotely control and monitor a system and to collect information about it. The SCADA system can be used in different industries, such as manufacturing, oil and gas, electric power generation and distribution, and water and sewage [35], [36], [37], [38], [39]. There are many commercial vendors worldwide offering proprietary SCADA systems, for example, Schneider Electric (France), Siemens (Germany), Rockwell Automation (USA), and Emerson Electric (USA).

The main components of SCADA systems consist of 1) remote terminal units (RTUs) and/or PLCs, which are microcontrollers or microprocessors that interact with and collect data from field devices such as sensors and actuators; 2) master terminal units (MTUs), which are connected to the RTUs, with the RTUs forward the data to the MTU via communication channels; 3) human–machine interface (HMI), which is usually installed in the MTU to visualize all SCADA operational information such as controlling and monitoring, as well as communication status between RTUs and MTUs.

There are four generations of SCADA architectures: the first generation of SCADA is referred to as monolithic SCADA, in which there were generally no networks, so SCADA systems were stand-alone systems that had virtually no connections to other systems. With the advent of the local area network (LAN), it became possible to connect SCADA systems to related systems, leading to the second generation of SCADA, called Distributed SCADA. However, communications were generally proprietary, which meant that connections outside the manufacturers of a particular SCADA system were not possible [38]. The third-generation SCADA system, called Networked SCADA,

TABLE II
LIST OF ABBREVIATIONS USED IN THIS ARTICLE

Abbreviation	Definition
AES	Advance Encryption Standard
AI	Artificial Intelligence
AMQP	Advanced Messaging Queuing Protocol
API	Application Programming Interface
BLE	Bluetooth Low Energy
CoAP	Constrained Application Protocol
DCPS	Data Centric Publish Subscribe
DDS	Data Distribution Service
DL	Deep Learning
DLRL	Data Local Reconstruction Layer
DoS/DDoS	Denial-of-Service/Distributed Denial-of-Service
DT	Digital Twin
DTLS	Datagram Transport Layer Security
ERP	Enterprise Resource Planning
FDI	Field Device Integration
FPGA	Field-Programmable Gate Array
GUI	Graphical User Interface
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology
JSON	JavaScript Object Notation
LAN	Local Area Network
M2M	Machine-To-Machine
MES	Manufacturing Execution System
ML	Machine Learning
MQTT	Message Queue Telemetry Transport
MTU	Master Terminal Unit
NAS	Network-Attached Storage
NN	Neural Network
OASIS	Organization for the Advancement of Structured Information Standards
OPC UA	Open Platform Communication Unified Architecture
OT	Operational Technology
PdM	Predictive Maintenance
PLC	Programmable Logic Controller
QoS	Quality of Service
REST	REpresentational State Transfer
RF	Random Forest
RTPS	Real Time Publish Subscribe protocol
RTU	Remote Terminal Unit
SASL	Simple Authentication Security Layer
SCADA	Supervisory Control And Data Acquisition
SHA	Secure Hash Algorithms
SSL/TSL	Secure Sockets Layer/Transport Layer Security
SVM	Support Vector Machine
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VGG	Visual Geometry Group
VPN	Virtual Private Network
WAN	Wide Area Network
XSS	Cross-site scripting
YOLO	You Only Look Once

has communication protocols that are no longer vendor-specific, leading to more connectivity options in the form of a wide area network (WAN). IoT-based SCADA architecture is the fourth generation, where cloud services are integrated with the traditional SCADA system to provide more robust monitoring and control [40].

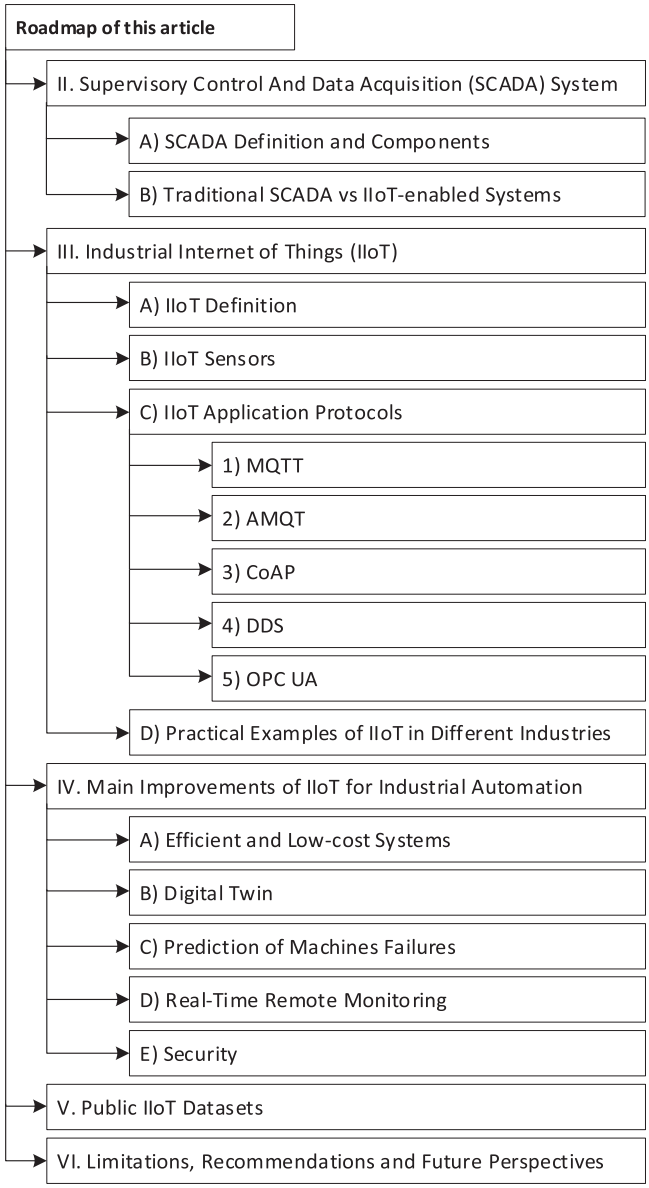

Fig. 2. Structure of this review article.

B. Traditional SCADA Versus IIoT-Enabled Systems

A traditional SCADA system is a centralized control system used to monitor and control field devices. It usually consists of a central control room connected to these devices. It works by using RTUs and/or PLCs to collect data from field devices, sending that data to the MTU for processing and analysis, and presenting that information to operators in the central control room via an HMI. However, SCADA systems have several limitations, including the following.

1) *Limited data collection:* They typically collect limited data from field devices, which can limit the amount of information available to operators for decision making.
2) *Latency:* Data collected by SCADA systems is often transmitted to the central control room, which can result in significant latency. This can limit the ability to respond quickly to changing conditions and potential problems.
3) *High cost:* They can be too expensive and require specialized server with vendor-dependent licensed software.

TABLE III
MAIN DIFFERENCES BETWEEN SCADA AND IIOT SYSTEMS

Feature	SCADA Systems	IIoT-enabled systems
Data Collection	Typically collects data from sensors and devices using RTUs and PLCs.	Collects data from a wide range of devices, including sensors, smart machines, and edge devices.
Data Analysis	Usually performs data analysis on-premises using specialized software.	Can perform data analysis both on-premises and in the cloud using a range of software tools, including ML/DL algorithms.
Connectivity	Typically relies on proprietary communication protocols and closed networks.	Relies on open communication protocols and can connect to a variety of networks.
Cost	Higher cost due to the need for specialized hardware and software.	Lower cost due to the use of off-the-shelf devices and software from different vendors.
Scalability	Limited scalability and can be difficult to expand.	Can be scaled to accommodate a growing number of devices.

4) *Lack of predictive maintenance (PdM):* Manual inspections and scheduled maintenance can be performed on SCADA systems, which diminishe the overall effectiveness and efficiency of the system.

On the other hand, IIoT-enabled systems can offer many advantages over SCADA systems to address these limitations.

1) *Improved real-time data collection and analysis:* SCADA systems typically have longer data collection intervals and processing times, making it difficult to make quick decisions in response to changes in the system. IIoT systems use edge computing and cloud-based processing to analyze data quickly and in real-time.
2) *Improved connectivity:* IIoT-enabled systems can communicate with a greater number of devices and sensors with open communication protocols, while SCADA systems often have a limited number of communication protocols, making it difficult to connect with newer devices or sensors.
3) *Improved PdM:* By collecting and analyzing data in real-time, IIoT-enabled systems can detect anomalies and predict machine failures before they occur, reducing downtime and maintenance costs.
4) *Better visualization:* IIoT-enabled systems can store and manage data in the cloud, allowing for greater flexibility and accessibility and making it easier to access and visualize data with web technologies over the Internet.

Overall, the relationship between SCADA and IIoT is that IIoT-enabled systems are an evolution of SCADA and incorporate advanced technologies to improve monitoring and control of industrial processes and infrastructure. Table III summarizes the key differences between traditional SCADA systems and IIoT-enabled systems.

III. INDUSTRIAL INTERNET OF THINGS

A. IIoT Definition

IIoT refers to the expansion and use of IoT in industrial areas. The main difference between IoT and IIoT is that IoT is typically associated with consumer devices and applications such as smart homes and wearables, which are generally low-risk, while the IIoT is more commonly used to connect machines and devices in industrial environments, with a focus on M2M communications, and any failure can result in high-risk losses and the amount of data collected in IIoT is much larger than in IoT. As a result, IIoT systems must meet higher performance requirements than IoT due to the critical nature of the industrial processes they monitor and control. Therefore, the key differences that distinguishing IIoT form IoT are industrial focus, a high level of reliability, and advanced analytics based on the large amounts of data generated in IIoT. The next section presents the advances in IIoT that are helping to transform industrial operations and increase efficiency and productivity in the industrial sector.

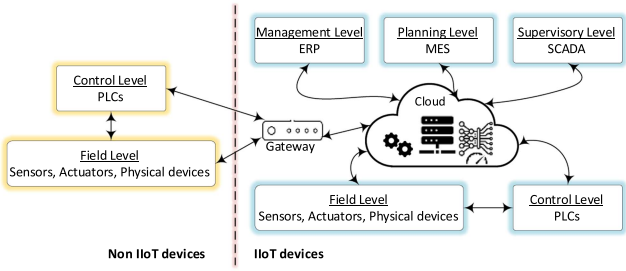

Fig. 3. Automation model concept for IIoT-enabled systems.

IIoT aims to improve efficiency, productivity, and real-time decision making in industry. The IIoT connects intelligent industrial devices so that they collect and exchange data through a central server, which can be installed locally or in the cloud. In this way, industries and businesses can access data faster and more efficiently, leading to greater transparency and intelligence throughout industrial processes. As a means of digital transformation, the IIoT is revolutionizing the concept of the automation pyramid by connecting all levels and offering industries greater potential for systems integration for better automation and optimization. The automation model for IIoT-enabled systems is shown in Fig. 3. In this model, all levels of the automation pyramid can be connected via the cloud using communication protocols. Thus, with the currently collected and analyzed data, a high production rate can be achieved with reduced operating costs. To avoid the immigration of industries into the IIoT-enabled system becoming too expensive, the legacy devices that already exist cannot be ignored in this process. These are non-IIoT devices that do not have intelligence or connectivity to the network. Therefore, these legacy devices can be connected to the IIoT-enabled network via an IIoT gateway, as shown in Fig. 3.

B. IIoT Sensors

A traditional sensor is a device that detects and measures certain events in its physical environment, such as temperature, humidity, and pressure. A smart or intelligent sensor, on the other hand, has built-in intelligence, the ability to self-adapt based on its environment, and the ability to better communicate in industrial networks [41], [42], [43], [44]. The terms IIoT sensors and smart sensors are often used interchangeably. IIoT sensors are designed to use the Internet for communication. Smart sensors are widely used in industrial environments to improve overall performance. They can be self-adapted to their operating environment by having a built-in microcontroller and data processing capabilities.

TABLE IV
EXAMPLES OF SENSORS USED IN IIOT-ENABLED SYSTEMS

No.	Sensor Name	Vendor	Measuring Parameters
1.	MaxSonar INT-D-01	Biz4Intellia	Level Monitoring
2.	Wireless Thermocouple Sensor INT-T-01	Biz4Intellia	Temperature
3.	INT-Av-01	Biz4Intellia	Distance, Temperature, pressure
4.	INT-Gas-02	Biz4Intellia	Carbon Dioxide (CO2)
5.	Intellia Asset GPS Tracker INT-ALT-01	Biz4Intellia	GPS, Temperature, Accelerometer
6.	Long Range Wireless Proximity and Light Sensor	NCD Industrial	Proximity, Light
7.	TCS34903FN Color Light-to-Digital	NCD Industrial	Color
8.	Wireless Particulate Matter Sensor	NCD Industrial	Air quality, Temperature, Humidity
9.	Long Range Wireless Accelerometer Gyro Magneto and Temperature Sensor	NCD Industrial	Accelerometer, Gyroscope, Magnetometer, Temperature
10.	Long Range Wireless 0-24VDC Voltage Monitor	NCD Industrial	Voltage Monitoring
11.	Wireless Motor Sensor for PdM	Phease IV - Leap Sensors	Temperature, Vibration, Electrical Current
12.	SG-LINK-200	LORD MicroStrain	Pressure, Strain, Load Cells, Accelerometer
13.	XS770A Wireless Vibration Sensor	Yokogawa	Vibration, Temperature
14.	RTS-227	Valmet	Rotation Frequency
15.	QCM50 Color Sensor	Banner	Color

This allows them to adjust their settings in response to changes in the environment. In this regard, the smart sensors support flexible clocking [45], i.e., the clock frequency can be reduced during a certain time interval to reduce power consumption when high accuracy is not required. In contrast, if the measurement conditions require high accuracy, the clock frequency must be increased [45]. For example, if a sensor observes a significant drift in temperature or vibration levels, it can modify its transmission frequency to match the new conditions. By doing so, more accurate and optimize measurements of industrial processes can be made yielding a variety of advantages related to real-time remote monitoring and advanced analytics in IIoT-enabled systems. However, it is not always suitable to integrate smart sensors into SCADA systems due to compatibility issues. SCADA systems employ proprietary communication protocols that may not be compatible with the protocols used by smart sensors.

There are various types of sensors used in IIoT systems, such as temperature sensors [46], humidity sensors [47], pressure sensors [48], proximity sensors [49], vibration sensors [50], force sensors [51], level sensors [52], gas sensors [53], color sensors [54], and accelerometer sensors [55]. These sensors play an essential role in IIoT-enabled systems. They work at the forefront of industry and are considered as the main source of the real-time data that helps maintain reliability and efficiency in industrial automation. IIoT sensors that have local processing capabilities can reduce the transmission of large sensor data from the edge to the cloud by enabling edge computing in the IIoT environment [56], [57], [58], [59]. Table IV lists some examples of sensors used in IIoT.

C. IIoT Application Protocols

The idea behind the IIoT is to connect the levels of the automation pyramid so that, for example, sensor data are available to all levels of the industrial network. An important aspect of connecting a large number of IIoT devices for IIoT-enabled systems is M2M communication protocols [30], [31], [60]. There are different types of IIoT protocols to meet the different requirements of the IIoT applications. Some of the IIoT applications rely heavily on information exchange between sensors via wireless interfaces and thus require a lightweight protocol with low overhead that ensures low power consumption and robust transmission. On the other hand, some of these applications involve more complex devices that require protocols that support many features such as access to the devices' profile and historical data. The key characteristics of the protocols to be used in the IIoT environment are light-weight, open source, cross-platform, and provide updates only when the IIoT node changes. In this section, we discuss the most important application protocols for the IIoT environment.

1) Message Queue Telemetry Transport (MQTT) Protocol: MQTT is an OASIS standard messaging protocol suitable for the IIoT applications [61], [62]. It is a publish/subscribe messaging protocol in which it consists of an MQTT server (broker) and MQTT clients (publishers or subscribers). The communication architecture of MQTT protocol is shown in Fig. 4. The MQTT client (publisher) generates data and publishes it to the MQTT broker on a specific topic. The MQTT client (subscriber) registers to the broker for specific topics to be informed through the broker when publishers publish data to these topics. The MQTT broker acts as an intermediate point to connect publishers and subscribers. It creates topics, stores generated data from the IIoT devices (publishers) to its belonged topics, and informs the subscribers with the stored data. The MQTT protocol is designed as a lightweight, open standard, simple, and easy to implement protocol. MQTT message header size is small; it is 2 bytes overhead and has a flexible payload with a maximum size of 256 MB. This protocol is a connection-oriented protocol runs over the TCP protocol. It uses TCP ports 8883 and 1883 for MQTT SSL/TSL and non-TSL connections, respectively. To ensure reliable message delivery, the MQTT protocol implements three quality of service (QoS) levels. The first level is QoS-0 referred as at most once delivery in which the message arrives at the receiver either once or it could be lost. The second level is QoS-1 known as at least once delivery in which the message arrives at the receiver at least once where the message is retransmitted to ensure that it is delivered at least once with a chance to be arrived as a duplicate. The third level is QoS-2 also known as exactly once delivery where neither loss nor duplication is acceptable [31], [60], [63], [64].

2) Advanced Messaging Queuing Protocol (AMQP): AMQP is an OASIS open standard application layer protocol for the IIoT to move messages between applications [65]. As the MQTT protocol, it supports reliable communication via message delivery guarantee primitives, including at most once, at least once, and exactly once delivery. AMQP requires a reliable transport protocol such as TCP to exchange messages and integrates TLS/SSL, which encrypts the data on transfer and simple authentication security layer, which allows for a secure authentication handshake between client and server for security. It supports

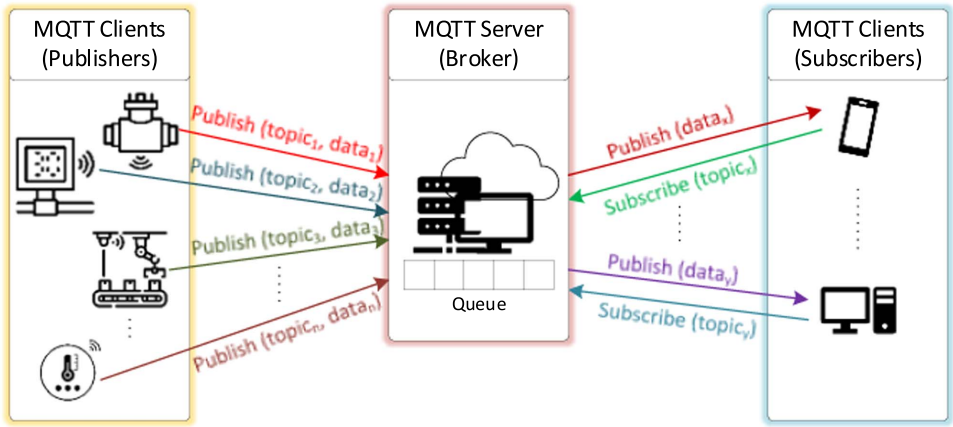

Fig. 4. Communication architecture for MQTT protocol.

a publish/subscribe messaging protocol architecture in which it consists of an AMQP server (broker) and AMQP clients (publishers or subscribers). The difference between MQTT and AMQP is that in AMQP broker consists of two main components: exchange and topic queues. Producer sends a message to an exchange. Exchanges then distribute message copies to queues, depending on rules defined by the exchange type and routing key provided in the message. The message is finally consumed by a subscriber. Messages received by the exchange have to be matched to the queue via a process called "binding." AMQP exchanges messages in various ways: directly, in fan-out form, by topic, or based on headers [64]. AMQP requires a fixed header of 8 bytes with message payloads size dependent on the broker [66].

3) Constrained Application Protocol (CoAP): CoAP was developed by the Internet engineering task force. It is suitable for IIoT applications because many IIoT applications are being developed to operate in constrained environments and devices, which are small, constrained embedded devices that run on low-power, very low-memory, and low-bandwidth bandwidth. CoAP is a connectionless M2M application layer protocol running on UDP. It is an asynchronous and lightweight protocol with a small header size of 4 bytes. It was developed based on the request/response client-server paradigm based on REpresentational State Transfer (REST) and supports GET, POST, PUT, and DELETE just like HTTP. However, unlike HTTP, CoAP handles this exchange asynchronously over UDP. Although CoAP is built on top of UDP, it has optional reliability and defines four types of messages: confirmable, nonconfirmable, acknowledgment, and reset messages. Requests and responses are transmitted in confirmable and nonconfirmable messages [60], [64], [67]. CoAP provides security through datagram transport layer security (DTLS), a secure network traffic protocol that supports packet loss handling, message reordering, and message sizing. However, DTLS requires numerous message exchanges to establish a secure session and is therefore characterized by high communication costs. Therefore, CoAP suffers from this challenge of DTLS. To overcome this problem, a lightweight secure CoAP for IoT (Lithe) was proposed by Raza et al. [68].

4) Data Distribution Service (DDS) Protocol: DDS is a real-time publish–subscribe protocol for M2M communications developed by the object management group (OMG). Unlike MQTT or AMQP, DDS is based on a brokerless publish/subscribe architecture that meets the real-time requirements for IIoT and M2M communications. It uses multicasting to provide excellent QoS and high reliability to its applications. DDS application programming interface (API) standards are language, operating system, and hardware independent. There are two layers: 1) data centric publish subscribe (DCPS) delivers data to subscribers and is a standard API for real-time, data-centric, topic-based, publish/subscribe; 2) data local reconstruction layer provides an interface to DCPS functions that enable the sharing of distributed data between IIoT devices. DCPS was built on the concept of a "global data space" that is accessible to all interested applications. Applications wishing to contribute information to this data space declare their intention to become publishers. Similarly, applications that wish to access portions of this data space declare their intent to become Subscribers. Each time a publisher adds new data to this "global data space," the middleware shares the information with all interested subscribers. DDS supports interoperability between different vendors when communicating via the real-time publish–subscribe protocol. However, DDS is heavy weight and consumes twice as much bandwidth as MQTT [69]

5) Open Platform Communication Unified Architecture (OPC UA) Protocol: OPC UA is an open-source, cross-platform, M2M communication protocol for industrial automation developed by the OPC Foundation [70]. The OPC UA integrates all functionalities of the OPC classic specification and is backward compatible to OPC classic. The OPC UA protocol typically uses the client–server approach for information access, i.e., it is configured to exchange data only between the OPC UA server and the OPC UA client. This client–server approach follows the request/response mechanism, which requires a standing communication between the client and the server, limited by network traffic. However, this drawback has been addressed by introducing the publisher/subscriber mechanism in OPC UA communication, where the publisher sends the data to the cloud network, called the broker, and multiple subscribers are connected to the network to receive data without the network traffic problem [71].

Table V presents a summary of the advantages and disadvantages associated with each protocol. The optimal selection of a protocol relies on the specific requirements of the application. For instance, the simplicity and lightweight nature of MQTT facilitate the ease of implementation and enable it to

TABLE V
ADVANTAGES AND DISADVANTAGES OF IIOT PROTOCOLS

Protocol	Advantages	Disadvantages
MQTT	Lightweight, efficient, widely adopted, support for publish/subscribe, good for low-bandwidth connections.	Limited security features, not ideal for systems that require high reliability or security.
AMQP	Provides reliable, secure, and high-performance messaging, widely adopted.	May require more resources, not well-suited for low-power or low-bandwidth devices.
CoAP	Designed for constrained devices, low overhead, provides a RESTful for easy integration with web services, widely adopted.	Built-in security features require high communication costs.
DDS	Designed for real-time data distribution and control, based on a brokerless publish/subscribe model.	Heavy weight, more complex to implement and maintain.
OPC UA	Supports multiple security mechanisms, widely adopted in industrial processes.	Can be complex to set up and use, requires significant resources.

accommodate resource-constrained devices. However, its security features may not be robust enough to satisfy certain application demands. In contrast, the advanced security features of OPC UA enhance its suitability for certain applications but can lead to complexities in implementation and greater resource demands. Consequently, a careful assessment of unique needs for the system is imperative to identify the most fitting protocol.

D. Practical Examples of IIoT in Different Industries

SCADA system can be used in a variety of sectors and industries, including manufacturing, oil and gas, electric power generation and distribution, and water and sewage [35], [36], [37], [38], [39]. The use of IIoT enhances the capabilities of these systems and helps improve efficiency and decision-making. In this context, there are some companies that produce integrated IIoT platforms to improve the overall performance of these industries.

1) IXON Cloud[1] offers an IIoT platform that includes tools such as remote access to machines via an M2M cloud cluster VPN connection, data visualization, data logging, and PdM. Industrial machines are connected to the IXON cloud through an edge gateway (IXrouter). When the IXrouter has access to the Internet, it logs into the IXON Cloud via a VPN connection. This gateway supports many protocols, such as OPC-UA, Modbus TCP, and MQTT.
2) Inductive Automation[2] offers Ignition, an IIoT platform used in many industries. Ignition IIoT uses the MQTT protocol to transmit data from field devices to an MQTT server in the cloud. In this way, real-time monitoring and data analysis can be performed more efficiently. One of their customers stated that using the Ignition platform improved their SCADA system for the municipal water district and the old SCADA system had many difficulties because it did not provide reliable real-time monitoring, could not expand and update its processes, supported only a small number of tags, and required a lot of money to increase the number of tags. So, integrating IIoT into their system helped to solve these problems.
3) FrameworX and FactoryStudio platforms by Tatsoft[3] provide IIoT capabilities for many industries. They include many modules, such as PLC drivers, OPC UA, MQTT, and SQL database. One of the case studies on the use of this IIoT platform in the manufacturing industry helped in the operation, monitoring, and analysis of production lines to improve performance. It collected data from various field devices to monitor production lines in real-time from any location and provided analysis and visualization tools to make informed decisions.
4) PTC ThingWorx[4] IIoT platform provides solutions for industrial use cases. ThingWorx leverages AI and ML techniques to analyze large volumes of complex IIoT data and provide the insights industry needs to make intelligent decisions in real-time. ThingWorx provides connectivity to PLCs and other field devices via OPC servers, enabling users to monitor and troubleshoot machines in real-time. It supports a wide range of IIoT protocols, including OPC-UA and MQTT. ThingWorx also includes ML analytics tool to make data-driven decisions. One of the case studies on the use of this IIoT platform in the oil and gas industry helped overcome the difficulties of transferring and using SCADA data for operational insights without real-time feature, which resulted in unnecessary downtime, and the tedious process of data extraction was an administrative burden and took time away from the actual analysis of the data. Using this platform, data were collected from multiple sources in real-time and sent to the cloud via MQTT. This solution provided a single service that processed all the data instead of having different individual processes on each SCADA server. By collecting data in real-time with the help of advanced analytics tool, downtime costs can be reduced by predicting equipment failures and maintenance needs.

IV. MAIN IMPROVEMENTS OF IIOT FOR INDUSTRIAL AUTOMATION

A. Efficient and Low-Cost Systems

The IIoT-enabled systems offer major improvements in efficiency and cost compared to traditional SCADA systems. The traditional SCADA systems can be too expensive and require specialized server with vendor-dependent licensed software [72]. Although automation companies, such as Schneider Electric (France), Siemens (Germany), and Emerson Electric (USA) provide various SCADA hardware and software with IoT-based solutions to their end users, the purchase and deployment of these systems require huge initial costs as well as annual payments for maintenance and support for these SCADA systems [40]. These systems may face the problem of interoperability, which leads to vendor lock-in issues due to noninteroperable communication between different vendors, resulting in unviable industrial automation solutions [40], [73].

Many research works have been conducted to utilize IIoT technologies to develop efficient and cost-effective systems for industrial automation. Babayigit and Sattuf [72] proposed an

[1]https://www.ixon.cloud/
[2]https://inductiveautomation.com/
[3]https://tatsoft.com/
[4]https://www.ptc.com/en

IIoT and web-based low-cost SCADA system to connect any type of PLC to the Internet by using Arduino microcontrollers to transmit data to a cloud server for online monitoring and further data analysis. They tested their framework both in the lab and on a wire drawing machine under factory conditions. Aghenta and Iqbal [40] implemented a low-cost open-source SCADA system for solar PV systems. Their prototype collects data from current and voltage sensors using an ESP32 Thing microcontroller and sends this data over a Wi-Fi network to the Thinger.io local IoT server which is hosted locally on a Raspberry PI 2 Model B microcontroller for data storage and remote monitoring. The data from this system are available within the deployed environment and is not accessed over the Internet to avoid security issues. Another work in [74] presented a low-cost open-source SCADA system for solar PV systems, where the Arduino Uno microcontroller acts as a sensor gateway to collect data from current and voltage sensors. The calculated sensor data are sent to the Raspberry PI 2 model B microcontroller, which has the Node-RED programming tool installed, to collect the sensor data from the Arduino Uno serial port connected to the Raspberry PI and send the collected data to the local EmonCMS IoT server for data storage and remote monitoring. Vargas-Salgado et al. [75] presented a low-cost web-based SCADA system for a hybrid renewable energy system, where a web interface with a MySQL database hosted by a PLESK server provides the data collected from Arduino-Raspberry PI microcontrollers; however, the maximum data storage allowed for a regular PLESK account is 6 GB.

As seen from previous studies, there are available components that can be used to build IIoT-based and low-cost SCADA systems to cope with the mostly expensive commercial SCADA systems and their compatibility issues. Besides the sensors used, the most important components to build IIoT-based SCADA systems are microcontrollers, such as Arduino, Raspberry PI, BeagleBone AI, and SparkFun ESP32 Thing and open-source web-based or local IoT platforms, such as Thinger.io, EmonCMS, and ThingsBoard.

B. Digital Twin (DT)

One of the benefits that the IIoT brings to industrial automation is the DT [76]. The DT is the digital representation of the physical world so that all physical entities in the manufacturing industry are combined and integrated into a dynamic virtual model that is capable of using sensor data in real-time to improve efficiency and decision making in the industry [26], [27], [28], [29], [77], [78], [79], [80]. The DT consists of three main components: physical components, virtual model, and data connecting the components, with data flowing from the physical components to the virtual model and vice versa [81], [82]. The DT enables the improvement of the production process and helps in predicting and managing maintenance [81], [82]. The combination of DT with AI enables testing and simulation of different scenarios before the physical components are deployed in production to ensure that the components function as expected. Even after the physical components are deployed in the real environment, the use of real-time data can help predict potential problems in the products or failures in the physical machines. DT helps to accurately understand what is happening and predict the future behavior of the physical components so that cost-effective systems can be developed [83].

Zhou et al. [84] presented a hybrid DL model based on the integration of MobileNetv2 [85], YOLOv4 [86], and Openpose [87] networks to determine the real-time state of physical components, i.e., equipment, product, and operator, as fundamental environmental parameters in building a DT system for smart factories. To improve smart manufacturing based on better integration of physical and virtual spaces, DT enabled the dynamic synchronization of physical components during the manufacturing process in large-scale scenes. MobileNetv2 was integrated into YOLOv4 as a new backbone that replaced YOLOv4's original CSPDarknet53 to provide better semantic information for the prediction layer and reduce computational costs. The extracted features from this integration were used as input to the Openpose network instead of the VGG-19. Thus, the integrated MobileNetv2 with YOLOv4 was used for small object (equipment and products) detection, while the Openpose part was used for human posture (operator) detection to enable modeling, monitoring, and optimization of the entire manufacturing process for the DT system.

Xu et al. [88] proposed a two-phase DT-assisted fault diagnosis using deep transfer learning for real-time monitoring and PdM, combining training and testing data from both virtual space simulation data and physical space monitoring data to solve the problem of data distribution and insufficient training data. In the first phase, they embedded a fault diagnosis model in the DT and then trained a DL model based on Stack Autoencoder on the virtual space simulation data with a variety of simulated data. After the model performed well in the virtual space, the physical space was constructed and connected to the virtual space in the second phase. In the second phase, a DL model was trained for fault diagnosis by transferring the knowledge gained in the first phase. Another work in [89] presented the same concept of using DT and deep transfer learning for intelligent fault diagnosis of machines.

Chhetri et al. [90] proposed an IoT sensor-based DT for additive manufacturing (3-D printing). They used IoT sensors to collect side-channel emission information such as acoustic, magnetic data, vibration, and power to create an up-to-date DT for localizing machine faults and predicting product quality in real-time.

Min et al. [91] presented a theoretical framework for building a DT based on IIoT and ML to optimize production control in the petrochemical industry. In this framework, the virtual factory had to continuously collect real-time data from the physical factory and use real-time data and historical data to train the DT model and verify the processes. The DT simulation model was trained using four different ML algorithms, including random forest (RF), AdaBoost, XGBoost, and LightGBM with historical data as well as real-time data from IoT sensors. This model was iteratively trained and improved based on repeatedly updated and accumulated data to adapt to continuous changes in the physical factory. The final model was deployed online and combined with the optimal solution simulated by real-time industrial Big Data on the DT model.

C. Prediction of Machines Failures

The manufacturing industry is characterized by a high level of machinery, which is the most expensive capital of the industry. Therefore, one of the top priorities of the industry is to keep them healthy in order to avoid huge costs for their replacement

and downtime, which are very costly for the industry. Every machine eventually breaks down if it is not maintained. Traditional industries try to prevent failure before it happens by checking their machines regularly. However, the exact time to perform maintenance is a major challenge because it is impossible to determine when failure will occur. So, if this preventive maintenance is scheduled very early, the usable life of the machine is wasted, resulting in additional costs. Thanks to IIoT-enabled systems, where the concept of PdM [92], [93], [94], [95], [96], [97] can be applied in which the required maintenance can be optimized and scheduled before the failure occurs where IIoT sensors transmit data via a network to a cloud for further analysis to support decision making. As seen from the previous section, the PdM is one of the key applications of DT.

Nikfar et al. [98] proposed a two-phase ML based for PdM of low-voltage industrial motors, in which gyroscope accelerometers sensors' were attached to the two different types of motors to collect vibration data and monitor the variations in vibration frequency. In the first phase, three ML algorithms including RF, support vector machine (SVM) and backpropagation neural network were tested to detect the abnormal behavior of the motors. Since the SVM algorithm performed best in the first phase, it was used in the second phase to predict three types of motor faults, including bearing wear, imbalance, and misalignment. While this work gave good results in the first phase, the problem in the second phase was that not enough data were collected to train the ML algorithm.

D. Real-Time Remote Monitoring

Real-time remote monitoring is the key function supported by IIoT-enabled systems to enable PdM, DT, and decision making at the right time. As IIoT enables the integration and connection of all industrial levels, the power of remote machine monitoring and the ability to leverage the importance of real-time data from IIoT sensors can be used from anywhere and at any time to emphasize industrial automation. In addition, using IIoT-based systems to build real-time remote monitoring systems provides more reliability, flexibility, and cost-effectiveness for industrial automation than using traditional SCADA systems [74]. Systems based on the traditional SCADA are susceptible to single-vendor components, which imposes a lot of overhead in terms of high cost, maintenance, integration, interoperability, and technological development advancements.

Magadan et al. [99] proposed a prototype of a low-cost IIoT system for real-time monitoring of vibration and temperature data of an electric motor. This system was built using a low-cost multisensor module that supports wireless communication using the Bluetooth Low Energy (BLE) protocol, a Raspberry PI 3 Model B microcontroller that receives sensor data via the BLE protocol and sends it to the cloud via HTTP, and a ThingSpeak, an IoT platform service for data storage, visualization, and analysis in the cloud. The authors of this study argued that the returned data from sensors, which is in the time domain, do not provide enough information about the vibrations of the motor. Therefore, they applied a Fourier transform in both the sensor module and the microcontroller, and the results were more accurate when the transform was calculated on the microcontroller.

Zhao et al. [100] developed a high-speed real-time IIoT-based monitoring system with data logging recording functions for a power system distribution. This system was implemented with a field-programmable gate array -based controller to collect related data in real-time, and a network-attached storage was used to store and retrieve data for multiple authorized users that can be accessed remotely via LAN. This system can provide a real-time remotely monitoring and visualization capabilities for system operators to promote better decision making.

Ganga et al. [101] proposed an IoT-based real-time monitoring system for electric motors. Their system was built based on an IoT2040 gateway with a customized Linux image to collect electric motor shaft vibration data from piezoelectric vibration sensors via an RS232 serial port and send this raw data to the cloud via a RESTful HTTP protocol. The collected data were analyzed to determine vibration thresholds using LabVIEW DIAdem which is a purchased data management software product for aggregating, reviewing, analyzing, and reporting measurement data.

Wang et al. [102] developed an IIoT-based prototype for continuous monitoring and analysis of device condition. Since many field devices are installed and calibrated according to their specific working conditions, this prototype extracts the field device details described by standards such as field device integration and sends them along with sensory measurements that converted to JSON form, to the Microsoft Azure IoT cloud platform via IIoT gateways using the AMQP protocol.

E. Security

Security is one of the most important issues in the field of industrial automation, where internal and/or external attacks on the system can cause severe damage to private data and infrastructure, resulting in a great financial loss in productivity and safety. In industrial systems, availability is the top priority, and these systems must operate continuously and be protected from security attacks, and a shutdown of these systems, even if it lasts only a few minutes, can cause high losses. Generally, SCADA systems are developed by professionals in the field where these systems are used, such as power engineers, who usually have no experience or training in security technologies. As a result, the first two generations of SCADA systems in particular were developed without security awareness, making them vulnerable to attack. In SCADA networks, it is not always possible to scan devices for vulnerabilities that can cause this network to crash, unlike IT networks. In addition, traditional SCADA systems use proprietary systems, so security patches are often not available and only the specific vendor can provide and deploy these patches, and the entire system may need to be recertified after patching, which is very expensive. Therefore, IIoT-enabled systems can provide more reliability and flexibility in terms of industrial automation security. In addition, traditional SCADA systems use proprietary systems, so security patches are often not available and only the specific vendor can provide and deploy these patches, and the entire system may need to be recertified after patching, which is very expensive. Therefore, IIoT-enabled systems can provide more reliability and flexibility in terms of industrial automation security.

Some of the key security requirements of IIoT systems to protect the network and data and identify various malicious activities and threats are as follows.

1) *Authentication:* The first step in securing systems is to authenticate the user identity and establish a trusted connection via M2M communication during sharing and data exchange between IIoT devices.

2) *Authorization:* It is to allow only the authorized users to access the IIoT resources and block the others.
3) *Availability:* It is to ensure that the IIoT resources are available for the authorized access at all permissible times.
4) *Integrity:* It is to ensure that the data are protected from unauthorized changes to ensure that it is reliable and accurate.
5) *Confidentiality:* It is to ensure that the data are encrypted and converted into a nonreadable format to protect the data from unauthorized viewing using symmetric and asymmetric algorithms, advance encryption standard to maintain confidentiality, and secure hash algorithms and Diffie Hellman for key exchange management are some popular methods in IIoT.
6) *Nonrepudiation:* It provides protection against denial of sending or receiving the communication and verifies the sender that the data have been sent and the identity of the receiver to the recipient [103], [104], [105], [106], [107]. Section V presents some of the publicly available IIoT cybersecurity datasets that opens the horizon for researchers to develop novel ML/DL models to enhance the safety and security of the IIoT systems.

V. Public IIoT Datasets

A. EDGE-IIoTSet: Cyber Security Dataset of IoT and IIoT

Ferrag et al. [108] generated cyber security dataset of IoT and IIoT applications, called Edge-IIoTset. They identified and analyzed 14 types of attack related to IoT and IIoT connectivity protocols, which are categorized into 5 threats, including, DoS/ DDoS attacks, Information gathering, Man in the middle attacks, Injection attacks, and Malware attacks. This dataset can be publicly accessed from http://ieee-dataport.org/8939 or from https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot.

B. WUSTL-IIOT-2021

Zolanvari et al. [21], [109] created this dataset, which consists of IIoT network data to be used in cybersecurity research by emulating actual industrial systems in the real world. The dataset includes a total of 1 194 464 observations, including 1 107 448 for normal traffic and 87 016 for attack traffic. The dataset contains 41 features selected based on the variation of their values during the attack phases. There are four types of attacks, including Command Injection, DoS, Reconnaissance, and Backdoor. The dataset was created to be imbalanced as this is a realistic scenario that occurs in the real world. The percentage of attack traffic in the dataset is less than 7.28%. DoS attacks are usually very traffic-intensive, so they account for 89.98% of the total attacks. This dataset can be publicly accessed from https://ieee-dataport.org/documents/wustl-iiot-2021 or from https://www.cse.wustl.edu/∼jain/iiot2/index.html.

C. X-IIOTID

Al-Hawawreh et al. [110] generated this cybersecurity dataset for IoT and IIoT systems at the University of New South Wales (UNSW) in Canberra. The dataset contains 421 417 normal traffic, 399 417 attack traffic, and 59 features. It includes 18 types of attack related to IoT and IIoT systems, which are categorized into 9 threats, including, Reconnaissance, Weaponization, Exploitation, Lateral Movement, Command and Control, Exfiltration, Tampering, Crypto Ransomware, and RDoS attack. This dataset can be publicly accessed from https://ieee-dataport.org/documents/x-iiotid-connectivity-and-device-agnostic-intrusion-dataset-industrial-internet-things or from https://www.kaggle.com/datasets/munaalhawawreh/xiiotid-iiot-intrusion-dataset.

D. UNSW-NB15

Moustafa et al. [111], [112] generated this cybersecurity dataset for IoT and IIoT systems by the IXIA PerfectStorm tool in the Cyber Range Lab of the Australian Centre for Cyber Security. It contains a total of 2 540 044 records, in which 321 283 records belong to the attack traffic. This dataset has nine types of attacks, namely, Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms. It was developed to generate totally 49 features with the class label. This dataset can be publicly accessed from https://ieee-dataport.org/documents/unswnb15-dataset or from https://research.unsw.edu.au/projects/unsw-nb15-dataset.

E. TON_IoT

Moustafa et al. [113], [114] generated this cybersecurity datasets of IoT and IIoT systems for evaluating the fidelity and efficiency of different cybersecurity applications based on AI algorithms. This dataset has 22 339 021 records of normal and attacks data. It has 461 043 records collected from the entire network dataset to include all the attacks and normal traffic. This dataset has nine types of attacks, namely, Backdoor, DoS, DDoS, Injection, Password, Man in the middle, Ransomware, Port scanning, and XSS. This dataset can be publicly accessed from https://ieee-dataport.org/documents/toniot-datasets or from https://research.unsw.edu.au/projects/toniot-datasets.

VI. Limitations, Recommendations, and Future Perspectives

IIoT has the potential to revolutionize industrial automation. However, there are some limitations that need to be addressed to achieve the full potential of IIoT for industrial automation.

1) *Power consumption:* IIoT relies on collecting data from many sensors that are designed to operate on built-in batteries that have a limited lifespan, which imposes additional replacement costs on the industry, especially when the industry depends on thousands of sensors.
2) *Sensor data quality:* IIoT sensors are deployed in harsh environments that can produce noisy data, which can negatively impact decision-making accuracy.
3) *Storage space:* Since industrial processes generate large amounts of data that require significant storage space, advanced data management techniques that can handle large amounts of data and ensure its security must be used.
4) *Poor network connectivity:* If the industrial environment has a limited or unreliable network, it can affect the efficiency of IIoT systems in transmitting data in real-time without loss. IIoT can access many devices and depends on the use of the Internet for communication. Therefore, IIoT should operate with robust network connectivity.

IIoT development may face several difficulties and obstacles that require careful consideration.

1) *Culture change:* Traditional industries may resist moving to IIoT-enabled systems because they fear adding new

risks to their system that they may not be able to manage and because they do not understand the technology associated with IIoT.

2) *Experts needed:* Due to the lack of experts, organizations do not know how to develop IIoT technologies or integrate them into their systems. IIoT development requires multidisciplinary experts in areas such as industrial engineering, networks, sensor technologies, data analytics, and AI.
3) *Integration of operational technology (OT) and information technology (IT):* IIoT-enabled systems require the convergence of OT and IT, so integrating data from both can provide a comprehensive view of industrial processes that enables companies to optimize operations and increase efficiency.
4) *Privacy:* While IIoT-enabled systems rely on the fully connected and integrated levels of the industrial model (see Fig. 3) and the use of the Internet to access the cloud, confidential information about products, machines, and personnel should be preserved and protected.

Therefore, it is highly recommended to pay attention to the previously mentioned limitations and obstacles when developing IIoT-enabled systems.

There are significant research developments in the IIoT and its supporting technologies, such as AI, Big Data, cloud computing, edge computing, sensors, networks, and communication protocols. However, more improvements are possible and needed to achieve optimal performance. Some of our suggestions for future perspectives can be briefly summarized as follows.

1) *Sustainable industrial automation:* As emerging to Industry 5.0, it is important to incorporate best green practices [115] into the IIoT that help reduce harmful environmental impacts and improve automation performance through energy conservation, emissions reduction, waste management, and cost reduction. Energy-efficient practices should be considered in the development of field devices such as sensors and M2M communication protocols. In addition, there is an open question to be answered by research community of how AI can be used to integrate the best green practices to better support sustainable industrial automation.
2) *Integration of Edge Computing, Fog Computing, and Cloud Computing:* To accelerate data flow, reduce latency and network congestion, and empower real-time decision making in IIoT-enabled systems, data processing and analysis should be performed in a three-tiered approach. The first tier belongs to edge computing, which represents field devices such as sensors that are closer to the data source. Fog computing, as the second tier, involves the use of more powerful computing resources at LAN for data processing. The use of cloud computing, accessed via WAN, forms the last level of data processing.
3) *Predictive maintenance:* It is one of the most important features of IIoT-enabled systems, helping to reduce downtime and minimize repair costs, resulting in significant cost savings and improved operational efficiency. However, there are no publicly available datasets for PdM, this is probably due to privacy concerns and the unique characteristics and properties of each system. Without ignoring these anxieties, the availability of such datasets is important for the research community to foster the robust development of ML/DL models for predicting machine failures.
4) *Security:* As we discussed earlier, although IIoT offers improvements in security compared to traditional SCADA, it is still a hot topic and one of the most important future directions works to be explored. Blockchain technology has proven useful in protecting data privacy. However, as the IIoT generates a huge amount of data, there are open issues on improving consensus mechanisms to validate transactions and maintain a consistent and immutable ledger in the blockchain network, as well as developing a light-weight and scalable AI-enabled blockchain to maintain the overall performance. Developing optimized DL models based on recent available datasets is also critical to detect potential threats such as malicious attacks or unauthorized access attempts in real-time.

VII. Conclusion

The IIoT helps industrial sectors to improve their performance and increase high-quality production rates. The IIoT is considered the cornerstone of digital transformation by providing all the latest data or information that any consumer needs at any given time. IIoT-enabled systems offer significant efficiency and cost advantages compared to traditional SCADA systems. Particularly, the role of ML/DL in IIoT application is appreciated for the improvement of overall system efficiency. On the other hand, open-source components can be used to build IIoT-based and cost-effective systems that are superior to the usually expensive commercial SCADA systems and their compatibility issues. In addition, real-time remote monitoring is the key function supported by IIoT-enabled systems to enable PdM, DT, and decision making at the right time. Furthermore, there are open research areas for the use of ML/DL that can be integrated into the IIoT ecosystem.

References

[1] MarketsandMarkets™, "Industrial IoT market size, share and trends forecast to 2026," Accessed: Sep. 15, 2022. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/industrial-internet-of-things-market-129733727.html
[2] C. Paniagua and J. Delsing, "Industrial frameworks for Internet of Things: A survey," *IEEE Syst. J.*, vol. 15, no. 1, pp. 1149–1159, Mar. 2021, doi: 10.1109/JSYST.2020.2993323.
[3] S. Munirathinam, "Industry 4.0: Industrial Internet of Things (IIOT)," in *Advances in Computers*, vol. 117, no. 1, P. Raj and P. Evangeline, Eds. Amsterdam, The Netherlands: Elsevier, 2020, pp. 129–164, doi: 10.1016/bs.adcom.2019.10.010.
[4] P. K. Malik et al., "Industrial Internet of Things and its applications in industry 4.0: State of the art," *Comput. Commun.*, vol. 166, pp. 125–139, Jan. 2021, doi: 10.1016/j.comcom.2020.11.016.
[5] A. Karmakar, N. Dey, T. Baral, M. Chowdhury, and M. Rehan, "Industrial Internet of Things: A review," in *Proc. Int. Conf. Opto-Electron. Appl. Opt.*, 2019, pp. 1–6. doi: 10.1109/OPTRONIX.2019.8862436.
[6] Y. Liao, E. de Freitas Rocha Loures, and F. Deschamps, "Industrial Internet of Things: A systematic literature review and insights," *IEEE Internet of Things J.*, vol. 5, no. 6, pp. 4515–4525, Dec. 2018, doi: 10.1109/JIOT.2018.2834151.
[7] W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, "Industrial Internet of Things: Recent advances, enabling technologies and open challenges," *Comput. Elect. Eng.*, vol. 81, Jan. 2020, Art. no. 106522, doi: 10.1016/j.compeleceng.2019.106522.
[8] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Inform.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014, doi: 10.1109/TII.2014.2300753.
[9] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018, doi: 10.1016/j.compind.2018.04.015.
[10] X.-G. Luo, H.-B. Zhang, Z.-L. Zhang, Y. Yu, and K. Li, "A new framework of intelligent public transportation system based on the Internet of

Things," *IEEE Access*, vol. 7, pp. 55290–55304, 2019, doi: 10.1109/ACCESS.2019.2913288.

[11] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, "An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges," *IEEE Internet of Things J.*, vol. 5, no. 5, pp. 3758–3773, Oct. 2018, doi: 10.1109/JIOT.2018.2844296.

[12] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-based smart cities: Recent advances and challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 16–24, Sep. 2017, doi: 10.1109/MCOM.2017.1600514.

[13] J. Zhao and X. Yue, "Condition monitoring of power transmission and transformation equipment based on industrial Internet of Things technology," *Comput. Commun.*, vol. 157, pp. 204–212, May 2020, doi: 10.1016/j.comcom.2020.04.008.

[14] T. R. Wanasinghe, R. G. Gosine, L. A. James, G. K. I. Mann, O. de Silva, and P. J. Warrian, "The Internet of Things in the oil and gas industry: A systematic review," *IEEE Internet Things J,* vol. 7, no. 9, pp. 8654–8673, Sep. 2020, doi: 10.1109/JIOT.2020.2995617.

[15] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial Internet of Things (IIoT) – Enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp. 192–202, Jun. 2016, doi: 10.1016/j.comnet.2016.01.009.

[16] C. K. M. Lee, S. Z. Zhang, and K. K. H. Ng, "Development of an industrial Internet of Things suite for smart factory towards re-industrialization," *Adv. Manuf.*, vol. 5, no. 4, pp. 335–343, 2017, doi: 10.1007/s40436-017-0197-2.

[17] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, pp. 102481, Jan. 2020, doi: 10.1016/j.jnca.2019.102481.

[18] R. A. Khalil, N. Saeed, M. Masood, Y. M. Fard, M.-S. Alouini, and T. Y. Al-Naffouri, "Deep learning in the Industrial Internet of Things: Potentials, challenges, and emerging applications," *IEEE Internet Things J,* vol. 8, no. 14, pp. 11016–11040, Jul. 2021, doi: 10.1109/JIOT.2021.3051414.

[19] S. Nayak, N. Ahmed, and S. Misra, "Deep learning-based reliable routing attack detection mechanism for industrial Internet of Things," *Ad Hoc Netw.*, vol. 123, Dec. 2021, Art. no. 102661, doi: 10.1016/j.adhoc.2021.102661.

[20] B. Chen and J. Wan, "Emerging trends of ML-based intelligent services for industrial Internet of Things (IIoT)," in *Proc. Comput., Commun. IoT Appl.*, 2019, pp. 135–139, doi: 10.1109/ComComAp46287.2019.9018815.

[21] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of Industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, Aug. 2019, doi: 10.1109/JIOT.2019.2912022.

[22] H. Naeem et al., "Malware detection in industrial Internet of Things based on hybrid image visualization and deep learning model," *Ad Hoc Netw.*, vol. 105, Aug. 2020, Art. no. 102154, doi: 10.1016/j.adhoc.2020.102154.

[23] M. H. ur Rehman, I. Yaqoob, K. Salah, M. Imran, P. P. Jayaraman, and C. Perera, "The role of Big Data analytics in industrial Internet of Things," *Future Gener. Comput. Syst.*, vol. 99, pp. 247–259, Oct. 2019, doi: 10.1016/j.future.2019.04.020.

[24] M. Javaid, A. Haleem, R. Pratap Singh, S. Rab, and R. Suman, "Upgrading the manufacturing sector via applications of Industrial Internet of Things (IIoT)," *Sensors Int.*, vol. 2, 2021, Art. no. 100129, doi: 10.1016/j.sintl.2021.100129.

[25] I. Singh, D. Centea, and M. Elbestawi, "IoT, IIoT and cyber-physical systems integration in the SEPT Learning Factory," *Procedia Manuf.*, vol. 31, pp. 116–122, 2019, doi: 10.1016/j.promfg.2019.03.019.

[26] T. P. Raptis, A. Passarella, and M. Conti, "Data management in industry 4.0: State of the art and open challenges," *IEEE Access*, vol. 7, pp. 97052–97093, 2019, doi: 10.1109/ACCESS.2019.2929296.

[27] D. Cortes, J. Ramirez, L. Villagomez, R. Batres, V. Vasquez-Lopez, and A. Molina, "Digital Pyramid: An approach to relate industrial automation and digital twin concepts," in *Proc. IEEE Int. Conf. Eng., Technol. Innov.*, 2020, pp. 1–7, doi: 10.1109/ICE/ITMC49519.2020.9198643.

[28] N. Dall'Ora, S. Centomo, and F. Fummi, "Industrial-IoT data analysis exploiting electronic design automation techniques," in *Proc. IEEE 8th Int. Workshop Adv. Sensors Interfaces*, 2019, pp. 103–109, doi: 10.1109/IWASI.2019.8791344.

[29] R. Cupek, M. Drewniak, A. Ziebinski, and M. Fojcik, "'Digital twins' for highly customized electronic devices—Case study on a rework operation," *IEEE Access*, vol. 7, pp. 164127–164143, 2019, doi: 10.1109/ACCESS.2019.2950955.

[30] S. Jaloudi, "Communication protocols of an industrial Internet of Things environment: A comparative study," *Future Internet*, vol. 11, no. 3, Mar. 2019, Art. no. 66, doi: 10.3390/fi11030066.

[31] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Fourth-quarter 2015, doi: 10.1109/COMST.2015.2444095.

[32] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," *Int. J. Crit. Infrastructure Protection*, vol. 34, Sep. 2021, Art. no. 100433, doi: 10.1016/j.ijcip.2021.100433.

[33] A. Shahzad, "The SCADA Review: System components, architecture, protocols and future security trends," *Amer. J. Appl. Sci.*, vol. 11, no. 8, pp. 1418–1425, Aug. 2014, doi: 10.3844/ajassp.2014.1418.1425.

[34] D. Upadhyay and S. Sampalli, "SCADA (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101666, doi: 10.1016/j.cose.2019.101666.

[35] W.-Y. Sean, Y.-Y. Chu, L. L. Mallu, J.-G. Chen, and H.-Y. Liu, "Energy consumption analysis in wastewater treatment plants using simulation and SCADA system: Case study in northern Taiwan," *J. Cleaner Prod.*, vol. 276, Dec. 2020, Art. no. 124248, doi: 10.1016/j.jclepro.2020.124248.

[36] R. Morrison, X. Liu, and Z. Lin, "Anomaly detection in wind turbine SCADA data for power curve cleaning," *Renew. Energy*, vol. 184, pp. 473–486, Jan. 2022, doi: 10.1016/j.renene.2021.11.118.

[37] L. Yang, X. Cao, and J. Li, "A new cyber security risk evaluation method for oil and gas SCADA based on factor state space," *Chaos, Solitons Fractals*, vol. 89, pp. 203–209, Aug. 2016, doi: 10.1016/j.chaos.2015.10.030.

[38] D. J. Kang, J. J. Lee, B. H. Kim, and D. Hur, "Proposal strategies of key management for data encryption in SCADA network of electric power systems," *Int. J. Electr. Power Energy Syst.*, vol. 33, no. 9, pp. 1521–1526, Nov. 2011, doi: 10.1016/j.ijepes.2009.03.004.

[39] T. Thepmanee, S. Pongswatd, F. Asadi, and P. Ukakimaparn, "Implementation of control and SCADA system: Case study of Allen Bradley PLC by using WirelessHART to temperature control and device diagnostic," *Energy Rep.*, vol. 8, pp. 934–941, Apr. 2022, doi: 10.1016/j.egyr.2021.11.163.

[40] L. O. Aghenta and M. T. Iqbal, "Low-cost, open source IoT-based SCADA system design using thinger.IO and ESP32 thing," *Electronics*, vol. 8, no. 8, Jul. 2019, Art. no. 822, doi: 10.3390/electronics8080822.

[41] M. Javaid, A. Haleem, R. P. Singh, S. Rab, and R. Suman, "Significance of sensors for industry 4.0: Roles, capabilities, and applications," *Sensors Int.*, vol. 2, 2021, Art. no. 100110, doi: 10.1016/j.sintl.2021.100110.

[42] T. Kalsoom, N. Ramzan, S. Ahmed, and M. Ur-Rehman, "Advances in sensor technologies in the era of Smart factory and industry 4.0," *Sensors*, vol. 20, no. 23, Nov. 2020, Art. no. 6783, doi: 10.3390/s20236783.

[43] V. P. Gupta, "Smart sensors and industrial IoT (IIoT): A driver of the growth of industry 4.0," in *Internet of Things*, V. D. Gupta, H. C. de Albuquerque, K. Ashish, and M. P. Lala, Eds. Cham, Switzerland: Springer, 2021, pp. 37–49, doi: 10.1007/978-3-030-52624-5_3.

[44] S. Y. Yurish, "Self-adaptive intelligent sensors and systems: From theory to practical design," in *Proc. Int. Workshop Robotic Sensors Environ.*, 2008, pp. x–xi, doi: 10.1109/ROSE.2008.4669170.

[45] S. Y. Yurish and N. V. Kirianaki, "Novel conversion methods for self-adaptive smart sensors," in *Smart Sensors and MEMS*, S. Y. Yurish and M. T. S. R. Gomes, Eds. Dordrecht, The Netherlands: Springer, 2005, pp. 51–90, doi: 10.1007/978-1-4020-2929-5_2.

[46] S. Zhang and F. Yu, "Piezoelectric materials for high temperature sensors," *J. Amer. Ceram. Soc.*, vol. 94, no. 10, pp. 3153–3170, Oct. 2011, doi: 10.1111/j.1551-2916.2011.04792.x.

[47] H. Farahani, R. Wagiran, and M. Hamidon, "Humidity sensors principle, mechanism, and fabrication technologies: A comprehensive review," *Sensors*, vol. 14, no. 5, pp. 7881–7939, Apr. 2014, doi: 10.3390/s140507881.

[48] S. Lee et al., "A transparent bending-insensitive pressure sensor," *Nature Nanotechnol.*, vol. 11, no. 5, pp. 472–478, May 2016, doi: 10.1038/nnano.2015.324.

[49] K. H. Grantz et al., "Age-specific social mixing of school-aged children in a US setting using proximity detecting sensors and contact surveys," *Sci. Rep.*, vol. 11, no. 1, Dec. 2021, Art. no. 2319, doi: 10.1038/s41598-021-81673-y.

[50] T. Li, J. Guo, Y. Tan, and Z. Zhou, "Recent advances and tendency in fiber Bragg grating-based vibration sensor: A review," *IEEE Sens. J.*, vol. 20, no. 20, pp. 12074–12087, Oct. 2020, doi: 10.1109/JSEN.2020.3000257.

[51] C. Lebosse, P. Renaud, B. Bayle, and M. de Mathelin, "Modeling and evaluation of low-cost force sensors," *IEEE Trans. Robot.*, vol. 27, no. 4, pp. 815–822, Aug. 2011, doi: 10.1109/TRO.2011.2119850.

[52] R. He, C. Teng, S. Kumar, C. Marques, and R. Min, "Polymer optical fiber liquid level sensor: A review," *IEEE Sens. J.*, vol. 22, no. 2, pp. 1081–1091, Jan. 2022, doi: 10.1109/JSEN.2021.3132098.

[53] J. Lee et al., "High-performance gas sensor array for indoor air quality monitoring: The role of Au nanoparticles on WO_3, SnO_2, and NiO-based gas sensors," *J. Mater. Chem. A*, vol. 9, no. 2, pp. 1159–1167, 2021, doi: 10.1039/D0TA08743B.

[54] O. Sakai et al., "In-vacuum active colour sensor and wireless communication across a vacuum-air interface," *Sci. Rep.*, vol. 11, no. 1, Dec. 2021, Art. no. 1364, doi: 10.1038/s41598-020-80501-z.

[55] R. Srivastava, N. Sahai, R. P. Tewari, and B. Kumar, "Comparative analysis of piezo electric and accelerometer sensor for the design of rate adaptive pacemaker," *Meas. Sensors*, vol. 16, Aug. 2021, Art. no. 100053, doi: 10.1016/j.measen.2021.100053.

[56] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in Industrial Internet of Things: Architecture, advances and challenges," *IEEE Commun. Surveys Tut.*, vol. 22, no. 4, pp. 2462–2488, Fourth-quarter 2020, doi: 10.1109/COMST.2020.3009103.

[57] M. Sun, Z. Zhou, X. Xue, W. Zhang, and W. Gaaloul, "Adaptive configuration of service-based smart sensors in edge networks," *IEEE Trans. Ind. Inform.*, vol. 18, no. 4, pp. 2674–2683, Apr. 2022, doi: 10.1109/TII.2021.3074513.

[58] D. Dhungana et al., "Multi-factory production planning using edge computing and IIoT platforms," *J. Syst. Softw.*, vol. 182, Dec. 2021, Art. no. 111083, doi: 10.1016/j.jss.2021.111083.

[59] N. Balashanmugam, "Perspectives on additive manufacturing in industry 4.0," in *Additive Manufacturing*, M. Manjaiah, K. Raghavendra, N. Balashanmugam, and J. P. Davim, Eds. Amsterdam, The Netherlands: Elsevier, 2021, pp. 127–150, doi: 10.1016/B978-0-12-822056-6.00001-1.

[60] A. Esfahani et al., "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 288–296, Feb. 2019, doi: 10.1109/JIOT.2017.2737630.

[61] "MQTT version 3.1.1," A. Banks and R. Gupta, Eds., *OASIS Standard*, Oct. 29, 2014, Accessed: Sep. 15, 2022. [Online]. Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html. Latest version: [Online]. Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html

[62] "MQTT Version 5.0," A. Banks, E. Briggs, K. Borgendale, and R. Gupta, Eds., *OASIS Standard,* Mar. 7, 2019, Accessed: Sep. 15, 2022. [Online]. Available: https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html. Latest version: [Online]. Available: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

[63] B. Mishra and A. Kertesz, "The use of MQTT in M2M and IoT systems: A survey," *IEEE Access*, vol. 8, pp. 201071–201086, 2020, doi: 10.1109/ACCESS.2020.3035849.

[64] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," in *Proc. IEEE Int. Syst. Eng. Symp.*, 2017, pp. 1–7. doi: 10.1109/SysEng.2017.8088251.

[65] AMQP, *OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0*, OASIS Standard, Oct. 29, 2012, Accessed: Sep. 15, 2022. [Online]. Available: http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-complete-v1.0-os.pdf

[66] J. E. Luzuriaga, M. Perez, P. Boronat, J. C. Cano, C. Calafate, and P. Manzoni, "A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks," in *Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf.*, 2015, pp. 931–936. doi: 10.1109/CCNC.2015.7158101.

[67] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny internet nodes," *IEEE Internet Comput.*, vol. 16, no. 2, pp. 62–67, Mar./Apr. 2012, doi: 10.1109/MIC.2012.29.

[68] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things," *IEEE Sens. J.*, vol. 13, no. 10, pp. 3711–3720, Oct. 2013, doi: 10.1109/JSEN.2013.2277656.

[69] "About the data distribution service specification version 1.2," U.S. Object Management Group, Needham, MA, USA, Accessed: Sep. 20, 2022. [Online]. Available: https://www.omg.org/spec/DDS/1.2/

[70] "Unified Architecture Part 1: Overview and concepts," *OPC Foundation*, Accessed: Sep. 20, 2022. [Online]. Available: https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-1-overview-and-concepts/

[71] S. P. Muniraj and X. Xu, "An implementation of OPC UA for machine-to-machine communications in a smart factory," *Procedia Manuf.*, vol. 53, pp. 52–58, 2021, doi: 10.1016/j.promfg.2021.06.009.

[72] B. Babayigit and H. Sattuf, "An IIoT and web-based low-cost SCADA system for industrial automation," in *Proc. 11th Int. Conf. Elect. Electron. Eng.*, 2019, pp. 890–894, doi: 10.23919/ELECO47770.2019.8990553.

[73] A. Hazra, M. Adhikari, T. Amgoth, and S. N. Srirama, "A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions," *ACM Comput. Surv.*, vol. 55, no. 1, pp. 1–35, Jan. 2023, doi: 10.1145/3485130.

[74] L. O. Aghenta and M. T. Iqbal, "Development of an IoT based open source SCADA system for PV system monitoring," in *Proc. IEEE Can. Conf. Elect. Comput. Eng.*, 2019, pp. 1–4, doi: 10.1109/CCECE.2019.8861827.

[75] C. Vargas-Salgado, J. Aguila-Leon, C. Chiñas-Palacios, and E. Hurtado-Perez, "Low-cost web-based supervisory control and data acquisition system for a microgrid testbed: A case study in design and implementation for academic and research applications," *Heliyon*, vol. 5, no. 9, Sep. 2019, Art. no. e02474, doi: 10.1016/j.heliyon.2019.e02474.

[76] F. Piccialli, N. Bessis, and E. Cambria, "Guest editorial: Industrial Internet of Things: Where are we and what is next?," *IEEE Trans. Ind. Inform.*, vol. 17, no. 11, pp. 7700–7703, Nov. 2021, doi: 10.1109/TII.2021.3086771.

[77] C. J. Turner, J. Oyekan, L. Stergioulas, and D. Griffin, "Utilizing industry 4.0 on the construction site: Challenges and opportunities," *IEEE Trans. Ind. Inform.*, vol. 17, no. 2, pp. 746–756, Feb. 2021, doi: 10.1109/TII.2020.3002197.

[78] W. Hu, T. Zhang, X. Deng, Z. Liu, and J. Tan, "Digital twin: A state-of-the-Art review of its enabling technologies, applications and challenges," *J. Intell. Manuf. Spec. Equip.*, vol. 2, no. 1, pp. 1–34, Aug. 2021, doi: 10.1108/JIMSE-12-2020-010.

[79] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," *IEEE Access*, vol. 8, pp. 108952–108971, 2020, doi: 10.1109/ACCESS.2020.2998358.

[80] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital twin in industry: State-of-the-art," *IEEE Trans. Ind. Inform.*, vol. 15, no. 4, pp. 2405–2415, Apr. 2019, doi: 10.1109/TII.2018.2873186.

[81] A. Agrawal, M. Fischer, and V. Singh, "Digital twin: From concept to practice," *J. Manage. Eng.*, vol. 38, May 2022, Art. no. 3, doi: 10.1061/(ASCE)ME.1943-5479.0001034.

[82] Q. Qi and F. Tao, "Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison," *IEEE Access*, vol. 6, pp. 3585–3593, 2018, doi: 10.1109/ACCESS.2018.2793265.

[83] M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," in *Transdisciplinary Perspectives on Complex Systems*, F.-J. Kahlen, S. Flumerfelt, and A. Alves, Eds. Cham, Switzerland: Springer, 2017, pp. 85–113, doi: 10.1007/978-3-319-38756-7_4.

[84] X. Zhou et al., "Intelligent small object detection for digital twin in smart manufacturing with industrial cyber–physical systems," *IEEE Trans. Ind. Inform.*, vol. 18, no. 2, pp. 1377–1386, Feb. 2022, doi: 10.1109/TII.2021.3061419.

[85] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, "MobileNetV2: Inverted residuals and linear bottlenecks," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 4510–4520, doi: 10.1109/CVPR.2018.00474.

[86] A. Bochkovskiy, C.-Y. Wang, and H.-Y. M. Liao, "YOLOv4: Optimal speed and accuracy of object detection," Apr. 2020. [Online]. Available: http://arxiv.org/abs/2004.10934

[87] Z. Cao, G. Hidalgo, T. Simon, S.-E. Wei, and Y. Sheikh, "OpenPose: Realtime multi-person 2D pose estimation using part affinity fields," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 43, no. 1, pp. 172–186, Jan. 2021, doi: 10.1109/TPAMI.2019.2929257.

[88] Y. Xu, Y. Sun, X. Liu, and Y. Zheng, "A digital-twin-assisted fault diagnosis using deep transfer learning," *IEEE Access*, vol. 7, pp. 19990–19999, 2019, doi: 10.1109/ACCESS.2018.2890566.

[89] M. Xia, H. Shao, D. Williams, S. Lu, L. Shu, and C. W. de Silva, "Intelligent fault diagnosis of machinery using digital twin-assisted deep transfer learning," *Rel. Eng. Syst. Saf.*, vol. 215, Nov. 2021, Art. no. 107938, doi: 10.1016/j.ress.2021.107938.

[90] S. R. Chhetri, S. Faezi, A. Canedo, and M. A. Al Faruque, "QUILT," in *Proc. Int. Conf. Internet Things Des. Implementation*, 2019, pp. 237–248, doi: 10.1145/3302505.3310085.

[91] Q. Min, Y. Lu, Z. Liu, C. Su, and B. Wang, "Machine learning based digital twin framework for production optimization in petrochemical industry," *Int. J. Inf. Manage.*, vol. 49, pp. 502–519, Dec. 2019, doi: 10.1016/j.ijinfomgt.2019.05.020.

[92] S. Mokhatab, W. A. Poe, and J. Y. Mak, "Gas processing plant operations," in *Handbook of Natural Gas Transmission and Processing*, 4th ed., S. Mokhatab, W. A. Poe, and J. Y. Mak, Eds. Amsterdam, The Netherlands: Elsevier, 2019, pp. 509–535, doi: 10.1016/B978-0-12-815817-3.00017-4.

[93] R. Kent, "Operations," in *Energy Management in Plastics Processing*, 3rd ed., R. Kent, Ed. Amsterdam, The Netherlands: Elsevier, 2018, pp. 319–344, doi: 10.1016/B978-0-08-102507-9.50006-4.

[94] J. C. A. Jauregui Correa and A. A. Lozano Guzman, "Guidelines for the implementation of a predictive maintenance program," in *Mechanical Vibrations and Condition Monitoring*, J. C. A. Jauregui Correa and A. A. Lozano Guzman, Eds. Amsterdam, The Netherlands: Elsevier, 2020, pp. 133–145, doi: 10.1016/B978-0-12-819796-7.00007-X.

[95] P. Bangert, "Introduction to machine learning in the power generation industry," in *Machine Learning and Data Science in the Power Generation Industry*, P. Bangert, Ed. Amsterdam, The Netherlands: Elsevier, 2021, pp. 77–92, doi: 10.1016/B978-0-12-819742-4.00004-4.

[96] H. M. Hashemian and W. C. Bean, "State-of-the-art predictive maintenance techniques∗," *IEEE Trans. Instrum. Meas.*, vol. 60, no. 10, pp. 3480–3492, Oct. 2011, doi: 10.1109/TIM.2009.2036347.

[97] M. Feng and Y. Li, "Predictive maintenance decision making based on reinforcement learning in multistage production systems," *IEEE Access*, vol. 10, pp. 18910–18921, 2022, doi: 10.1109/ACCESS.2022.3151170.

[98] M. Nikfar, J. Bitencourt, and K. Mykoniatis, "A two-phase machine learning approach for predictive maintenance of low voltage industrial motors," *Procedia Comput. Sci.*, vol. 200, pp. 111–120, 2022, doi: 10.1016/j.procs.2022.01.210.

[99] L. Magadán, F. J. Suárez, J. C. Granda, and D. F. García, "Low-cost real-time monitoring of electric motors for the industry 4.0," *Procedia Manuf.*, vol. 42, pp. 393–398, 2020, doi: 10.1016/j.promfg.2020.02.057.

[100] L. Zhao, I. Brandao Machado Matsuo, Y. Zhou, and W.-J. Lee, "Design of an industrial IoT-based monitoring system for power substations," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 5666–5674, Nov. 2019, doi: 10.1109/TIA.2019.2940668.

[101] D. Ganga and V. Ramachandran, "IoT-based vibration analytics of electrical machines," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4538–4549, Dec. 2018, doi: 10.1109/JIOT.2018.2835724.

[102] G. Wang, M. Nixon, and M. Boudreaux, "Toward cloud-assisted Industrial IoT platform for large-scale continuous condition monitoring," *Proc. IEEE*, vol. 107, no. 6, pp. 1193–1205, Jun. 2019, doi: 10.1109/JPROC.2019.2914021.

[103] P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T.-H. Kim, "A taxonomy of security issues in industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges," *IEEE Access*, vol. 9, pp. 25344–25359, 2021, doi: 10.1109/ACCESS.2021.3057766.

[104] A. D. Jurcut, P. Ranaweera, and L. Xu, "Introduction to IoT security," in *IoT Security*. Hoboken, NJ, USA: Wiley, 2020, pp. 27–64, doi: 10.1002/9781119527978.ch2.

[105] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems," *Future Gener. Comput. Syst.*, vol. 108, pp. 1267–1286, Jul. 2020, doi: 10.1016/j.future.2018.04.019.

[106] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *J. Supercomput.*, vol. 74, no. 12, pp. 6428–6453, Dec. 2018, doi: 10.1007/s11227-017-2048-0.

[107] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, pp. 93–106, Apr. 2018, doi: 10.1016/j.jmsy.2018.04.007.

[108] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.

[109] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "'WUSTL-IIOT-2021 dataset for IIoT cybersecurity research," Washington University, St. Louis, MO, USA, Oct. 2021, Accessed: Nov. 20, 2022. [Online]. Available: http://www.cse.wustl.edu/∼jain/iiot2/index.html

[110] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3962–3977, Mar. 2022, doi: 10.1109/JIOT.2021.3102056.

[111] N. Moustafa, "UNSW_NB15 dataset," IEEE Dataport, 2019, doi: 10.21227/8vf7-s525.

[112] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf.*, 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.

[113] N. Moustafa, "ToN_IoT datasets," IEEE Dataport, 2019, doi: 10.21227/fesz-dm97.

[114] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustain. Cities Soc.*, vol. 72, Sep. 2021, Art. no. 102994, doi: 10.1016/j.scs.2021.102994.

[115] United Nations Industrial Development Organization, "Green industry initiative," 2020, Accessed: Feb. 26, 2023. [Online]. Available: https://www.unido.org/our-focus-cross-cutting-services-green-industry/green-industry-initiative