Hindawi
Scientific Programming
Volume 2021, Article ID 6641562, 11 pages
https://doi.org/10.1155/2021/6641562

Research Article

A Survey of Industrial Internet of Things Platforms for Establishing Centralized Data-Acquisition Middleware: Categorization, Experiment, and Challenges

Jin-Sung Ok,[1,2] **Soon-Do Kwon**,[2] **Cheol-Eun Heo**,[2] **and Young-Kyoon Suh**[1]

[1]*School of Computer Science and Engineering, Kyungpook National University, Daegu 41566, Republic of Korea*
[2]*Smart Yard R&D Department, Daewoo Shipbuilding & Marine Engineering Co., Ltd. (DSME), Geoje 53302, Republic of Korea*

Correspondence should be addressed to Young-Kyoon Suh; yksuh@knu.ac.kr

Received 20 November 2020; Revised 1 February 2021; Accepted 15 April 2021; Published 28 April 2021

Academic Editor: Shah Nazir

The development of industrial Internet of Things (IIoT), big data, and artificial intelligence technologies is leading to a major change in the production system. The change is being propagated into the wave of transforming the existing system with a vertical structure into the corresponding horizontal platform or middleware. Accordingly, the way of acquiring IIoT data from an individual system is being altered to the way of being increasingly centralized through an integrated middleware of a scalable server or through a large platform. That said, middleware-based IIoT data acquisition must consider multiple factors, such as *infrastructure* (e.g., operation environment and network), *protocol heterogeneity*, *interoperability* (e.g., links with legacy systems), *real-time*, *and security*. This manuscript explains these five aspects in detail and provides a taxonomy of eighteen state-of-the-art IIoT data-acquisition middleware systems based on these aspects. To validate one of these aspects (network), we present our evaluation results at a real production site where IIoT data-acquisition loss rates are compared between wireless (long-term evolution) and wired networks. As a result, the wired communication can be more suitable for centralized IIoT data-acquisition middleware than wireless networks. Finally, we discuss several challenges in establishing the best IIoT data-acquisition middleware in a centralized way.

1. Introduction

Digital transformation, also known as *DT* or *DX*, is an important keyword for modern production systems. The utilization of technologies such as industrial Internet of Things (IIoT), big data, and artificial intelligence (AI) in existing systems enables digital transformation to immediately respond to customers' demands and build a production system that improves the current production efficiency [1, 2]. Thus, numerous research institutes and enterprises are conducting research on upgrading production systems that apply new technologies to the industrial environment.

Compared to building a new system from scratch, changing the existing system brings many considerations. One of the most time-consuming and costly processes is to acquire high-quality data. Most of the legacy IT and production systems, including Manufacturing Execution System (MES) and Supervisory Control and Data Acquisition (SCADA), have a vertical structure.

To flatten the vertical structure for better data acquisition, the new system must be able to *aggregate* each production data. To this end, numerous middleware platforms adopt a horizontal structure that integrates the data acquisition [3–12]. The proposed systems have been applied in actual industrial fields.

To establish centralized data-acquisition middleware, we must determine whether the above middleware platforms meet a set of major functionalities. This manuscript proposes the following functionalities: (i) wired and/or wireless network compatibility, (ii) support for a variety of compatible industrial protocols, (iii) automated real-time data collection, (iv) data integration and external transmission, and (v) security. As necessary functions and standards have not been well standardized and established, the existing systems are based on their own criteria, which are nonconsensual. Therefore, whether we are equipped to build high-quality IIoT data acquisition middleware is difficult to discern. Such ambiguous criteria may cause *duplicate development and increased development costs*.

To address this problem, we propose and describe a set of functionalities that must be addressed when developing centralized IIoT data acquisition middleware. We then review eighteen cutting-edge IIoT middleware systems and provide a taxonomy of these systems based on clearly motivational functionalities. One of these functionalities (communication type) was assessed in experiments at our real production site. The acquisition percentages of IIoT data under wired and wireless (long-term evolution, LTE) communications were 99.940% and 98.983%, respectively. From this result, we inferred that wired communication is more robust for centralized IIoT data acquisition than wireless communication. This empirical result sheds light on the potential validity of the proposed functionalities.

The main contributions of this manuscript are summarized as follows:

(i) We propose a number of considerations for building a centralized IIoT data-acquisition middleware

(ii) We elaborate on the distinctions between IoT and IIoT data-acquisition systems

(iii) We review a rich body of existing IIoT systems and qualitatively analyze them along with well-motivated criteria

(iv) We present our evaluation results obtained from a real industrial site with respect to IIoT data-acquisition loss between wireless and wired networks

(v) We draw several challenges for constructing IIoT data-acquisition middleware in a central server

The remainder of this manuscript is organized as follows. The following section proposes a set of considerations to establish the best IIoT data-acquisition middleware, classifies these considerations into five categories, and provides the key components of each consideration. The subsequent section reviews recent IIoT data-acquisition middleware systems. Thereafter, we present our experiment results showing different data-acquisition performances among IIoT devices (in this case, welding machines). Finally, we suggest the future research directions of our work.

2. Functionalities for Centralized IIoT Data-Acquisition Middleware

To build the Smart Factory or cyber-physical system (CPS) in a short time, the production data-acquisition system that serves as a backbone should be architected and well-designed. IIoT data-acquisition middleware enables fast and easy development of the applications. Most IoT systems develop applications for a new environment without integrating with existing systems. However, building IIoT systems often require upgrading existing production systems because IIoT data are not only obtained from existing sensors, gateways, and controllers but also fused with other application data. If the upgrade is necessary, modification of the existing system need to be minimized, and the core system of the current production system should remain unchanged. The reason is that upgrading the IIoT system incurs high investment cost.

To the best of our knowledge, data acquisition at industry sites has been little investigated. In this article, we fill this gap by exploring the various factors demanded of a solid and reliable middleware system for IIoT data-acquisition. A taxonomy of these factors is illustrated in Figure 1.

In the illustrated taxonomy, the first consideration is the *infrastructure*, including the operation and network environment. The infrastructure factor is divisible into two subfactors: operation environment and network. The first subfactor is further divided into on-premises, cloud, and hybrid environments. Most industrial sites have applied on-premises systems that satisfy the security and management requirements within the technical limitations. At present, numerous sites have adopted the cloud environment which allows users to gather and manage their IIoT data for further analysis and development [13]. Within the cloud environment, building systems can be quickly built and can be flexibly managed. However, the cloud incurs a security risk and requires additional hardware or programs for sending data to the cloud. For these reasons, most industry sites still prefer the on-premises environment. Other companies have built hybrid environments that combine the advantages of on-premises and cloud.

The second subfactor is *network*. The IIoT data-acquisition network environment is largely distinguished by wired and wireless networks. Wired communication is classified into analog signal, serial communication, and LAN communication. It has several advantages, such as cost-effectiveness, stability, and low maintenance. However, it can be disadvantageous when not installed in mobile environments. Recently, wireless communications have significantly expanded owing to technological advances and reduced system-development costs [14]. Wireless networks can utilize licensed frequency bands, such as 3 G, LTE, 5 G, and NB-IoT [15, 16], but licensed frequency standards and abilities vary among countries and local environments. If a network uses licensed frequency bands, it must use the demilitarized zone (DMZ) for safety purposes. Thus, numerous industrial sites have attempted to use unlicensed frequency bands in their local networks for IIoT data acquisition.

Short-distance local networks such as Wireless Fidelity (Wi-Fi), Bluetooth Low Energy (BLE), and ZigBee are also available. Recently, many industry sites have attempted to apply low-power wide-area networks (LPWAN), including Long Range (LoRa) and Sigfox, which are specialized for IoT and support small data transfer with low-power consumption [17–22]. In contrast to wired communication, wireless communication must guarantee stable data acquisition and control.

The second factor that must be considered is *heterogeneity* (in protocol). This factor can be divided into industrial protocol, communication protocol, and database driver. In

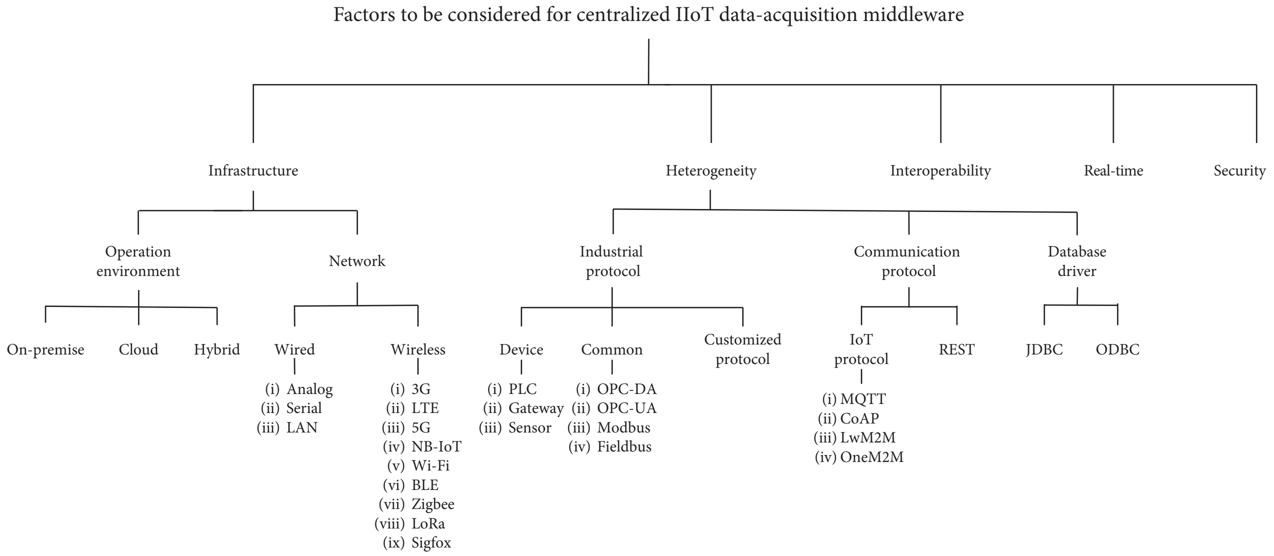


Figure 1: Proposed taxonomy of functionalities for centralized IIoT data-acquisition middleware.

general, most of the time and cost of an entire project is spent on setting and developing IIoT protocols and drivers. The first subfactor is industrial protocol. This can be further divided into device, common, and customized protocol levels.

At the device level, typically the gateway or controller uses programmable logic controllers (PLC). Some sensors and gateway have manufacturer-specific protocols. Therefore, a variety of PLC drivers, sensor protocols, and gateway protocols are required to obtain data from industrial equipment. Recently, the IIoT system is used as part of or in place of SCADA or MES (mentioned in the Introduction), so data-acquisition middleware with the device-level protocols is required.

At the common level, recently common protocols are adapted for many sites. Standard protocols are being introduced by several manufacturers and research institutes. The Open Platform Communications (OPC) Foundation developed two protocols—OPC-DA (Data Access) and OPC-UA (Unified Architecture)—for real-time monitoring and control systems. Again, it is very challenging to change the existing products and systems. Thus, protocols for existing equipment are necessitated. Moreover, because the existing applications including SCADA and MES use traditional industrial protocols such as Modbus and Fieldbus, the existing drivers must also be compatible.

At the customized protocol level, a specialized protocol for various purposes such as security and research needs to be developed.

The second subfactor is communication protocol. Two components associated with the communication protocol are IoT protocol and Representational State Transfer (REST).

The existing HTTP-based protocol is built for client-server architectures. Therefore, it may have limited ability to acquire real-time IIoT data. One such limitation is the request-response method, which cannot easily receive various IIoT data in real time. Moreover, a number of packets are needed to transmit and receive data. Thus, many institutes, companies, and researchers have developed their own IoT protocols.

In 2013, IBM developed Message Queuing Telemetry Transport (MQTT), which is a lightweight protocol using a publish/subscribe messaging model in a TCP/IP environment. MQTT provides a total of three quality of service (QoS) levels. In the adjustment of the QoS level, factors such as network quality and usage conditions should be considered. MQTT is increasingly used in embedded IIoT equipment, requiring light network environment.

Another protocol is Constrained Application Protocol (CoAP), a lightweight message-transfer protocol for use among devices on the same constrained network. OMA Lightweight M2M (LwM2M) is a device management protocol designed for sensor networks and machine-to-machine (M2M) environments. As an extensible resource and data model, LwM2M adopts an efficient secure data transfer standard called the CoAP.

The other is the oneM2M protocol, developed in July 2012 by eight organizations: (1) Association of Radio Industries and Businesses (ARIB), (2) the Alliance for Telecommunications Industry Solutions (ATIS), (3) China Communications Standards Association (CCSA), (4) European Telecommunication Standards Institute (ETSI), (5) Telecommunications Industry Association (TIA), (6) Telecommunication Technology Committee (TTC), (7) Telecommunications Technology Association (TTA), and (8) Telecommunications Standards Development Society, India (TSDSI).

The third subfactor is database driver. The database drivers, such as Java Database Connectivity (JDBC) and Open DataBase Connectivity (ODBC), for integrated system monitoring, are required to connect to the database.

The third component that must be considered is *interoperability*, which is the component for interchanging production data with legacy IT systems. An interface with legacy IT applications is important. REST and MQTT protocols, which are widely used in IT systems, are needed as well.

Real-time is the fourth factor to be considered. This factor means the real-time equipment control and monitoring function. Equipment and a machine can be controlled manually and automatically. Remote control should be used in a wireless or wired network environment so that it can be controlled manually. The automatic and intelligent control should be able to perform real-time monitoring, analyze the current data set, and predict future situations for future systems, such as CPS.

The final factor is *security*. Security is divided into network, software, and hardware security. Network security aims to minimize the impact of unauthorized external disturbances by utilizing specific communication protocols [23–27]. Software security prevents other systems from accessing IIoT systems including sensors, gateways, and legacy systems. Software security assigns a security ID to each machine and sensor. Some recent security developments are based on blockchain technology [28, 29].

Nevertheless, there are many security challenges in the existing IIoT environment. For instance, most of the systems are trying to resolve the security hardware. To prevent physical access from the outside, the DMZ installations and local networks are utilized. Many companies have various policies on security. Depending on the environment of the production system, appropriate methods should be chosen to ensure security.

Note that to improve the production efficiency through AI and analysis using IIoT data, many industrial sites and research institutes have been actively conducting research on acquiring data quickly at a low cost.

The following section provides detailed descriptions of the discussed factors that need to be considered during data acquisition.

3. Key Components of IIoT Data-Acquisition Middleware

Recently, a production system is rapidly being changed to meet customers' demands. To make the system more flexible and intelligent, the system needs to collect and integrate information from a variety of IIoT devices. Figure 2 illustrates such a system centrally positioning IIoT data-acquisition middleware. The industrial data gathered through this centralized middleware can be used for data-driven decision making. Furthermore, other kinds of systems, such as intelligent and flexible systems as well as simulation systems, can utilize the collected data for further analyses and services.

To generate valuable information in an IIoT environment, real-time collection of consistent IIoT data is essential. Accordingly, middleware technology for robust data acquisition is solicited. Considering the fact that IIoT data obtained using such acquisition middleware usually come from many applications, building such middleware needs to consider the following key components: network bridge, licensed frequency band, LPWAN, industrial protocols, production IoT, and cloud.

3.1. Network Bridge and LPWAN. As mentioned earlier, networks can be classified into two broad categories: wired and wireless (See Figure 1). Many industrial sites adopt wired communication owing to its stability and speed. In a wired communication, data are often received from previously developed serial interfaces, such as RS232 and RS485. In this case, only a short-distance communication is possible. Thus, a network bridge is required to enable long-distance communication. For example, many production sites are heavily utilizing network bridges that can change serial communications to transmission control protocol/Internet protocol (TCP/IP).

Recently, with the increased use of IIoT systems, increasing data are received through wireless communication owing to the cost and deployment duration. In a wireless communication, BLE, ZigBee, Wi-Fi, etc., can be utilized for short-distance communication (See Figure 1). In this case, the data is sent to the central server by improving the distance using a dedicated network bridge. Furthermore, with the development of telecommunication infrastructures, both licensed frequency band (e.g., 3 G, LTE, NB-IoT, and 5 G) and unlicensed frequency band (e.g., LPWAN) have become widely used by many industrial sites. In the case of the licensed frequency band, certain fees are paid for use, as the frequency of the license plate is managed by a professional company or institution. Owing to its superior speed and capability to provide stable communication and large bandwidth, such a licensed frequency band is being used by many industries although it comes at high costs.

Conversely, regarding the wireless communication, batteries are considered as a critical factor, particularly in LPWAN enabling long-distance communication. When IIoT systems need the transfer of small data with low-power consumption, LPWAN has three types: Sigfox, LoRaWAN, and NB-IoT (see Figure 1). Its communication distance is in the range of 1–20 km. As described previously, the data-acquisition middleware requires a structure to make it possible to acquire data through both wired and wireless communications.

3.2. Industrial Protocols. Industrial devices are essential to achieve high reliability, durability, scalability, and ease of maintenance. PC-based controllers are used in complex operations. In fact, PLC—an industry-specific system that operates independently of the OS—is more widely used, thanks to its high compatibility with industrial protocols such as Fieldbus and Modbus (See Figure 1). Furthermore, PLC has the ability to easily acquire analog signals such as voltage or current and incurs lower cost compared to industrial PCs. Currently, the connection with IT systems has become a hot topic in PLC markets. Along with this wave, most PLCs provide common protocols to obtain and control variables over the TCP/IP environment.

However, it is costly to upgrade existing PLC programs for the purpose of sending data to other systems, in terms of expense and time. Therefore, it is of paramount importance to support various PLC protocols so that data can be

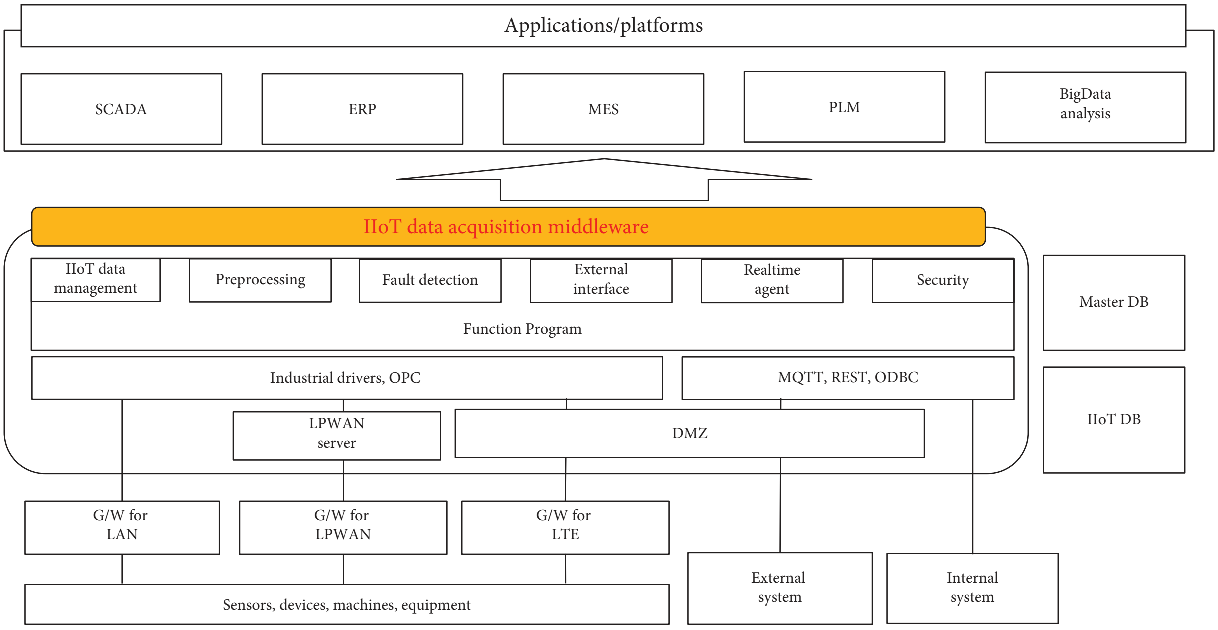


Figure 2: An overall architecture of a centralized IIoT server with data-acquisition middleware.

acquired without altering the existing PLC programs. Consequently, a number of commercial programs have been released for obtaining PLC data directly.

With the early development of PLC, a standard interface, OPC has been established. OPC enables real-time monitoring and links to automation systems, such as Human Machine Interface (HMI) and SCADA. OPC has improved the security and connection speed of the PLC protocol. In 2008, OPC-UA—vendor-dependent and highly secure protocol—was developed by the OPC Foundation [30]. It is used much in interworking with IT systems. The previous versions of OPC had a client-server architecture, which made it difficult to process multiple messages simultaneously. Conversely, OPC-UA provides publish/subscribe functions to enable 1 : N and N : N communications in real time. Moreover, it has a reliable version for cloud environments. In recent years, many researchers have been conducting research on Time-Sensitive Networking (TSN) linked with OPC to achieve 18 times faster real-time remote control and monitoring.

3.3. Production IT. Many companies have built ERP and MES for managing quality products. Before the emergence of Industry 4.0, the old systems used to operate in a vertical structure. In ISA-95 standard, the systems operate by sending and receiving data only at each of the front and rear levels. However, the development of IIoT has eliminated the boundaries of data. Data-acquisition middleware is needed to directly obtain data from MES, ERP, and the control process. The middleware requires protocols or drivers to obtain information from legacy IT systems. For instance, considering the fact that ODBC and JDBC are usually required to connect to the database, the middleware can support the drivers. In the case of a three-tier system, another interface such as REST can be used, particularly in the environment where there is little direct access to the data due to security reasons.

3.4. Cloud vs. On-Premises. Recently, the cloud has been widely adopted for its efficiency and cost-effectiveness. Many IT companies have customers who wish to use infrastructure and resources in the forms of SaaS, PaaS, and IaaS. For IIoT data acquisition, the cloud system acquires data in a different manner from an on-premises environment. The IIoT equipment, including sensors, actuators, and gateways, provide data while being located at the industrial site. Numerous existing equipment are mostly connected to networks such as LAN. This industrial equipment often has its own industrial protocols. In this case, the transfer of IIoT data to the cloud environment is required. Edge consists of a device or a program that converts the sensor's analog signal or serial signals to LAN communication. Edge also uses network bridges called protocol converters or gateways. The configuration of network bridges or the edge can be applied to industrial sites for industrial controllers, such as PLC, industrial computers, and dedicated converters, that change specific signals. Thus, an edge program that can connect to the cloud system needs to be installed on IIoT equipment. For example, offering an API is possible with standard protocols, such as MQTT and OPC-UA, or customized protocols of their own companies. Usually, due to installation of the edge program, OS-based products are needed. In this case, it is necessary to establish an environment where packages or APIs can be used, such as Linux OS or Windows OS.

Unlike the cloud systems using edge, the on-premises system makes it easy to obtain IIoT data in a centralized network management environment. Usually, the on-premises system uses network bridges for extended communication distance. The central server manages a variety of information, including the IIoT device ID, protocols, acquisition rate, and resources. In the on-premises system, the network bridge has a wider range of configurable choices than that of the cloud system. Some cloud systems need to change equipment due to the requirement of some protocols such as MQTT, REST, and OPC-UA. However, the on-premises is more flexible than the cloud and can acquire data directly from IIoT equipment that are easy to use various gateways.

3.5. Qualitative Analysis of Existing IIoT Data-Acquisition Middleware Systems. In this section, we qualitatively analyze a variety of IIoT data acquisition middleware systems based on well-motivated criteria.

Table 1 lists the IIoT data-acquisition middleware systems developed by each vendor [31–48]. We comprehensively analyzed these systems in terms of the five major aspects in the second and third levels of Figure 1: (1) operating environment, (2) protocol, (3) driver, (4) real-time, and (5) security.

Edge software provided by IT vendors includes cloud-based middleware, such as Azure IoT Hub, AWS Industrial IoT, Oracle Internet of Things Cloud service, and Predix. These middleware systems provide software packages or APIs for the connection from IIoT equipment to their clouds using edge devices. The OPC-UA protocol is applied considering real-time control and monitoring, as well as the interface industrial system. In addition, due to the various conditions of industrial sites, IIoT data are acquired in cooperation with specialized partners in the field to suit the site situation. Kepware, PI Collect, AVEVA Edge, and MindSphere Connect that show strength in the current OT field can easily make connection of the current IIoT equipment to their systems. The companies are also increasing the ease of connectivity by providing various industrial protocols, such as the PLC interface, Modbus, and OPC-DA/UA. Moreover, some companies and research institutions use their own technology and thus create systems optimized for specialized environments [46–51]. In this case, although a middleware system does not have many functionalities, it offers great features that are specialized in the environment of operation.

Every middleware provides real-time "monitoring" functions, but some middleware services (such as Oracle Internet of Cloud Service, ThingPlug, and N-MAS) do not allow the control of IIoT devices in real time. Finally, all middleware systems well support security for communication from IIoT devices to their respective middleware.

4. Experiment: A Reliability Test of IIoT Data Acquisition at a Real Industrial Site

For convenient operation at industrial sites, IIoT data acquisition needs to be centralized. To minimize investment, we should have to determine the feasibility of acquiring the IIoT data from the legacy network infrastructure in a centralized way. To this end, we designed an IIoT data-acquisition experiment leveraging the wired and wireless networks used in office work. During this experiment, we measured data-acquisition rates for 24 h during weekdays and analyzed the network loads. Briefly, the results demonstrate that IIoT data can be "indeed" acquired by the networks used in general office work.

4.1. Environment Settings. By our intended design, we conducted two actual experiments in terms of central IIoT data acquisition in an on-premises environment via two methods, as shown in Figures 3 and 4. The difference between the two experiments was the communication environment through which the data was acquired.

For the wireless networks, we utilized LTE communication using a licensed band network (KT Corporation) in South Korea. In particular, we used a router with Private-LTE (P-LTE) for security purposes. The external LTE servers checked the router's IP and port number and switched to the designated IP and port number assigned by the customer. Subsequently, the data were sent to the internal DMZ server, which checked the IP and port number for security reasons. Finally, the data were safely sent to the internal server. The total processing time was one second.

The first method was to acquire IIoT data *via wired communication* (Figure 3(a)). The second method was to acquire data centrally *via LTE communication* (Figure 3(b)). The wired communication is the most adopted communication in the field, while LTE is now prevalent.

Configurations are exhibited in detail in Table 2. Test device is the welding machine used in a shipyard where ships and offshore plants are built. We used a total of 14 tags, including ID, voltage, current, temperature, and product information. The used protocol is a user-defined protocol. When data is requested, the welding machine sends the requested data (Figure 4). The requested data requires a total of 15 tags per a second. Because the data interface of the welding machine is RS232, the maximum transmission distance is 15 m. Thus, the machine requires a network bridge to transmit data at a long distance.

The data path of the welding machine is divided into two routes. In the first route, the IIoT data acquisition middleware requests tag data through the network bridge *via* TCP/IP communication, and the network bridge then sends tag data to the welding machine *via* RS232 interface. In the second route, the welding machine responds according to the command and then forwards all tag data back to the middleware.

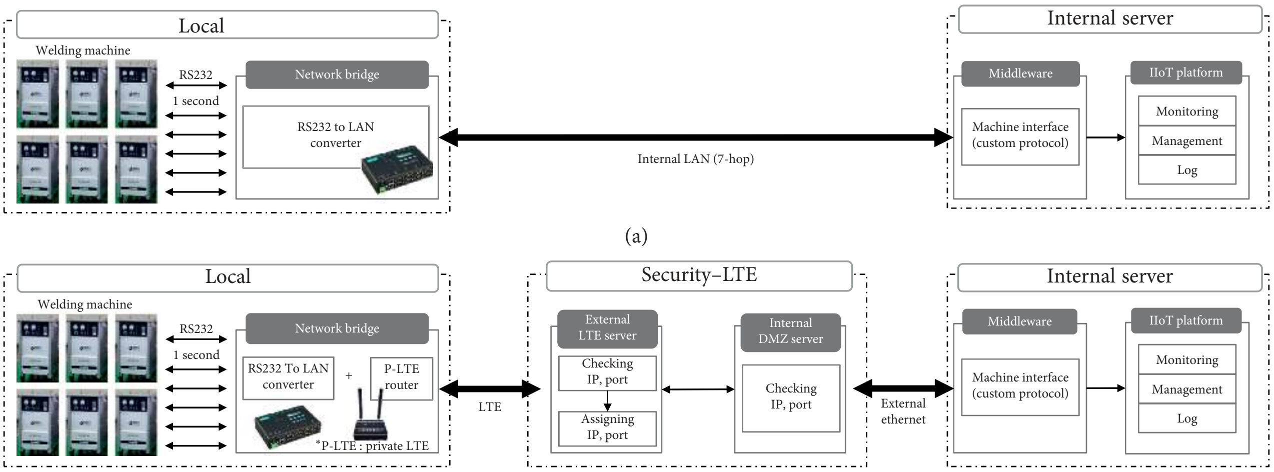
The rate at which all data were acquired was once per second. Therefore, 86,400 s tag sets were acquired per a day. The experimental period was 10 days, excluding weekends, when the equipment was not in operation all day.

The applied network bridge model was NPORT-5610 in MOXA, which has eight ports that convert RS232 to TCP/IP communication. In the NPORT model, we used the TCP/IP server mode to communicate with the middleware.

The data acquisition middleware used PTC's KEPServerEX 6.4 with U-CON driver, which can handle the welding machine's customized protocol. The data acquisition middleware was linked to our IIoT platform to monitor, manage, and store the data being collected.

Table 1: Qualitative analysis of IIoT data acquisition middleware systems.

Middleware (company)	Operation environment	Industrial protocols	Communication protocol	Db driver	Real time	Security
Azure IoT Hub (Microsoft) [31]	Cloud	OPC-UA, modbus	MQTT, REST	O	O	O
AWS Industrial IoT (Amazon) [32]	Cloud	OPC-UA, modbus	MQTT, REST	O	O	O
IBM PSB (IBM) [33]	On-premises	OPC-UA	MQTT, REST	O	O	O
Oracle Internet of Things Cloud Service (Oracle) [34]	Cloud	X	REST	O	X	O
Predix edge (GE digital) [35]	Cloud	OPC-UA, modbus	MQTT, REST	O	O	O
Kepware (PTC) [36]	On-premises	PLCs, modbus, OPC-DA/UA	MQTT, REST	O	O	O
PI Collect (OSIsoft) [37]	On-premises	PLCs, modbus, OPC-DA/UA	MQTT, REST	O	O	O
AVEVA Edge (Aveva) [38]	On-premises	PLCs, modbus, OPC-DA/UA	MQTT, REST	X	O	O
Mind Sphere Connect (Siemens) [39]	Cloud	PLC (Siemens), modbus, OPC-UA	MQTT, REST	X	O	O
WISE-PaaS (Adventech) [40]	Cloud	OPC-UA	MQTT, REST	O	O	O
ThingPlug (SKT) [41]	Cloud	X	MQTT, REST, OneM2M	O	X	O
N-MAS (Ntels) [42]	Cloud, om-premises	X	MQTT, REST	O	X	O
ThingSPIN (Hancom MDS) [43]	On-premises	OPC-UA, modbus	REST	O	O	O
TeraONE (DataStreams) [44]	On-premises	OPC-UA	REST, OneM2M	O	O	O
MOBIUS (KETI) [45]	On-premises	X	REST, OneM2M	X	O	O
IoTEP [46]	On-premises	X	MQTT, REST, LwM2M	O	O	O
SEnviro Connect [47]	Cloud	X	MQTT, REST	O	O	O
SPLS [48]	Cloud	X	—	O	O	O



(a)

(b)

Figure 3: Experiment architecture of IIoT data-acquisition middleware using a welding machine. (a) On-premises environment using wired communication. (b) On-premises environment using LTE communication.

4.2. Result Analysis. In this section, we present and discuss our experiment results regarding the network sensitivity of IIoT data-acquisition middleware.

In our experiment the data-acquisition rates were calculated on a per-second basis. Thus, if the total count of data received reaches 864,000, its daily acquisition rate means 100% for 10 days.

As shown in Figure 5, we compare the data-acquisition ratios of wired and LTE communications for a total of 10 days. In the wired communication, the data-acquisition rate is from 99.984% to 98.537%. In LTE communication, on the contrary, the data-acquisition rate is 99.984% to 97.739%.

Figure 6 illustrates the per-hour data-acquisition rates for 24 h. Business hours are from 08 : 00 to 20 : 00 during the daytime and from 20 : 00 to 06 : 00 during the overnight. Most employees typically work during the daytime, so it is possible to confirm whether the network load was affected by the use of an internal network. According to our results, the

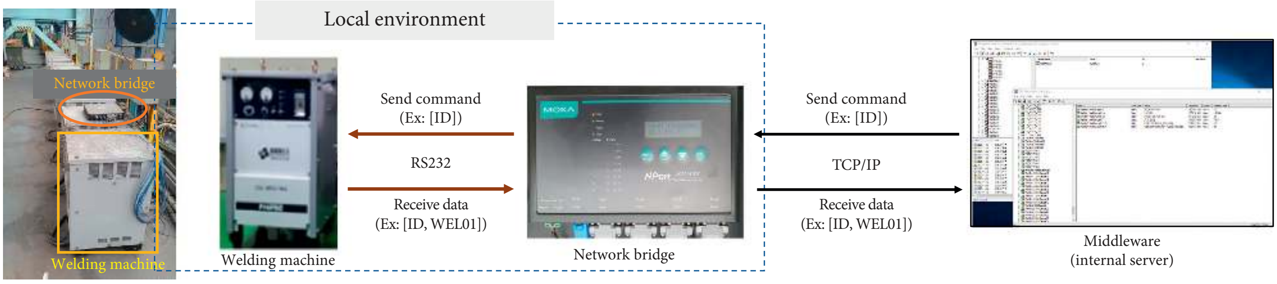


Figure 4: Environment settings and data descriptions for acquiring welding machine data at shipyard.

Table 2: Configuration settings in different communication methods.

	Wired communication	LTE communication
IIoT device	Welding machine	
Interface to IIoT device	RS232 (serial communication)	
Number of tags	15 EA	
Protocol	Customized protocol	
Network bridge	Used in RS232 to LAN converters	
LAN speed	100 Mbps	
Period of test	10 days	
Hop count (network distance)	7	8 or more
Latency (ping test)	Under 1 ms	Under 80 ms
Number of devices	10 EA	4 EA
Total number of dataset	9,929,890	3,276,842

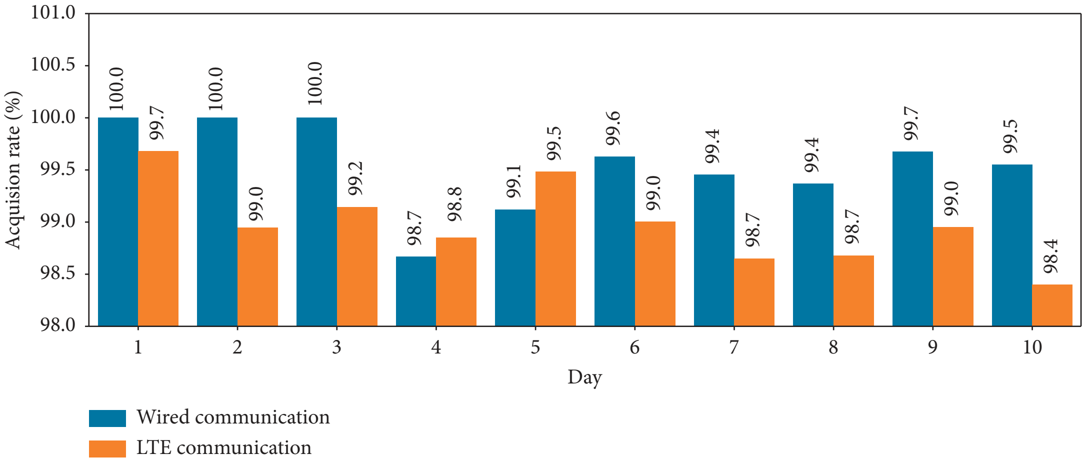


Figure 5: Average rate of IIoT data acquisition over 10 days.

network load turned out to be unaffected about acquiring IIoT data.

Table 3 exhibits our results about the interarrival time of data. A one-second interval (at the second row below the header of Table 3) is considered as *normal*, and *unstable*, otherwise. Because the ratio of the 1 s interval differs by about 1% between wired and LTE communications (99.730% vs. 98.857%), we empirically confirmed that wired communication was not significant but more reliable than wireless communication in our IIoT environment (although this observation could be obvious).

Table 4 demonstrates the average data-acquisition rate of each of the welding machines used in our experiments. In the table, for all datasets, the averages were 99.940% for wired communication and 98.983% for LTE communication, respectively. In the case of wired communication, the hop count was seven, but the network in the case of LTE was more complex as it passed through eight hops or more through the external networks and the internal DMZ server. Thus, a lower data-acquisition rate was expected. Moreover, wired communication did not acquire 100% of the data due to communication errors in the device, middleware, and timer.

In this experiment, the overall average data-acquisition rate including wired and wireless communication was 99.701% despite centralized acquisition. We also confirmed

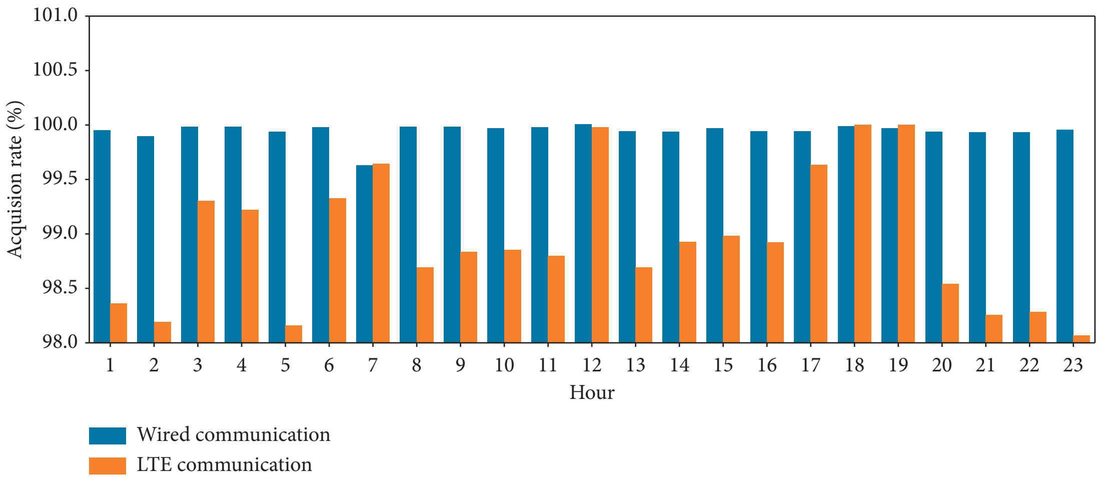


Figure 6: Average rate of IIoT data acquisition per hour for a day.

Table 3: Interarrival times between previous and current data packets.

Data Inter-arrival Time	Wired communication		LTE communication	
	Total count	Ratio (%)	Total count	Ratio (%)
0-1	20841	0.201	6858	0.200
1	10333828	99.730	3381751	98.857
2	4797	0.046	28386	0.830
3-5	1393	0.013	3541	0.104
5-10	518	0.005	183	0.005
>10	404	0.004	103	0.003

Table 4: Average data-acquisition rates of different welding machines.

	ID	Total count	Acquisition ratio (%)
Wired communication (average ratio: 99.940%)	Welder #1	863779	99.974
	Welder #2	863715	99.967
	Welder #3	863785	99.975
	Welder #4	863754	99.972
	Welder #5	863742	99.970
	Welder #6	860002	99.537
	Welder #7	863761	99.972
	Welder #8	863845	99.982
	Welder #9	863861	99.984
	Welder #10	863862	99.984
	Welder #11	863861	99.984
	Welder #12	863862	99.984
LTE communication (average ratio: 98.983%)	Welder #13	863862	99.984
	Welder #14	858271	99.337
	Welder #15	844462	97.739
	Welder #16	854244	98.871

that 98.983% of the data can be acquired although LTE communication was used.

To configure the same data acquisition middleware in the cloud, the use of an edge device is required to transfer data from the device to the cloud, taking into consideration security, as data is sent to external networks. In the cloud environment, the initial cost of infrastructure configuration is low. Thus, having a small number of IIoT equipment is advantageous. However, in the case of large-scale facilities, the operating costs increase with the increase in data transmission volume and data processing problems. Therefore, it seems that cost, maintenance, and security should be addressed well when an operation environment is selected. Currently, numerous hybrid systems combined with the on-premises and cloud are being used to do so.

5. Conclusion and Future Work

We conducted an in-depth survey of recent IIoT platforms with potentiality for horizontal data acquisition. We reviewed various data-acquisition middleware products released by eighteen companies and research institutes. Through our investigation, we derived well-defined criteria by which the systems can be categorized. We also presented the major functionalities for building high-quality centralized IIoT data-acquisition middleware. To justify one of these criteria (network), we empirically evaluated the performance of centralized data acquisition via wired and LTE communications using an actual IIoT device (a welding machine). The overall average rate of 16 welding machines across the wired and wireless networks was 99.701%, validating the centralized IIoT data acquisition. Finally, we identified several challenges that must be resolved to construct the best data acquisition middleware in a centralized environment.

We expect that our work will help to clarify the criteria and the important considerations of high-quality IIoT data acquisition middleware systems. We plan to build our own data acquisition middleware that can fully meet the suggested functionalities. The middleware configuration and operation will be tested in a real production environment.

Data Availability

The experiment data are the property of Daewoo Shipbuilding & Marine Engineering Co., Ltd. (DSME). Therefore, the experiment data are proprietary to DSME.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported in part by DSME, Korea, under the DSME Industrial Application R&D Institute support research program and in part by Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (no. 2016-0-00145, Smart Summary Report Generation from Big Data Related to a Topic). The results of this experiment and research use DSME assets.

References

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial internet of things: challenges, opportunities, and directions,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[2] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, “Digital twin in industry: state-of-the-art,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 4, pp. 2405–2415, 2018.

[3] M. Zdravković, M. Trajanović, J. Sarraipa et al., “Survey of internet-of-things platforms,” in *Proceedings of the 6th International Conference on Information Society and Techology*, Kopaonik, Serbia, February 2016.

[4] J. Guth, U. Breitenbücher, M. Falkenthal et al., *A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences*, Internet of Everything, London, UK, 2017.

[5] J. Guth, U. Breitenbücher, M. Falkenthal, F. Leymann, and L. Reinfurt, *Comparison of IoT Platform Architectures: A Field Study Based on a Reference Architecture*, Cloudification of the Internet of Things, Stuttgart, Germany, 2016.

[6] A. A. Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: a survey on enabling technologies, protocols, and applications,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[7] L. D. Xu, W. He, and S. Li, “Internet of things in industries: a survey,” *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[8] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, “IoT middleware: a survey on issues and enabling technologies,” *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 1–20, 2017.

[9] A. Atmani, I. Kandrouch, N. Hmina, and H. Chaoui, “Big data for Internet of Things: a survey on IoT frameworks and platforms,” in *Advanced Intelligent Systems for Sustainable Development (AI2SD’2019). AI2SD 2019. Lecture Notes in Networks and Systems*, M. Ezziyyani, Ed., vol. 92, Springer, Cham, Switzerland, 2020.

[10] H. Hejazi, H. Rajab, T. Cinkler, T. Cinkler, and L. Lengyel, “Survey of platforms for massive IoT,” in *in Proceedings of the IEEE International Conference on Future IoT Technologies*, pp. 1–8, Eger, Hungary, January 2018.

[11] M. Aazam, S. Zeadally, and K. A. Harras, “Deploying fog computing in industrial internet of things and industry 4.0,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4674–4682, 2018.

[12] H. Cho and J. Jeong, “Implementation and performance analysis of power and cost-reduced OPC UA gateway for industrial IoT platforms,” in *Proceedings of the 28th International Telecommunication Networks and Applications Conference*, pp. 1–3, Sydney, Australia, November 2018.

[13] H. Choi, J. Song, and K. Yi, “Brightics-IoT: Towards Effective Industrial IoT Platforms for Connected Smart Factories,” in *Proceedings of the IEEE International Conference on Industrial Internet*, pp. 146–152, Seattle, WA, USA, October 2018.

[14] W. Wang, S. L. Capitaneanu, D. Marinca, and E.-S. Lohan, “Comparative analysis of channel models for industrial IoT wireless communication,” *IEEE Access*, vol. 7, pp. 91627–91640, 2019.

[15] P. Duan, Y. Jia, L. Liang, J. Rodriguez, K. M. S. Huq, and G. Li, “Space-reserved cooperative caching in 5G heterogeneous networks for industrial IoT,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2715–2724, June 2018.

[16] C. Hsu, Y. Hsu, and H. Wei, “Energy-efficient and reliable MEC offloading for heterogeneous industrial IoT networks,” in *Proceedings of the 2019 European Conference on Networks and Communications (EuCNC)*, pp. 384–388, Valencia, Spain, June 2019.

[17] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, “A comparative study of LPWAN technologies for large-scale IoT deployment,” *The Korean Institute of Communications and Information Sciences*, vol. 5, pp. 1–7, 2019.

[18] G. Premsankar, B. Ghaddar, M. Slabicki, and M. D. Francesco, “Optimal configuration of LoRa networks in Smart cities,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, 2020.

[19] A. Mahmood, E. Sisinni, L. Guntupalli, R. Rondón, S. A. Hassan, and M. Gidlund, “Scalability analysis of a LoRa network under imperfect orthogonality,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, 2019.

[20] E. Sisinni, P. Ferrari, D. Fernandes Carvalho et al., “LoRaWAN range extender for industrial IoT,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5607–5616, 2020.

[21] L. Leonardi, F. Battaglia, and L. Lo Bello, "RT-LoRa: a medium access strategy to support real-time flows over LoRa-based networks for industrial IoT applications," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10812–10823, 2019.

[22] M. Ballerini, T. Polonelli, D. Brunelli, M. Magno, and L. Benini, "NB-IoT versus LoRaWAN: an experimental evaluation for industrial applications," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7802–7811, 2020.

[23] M. Zhu, L. Chang, N. Wang, and I. You, "A smart collaborative routing protocol for delay sensitive applications in industrial IoT," *IEEE Access*, vol. 8, pp. 20413–20427, 2020.

[24] R. Amin, S. Nazir, and I. García-Magariño, "A collocation method for numerical solution of nonlinear delay integro-differential equations for wireless sensor network and internet of things," *Sensors*, vol. 20, no. 7, p. 1962, 2020.

[25] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods," *IEEE Access*, vol. 8, pp. 152316–152332, 2020.

[26] X. Huang and S. Nazir, "Evaluating security of internet of medical things using the analytic network process method," *Security and Communication Networks*, vol. 2020, Article ID 8829595, 14 pages, 2020.

[27] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial IoT systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6092–6102, 2020.

[28] Editorial, "Blockchain in industrial IoT applications: security and privacy advances, challenges, and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4119–4121, 2020.

[29] T. Kumar, E. Harjula, M. Ejaz et al., "Blockedge: blockchain-edge framework for industrial IoT networks," *IEEE Access*, vol. 8, pp. 154166–154185, 2020.

[30] OPC Foundation, "OPC unified architecture release 1.04," 2017, https://opcfoundation.org/, viewed.

[31] 2020 https://docs.microsoft.com/ko-kr/azure/architecture/guide/iiot-guidance/iiot-architecture.

[32] 2020 https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html.

[33] S. Bonnaud, C. Didier, and A. Kohler, "Industry 4.0 and cognitive manufacturing," 2020, https://www.ibm.com/downloads/cas/m8j5ba6r.

[34] 2020, https://docs.oracle.com/en/cloud/paas/iot-cloud/.

[35] 2020, https://www.ge.com/digital/iiot-platform/predix-edge.

[36] 2020, https://www.kepware.com/en-us/products/kepserverex/.

[37] 2020, https://www.osisoft.com/pi-system/.

[38] 2020, https://www.aveva.com/en/products/edge/.

[39] 2020, https://siemens.mindsphere.io/en.

[40] 2020, https://wise-paas.advantech.com/ko-kr/marketplace.

[41] 2020, https://www.sktiot.com/iot/introduction/thingplug/thingplugMain.

[42] 2020, https://www.ntels.com.

[43] 2017, https://www.hancommds.com.

[44] 2020, http://www.datastreams.co.kr/.

[45] 2020, http://tech.iotocean.org/.

[46] F. Terroso-Saenz, A. González-Vidal, A. P. Ramallo-González, and A. F. Skarmeta, "An open IoT platform for the management and analysis of energy data," *Future Generation Computer Systems*, vol. 92, pp. 1066–1079, 2019.

[47] S. Trilles, A. González-Pérez, and J. Huerta, "An IoT platform based on microservices and serverless paradigms for smart farming purposes," *Sensors*, vol. 20, no. 20, p. 2418, 2020.

[48] Y. Zhang, Z. Guo, J. Lv, and Y. Liu, "A framework for smart production-logistics systems based on CPS and industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4019–4032, 2018.

[49] S. Nazir, Y. Ali, N. Ullah, and I. García-Magariño, "Internet of things for healthcare using effects of mobile computing: a systematic literature review," *Internet of Things for Healthcare Using Wireless Communications or Mobile Computing*, vol. 2019, Article ID 5931315, 20 pages, 2019.

[50] R. S. Alonso, I. Sittón-Candanedo, Ó. García, J. Prieto, and S. Rodríguez-González, "An intelligent edge-IoT platform for monitoring livestock and crops in a dairy farming scenario," *Ad Hoc Networks*, vol. 98, Article ID 102047, 2020.

[51] A. R. Jadhav, S. Kiran, and R. Pachamuthu, "Development of a novel IoT-enabled power- monitoring architecture with real-time data visualization for use in domestic and industrial scenarios," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–14, 2021.