I.J. Wireless and Microwave Technologies, **2024, 4, 29-47**
Published Online on August 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2024.04.03

Smart Factory based on IIoT: Applications, Communication Networks and Cybersecurity

Yazen S. Sheet*
Department of Electrical Engineering, University of Mosul, Mosul, Iraq
E-mail : yazenalnuaimi@uomosul.edu.iq
ORCID ID: https://orcid.org/0000-0002-2183-0711
*Corresponding Author

Mohammed Younis Thanoun
Department of Electrical Engineering, University of Mosul, Mosul, Iraq
E-mail: myounisth@uomosul.edu.iq
ORCID ID: https://orcid.org/0000-0002-2852-3917

Firas S. Alsharbaty
Department of Electrical Engineering, University of Mosul, Mosul, Iraq
E-mail: Alsharbaty@uomosul.edu.iq
ORCID ID: https://orcid.org/0000-0002-0353-1777

Received: 18 March, 2024; Revised: 20 May, 2024; Accepted: 04 June, 2024; Published: 08 August, 2024

Abstract: Smart factory represents one of the main Industrial Internet of Things applications that contribute in the industrial activities in the smart cities. This field acquires a special attention with the age of industry 4 from upgrading the passive machine into cyber physical system point of view. However, the process of developing the traditional factory into smart factory faces some issues regarding to handle smart and safe management such as handling the requirements of smart factory applications and the communication networks that should transfer the data among different parts. The current review paper highlights the up-to-date related works in the field of industry 4 in terms of industrial internet of things (IIoT) to filling the gap between the operational technologies and information technologies. Hence, the different architectures of IIoT are taken into consideration of research paper scope in terms of investigation and analysis. This work concentrates on the smart factory application and aims to connect between applications requirements and communication networks in the field of the smart factory in order to hold the optimum management to this aspect. Moreover, the expected cyberthreats and cyberattacks in the smart factory are captured in this work to explain the suitable countermeasures against such cyberattacks.

Index Terms: Industry 4.0, IIoT, Smart Factory, Communication Technologies, Cybersecurity

1. Introduction

In recent years, many works exploit Internet of Things (IoT) technologies in different aspects such as real-world situations. The scope of IoT focuses on the connection of physical devices and the exchange of data through the internet, without the need for human-to-machine or human-to-human interaction However, the specific phrase 'Internet of Things' was introduced by Kevin Ashton in 1999[1]. Enabling the connection of non-traditional objects to the Internet may enhance the sustainability and safety of enterprises and society. It also facilitates efficient interaction between the physical world and its digital equivalent, sometimes referred to as a Cyber-physical System (CPS). The Internet of Things (IoT) and Industrial IoT are commonly portrayed as a revolutionary technology that can address various societal challenges, including smart cities, intelligent transportation, pollution monitoring and manufacturing. Table 1 illustrates the differences between IoT and IIoT[2, 3].

Table 1. IoT and IIoT DIFFERENCES

Property	Internet of Things (IoT)	Industrial IoT
Connected things	User-level devices	Manufacturing Systems
Service model	Human-based	Machine-based
Capacity	Small connectivity	Large connectivity
Communication	Generally, wireless	wired and wireless
Data Volume	Medium to high	High to very high

Implementing the Industrial Internet of Things with information communication (ICT) technologies has led to the emergence of the Fourth Industrial Revolution known as Industry 4.0.(see Fig .1)[4].

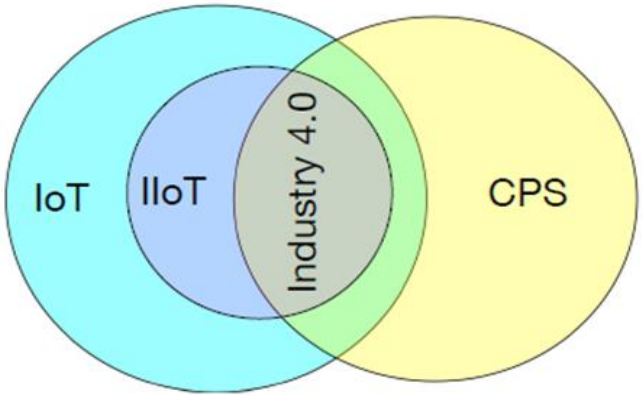

Fig.1. Industry 4.0 concept[5]

Industry 4.0 represents the fourth industrial revolution, including the intelligent transition of personal and industrial systems utilizing various technologies. However, previous generations before the industry 4.0 revolution did not contain intelligent transformation and automation to completing operations in an integrated manner. Industrial Internet of Things (IIoT) commonly used to refer to this concept which has numerous applications in various fields, such as Agriculture, healthcare, and manufacturing.

A smart factory can be considered as most important IIoT applications that involves networked components, machines, and systems that communicate with each other to facilitate real-time data collecting, analysis, and decision-making [6]. IIoT helps smart factories to accomplish their assigned tasks without human intervention by automating production processes using three basic elements: sensors, communication networks, and control unit to make decisions. It has many applications like functional safety, monitoring and remote control which have strong data rates and latency requirements. To achieve the requirements of smart factories in Industry 4, it requires a reliable communication network and addressing the related cybersecurity issues. However, the process of developing the field of smart factory requires filling the gap between IIoT, the communication networks and information technologies. In this context, this work aims to address the previous issues by subject the following objectives:

- Presents the up-to-date of Industry 4.0 revolution and related technologies.
- Explain the IIoT architecture and the fields which can be used.
- Illustrates the Smart Factory concept and specify its applications related to some metrices such as latency and data rate.
- Provide a survey for communications technologies (wired and wireless) which can be candidate to satisfy the requirements of smart factory applications.
- Addresses the security attacks which can be target the IIoT layers and explain the countermeasures for that.

This work is structured into six sections. Additionally, the introduction, in Section 2, a review of some related works has been made an overview to Industry 4 has been provided in section 3. Section 4 illustrates IIoT architecture and applications. Section 4 explains the smart factory concept. In Section 6, cybersecurity concerns have been outlined, finally section 7 presents the conclusion.

2. Related Works and Contributions

Many works have been made to examine the interdependencies of architectures, applications, requirements, security concerns, and technologies of IIoT ,for instance in [7] the authors presented a comprehensive overview of existing research on IIoT, covering topics such as architectures, frameworks, communication protocols, data

management techniques, and machine learning in manufacturing. They discussed the recent challenges faced by IIoT systems and their enabling technologies. The work in [8] discussed the historical development of IoT and the architecture of IIoT, comprising the edge tier, platform tier, and cloud tier. It explained the uses of Industrial Internet of Things (IIoT) in several industries like manufacturing, agriculture, cities, households, healthcare, and transportation. It also highlighted the significance of dealing with security, safety, and privacy issues in the IoT ecosystem. In [9], the authors discussed the significant role played by the Internet of Things (IoT) in transforming traditional factories into smart factories in the context of Industry 4.0. The authors highlighted various applications of IoT in smart factories, including optimized production processes, predictive maintenance, energy usage monitoring, workplace safety enhancement, supply chain optimization, and inventory management. The survey in [10] discussed various aspects of IIoT, including its network infrastructure, protocols, devices, and the relationship between IIoT and key technologies such as big data storage, cloud computing, and data analytics. In addition, the authors handled the benefits of implementing IIoT in the industrial and address security challenges and presents countermeasures to mitigate IIoT-based security attacks. The authors in [11] explained the challenges and requirements of real-time communication in industrial networks, particularly in the context of Industry 4.0. They reviewed existing real-time networking technologies and presented recent works in the field also they emphasized the need for reliable and flexible networks to support diverse data types with varying criticality, such as control traffic, sensor data, and configuration messages. The authors in [12] addressed the significance of wireless communication in smart manufacturing, which sought to enhance production processes by continuously monitoring, controlling, and adjusting operations to improve efficiency and enable personalized manufacture. The nominated research explained the necessity for wireless communications to fulfill specific requirements of industrial IoT and automation systems by providing low-latency and reliable connectivity. In general, this review paper aims to explain the interconnection among communication networks and cyber security to meet the requirements of the different applications of smart factory, Fig. 2 explains the flow chart of paper methodology. Table 2 shows a comparison between the methods of mentioned previous works and the current work.

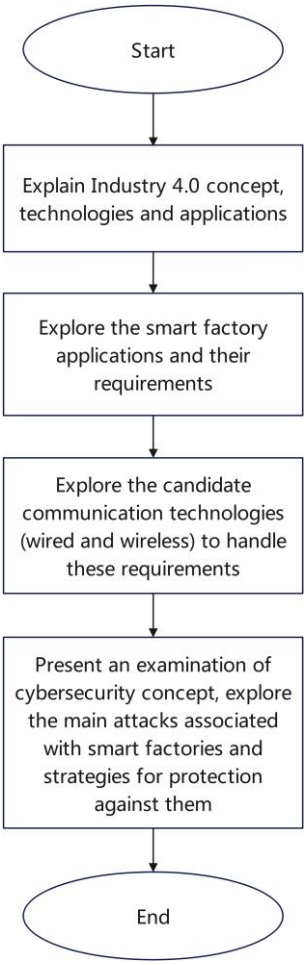

Fig.2. Flow chart of methodology

Table 2. Comparison among this work and previous related works

Ref.	IIoT					
	Architectures	Applications	SFA	Requirements of SFA	Communication Technologies (wired &Wireless)	Security Issues
[7]	Yes	No	No	No	No	No
[8]	Yes	Yes	No	No	No	Yes
[9]	Yes	No	Yes	No	No	No
[10]	Yes	Yes	No	No	No	Yes
[11]	No	No	Yes	Yes	Yes	No
[12]	No	No	Yes	Yes	Wireless only	No
Work	Yes	Yes	Yes	Yes	Yes	Yes

SFA: Smart Factory Applications

3. Industry 4.0 Concept

The concept of Industry 4.0 began in Germany and has been acknowledged by other prominent industrial nations. However, it is referred to as "Connected Enterprise" in the United States and the "Fourth Industrial Revolution" in the United Kingdom.[13].The progression from manual work to the industry 4.0 idea in industrial manufacturing systems can be depicted as a journey through the four industrial revolutions. Fig. 3 illustrates the progress of the industry revolution.

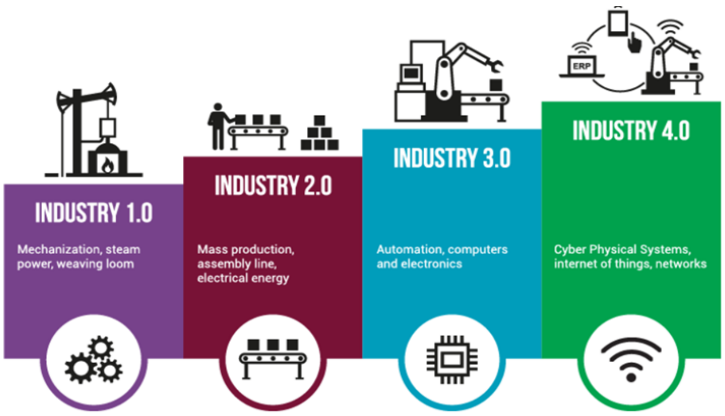

Fig.3. The stages of Industry 4.0 Revolutions[16]

The first industrial revolution occurred in the 1800s, marked by the introduction of mechanization and the development of mechanical power. It facilitated the shift from manual work to the initial stages of mechanized production, primarily in the textile sector[14].

The second revolution occurred throughout the 1900s and was characterized by the use of mass production using assembly lines, which were driven by electricity.

The beginning of the third industrial revolution occurred in the 1970s, in which computers were employed to enhance the advancement of automated production processes and machinery.

The principle of Industry 4.0 is represented by the presence of Smart Factories and the comprehensive utilization of digital manufacturing and intelligent automation of cyber-physical systems, utilizing decentralized control and improved communication through IoT features[15].

Industry 4.0 is made up of four interconnected components or levels that collaborate to build specific industrial applications. The four industrial levels consist of device, control, production, and enterprise [8] it encompasses a multitude of diverse standards or frameworks; this characteristic enables the construction of Industry 4.0 frameworks in a heterogeneous manner. Due to this complex structure, a new structure includes many incorporating technologies have been developed. Industry 4.0 is characterized by the collaboration of multiple technologies which can be considered as the facilitator of Industry 4.0 revolution. The implementation of these technologies differs between industries with certain businesses relying on a more general product level[17]. The main supporting technologies for Industry 4.0 are listed in the following points, however the comprehensive technologies extend beyond these ones[18]:

- **CPS, or Cyber-Physical Systems**: are automated systems that facilitate the integration of physical activities with computing and communication infrastructures.
- **The Internet of Things (IoT)**: refers to the concept of collecting data through sensors from physical objects and send these data to other parts using wired networks or high-speed wireless communication network.
- **Cloud manufacturing**: is a form of cloud computing technology that is specifically used in the manufacturing sector. Utilizing cloud computing systems should be suitable for Industry 4.0 to increase the need for resources. Cloud infrastructure is a highly accessible computing facility that allows for efficient computer processing.
- **AI Methods such as Machine learning**: is a collection of computer methods that specifically aim to extract essential knowledge and make suitable decisions from data which can be received from Additional sources at any given moment and can be both structured and unstructured, including design records, customer orders, supplier deliveries, stock information, and logistics-related data which called Bigdata and it is a significant concept in Industry 4.0

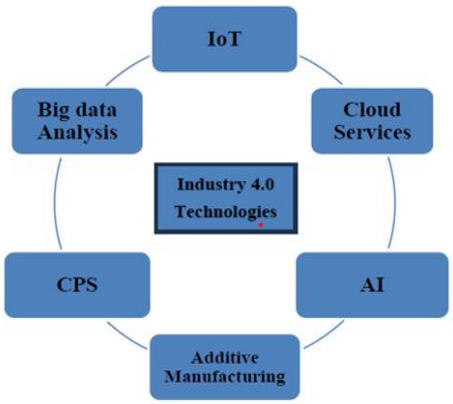

Fig.4. Industry 4.0 Enabling Technologies

4. Industrial Internet of Things (IIoT)

The IIoT, or Industrial Internet of Things, is the application of IoT technologies to improve and optimize industrial manufacturing processes. An essential attribute of the Industrial Internet of Things (IIoT) is the integration of sensors into all manufacturing process components. These sensors work as sensory parts, gathering data throughout the entire production process and the lifespan of the product. Based on large number of modern technologies, IIoT allows for the development of novel business models through enhancing productivity, maximizing operational efficiency, optimizing corporate operations, and protecting systems[19]. In the following sections, the architecture, applications of IIoT will be clarified.

4.1. IIoT Architecture

A critical problem that companies encounter while adopting IIoT is selecting the appropriate architecture. As the IIoT is fundamentally centered around devices connectivity within a network, the architecture becomes a vital role. The design of IIoT systems is generally conceived as a layered modular structure of digital technologies each layer has distinct functions. Various businesses have different requirements for the Industrial Internet of Things (IIoT), for instance, the data generated during the takeoff and landing of an airplane is very distinct from that produced by the simple gasket manufacturing process. Because the IIoT entails the transfer of data, it is crucial to select the appropriate IIoT architecture which suits the requirements of selected application. Fig 5. represents the IIoT general architecture.

Perception layer: the perception layer is regarded as physical layer of IIoT architecture. It is also known by alternative terms such as sensor layer, devices layer, and others. The purpose of this layer is to gather data and detect smart things inside a manufacturing environment using several sensors. The technologies utilized in this layer include sensors, actuators, imaging devices, RFID tags, and other similar components, each having distinct computational and energy prerequisites. The primary function of this layer is to gather data from the environment and transmit it to the network layer following the process of digitization[21].

Network layer: The network layer is widely regarded as the most advanced layer in the architecture of the Industrial Internet of Things (IIoT). It is also called data transmission layer. The fundamental responsible of this layer is to transmitting and receiving the information of industrial processes between physical things, devices, sensors, networks, and servers using latest wired and wireless communication technologies[20].

Middleware layer: This layer is referred to as the third level or support layer also called as processing layer. The function of this layer is to handle and stores the data acquired from the network layer. It offers database and cloud services to IoT systems for the application layer to use. This layer additionally examines, manipulates, and stores data through the utilization of modern computing technologies. The middleware layer has the ability to automatically

process and compute acquired information by utilizing advanced technologies like cloud computing and big data analytics [15].

Application layer: The application layer is commonly known as the termination layer of IIoT. Its leverages the data obtained from the middleware layer to deliver good services to the final users. Additionally, it is integrated with industrial businesses to have access to intelligent applications. Users can utilize the intelligent services at this level using internet-enabled devices such as smartphones, tablets, computers, wearable devices, and various other smart gadgets. This layer incorporates the IoT network to create many intelligent applications, including smart factories, healthcare, agriculture, and smart cars[22],which have been explained in the following section.

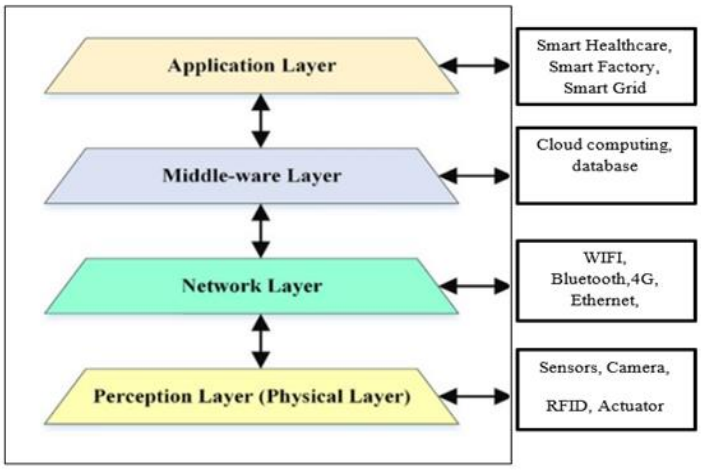

Fig. 5. IIoT General Architecture[20]

4.2. IIoT Applications

Industrial Internet of Things (IIoT) applications are the outcome of combining complicated physical machinery with interconnected sensors and software. The interconnected devices gather, exchange, and analyze data, transforming it into practical insights for industrial enterprises. This level of intelligence enables more educated decision-making, resulting in enhanced operational efficiencies, heightened safety, and increased production. The implementation of Industrial IoT applications is revolutionary, since it completely changes old industries and opens up new possibilities. They are utilized in various industrial sectors, including, agriculture, healthcare, transportation, smart Grid and smart factory [23]. In the following subsections some of IIoT applications have been explained with focusing on smart factory application in a separate section. Fig 6. illustrates the IIoT applications.

a. Smart Agriculture

Agriculture is the primary provider of food on a global scale. It has been crucial to the advancement of civilizations throughout history. According to the United Nations (UN), the global population is projected to grow by 2 billion people by 2050, reaching a total of 11 billion by the end of the century [6]. Hence, the worldwide need for food and water would persistently grow. Agriculture, which encompasses operations such as irrigation, watering, and cleaning of livestock and aquaculture, is the largest consumer of water globally. It accounts for around 70% of the world's yearly water usage. Hence, smart agriculture provides a means to achieve sustainability by utilizing technological advancements. it includes the utilization of information and communication technologies (ICTs) in the cyber-physical process of managing farms. This involves employing advanced technologies like the Internet of Things (IoT), cloud computing, robotics, and artificial intelligence (AI) to enhance the precision of operations. By providing each plant or animal with precisely tailored resources for optimal growth, smart farming optimizes overall performance while minimizing waste, inputs, and pollution[24]. Extensive studies have been conducted in this specific field, and a selection of these has been explained in the following paragraphs. The article [25] explored several facets of the technological advancements in the field of Internet of Things (IoT) in agriculture. It clarified the primary constituents of smart farming that are based on the Internet of Things (IoT) and a comprehensive analysis of network technologies employed in IoT-based agriculture has been published, encompassing network architecture and layers, network topologies utilized, and protocols. Furthermore, there has been a notable emphasis on security concerns in the realm of IoT agriculture. The authors in [26] provided an in-depth review of the latest technologies that are being developed for smart agriculture based on the internet of things (IoT). They offered a categorization of IoT applications for intelligent agriculture, encompassing seven distinct categories: smart monitoring, smart water management, agrochemical applications, disease control, smart harvesting, supply chain management, and smart agricultural practices.

b. Smart Healthcare

IoT technologies are currently utilized in healthcare to enhance patient care and outcomes, presenting novel prospects for remote monitoring, customized treatment strategies, and effective healthcare provision. The Internet of Things (IoT) has the potential to not only enhance patient care, but also significantly lower healthcare costs through the optimization of processes, automation of routine tasks, and reduction of costly interventions[27]. By facilitating real-time data gathering and monitoring, it improves response times and patient outcomes, ultimately enhancing patient care. Secondly, IoT solutions improve healthcare operations by automating administrative tasks, which not only saves time but also reduces the need for a huge administrative employee resulting reduced in cost, improved health results[8]. Many works have been done in healthcare to explain the benefits of IoT in this field where the authors in [28] presented A review of enabling technologies in healthcare applications, standardized protocols, security and market potential provides a complete overview of IoT-based healthcare technologies and their applications. They analyzed the improvements in IoT-based healthcare approaches, protocols, and networks, and highlights the necessity of security and privacy in IoT healthcare systems.

c. Smart Grids

The Internet of Things (IoT) has the capability to facilitate the implementation of many technologies in Smart Grid (SG) systems. The extensive sensing and processing capabilities of the Internet of Things (IoT) can enhance the abilities of Smart Grids (SG) in areas like as data processing, early warning systems, self-repair mechanisms, disaster recovery, and overall reliability. The integration of IoT and SG can significantly advance the progress of intelligent terminals, meters, and sensors, as well as information equipment and communication devices. The Internet of Things (IoT) can be utilized to achieve dependable data transmission in both wired and wireless communication infrastructures across several sectors in SG, including power generation, transmission lines, distribution, and consumption/utilization[29].

The concept of Smart Grids, which intelligently integrate new technologies to monitor and control electrical systems, is introduced in [30]. The authors discussed the main factors influencing the composition of a Smart Grid, including innovative equipment and services, communication, control, monitoring, and self-diagnosis technologies.

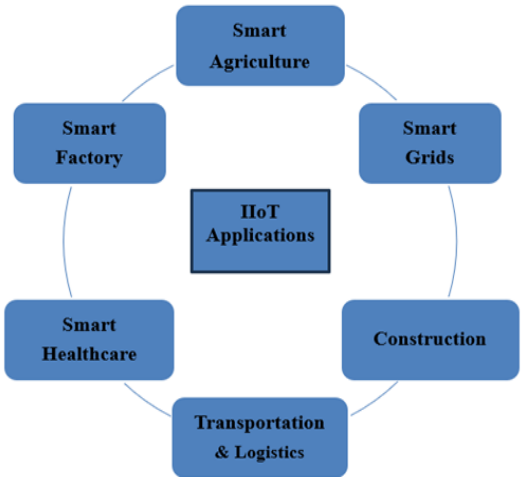

Fig. 6. IIoT Applications

5. Smart Factory

The smart factory is considered as one of the most important applications of the Industrial Internet of Things that were mentioned previously. In the following subsections, the smart factory will be defined in terms of its concept, applications and requirements, communication technologies, and Security Issues.

5.1. Concept of Smart Factory

A smart factory is a flexible and networked manufacturing systems that can learn and adjust to changing needs by using a constant flow of data from connected operations and production systems. As a result, everything in a smart factory will be connected, exchanging data, identifying and evaluating circumstances, and organically fusing the real and virtual worlds. To put it another way, a "smart factory" combines cyber and physical technologies in order to enhance the management, performance, quality, controllability, and transparency of production processes[31]. The architecture of the smart factory is similar to the architecture of the Industrial Internet of Things described previously and consists of four layers[32, 33] as shown in Fig .7.-:

Physical layer: consists of all production resources, such as tools, machinery, sensors, and actuators.

Network layer: Data transmission and sharing between levels need modern network technology and communication protocols for fast, reliable real-time communication.

Data layer: Also called cloud layer, this layer acts as the hub for information for the smart factory, enabling a range of Big Data applications such as data management, data storage and analysis, and data interchange through cloud computing technologies.

Terminal or Application layer: Through end-user devices (terminals), such as PCs, tablets, smartphones, and monitoring equipment, people are connected to the resources and assets of the smart factory as well as the information that is available.

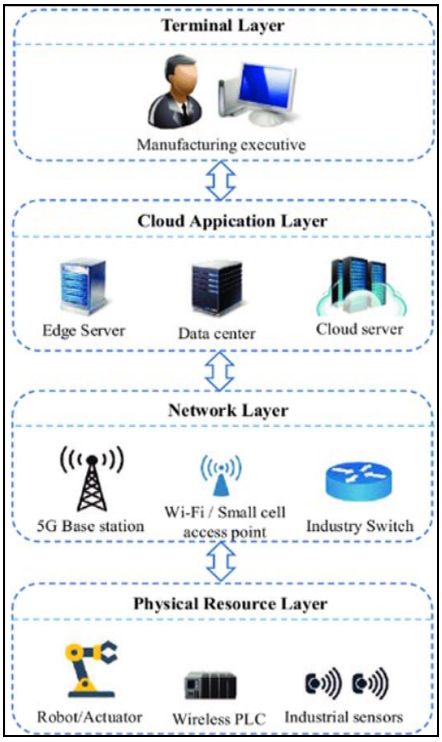

Fig. 7. Smart Factory Architecture[34]

5.2. Applications and Requirements of Smart Factory

Factories which integrating Internet of Things (IoT) and its technologies in their infrastructure can optimize the production processes, reduce delivery times and enable substantial reduction in operational costs, while improving production efficiency. There are numerous potential applications in smart factory to management, monitoring and automated processes, some of these applications have critical requirements for some metrices like latency, bandwidth, availability and so on. In the following subsections, high-level applications with their requirements are identified.

a. Automated Guided Vehicles

As a result of the increasing demand for goods and products, factories and warehouses are exposed to great pressure from customers to fulfill these requests, as traditional automation is no longer efficient to do that, therefore, more flexible, moveable assistance systems have been resorted to that are controlled through sensors, such as robots and forklifts, and they are self-driving and operating.

These machines make quick decisions to organize works and prevent collisions in the industrial environment, so they require a reliable communication network that meets the requirements of these systems in terms of latency, jitter and data rate[35].

b. Augmented Reality and Wearable Systems

Industrial wearable devices are considered as the means of human-machine interaction (HMI), they provide the essential means to include human workers into smart factories, where manufacturing, maintenance, and control remain dependent on human intervention. Wearable systems facilitate remote control, real-time monitoring through augmented reality, aggregation of sensor data, and implementation of safety systems. However, they also introduce the need for energy efficiency, compact size, and wireless networking. Only the network requirements pertaining to wearables and augmented reality are taken into account in this section[36].

c. Remote control of operations

This application refers to Remote controlling of equipment and machinery in a smart factory. Remote operation allows the smart industrial management to manage various operations from a distance. The real-time requirements for this application are considered to be high due to the involvement of moving machinery. These equipments are controlled remotely using the paradigm of the Industrial Internet of Things, and these machines are usually controlled a way from controlling device perhaps outside of plant floor [37].

d. Monitoring and Predictive Maintenace

Factory floors can utilize sensors to collect an enormous amount of real-time data, which can be used to enhance corporate automation, monitoring, and decision-making processes. In order to achieve this objective, it is necessary to send potentially extensive data streams that share a link with real-time control traffic. Use cases encompass the gathering of data through sensor networks and the use of predictive maintenance on sensor data from the Industrial Internet of Things (IIoT)[38]. The utilization of real-time data from IIoT sensors can facilitate strategic decision-making and facilitate the automation of specific applications[39].This application, although it relies to some extent real-time data streams, does not involve any tasks that have strict real-time requirements. Therefore, the criteria in this regard are minimal. Nevertheless, the large volume of data generated by the wide range of sensors typically results in higher bandwidth requirements.

e. Safety and Protection

An essential aspect in developing the Industrial Internet of Things is safeguarding critical industrial systems, safeguarding in this context refers to ensuring the physical safety of equipments and workers by reducing potential risks posed by environmental conditions. These conditions like gas leaks, fires, and high temperatures that can lead to work disruptions, institutional damage, and harm to individuals. It is crucial to promptly detect and alert about these risks, therefore it requires the highest level of predictability and low latency requirements while bandwidth requirements are low. However, reactive systems need to function independently to making distributed solutions[40]. Table .3 summarize the applications of smart factory and their requirements respect to some metrices[9,10,41].

Table 3. The Requirements of Smart factory Applications

Application	Requirements				
	Latency	Bandwidth	Availability	Mobility	Density
Automated Guided Vehicles	Medium (10-20ms)	Variable (<100Mbps)	99.9999%	Needed	Low
Augmented Reality	Medium (10ms)	High (<1Gbps)	99.99%	Needed	Depending on No. of Workers
Remote Control	High (0.1-1ms)	Low	99.9999%	Not Necessary	Medium
Monitoring and Predictive Maintenace	Low (20-100ms)	Variable	99.99%	Not relevant	High
Safety and Protection	Medium (10ms)	Low (<1Mbps)	99.9999%	Not Necessary	Medium

5.3. Communication Networks Technologies in Smart Factory

There is a wide variety of Communication technologies can be used in smart factory environment to achieve the requirements of smart factory applications which explained previously, regardless of whether they are open standards or exclusive to an industry, these technologies continuously evolve in terms of their features and capabilities which have the ability to function with both wired and wireless connections. In the following subsections, wired and wireless communication technologies have been explained.

a. Wired Communication Technologies

Although wireless communication technologies have made significant advancements and offer tremendous flexibility, wired communication technologies continue to be utilized in several industrial applications that demand high performance, such as remote control with a response time of less than 1 millisecond. Furthermore, several applications are stationary and unchangeable as a result of their high reliance on electrical power for operation. Consequently, wired communication methods are appropriate for that purpose. Fieldbus and industrial Ethernet are examples of wired communication technology. Additionally, Time Sensitive Network is a robust networking technology that enables the implementation of such applications[42].

Fieldbus technique has been utilized in automated manufacturing from the 1970s, having a significant historical background. Multiple standards were established due to the development of various products by different companies. The often-employed Fieldbus protocols comprise Modbus, Controller Area Network (CAN), Highway Addressable Remote Transducer (HART), INTERBUS, PROFIBUS, Foundation Fieldbus (FF), and Control & Communication Link

(CC-Link)., and others. In the era of the Industrial Internet, Fieldbus technology is being gradually replaced due to the inability of devices using different protocols to establish communication with one another[43].

As communication technologies developed, Ethernet emerged in 1985 based on IEEE 802.3 standard was produced to define the characteristics of this well recognized wired networking technology. This technology has evolved in recent years and has been introduced in several versions, including industrial versions that are progressively substituting Fieldbus as the preferred solution for equipment interconnection[44].

Industrial Ethernet protocols encompass EtherNet/IP, Modbus-TCP, Powerlink, EtherCAT, PROFINET, and others. Industrial Ethernet has several advantages over Fieldbus technology, including high transmission speeds, extended transmission distances, improved interoperability, configurable network topologies, and simple integration.[45].

Time-Sensitive Networks (TSN)/Ethernet refers to set of standards which developed by the Time-Sensitive Networking task subgroup as part of IEEE 802.1 working group. Time-sensitive network is a powerful Ethernet technology which serves as the primary communication tool in the industry 4.0 environment. Their main objective is to meet real-time demands in extensive process areas and facilitate real-time communication between control systems, operators, sensors, and actuators in industrial systems. Additionally, they support Industrial Ethernet standards and other protocols to enable real-time communication[46]. Fig .8 illustrates the wired communication Technologies.

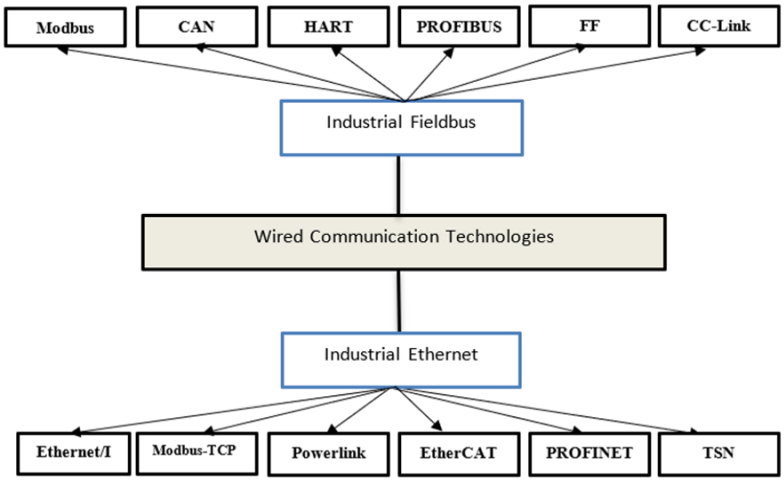

Fig.8. Wired Communication Technologies

b. Wireless Communication Technologies

Several wireless communications technologies have emerged in recent years, exhibiting differences in data transfer rates, operating frequencies, coverage range, and power consumption amounts[47].

To review these techniques, they can be classified into several categories according to the coverage area of each type, as shown below:

Wireless Wide Area Netwok (WWAN): This category is characterized by a wide range of coverage and includes cellular communications systems that founded by 3GPP. The famous generations of this standard are the fourth generation (4G) and the fifth generation (5G)[48], they can be used in industrial applications due to their high specifications. WiMAX is Another technology within this category which based on IEEE802.16. This technology works with a range of frequencies (2GHz-66GHz) and at various transfer rates. The drawback of these technologies is high power consumption, so Low Power – Wide Area Network (LP-WAN) technology was developed, it has a wide coverage range and low power consumption and offers promising solutions for low-power Internet of Things technology[49].

Wireless Local Area Network (WLAN): are used for wireless local networks to link two devices or more in limited area like office, home or production line, the most widely used is Wi-Fi technology based on the IEEE 802.11 standard with many versions and different frequency ranges (2GHz-60GHz) and data rates from 1 Mbps to 1Gbps[50].

Wireless Personal Area Network (WPAN): Another group is wireless personal area networks, which have a smaller coverage area compared to the others. The predominant technology used in this category is Bluetooth, which is based on the IEEE 802.15.1 standard. Bluetooth operates at a frequency of 2.4 GHz and may achieve data rates of up to 3 Mbps. There exists an alternative version that has a lower power consumption and a lower data rate[51].However, Bluetooth technology has a significantly higher energy consumption. Consequently, a low-power, low-cost alternative known as low-rate wireless personal area networks (LR-WPAN) has been presented and is widely employed in various industries. The popular LR-WPAN technologies are ZigBee, WirelesHART, and 6LoWPAN[52].

Radio Frequency Identification (RFID): Radio-frequency identification (RFID) is a technology that utilizes electromagnetic fields to automatically retrieve information from a tag. Near Field Communication (NFC) technology is a derivative of RFID technology[53]. Fig.9 illustrates the wireless communication Technologies.

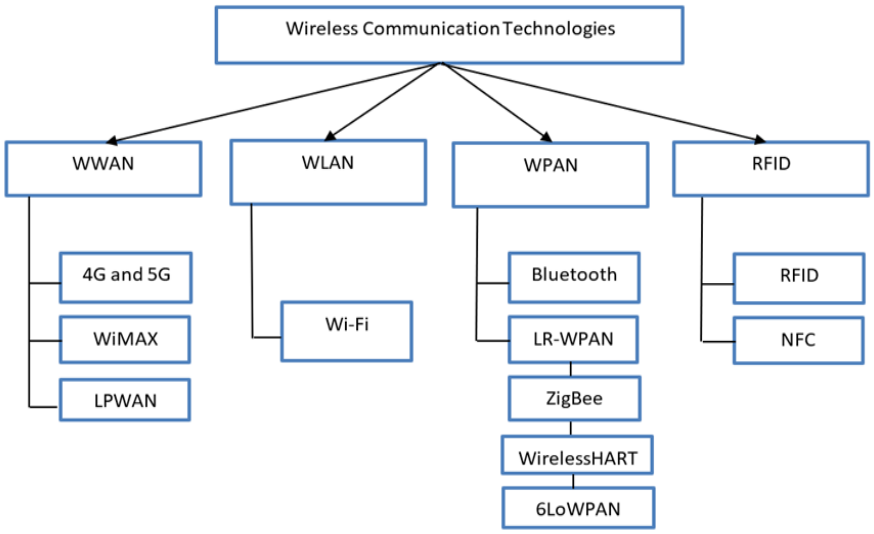

Fig.9. Wireless Communication Technologies

Table 4. Overview of Wireless Communication Technologies[12, 45]

Cat.	Tech.		Std.	Range	Data Rate	Power
WWAN	4 G		3GPP	10 km	100 Mbps	High
	5 G		3GPP	1 km	10 Gbps	High
	WiMAX		IEEE 802.16	<50 km	(50 – 100) Mbps	High
	LPWAN		Lora WAN R1.0	30 km	<200 kbps	Low
WLAN	Wi-Fi		IEEE 802.11	50 m	1 Gbps	High
WPAN	Bluetooth		IEEE 802.15.1	100 m	3mbps	Medium
	LR-WPAN	ZigBee	IEEE 802.15.4	10-20m	250kbps	Low
		WHART		10-20m	250kbps	Low
		6LoWPAN		10-20m	250kbps	Low
RFID	RFID		ISO 18,000-6C	1-5m	40-160kbps	Medium
	NFC			0.05m	400 kbps	Low

b. Related works of communications technologies in smart factory

Due to the spread of smart factories in previous years and the fact that communication networks constitute the backbone for achieving the requirements of smart factories therefore, some of related works have been reviewed in the following paragraphs.

The authors in [54,55] employed WPAN technologies in smart factory networking where Bluetooth wireless mesh networking have been made in [54] to provide effective connectivity to gather real-time data from the work floor and facilitate communication with sensor devices. The work in [55] proposed a real-time communication model for smart manufacturing lines utilizing OPC UA and IEEE 802.15.4e wireless communication infrastructure. They discuss the difficulties of delivering substantial data volumes in industrial wireless network environments and the necessity for real time connection. Although these techniques are preferred to using in smart factory environment for their easy installation and low power consumption. However, they have drawbacks such as low data rates that may not meet smart factory application requirements, limited workspace coverage, and cybersecurity concerns due to their accessibility to all users.

The paper [56] proposed a simulation model that is built using the OMNeT++ framework to integrates the preexisting TSN model NeSTing with a simpler 5G model. The research discussed the challenges and advantages of combining 5G with TSN within the field of industrial automation and examines the importance of reliable and low-latency communication in time-sensitive applications, Although The benefits of integrating 5G and TSN for smart factory networking which present high bandwidth and low latency ,there are many Drawbacks of combining 5G with TSN for smart factory networking include complexity, integration challenges, costs, and security considerations due to the increasing connectivity and data intensity of smart factories.

The authors in [57] offered insights into several protocols and technologies utilized for real-time communications in smart factories. They focused on time-sensitive networking (TSN), which guarantees precise synchronization among communication units. The work emphasized the significance of dependability in industrial communications and examines many leading technologies like PROFINET, EtherNet/IP, Sercos III, EtherCAT, and OPC UA.

The works in[58-61] explored Time Sensitive Networking (TSN) as communication framework for industrial systems. The work in [58] proposed TSN and OPC UA model to overcome the constraints of some industrial communication systems and fulfill the needs of Industry 4.0. The authors proposed TSN as the communication infrastructure to link diverse industrial automation subsystems, offering real-time functionalities and OPC UA to facilitates both horizontal and vertical communication between subsystems in the field layer and upper levels.

The authors in [59] explored the use of Time-Sensitive Networking (TSN) in industrial automation to enable real-time communication with minimal latencies and compatibility among devices from various manufacturers. The authors examined two TSN techniques, Time-Aware Shaper (TAS) and frame preemption (FP), and contrasted them with strict priority scheduling (ST) regarding latency guarantee, jitter, and their effect on non-critical traffic, the evaluation is carried out utilizing the simulation framework OMNeT++ and the NeSTiNg library.

The work in [60] highlighted the significance of communication networks and protocols in guaranteeing measurement accuracy, reliability, and safety in smart factory. it analyzed the constraints of current technologies like Ethernet and Wi-Fi in handling time-sensitive and crucial data which led The IEEE 802.1 Working Group to create the TSN standards to transform Ethernet in order to accommodate time-sensitive, mission-critical, and safety-critical data, therefore the work examined the TSN standardization activity, including its importance for industrial systems.

The authors in [61] offered an in-depth analysis of the performance of Time Sensitive Networking (TSN) in industrial automation applications. It highlighted the strict demands of industrial networks, including timing, latency, jitter, and loss, and shows how TSN may fulfill these criteria. Various network topologies, including as priority queuing, time-aware shaping, and credit-based shaping, are simulated and assessed to gauge their efficacy in satisfying the delay requirements of various traffic classes. The performance assessment is carried out via OMNET++. Simulation framework which explained that a TSN-based network may effectively fulfill all application needs by guaranteeing fast and reliable transmission of data in industrial automation environments.

The article [62] outlined a practical approach for integrating the Industrial Internet of Things (IIoT) through the utilization of 5G technology. The authors highlighted the capabilities of 5G in terms of enhanced performance, flexibility, and security, making it well-suited for facilitating IIoT applications in industrial environments. The work described a system comprising various infrastructure and application components, an IoT end device utilizing 5G technology is employed to gather sensing data from assets on the shop floor and send it through an industrial 5G network. An intelligent assistant on the application side uses this data to produce helpful insights for sustainable asset operation.

Table 5. Summarize of Related Works for Communication Technologies

Ref.	Year	Main Contribution	Method	Tools
[55]	2019	Implementation of a Bluetooth Mesh Networking for smart factory	Practical Implementation	Raspberry Pi with RF52840 as gateway
[55]	2021	Integrating Wireless Network (IEEE 802.15.4) with OPC UA protocol in Smart Factory	Simulation Model	OMNET++ Simulation Framework
[56]	2020	Integrating 5G with Time-Sensitive Networking (TSN) in smart factory	Simulation Model	OMNET++ Simulation Framework
[57]	2021	Overview of various communication technologies used in real-time Factory-Floor communications	Review	----------
[58]	2020	Proposed two-tier Communication Architecture using TSN and OPC UA	Practical Implementation	Robot controller, Two Cisco Industrial Ethernet (IE 4K) TSN switches and others
[59]	2021	Evolution of TSN Mechanisms in Industrial Communications	Simulation Model	OMNET++ Simulation Framework
[60]	2022	Providing a comprehensive overview of Time Sensitive Networking (TSN) and its relevance in Smart Factory	Review	----------
[61]	2022	Analysis of the performance of Time Sensitive Networking (TSN) in Smart Factory	Simulation Model	OMNET++ Simulation Framework
[62]	2023	Utilization of 5G technology for IIoT applications	Practical Implementation	5G end devices and IoT Tools
[63]	2023	Analysis of Ethernet/IP as a means to enhance industrial communication.	Practical and software Implementation	PLC simulator PLC hardware C++ platform

The authors in [63] focused on the deployment and efficiency of Ethernet/IP (EIP) in industrial networks. they aimed to confirm the accuracy of data transfer among a control box, a Programmable Logic Controller (PLC), and a robot within an industrial environment, they employed a distinctive method by using both a virtual PLC simulator and a physical PLC hardware. A novel industrial communication module was created using C++ for the Linux Debian platform to illustrate the wide range of EIP in enabling effective data transport in an industrial setting. Table. 5 summarize the previously related works.

6. Security Issues in Smart Factory based IIoT Architecture

6.1 Definition of Cyber Security

In the old traditional factories, their parts and units are secured through the physical isolation of plant parts, components and sites, as well as through development of strong and strict rights access management to prevent malfunctions leading to production interruptions and damage[64].

Today, the Factories are smart and comprised of a heterogeneous communication structure where elements of the Factory communication systems are realized through the use of new technologies, ranging from wireless Internet of Things connectivity to wired industrial protocols like Ethernet to transfer the related information of machines and the environments. Also, any system can communicate with other production structures and processes Via the Internet, a worldwide communication network. As a result for that, these systems are vulnerable to cyber security threats, which must be taken into account when designing communication networks to connect smart factory systems[65], therefore, Cybersecurity can be defined as a modern technical tool that works to protect operational systems and cybernets from any technical attack that is intended to be aimed at, Access to sensitive information and data, change, and destroy or spy them[66].

There are three important objectives for Cybersecurity to achieve information protection of an enterprise, these objectives are called CIA triad (Fig .10.): Confidentiality, Integrity and Authentication[67-69].

Confidentiality: is protecting information to prevent unauthorized access to get this information, this is done by data encryption methods.

Integrity: Ensures that information remains unchanged, complete, and accurate without unauthorized modifications.

Availability: Ensures data can easily accessed as required. Data availability is essential for the everyday functioning of any business, organization, or entity. It guarantees that authorized individuals have unrestricted access to data as needed.

Fig. 10. CIA Triad

6.2 Expected Attacks and Countermeasures for IIoT layers

To illustrate an expected attack, they have been classified according to each layer of IIoT which they belong, as well as the specify the most important countermeasures against these attacks. Fig. 11 shows type and effect of attacks on each layer[70]**.**

Perception Layer Attacks: Attacks on this layer target the physical components of the Internet of Things and physical devices with the objective of causing physical harm to the system. The impact of attacks on this layer leads to disruption of production processes and causes safety risks due to incorrect information being given by IIoT sensors, leading to wrong decisions that affect the entire system. Solutions to these attacks include encryption, Authentication, and Access control[71].

Network Layer Attacks: The network layer is vulnerable to attacks that can harm network devices. This layer manages the transfer of data and connections to other smart devices, network equipment, and servers. It consists of Internet gateways, switches, and routing devices that utilize modern technologies like WIFI, LTE, Bluetooth, 3G, Zigbee, etc. Attacks on this layer result in data leakage and modify it, violation of privacy, and network congestion due to excessive data, eventually leading to system failure and disrupting information transition process[72]. Some of solutions at this layer are encryption, integrity verification mechanisms and Intrusion detection system to monitor the network traffic to note any abnormal situation[73].

Processing Layer Attacks: This layer serves as an intermediary between the network layer and the application layer, providing large storage space for data received from the prediction layer. An intelligent cloud computing occurred in this layer, making it a target for attacks such as data manipulation during processing to introduce false information leading to wrong analysis and injecting malicious data into databases to disrupt processes. Some solutions for these attacks are: blockchain, encryption and access control[74].

Application Layer Attacks: The application layer offers services based on user requests. The lowest layers' processed information is used to create beneficial services for end users, these information serves as a foundation for several applications that might help the user in areas such as healthcare, education, transportation, manufacturing and logistic. Phishing attacks are an attack that targets this layer by imitating an official ID to gain critical information through infected websites or emails. Viruses, worms, Trojan horses, and spyware are forms of cyber-attacks targeting this layer. The countermeasures at this layer include: protection software (Anti-Virus, Anti Spyware, etc.), Firewall, Access control and user authentication[75]. Table 6 summarizes IIoT layer attacks, their effects and countermeasures.

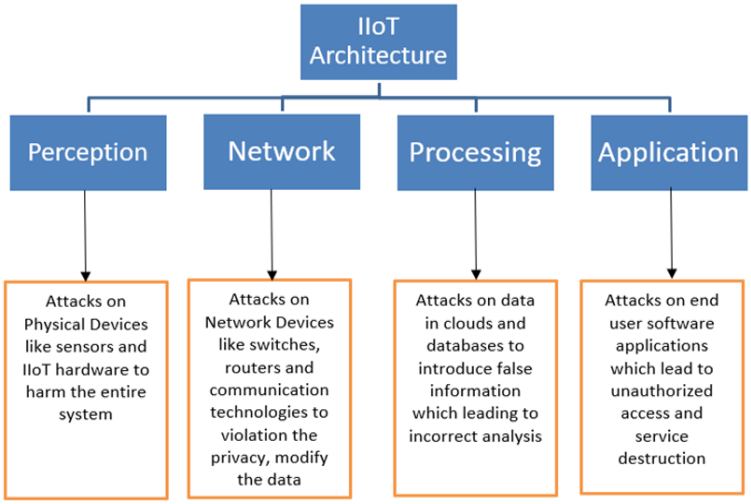

Fig. 11. IIoT Architecture Attacks

Table 6. IIoT layers Attacks, Effects and Countermeasures

IIoT layer	Possible Attacks	Effects	Countermeasures
Application Layer	Phishing, Virus, Worms, Spyware, Unauthorized access, Trojan Horses	Data leakage, infected data, Privacy Violation, Service Disruptions	Protection software, Firewall, Access Control, User Authentication
Processing Layer	Data Breach, Flooding attack in cloud, Exhaustion, Malware	Data leakage in cloud, Service Hijacking, Privacy Violation	Fragment data and store in different servers, Encryption, authentication
Network Layer	Man in the Middle, DoS/DDoS, Traffic Analysis, Sybil attack, Routing information attack, Replay attack	Data Manipulation and Modification, Network Congestion, Message destruction, Routing loops,	Encryption, Integrity Mechanisms, Intrusion Detection System, authentication
Perception Layer	Permanent DoS, Sleep Denial, RF jamming, Physical Tampering, Malicious Code Injection	Resource Destruction, Node Shutdown, Safety Risks	Encryption, Authentication, Access Control, Physical secure design

6.3 Related Works of Cybersecurity issues in smart factory

Many works have been presented related with security concern in Industrial environments, some of them have been explained in the following review:

The authors in [76] conducted a realistic case study on a real modular smart manufacturing system to showcase different attack scenarios and suggest security measures. The testbed system has seven assembly stations, programmable logic controllers, human-computer interfaces, and an industrial robotic arm.

The work highlighted the importance of network segmentation and system compartmentalization in preventing attackers from gaining whole control of the production unit.

The authors in [77] analyzed the security of TSN automotive Ethernet using the Microsoft STRIDE threat model. The potential security measures for Time-Sensitive Networking (TSN) are outlined, including the security protocol included into TSN. The work investigated the per-stream filtering and policing (PSFP) technique described in IEEE 802.1Qci and proposed an anomaly detection system that utilizes PSFP. The anomaly detection system aimed to ensure

real-time performance of TSN by identifying individuals displaying abnormal behavior and preventing denial of service (DoS) attacks.

The work [78] tried to guarantee authorized individuals secure access to sensing equipment and real-time data. The suggested approach utilized fuzzy extraction technology for biometric verification and integrates three factors for user authentication: smart card, password, and personal biometrics. Moreover, the system has been proven to resist certain well-known attacks based on an informal security analysis.

The authors in [79] provided a collaborative DDoS defense technique for IIoT in their article. Edge Defense is a security mechanism specifically created for single point DDoS defense in the IIoT context. It is designed to detect, identify, classify, and mitigate DDoS attacks. A collaborative model is created for multi-point DDoS defense to distribute defense information around the network using blockchain technology.

The work [80] addressed the vulnerability of IoT devices in the Smart Factory like DDoS, ARP and IP fragmentation attacks and the necessity for strong security measures to protect vital infrastructures. They described RFPCA model, batch processing model and timestamp methods to detecting and mitigating DDoS, ARP and IP fragmentation attacks respectively. Table 7 summarizes the previous related works.

Table 7. Summarize of Cybersecurity related works

Ref.	Year	Main Contribution	Targeted Layer	Solution /Countermeasures
[76]	2021	A realistic case study on a real modular smart manufacturing system has been made to showcase different attack scenarios and suggest security measures	Perception layer to get initial access	Network segmentation to prevent the attacker from whole access control
[77]	2021	Analyzed the security of TSN Ethernet and proposed an anomaly detection system to ensure real-time performance of TSN	Network layer /DDoS attacks	Intrusion Detection System
[78]	2022	The suggested approach utilized encryption and fuzzy extraction technology for biometric verification and integrates three factors for user authentication: smart card, password, and personal biometrics	Network and Processing layers to get access to user data	Encryption, Authentication Mechanisms, Information analysis
[79]	2022	A collaborative model is created for multi-point DDoS defense to distribute defense information around the network using blockchain technology	Network layer /DDoS attacks	Anomaly detection system, flow analysis
[80]	2023	Addressed the vulnerability of IoT devices in the Smart Factory like DDoS, ARP and IP fragmentation attacks and the necessity for strong security measures to protect vital infrastructures	Network Layer/DDoS, ARP and IP frag. attacks	Intrusion Detection System and filtering

7. Conclusion

Smart factory is one of most important applications of IIoT which have various aspects such as its applications, communication networks, and cybersecurity issues. This work highlights the importance of efficient communication technologies to support smart factory applications such as functional safety, monitoring, and remote control. Various communication technologies, including both wired and wireless types, can fulfill the needs of smart factory applications which have requirements related to latency and data rate and usually there is no single communication technology that meets these requirements, therefore, there is a need for integration between these networks, which leads to cybersecurity threats and complexity in the system. Wired networks are suitable for time-sensitive applications, offer enhanced cybersecurity, and are well-suited for loud industrial environments. However, they may lack flexibility for growth and might be challenging to connect certain machines and devices. Time sensitive Networking based ethernet is one of the most efficient wiring techniques which can meet the system requirements related to some metrices like data rate and latency. In the other hand, Wireless technologies offer greater flexibility for growth and access throughout the factory, but they encounter challenges such as cybersecurity risks, signals interference, and industrial noise effects, resulting in reduced network efficiency.

The fifth-generation (5G) network is a suitable wireless technology for smart factory applications however, it may be costly and not suitable for medium or small-sized companies. Another candidate technology is Wi-Fi technology especially in latest versions to meet the applications requirements. A hybrid network could be an appropriate approach to fulfill the system requirements. Anyway, the cybersecurity concerns must be taken into account as a challenge which can denied the service therefore, expected attacks and countermeasures for smart factory based IIoT have been explored in this work.

Acknowledgment

The authors express their gratitude to the University of Mosul, College of Engineering, Department of Electrical, for providing the necessary facilities that contributed to enhancing the quality of this paper.

References

[1] A. Karmakar, N. Dey, T. Baral, M. Chowdhury, and M. Rehan, "Industrial Internet of Things: A Review," presented at the 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), 2019.

[2] N. S. Himanshu, Dr. Rajinder Singh, "Evolution of IoT to IIoT: Applications & Challenges," presented at the International Conference on Innovative Computing and Communication (ICICC 2020).

[3] M. Alabadi, A. Habbal, and X. Wei, "Industrial Internet of Things: Requirements, Architecture, Challenges, and Future Research Directions," IEEE Access, vol. 10, pp. 66374-66400, 2022, doi: 10.1109/access.2022.3185049.

[4] 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, doi: 10.1109/tii.2018.2852491.

[5] V. R. Kebande, "Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0," Forensic Science International: Reports, vol. 5, 2022, doi: 10.1016/j.fsir.2022.100257.

[6] S. Grabowska, "Smart Factories in the Age of Industry 4.0," Management Systems in Production Engineering, vol. 28, no. 2, pp. 90-96, 2020, doi: 10.2478/mspe-2020-0014.

[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," Computers & Electrical Engineering, vol. 81, 2020, doi: 10.1016/j.compeleceng.2019.106522.

[8] S. Munirathinam, "Industry 4.0: Industrial Internet of Things (IIOT)," in The Digital Twin Paradigm for Smarter Systems and Environments: The Industry Use Cases, (Advances in Computers, 2020, pp. 129-164.

[9] M. Soori, B. Arezoo, and R. Dastres, "Internet of things for smart factories in industry 4.0, a review," Internet of Things and Cyber-Physical Systems, vol. 3, pp. 192-204, 2023, doi: 10.1016/j.iotcps.2023.04.006.

[10] M. S. Farooq et al., "A Survey on the Role of Industrial IoT in Manufacturing for Implementation of Smart Industry," Sensors (Basel), vol. 23, no. 21, Nov 3 2023, doi: 10.3390/s23218958.

[11] I. Behnke and H. Austad, "Real-Time Performance of Industrial IoT Communication Technologies: A Review," IEEE Internet of Things Journal, pp. 1-1, 2023, doi: 10.1109/jiot.2023.3332507.

[12] A. R. M. Noor et al., "Wireless Communications for Smart Manufacturing and Industrial IoT: Existing Technologies, 5G and Beyond," Sensors (Basel), vol. 23, no. 1, Dec 21 2022, doi: 10.3390/s23010073.

[13] H. A. Rabeh Morrar, and Saeed Mousa, "The Fourth Industrial Revolution (Industry 4.0): A Social Innovation Perspective," 2017.

[14] A. Rojko, "Industry 4.0 Concept: Background and Overview," International Journal of Interactive Mobile Technologies (iJIM), vol. 11, no. 5, 2017, doi: 10.3991/ijim.v11i5.7072.

[15] S. K. Arun Kumar, "Industry 4.0: Overview, Components, and Initiatives of Indian Government," International Journal of Research in Business Studies, vol. 6 (2),, 2021.

[16] E. Asadollahi-Yazdi, P. Couzon, N. Q. Nguyen, Y. Ouazene, and F. Yalaoui, "Industry 4.0: Revolution or Evolution?," American Journal of Operations Research, vol. 10, no. 06, pp. 241-268, 2020, doi: 10.4236/ajor.2020.106014.

[17] S. G. Ercan Oztemel, "Literature review of Industry 4.0 and related technologies," J. Intell. Manuf., vol. vol. 31, no. 1, pp. 127-182, Jan. 2020.

[18] E. B. Barbara Bigliardia, Giorgia Casellaa, "Enabling technologies, application areas and impact of industry 4.0: a bibliographic analysis," presented at the International Conference on Industry 4.0 and Smart Manufacturing (ISM 2019), 2020.

[19] K. P. T. H D Nguyen, X Zeng, L. Koehl, P. Castagliola, Pascal Bruniaux, "Industrial Internet of Things, Big Data, and Artificial Intelligence in the Smart Factory: a survey and perspective," presented at the ISSAT International Conference on Data Science in Business, Finance and Industry, Vietnam, 2019.

[20] A. A. Zeeshan Hussain, Javed Iqbal,Iram Bibiand Abdullah Gani, "Secure IIoT-Enabled Industry 4.0," Sustainability, 2021, 13, 12384., doi: https://doi.org/10.3390/su132212384.

[21] Z. I. Shahid Latif, Zil e Huma,Jawad Ahmad, "Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions," Transactions on Emerging Telecommunications Technologies, November 2021, doi: DOI: 10.1002/ett.4337.

[22] I. Ungurean and N. C. Gaitan, "A Software Architecture for the Industrial Internet of Things-A Conceptual Model," Sensors (Basel), vol. 20, no. 19, Sep 30 2020, doi: 10.3390/s20195603.

[23] S. Zaigham Mahmood, Shijiazhuang, "The Internet of Things in the Industrial Sector" (Computer Communications and Networks). Springer Nature Switzerland AG, 2019.

[24] M. A. F. Othmane Friha, Lei Shu, Leandros Maglaras, and Xiaochan Wang, "Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies," IEEE/CAA J. Autom. Sinica, vol. vol. 8, no. 4,, pp. pp. 718-752, Apr. 2021.

[25] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming," IEEE Access, vol. 7, pp. 156237-156271, 2019, doi: 10.1109/access.2019.2949703.

[26] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, and X. Wang, "Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies," IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 4, pp. 718-752, 2021, doi: 10.1109/jas.2021.1003925.

[27] M. S. Hossain and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring," Computer Networks, vol. 101, pp. 192-202, 2016, doi: 10.1016/j.comnet.2016.01.009.

[28] R. Chataut, A. Phoummalayvane, and R. Akl, "A review of IoT applications in healthcare," Sensors (Basel), vol. 23, no. 16, Aug 16 2023, doi: 10.3390/s23167194.

[29] A. Ghasempour, "Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges," Inventions, vol. 4, no. 1, 2019, doi: 10.3390/inventions4010022.

[30] J. J. Moreno Escobar, O. Morales Matamoros, R. Tejeida Padilla, I. Lina Reyes, and H. Quintana Espinosa, "A Comprehensive Review on Smart Grids: Challenges and Opportunities," Sensors (Basel), vol. 21, no. 21, Oct 21 2021, doi: 10.3390/s21216978.
[31] 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 (Basel), vol. 20, no. 23, Nov 27 2020, doi: 10.3390/s20236783.
[32] J. W. Baotong Chen, Lei Shu, Peng Li, Mithun Mukherjee and Boxing Yin, "Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges," doi: 10.1109.
[33] M. Ryalat, H. ElMoaqet, and M. AlFaouri, "Design of a Smart Factory Based on Cyber-Physical Systems and Internet of Things towards Industry 4.0", Applied Sciences, vol. 13, no. 4, 2023, doi: 10.3390/app13042156.
[34] H. Zemrane, A. N. Abbou, Y. Baddi, and A. Hasbi, "Internet of Things Smart Factories Ecosystem based on SDN," Procedia Computer Science, vol. 175, pp. 723-729, 2020, doi: 10.1016/j.procs.2020.07.107.
[35] L. Lo Bello and W. Steiner, "A Perspective on IEEE Time-Sensitive Networking for Industrial Communication and Automation Systems," Proceedings of the IEEE, vol. 107, no. 6, pp. 1094-1120, 2019, doi: 10.1109/jproc.2019.2905334.
[36] A. Gallala, B. Hichri, and P. Plapper, "Survey: The Evolution of the Usage of Augmented Reality in Industry 4.0," IOP Conference Series: Materials Science and Engineering, vol. 521, no. 1, 2019, doi: 10.1088/1757-899x/521/1/012017.
[37] A. G. Frank, L. S. Dalenogare, and N. F. Ayala, "Industry 4.0 technologies: Implementation patterns in manufacturing companies," International Journal of Production Economics, vol. 210, pp. 15-26, 2019, doi: 10.1016/j.ijpe.2019.01.004.
[38] S. M. Lee, D. Lee, and Y. S. Kim, "The quality management ecosystem for predictive maintenance in the Industry 4.0 era," International Journal of Quality Innovation, vol. 5, no. 1, 2019, doi: 10.1186/s40887-019-0029-5.
[39] S. Muruganandam, A. A. Salameh, M. A. A. Pozin, S. V. Manikanthan, and T. Padmapriya, "Sensors and machine learning and AI operation-constrained process control method for sensor-aided industrial internet of things and smart factories," Measurement: Sensors, vol. 25, 2023, doi: 10.1016/j.measen.2023.100668.
[40] M. G. Tommi Kivel ̈a, and Kai Furmans, "Towards an approach for assuring machinery safety in the IIoT-age," Logistics Journal: Proceedings, 2018, doi: 10.2195/lj_Proc_kivelae_en_201811_01.
[41] J. H. David Lou , Dhruvin Patel , Ulrich Graf and Matthew Gillmore (Itron). "The Industrial Internet of Things Networking Framework," Industry IoT Consortium. https://www.iiconsortium.org/iicf, 03-08-2022.
[42] S. Wang, J. Ouyang, D. Li, and C. Liu, "An Integrated Industrial Ethernet Solution for the Implementation of Smart Factory," IEEE Access, vol. 5, pp. 25455-25462, 2017, doi: 10.1109/access.2017.2770180.
[43] J. P. Thomesse, "Fieldbus Technology in Industrial Automation," Proceedings of the IEEE, vol. 93, no. 6, pp. 1073-1101, 2005, doi: 10.1109/jproc.2005.849724.
[44] D. Morato, C. Perez-Gomara, E. Magana, and M. Izal, "Network Simulation in a TCP-Enabled Industrial Internet of Things Environment-Reproducibility Issues for Performance Evaluation," IEEE Transactions on Industrial Informatics, vol. 18, no. 2, pp. 807-815, 2022, doi: 10.1109/tii.2021.3084128.
[45] Y. Y. a. P. J. Qingzong Li, "Remote Monitoring and Maintenance for Equipment and Production Lines on Industrial Internet: A Literature Review," Machines 2023, 2023, doi: https://doi.org/10.3390/ machines11010012.
[46] H. Trifonov and D. Heffernan, "OPC UA TSN: a next-generation network for Industry 4.0 and IIoT," International Journal of Pervasive Computing and Communications, vol. 19, no. 3, pp. 386-411, 2021, doi: 10.1108/ijpcc-07-2021-0160.
[47] A. Seferagic, J. Famaey, E. De Poorter, and J. Hoebeke, "Survey on Wireless Technology Trade-Offs for the Industrial Internet of Things," Sensors (Basel), vol. 20, no. 2, Jan 15 2020, doi: 10.3390/s20020488.
[48] Z. Diao, F. Sun, and W.-T. Pan, "Application of Internet of Things in Smart Factories under the Background of Industry 4.0 and 5G Communication Technology," Mathematical Problems in Engineering, vol. 2022, pp. 1-8, 2022, doi: 10.1155/2022/4417620.
[49] D. Magrin, M. Capuzzo, A. Zanella, L. Vangelista, and M. Zorzi, "Performance Analysis of LoRaWAN in Industrial Scenarios," IEEE Transactions on Industrial Informatics, vol. 17, no. 9, pp. 6241-6250, 2021, doi: 10.1109/tii.2020.3044942.
[50] P. Dhawankar, H. Le-Minh, and N. Aslam, "Throughput and Range Performance Investigation for IEEE 802.11a, 802.11n and 802.11ac Technologies in an On-Campus Heterogeneous Network Environment," presented at the 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2018.
[51] L. Leonardi, G. Patti, and L. Lo Bello, "Multi-Hop Real-Time Communications Over Bluetooth Low Energy Industrial Wireless Mesh Networks," IEEE Access, vol. 6, pp. 26505-26519, 2018, doi: 10.1109/access.2018.2834479.
[52] F. Chen, N. Wang, R. German, and F. Dressler, "Simulation study of IEEE 802.15.4 LR - WPAN for industrial applications," Wireless Communications and Mobile Computing, vol. 10, no. 5, pp. 609-621, 2009, doi: 10.1002/wcm.736.
[53] R. Ramanathan and J. Imtiaz, "NFC in industrial applications for monitoring plant information," presented at the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2013.
[54] T. C. Yang Lam, S. S. Ling Yew, and S. L. Keoh, "Bluetooth Mesh Networking: An Enabler of Smart Factory Connectivity and Management," presented at the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2019.
[55] A. Chai, Y. Ma, Z. Yin, and M. Li, "Real-Time Communication Model Based on OPC UA Wireless Network for Intelligent Production Line," IEEE Access, vol. 9, pp. 102312-102326, 2021, doi: 10.1109/access.2021.3097399.
[56] L. Martenvormfelde, A. Neumann, L. Wisniewski, and J. Jasperneite, "A Simulation Model for Integrating 5G into Time Sensitive Networking as a Transparent Bridge," presented at the 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2020.
[57] A. B. D. K. Arnold B D Kinabo, Albert A Lysko, "An Overview of Time-Sensitive Communications for the Factory Floor," presented at the 2021 IST-Africa Conference (IST-Africa), South Africa, South Africa, 2021.
[58] Y. Li, J. Jiang, C. Lee, and S. H. Hong, "Practical Implementation of an OPC UA TSN Communication Architecture for a Manufacturing System," IEEE Access, vol. 8, pp. 200100-200111, 2020, doi: 10.1109/access.2020.3035548.
[59] A. Arestova, K.-S. Jens Hielscher, and R. German, "Simulative Evaluation of the TSN Mechanisms Time-Aware Shaper and Frame Preemption and Their Suitability for Industrial Use Cases," presented at the 2021 IFIP Networking Conference (IFIP Networking), 2021.

[60] T. Fedullo, A. Morato, F. Tramarin, L. Rovati, and S. Vitturi, "A Comprehensive Review on Time Sensitive Networks with a Special Focus on Its Applicability to Industrial Smart and Distributed Measurement Systems," Sensors (Basel), vol. 22, no. 4, Feb 19 2022, doi: 10.3390/s22041638.
[61] M. Seliem, A. Zahran, and D. Pesch, "TSN-based Industrial Network Performance Analysis," presented at the 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), 2022.
[62] J. Meira et al., "Industrial Internet of Things over 5G: A Practical Implementation," Sensors (Basel), vol. 23, no. 11, May 30 2023, doi: 10.3390/s23115199.
[63] J. Seong, R. Ranjan, J. Kye, S. Lee, and S. Lee, "Enhancing Industrial Communication with Ethernet/Internet Protocol: A Study and Analysis of Real-Time Cooperative Robot Communication and Automation via Transmission Control Protocol/Internet Protocol," Sensors (Basel), vol. 23, no. 20, Oct 19 2023, doi: 10.3390/s23208580.
[64] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing Smart Factory of Industrie 4.0: An Outlook," International Journal of Distributed Sensor Networks, vol. 12, no. 1, 2016, doi: 10.1155/2016/3159805.
[65] O. Gilles, D. Gracia Pérez, P. A. Brameret, and V. Lacroix, "Securing IIoT communications using OPC UA PubSub and Trusted Platform Modules," Journal of Systems Architecture, vol. 134, 2023, doi: 10.1016/j.sysarc.2022.102797.
[66] T. Gebremichael et al., "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges," IEEE Access, vol. 8, pp. 152351-152366, 2020, doi: 10.1109/access.2020.3016937.
[67] B. Alotaibi, "A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities," Sensors (Basel), vol. 23, no. 17, Aug 28 2023, doi: 10.3390/s23177470.
[68] D. C. Spyridon Samonas, "THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY," Journal of Information System Security, vol. Volume 10, no., Issue 3, 2014.
[69] K. Y. Chai and M. F. Zolkipli, "Review on Confidentiality, Integrity and Availability in Information Security," Journal of ICT In Education, vol. 8, no. 2, pp. 34-42, 2021, doi: 10.37134/jictie.vol8.2.4.2021.
[70] G. Tsochev, "Some Security Problems and Aspects of the Industrial Internet of Things," in Proceedings of the 2020 IEEE International Conference on Information Technologies (InfoTech-2020), St. St. Constantine and Elena, Bulgaria, 17-18 September 2020, doi: 10.1109/InfoTech49733.2020.9211078.
[71] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures," IoT, vol. 2, no. 1, pp. 163-186, 2021, doi: 10.3390/iot2010009.
[72] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures," presented at the 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2018.
[73] a. Z. J. Shantanu Pal, "Analysis of Security Issues and Countermeasures for the Industrial Internet of Things," applied sciences, 2021, 11, 9393. , doi: https://doi.org/10.3390/ app11209393.
[74] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions," Electronics, vol. 11, no. 20, 2022, doi: 10.3390/electronics11203330.
[75] G. Nebbione and M. C. Calzarossa, "Security of IoT Application Layer Protocols: Challenges and Findings," Future Internet, vol. 12, no. 3, 2020, doi: 10.3390/fi12030055.
[76] F. Maggi et al., "Smart Factory Security: A Case Study on a Modular Smart Manufacturing System," Procedia Computer Science, vol. 180, pp. 666-675, 2021, doi: 10.1016/j.procs.2021.01.289.
[77] F. Luo, B. Wang, Z. Fang, Z. Yang, Y. Jiang, and K. Demertzis, "Security Analysis of the TSN Backbone Architecture and Anomaly Detection System Design Based on IEEE 802.1Qci," Security and Communication Networks, vol. 2021, pp. 1-17, 2021, doi: 10.1155/2021/6902138.
[78] L. L. a. J. Z. Huanhuan Hu, "Secure Authentication and Key Agreement Protocol for Cloud-Assisted Industrial Internet of Things," Electronics, 2022, 11, 1652., doi: https://doi.org/10.3390/ electronics11101652.
[79] H. Huang, P. Ye, M. Hu, and J. Wu, "A multi-point collaborative DDoS defense mechanism for IIoT environment," Digital Communications and Networks, vol. 9, no. 2, pp. 590-601, 2023, doi: 10.1016/j.dcan.2022.04.008.
[80] H. G. G. Tze Uei Chai , Soung-Yue Liew 1 and Vasaki Ponnusamy "Protection Schemes for DDoS, ARP Spoofing, and IP Fragmentation Attacks in Smart Factory," Systems, 2023, 11, 211, doi: https://doi.org/10.3390/ systems11040211.

Authors' Profiles

Yazen S. Sheet completed the B.S. in electrical engineering/electronics and communication from the University of Mosul, Iraq, in 2005 and received an M.Sc. degree in computer networks in 2011 from Mosul University. He interested in the field of computer networks and communication and he had published many papers in this field. He has been working as a communications and computer network lecturer at the University of Mosul Since 2011. He is a member of the computer networks lab in the Electrical Dept. / Engineering College.

Mohammed Younis Thanoun completed the B.S. in electrical engineering/ electronic and communication from the University of Mosul, Iraq, in 1991 and received the M.Sc. degree in electronic and communication in 2000 and Ph.D. in 2011 from Mosul University. He is interested in the field of computer networks and communication and he has published research papers in Deep Learning, SDN, machine learning algorithms and cybersecurity engineering He has been working as an assistant professor at the University of Mosul since 2021. He is a member of the computer networks lab in the Electrical Dept. / Engineering College.

Firas S. Alsharbaty completed the B.S. in electrical engineering/ electronic and communication from the University of Mosul, Iraq, in 2007 and received the M.Sc. degree in computer networks and communication in 2010 and Ph.D. in 2023 from Mosul University. He is interested in the field of computer networks and communication and he has published research papers in WiMAX (802.16d, 802.16e), Mesh, LTE, ZigBee, cybersecurity engineering, and industrial communication networks, communication networks infrastructure. He has been working as an assistant professor at the University of Mosul since 2021. He is a member of the computer networks lab in the Electrical Dept. / Engineering College.

How to cite this paper: Yazen S. Sheet, Mohammed Younis Thanoun, Firas S. Alsharbaty, "Smart Factory based on IIoT: Applications, Communication Networks and Cybersecurity", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.14, No.4, pp. 29-47, 2024. DOI:10.5815/ijwmt.2024.04.03