Computer Systems Science & Engineering
DOI:10.32604/csse.2021.015206
Article

Tech Science Press

Cyber Security and Privacy Issues in Industrial Internet of Things

NZ Jhanjhi[1], Mamoona Humayun[2,*] and Saleh N. Almuayqil[2]

[1]School of Computer Science and Engineering (SCE), Taylor's University, Selangor, Malaysia
[2]Department of Information Systems, College of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia
[*]Corresponding Author: Mamoona Humayun. Email: mahumayun@ju.edu.sa
Received: 10 November 2020; Accepted: 20 December 2020

Abstract: The emergence of industry 4.0 stems from research that has received a great deal of attention in the last few decades. Consequently, there has been a huge paradigm shift in the manufacturing and production sectors. However, this poses a challenge for cybersecurity and highlights the need to address the possible threats targeting (various pillars of) industry 4.0. However, before providing a concrete solution certain aspect need to be researched, for instance, cybersecurity threats and privacy issues in the industry. To fill this gap, this paper discusses potential solutions to cybersecurity targeting this industry and highlights the consequences of possible attacks and countermeasures (in detail). In particular, the focus of the paper is on investigating the possible cyber-attacks targeting 4 layers of IIoT that is one of the key pillars of Industry 4.0. Based on a detailed review of existing literature, in this study, we have identified possible cyber threats, their consequences, and countermeasures. Further, we have provided a comprehensive framework based on an analysis of cybersecurity and privacy challenges. The suggested framework provides for a deeper understanding of the current state of cybersecurity and sets out directions for future research and applications.

Keywords: Industrial Internet of things (IIoT); cybersecurity; industry 4.0; cyber-attacks

1 Introduction

The number of businesses entering I4.0 (also referred to as Industrial Internet, Internet of Things) is increasingly growing, by connecting industrial units through the internet with the intent of improving productivity and efficiency. These internet-enabled industries are key targets of Cyber Security (CS) threats, and it is one of the key challenges that need to be dealt with [1]. In the context of I4.0, CS plays a key role in maintaining organizational competitiveness. The number of cyber vulnerabilities targeting critical infrastructure affects the entire business process and companies' reputations. In the I4.0 era, hyper-connectivity between smart devices and smart networks provides a lucrative opportunity to cybercriminals who can easily find weaknesses insecure entry points in networks and sometimes devices too. These cyber-attacks not only cause an interruption to the standard functionality of an organization but also impact overall society and sometimes even the psyche of the victim countries [2].

According to the annual report on CS published by CISCO in 2018, 31% of organizations faced cyber-attacks on operational technology while 38% of organizations expected the extension of cyber-attack to change from Information technology level to Operational Technology level. According to this report, 75% of experts perceived CS as a priority. By comparison, only 16% of experts believed that their company is ready to face CS challenges. Lack of knowledge about CS threats and poor technical and managerial skills are considered a reason for this problem [3].

CS is now becoming a key consideration for Europe and various other international organizations. For instance, IEC has published guidelines about CS and privacy and the possible ways of implementing these principles [4]. Similarly, the ESCO has collected all possible standards and guidelines related to CS to help the European digital market in overcoming existing CS challenges. Despite these efforts, a lot of security threats are being reported daily, especially in the context of I4.0 [5]. This shows that cyber-security is an issue that needs to be researched especially in the I4.0 paradigm. Further, there is a need to provide a detailed review of possible security threats targeting I4.0 along with possible countermeasures. This will help practitioners in getting awareness about possible threats, and they can take preventive measures on time. Keeping in view the above facts, this study aims to provide a detailed review of CS threats targeting IIoT along with their consequences and countermeasures. IIoT refers to interconnected sensors, tools, and other devices that are interconnected with industrial computer applications, including manufacturing, production, and energy management. This connectivity facilitates the collection, distribution, and review of data, potentially promoting productivity and quality improvements along with other economic benefits. The reason for choosing IIoT is manifold; firstly, it is one of the key pillars of I4.0. Secondly, it is the main driving force towards the I4.0 revolution.

The structure of the remaining paper is organized as: the next section of the paper will discuss some key terminologies in detail for a better understanding of the area under research. Section 3 discusses the architecture of IIoT and I4.0 characterization. Section 4 will discuss the research methodology and proposed framework along with possible threats targeting IIoT layers, the consequence of these attacks, and countermeasures. Section 5 will present the result of the paper by providing a detailed discussion of our findings. Section 6 will conclude the paper by discussing some open issues for the research. Tab. 1 list the acronym and abbreviation used in this study for clarity and understanding.

Table 1: List of the acronym and abbreviations

Acr	Abbreviations	Acr	Abbreviations
IIOT	Industrial internet of things	UDP	User Datagram Protocol
CS	Cybersecurity	DTLS	Datagram Transport Layer Security
I4.0	Industry 4.0	CARP	Channel-aware routing protocol
IEC	International electro-technical Commission	NIST	National Institute of Standards and Technology
ESCO	European cybersecurity organization	DoS	Denial of service
CPS	Cyber-physical systems	MITM	Man-in-the-Middle attack
IOS	Internet of Services	WSN	Wireless Sensor Networks
ICT	Information and Communication Technologies	IDS	Intrusion detection system
RPL	Routing protocol for low power	CSP	Cloud service provider
ITU	International Telecommunications Union	SST	Spread spectrum techniques
HTTP	Hypertext transfer protocol	COAP	Constrained application protocol
MQTT	Message queue telemetry transport	XMPP	Extensible messaging and presence protocol

2 Background

I4.0 is a single paradigm, but it has many visions and dimensions. To fully understand it, we need to see these different dimensions. Below we discuss it.

2.1 Industry 4.0

The term I4.0 also known as industrial internet, has brought a great revolution in the industry. It originated in Germany when the German government promoted the computerization of the manufacturing industry. The idea behind I4.0 was to connect all the participants using the internet so that they could exchange information with each other. This idea is based on a cyber-physical system, a system of computational elements collaborating in a coordinated and controlled way. I4.0. Provides better business gain and has accelerated productivity a lot. It has impacted almost every field of life; proponent of I4.0 considers it as the third wave of innovation [6].

Below we discuss some definitions of I4.0 from the current literature for a better understanding.

"The industrial internet is an IoT, machines, computers, and people enabling intelligent industrial operations using advanced data analytics for transformational business outcomes, and it is redefining the landscape for business and individuals alike [6]". "I4.0 is a collective term for technologies and concepts of value chain organization. Within the modular structured Smart Factories of I4.0, CPS monitors physical processes, creates a virtual copy of the physical world, and makes decentralized decisions. Over the IoT, CPS communicates and cooperates with other CPS and humans in real-time. Via the IOS, both internal and cross-organizational services are offered and utilized by participants of the value chain" [7].

I4.0 is the interaction between IoT and CPS which includes embedded systems, sensors and actuators, hardware, and software along with the connection to other systems. Fig. 1 describes the perspective of I4.0 that is inevitable to compete in today's' fast-paced economy and to satisfy heterogeneous customers.

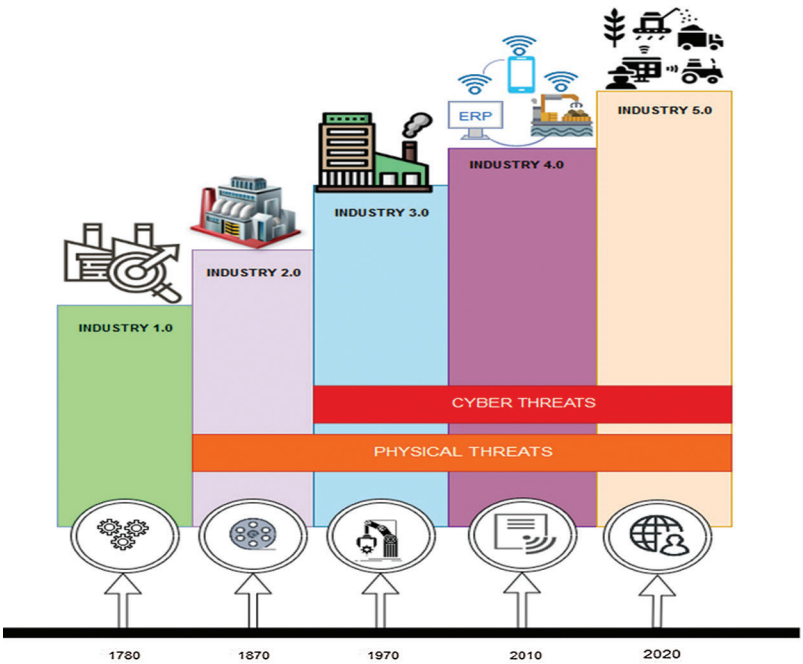

Figure 1: Industrial IIoT Evolution

2.2 Industrial Internet of Things (IIoT)

IoT is a network of connected devices that are communicating with each other through the internet [8]. When the same IoT is applied in industrial settings, it becomes IIoT. Researchers have used the term I4.0 and IIoT interchangeably. However, we have taken IIoT as one of the pillars of I4.0. Below we present some definitions of IIoT from literature.

"Industrial Internet: a short-hand for the industrial applications of IoT, also known as the IIoT" [9]. "The IIoT is the use of IoT technologies in manufacturing" [10]. "The IoT represents a scenario in which every object or 'thing' is embedded with a sensor and is capable of automatically communicating its state with other objects and automated systems within the environment. Each object represents a node in a virtual network, continuously transmitting a large volume of data about itself and its surroundings" [11].

"In general, the terms "IoT" apply to expand network access and computational capabilities to objects, devices, sensors, and things that are not typically considered computers as shown in Fig. 2. These "smart objects" require minimal human involvement in the creation, sharing and consumption of information; they also have connectivity to remote data collection, analysis, and management capabilities" [12]. "Group of infrastructures, interconnecting connected objects and allowing their management, data mining and the access to data they generate" where connected objects are "sensor(s) and/or actuator(s) carrying out a specific function that can communicate with other equipment" [9].

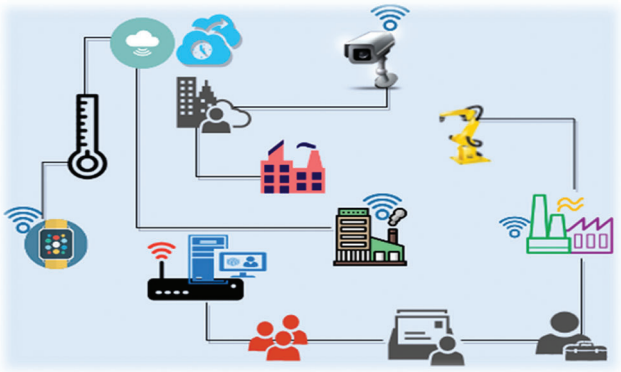

Figure 2: Internet of Things (IoT)

The above definitions provide a good overview of IIoT; however; for this paper, we have taken IIoT as one of the key pillars of IIoT. This pillar is divided into four layers as shown in Fig. 3, and each layer has its security requirements that will be discussed in detail in the next section.

2.3 Cyber Security

Cyber protection is the practice of using different methods to secure computers, networks, programs, and data from unauthorized access or attacks. It can also be defined as the security of organizational cyberspace from various internal and external security attacks. CS has become a matter of global interest for researchers and practitioners. Below we provide some definitions of CS from literature.

CS is defined as "preserving the integrity, confidentiality, and timely availability of information in Cyberspace" [13]. *Merriam Webster dictionary* defines it as "measures taken to protect a computer or computer system against unauthorized access or attack" [14]. The ITU defines CS as: "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" [15].

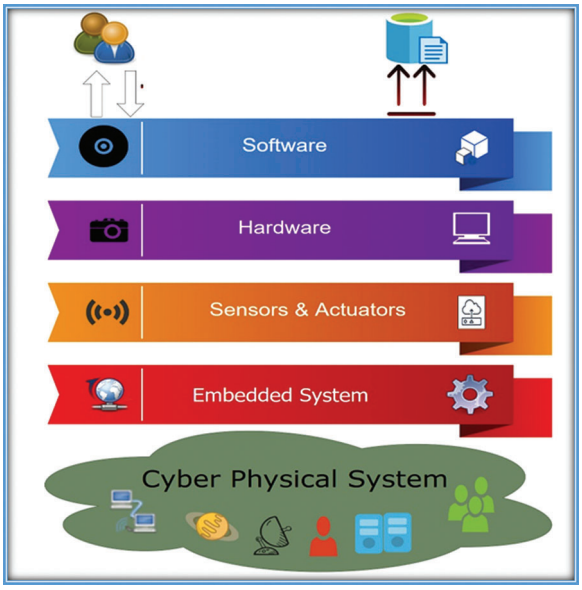

Figure 3: Pillars of IIoT

"The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets, and critical infrastructure" [13]. Oxford university press has defined CS as "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this" [16].

2.4 Cyber-Physical System (CPS)

CPS is a system of interacting physical entities manipulating computational elements. CPS are physical and engineered structures whose activities are controlled, organized, regulated, and incorporated by a center of computing and communication. They allow us to combine computation and communication with physical processes to add capabilities to physical systems [17].

"A system comprising a set of interacting physical and digital components, which may be centralized or distributed, that provides a combination of sensing, control, computation and networking functions, to influence outcomes in the real world through physical processes" [17]. "A cyber-physical system can be defined as a set of cyber-physical devices that include computing hardware and software that control mechanical activity through embedded processing, networking and connectivity, awareness of the environment and other objects through sensors, and finally a means of interacting with the environment through actuators" [18].

CPS is characterized as disruptive technologies between its physical assets and computational capabilities for the management of interconnected systems [17]. The real-time character of their encounters with the physical world is what sets CPS apart from more traditional information and communications systems. Although data and/or information is handled by both CPS and ICT systems, the focus of CPS is on the control of physical processes. The CPS uses sensors to obtain information, including physical parameter measurements, and actuators to regulate physical processes [9].

3 Literature Review

In this section, we will discuss the pillars of I4.0. The detailed architecture of IIoT and CS characterization for I4.0 will pave the way for the next section. I4.0 is mainly based on nine pillars. In a

single research, it is not possible to address each pillar in detail; however, for the readers' understanding of I4.0, each pillar is discussed briefly in Sub-section 3.1. The reason for choosing IIoT as the topic for this research is manifold: firstly; researchers have discussed several pillars of I4.0, but all of them highlight IIoT as a key pillar of I4.0. Secondly; IIoT has revolutionized industry 4.0 [19]. After giving an overview of the I4.0 pillars, the next subsection provides a detailed overview of IIoT architecture. With the advancement in the industrial paradigm, a lot of CS threats are being reported daily. These cyber-attacks are a big challenge for the Industrial revolution. Therefore, Sub-section 3.3 provides us with CS characterization for I4.0.

3.1 Pillars of I4.0

Researchers and practitioners have defined various enabling factors of I4.0. However; eight factors are common in many research papers as shown in Fig. 4. Below we discuss these eight pillars of I4.0.

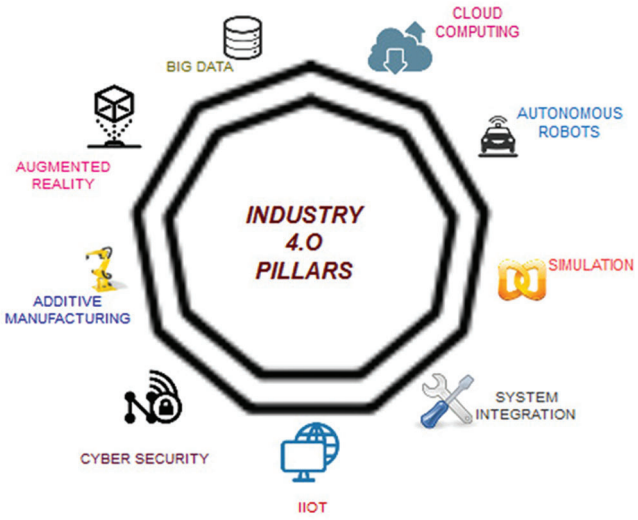

Figure 4: Pillars of Industry 4.0

Autonomous robots. This pillar of I4.0 assists in promoting I4.0 by providing a variety of services, including interaction with each other to perform assigned tasks, interacting safely with a human being, and learning from humans as well. Due to these features, robots are becoming more autonomous and flexible [6].

Simulation. I4.0 is a complex architecture, 3D simulation helps in testing and optimizing the machine settings before the start of production. It reduces time and improves quality by virtualizing the physical world [19].

Horizontal and vertical system integration. In today's fast-paced economy, the interconnection between companies and suppliers is vital for fast and quick delivery. The engineering department needs to be directly connected with the production department to accelerate the production process. I4.0 provides this mechanism by providing interconnectivity between all these units [6,19].

Industrial Internet of Things. IIoT is one of the key pillars and enablers of the I4.0 revolution. IoT that is Interconnectivity among devices using the internet to promote real-time responses has revolutionized the smart industry. The same concept, when applied in manufacturing and huge industry settings, has resulted in I4.0. Using IIoT, machines are fitted using sensors and are interconnected with each other in a centralized way, this has not only made real-time response possible but also increased productivity a lot [5,7].

Cyber Security. As machines, robots, and sensors are interconnected in I4.0. Paradigm, the risk of CS threats has also increased a lot. A lot of cybercrimes are being reported even in developed countries. A sophisticated and protected machine access mechanism is necessary to provide a secure communication mechanism. New ways of performing cyber-attacks and breaching security are being reported from all over the world. Hence; a proper CS mechanism is a key pillar of I4.0 and a step towards its success [13,20].

Cloud. The setup of I4.0 involves a huge amount of data and its sharing across sites and companies. This storage and sharing of data can be improved by taking the benefits of cloud technology, which is a more cheap and reliable way of data storage and retrieval [6,19,21].

Additive manufacturing. It includes technologies that assist I4.0 in improving their performance by producing customized products in small batches. Transportation and inventory management cost also reduce with the help of these technologies [7,19,22].

Augmented reality. Augmented-reality tools which include marker-based apps and location-based apps have assisted industrial settings a lot, especially healthcare, e-commerce, and manufacturing. They provide real-time information that helps in quick decision making and improving work processes [2,5,19].

Big data and analytics. The industrial world has a massive amount of untapped data. The analysis of this data helps optimize product quality, improve services, and save energy. This will also help in real-time decision making [6,19,23].

3.2 IIoT Architecture

I4.0 is having nine key pillars, as discussed above; each one is important. However; for this research, we will only discuss cyber threats targeting IIoT in the context of I4.0. Before proceeding towards research methodology, we will discuss IIoT architecture in detail. IIoT architecture is composed of 4 layers, as shown in Fig. 5. Below we explain the functionality of these layers in detail [6,22–24].

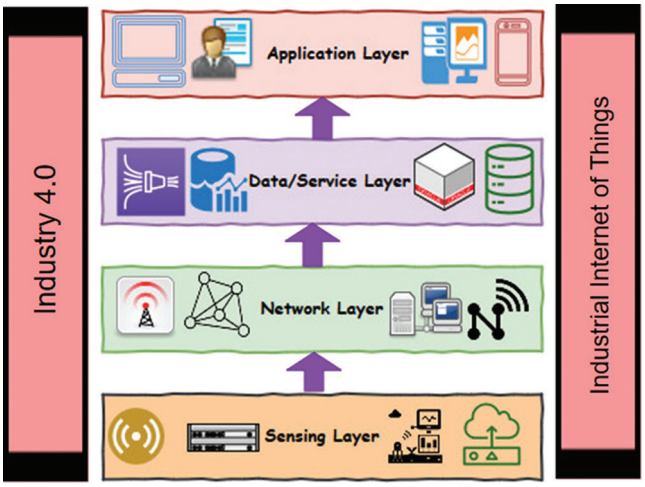

Figure 5: Industry 4.0 Architecture

Application layer. This layer is the topmost layer that initiates actual communication. This layer also interacts with the end-user directly. It consists of different applications each one has its application layer protocol. The protocols involved in this layer include HTTP, advanced message queuing protocol MQTT, COAP, XMPP, web socket protocol, and various other data distribution services [7,19].

Service layer. This layer pair service with its requester using addresses and names. This layer process data, make decisions and deliver required services over the network using different protocols. It is not platform specific and thus enables the IoT programmer to work with heterogeneous objects independent of the hardware platform. The protocol used at this layer include UDP and DTLS [6,22].

Networking Layer. In Industry 4.o settings, industries have to share a lot of data between the cloud and equipment, including both products and machines. In all cases, the network layer plays a vital role, just like the human nervous system. Various inter factory networks are interconnected, including industrial internet, near field communication using RFIDs, mobile communication networks, civilian internet, etc. This layer is divided into two sub-layers: a routing layer that is responsible for the transfer of data from source to destination and an encapsulation layer that performs other network operations. The protocol used for routing includes RPL, Cognitive RPL, CARP, etc. While the protocol used at the encapsulation layer includes IPv6 over low power wireless personal area network 6Lo, 6LoWPAN, 6TiSCH, IPv6 over Bluetooth Low, and IPv6 over G.9959 [5,6,19].

Sensing and actuator layer. This layer involves hardware including sensors, RFID tags, embedded systems, autonomous robots, and various other forms of soft sensors. All these are the primary entities that are deployed in the I4.0 paradigm to achieve better outcomes. These hardware elements provide information storage, collection, information processing, communication, control, and management. This layer is divided into two parts, perception node that includes sensors and controller, responsible for data acquisition and control, Second part is the perception network that communicates with the network layer and sends and collects data through the gateway and also sends control instructions to the controller. The technologies involved in this layer include RFID, RSN, WSNs and GPS, etc. [5,6,19].

3.3 Cyber Security Characterization for Industry 4.0

After discussing I4.0 and one of its pillar IIoT, this section takes advantage of

- Defining system vulnerability
- Cyber-attacks
- The risk associated with cyber-attacks
- Countermeasures used to deal with possible attacks

All these elements are associated with CS. The brief discussion of these points will help in a better understanding of this research's findings.

System vulnerability. Vulnerabilities are the weaknesses in the system that are exploited by hackers to compromise the security of CPS. According to NIST, Vulnerability refers to liabilities in the information system, security procedures, audits, and controls or implementation that could be exploited by the source of threats. There exist several vulnerabilities in each component of IIoT: these vulnerabilities are concerned with application servers, communication infrastructure, human-computer interfaces, remote terminal units, and even the sensors and actuators. The reasons behind these vulnerabilities are lack of proper security measures, multiple pathways through the networks, and lack of isolation between unrelated networks [5,15].

Cyber-attacks. According to NIST; a cyber-attack is an event that impacts organizational operations, assets, or individuals through unauthorized access, disclosure, DoS, information modification, or any other way. These attacks can be categorized as active mode and passive mode attacks. Active mode attacks involve making changes in system resources or affecting system operations (examples of active mode attacks include DoS attacks and compromised key attacks); while the target of passive mode attacks is to make use of victim information instead of changing it [13,16].

Risk. According to NIST, risk can be defined as the severity of the level of attack on organizational operations, assets, or individuals as a result of a cyber-attack and the probability of that threat occurring. These security risks impact integrity, confidentiality, and availability of information systems. The chances of security risks increase in the I4.0 context due to a wide range of interconnected devices, including the cloud. Therefore; the risk associated with each element should be identified in advance, and proper prevention and avoidance mechanisms should be introduced to sustain organizational competitiveness and to avoid the higher cost of danger [5,13,25].

Countermeasures. It refers to the procedures and techniques that are used to avoid, prevent, and eliminate possible attacks so that the harm it causes could be minimized. Industries that are operating under IIoT infrastructure need to identify possible threats and the risk associated with each threat. Industries should have a proper avoidance and detection mechanism to protect their assets from cyber-attacks. Some high-level approaches of protection include; strengthen the perimeter (it involves separations of sensitive nodes from the common nodes using firewalls or any other security mechanism), Applying defense-in-depth (by applying various layers of defense), and properly controlling and managing remote access [25,26].

4 Research Methodology and Proposed Framework

A detailed review of the existing literature is performed in this study to highlight possible CS attacks targeting IIoT. This review aims to collect possible cyber-attacks that target every four layers of IIoT, identify the possible consequences of these attacks, and providing countermeasures to protect against these attacks. The detailed methodology is shown in Fig. 6. To compile the data and to provide a detailed overview to the readers, we have synthesized CS attacks targeting each layer of IIoT separately. In the following subsections, we discuss possible attacks targeting each layer of IIoT.

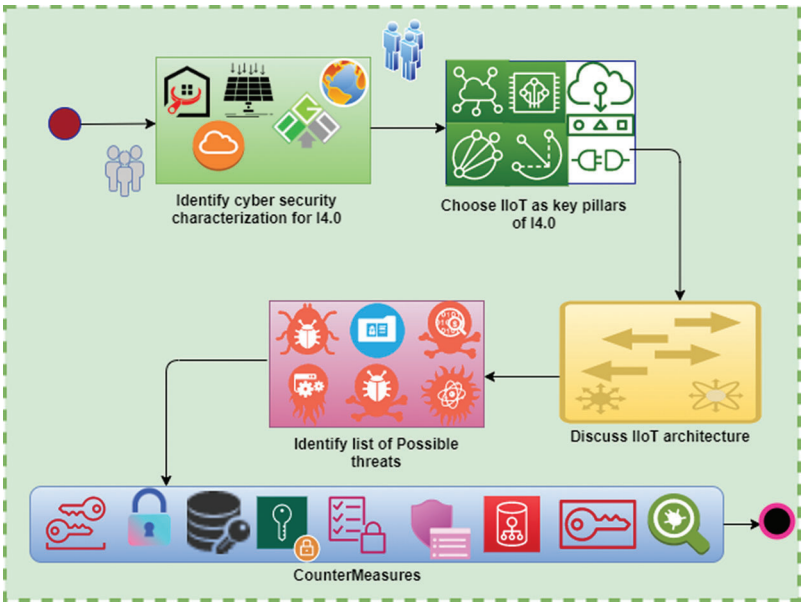

Figure 6: Research Methodology

4.1 Sensing Layer

IIoT sensing and actuator layer is the target of direct physical attacks. According to our findings, possible attacks targeting the sensing layer of IIoT include tampering, sensor threats, and DoS. Tampering attacks may be launched through physical damage, malicious code injection, and node jamming. Weak authentication and careless deployment may cause sensor threats while the DoS attack may be launched through changing the physical link, distortion, and Jamming. This study also highlighted countermeasures against each attack. The possible countermeasures to address the problems of tampering include tamper-resistant packaging and tamper-proofing & hiding. The measures that need to be taken against sensor threats include IDS, public key encryption, protecting sensed data, and enhancing the service management system. On the other hand, DoS may be protected through traffic monitoring and SST [27–47].

4.2 Network Layer

In IIoT automation, communication between nodes is key and networking attacks are especially harmful. According to our review results, two main attacks targeting the network layer of IIoT are MITM and DoS. However, these attacks cause further sub attacks as shown in our framework. According to Framework, MITM can be launched in many ways, including eavesdropping, routing attack, and replay attack. On the other hand, DoS may be launched through exhaustion, collision, wormhole, spoofing, unfair behavior, sinkhole attack, Sybil attack, flooding, node replication, and selective forwarding. According to our findings, MITM may be addressed through a semi-dynamic controller signature, detecting and blocking fake links and encryption. On the other hand, DoS attack at the network layer may be addressed through anti-jamming, identity-based authentication, IP security, digital signature, intrusion detection system, using link quality indicator, using a mobile agent to defend nodes, monitoring neighbor nodes, cryptography and packet tracing [44,48–63].

4.3 Data/Service Layer

In the IIoT setup, data is centralized and aggregated at the data processing layer usually within the cloud. The security of this data is crucial for any cyber environment. According to the existing literature on IIoT, this layer is a target of four main attacks, namely, Malware, session hijacking, malicious insider, and CSP risks. All these attacks have further subtypes: Malware attack has three main subtypes that are virus, worm, and botnets. Session hijacking attack at the service layer includes active session hijacking and passive session hijacking. Malicious insider attacks include DoS, extracting information, and executing privileges. The risk and attacks associated with CSP are back door attack, social engineering, and password guessing. According to our findings, the possible solution to Malware attacks is antimalware software and avoiding suspicious emails, websites, and other links. The possible solution for addressing session hijacking attacks is by educating users, IDS, using SSL, and monitoring MAC address and CAPTCHA protection. The possible solution for malicious insider includes periodic risk assessment, employee training, assigning fewer privileges, strict security policy, and monitoring disruptive behavior. Cloud service provided risk may be addressed through input monitoring, encrypted communication, and cloud education [52,54–71].

4.4 Application Layer

The IIoT application layer is the target of several security attacks. There are mainly four types of attacks that target the application layer of IIoT, namely, sniffing, phishing, malicious code injection, and DoS. These attacks have further sub attacks i.e., sniffing is of two types: active sniffing and passive sniffing. DoS attack at the application layer may be through exhaustion and flooding. Phishing attacks may be subdivided into social engineering attacks and malware-based phishing. Malicious code injection attacks include injecting the packet as well as injecting the nodes. According to our findings, the countermeasures used to protect

against sniffing attacks are encryption and Mac filtering. DoS attacks at the application layer may be protected using firewall & proxies, filtering, and IP security. Malicious code injection can be protected using authentication and IDS, and phishing attacks can be addressed through user education, strong authentication mechanism, network-level protection, and using client and server-side security tools [60–62,64–70,72–79].

Fig. 7 shows the proposed framework. According to Fig. 7, IIoT is a key pillar of industry 4.0. It is composed of 4 layers namely; the application layer, data layer, network layer, and physical layer. The proposed framework helps to know the possible cyber-attacks targeting all four layers of IIoT. Further, the way to mitigate these attacks is also mentioned in the framework. The application layer is the main target of phishing, sniffing, DoS, and code injection attacks. The right part of the framework shows the possible countermeasures for these attacks. In the same way, the security attacks targeting other layers of IIoT is mentioned along with possible countermeasures.

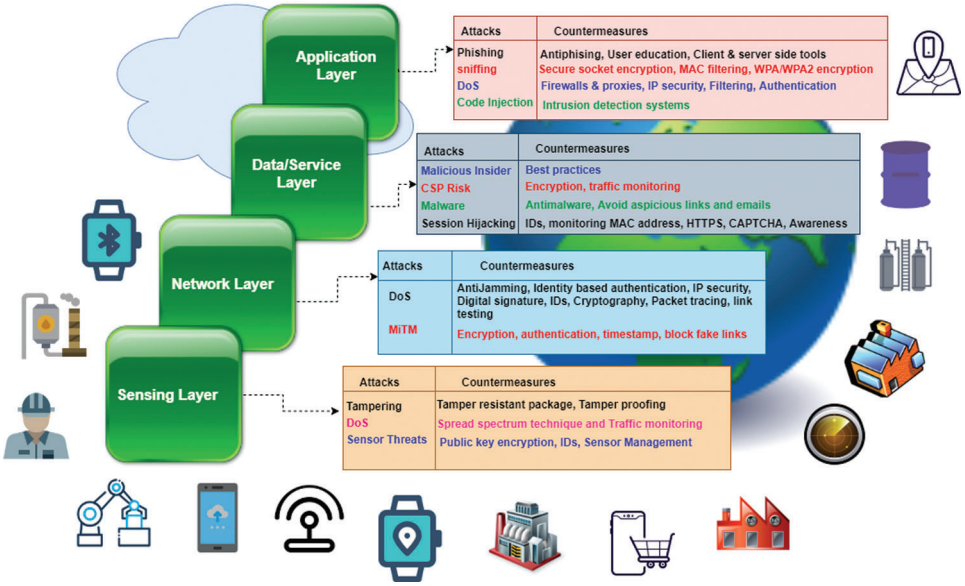

Figure 7: Proposed Framework

5 Results and Discussion

Despite the importance of IIoT in the I4.0, it is prone to various security attacks. A lot of research efforts have been done to protect IIoT infrastructure from possible cyber-attacks. After going through the existing literature on IIoT, we realized that there is a need to provide a detailed review that may discuss all possible cyber-attacks targeting all layers of IIoT and the countermeasures to protect this sensitive infrastructure from security attacks. Further, CS attacks targeting IIoT architecture have been discussed in many studies but there exist no studies that provide layer-wise attacks. To overcome this gap, this paper provides a detailed overview of the possible cyber-security threats targeting each layer of IIoT along with their countermeasures. In the sub-section below, we discuss our results both in tabular and graphical form.

5.1 Sensor Layer Security

This subsection discusses attacks that target the sensor layer of IIoT. Tab. 2 presents possible attacks, countermeasures, and frequency of occurrence for these attacks in the existing literature.

Table 2: CS attacks targeting physical layer of IIoT

	Attacks	Causes/ Consequences	Countermeasures	Freq	References
Physical layer	Tampering	Physical damage	Tamper-resistant packaging	14	[24,25,27–32,36–40,71]
		Malicious code injection	Tamper proofing and hiding		
	Sensor Threats	Weak authentication mechanism	Protecting sensed data Encryption Adopt intrusion mechanism	8	[33–35,41–55]
		Careless deployment	Enhancing the sensor management system		
	Denial of Service	Changing physical link	SST	20	[18,38,41–43,48,50,52,65,66,69,72–80]
		Distortion	SST		
		Jamming	Traffic monitoring		

According to the data of Tab. 2 and its corresponding Fig. 8, the three key attacks targeting the physical layer of IIoT include tampering, sensor threats, and DoS. According to Tab. 2, DoS has the highest probability of occurrence, which is 38%. Then comes Sensor threats with 35% occurrence and last but not the least is tampering.

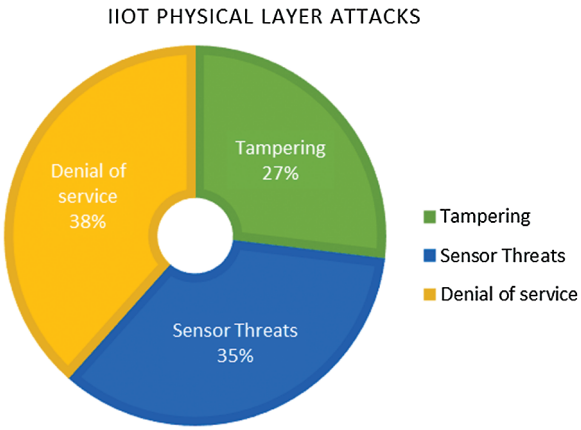

Figure 8: CS attacks targeting the application layer of IIoT

The above statistics show that individuals, as well as organizations, should take proper measures to protect their assets. The use of security tools, proper management, and careful deployment is necessary to protect the networks from these attacks.

5.2. Network Layer Security

This subsection discusses attacks that target the Network layer of IIoT. Tab. 3 presents possible attacks, countermeasures, and frequency of occurrence for each attack extracted from existing literature along with referred studies.

Table 3: CS attacks network layer of IIoT

	Attacks	Sub-Attacks	Countermeasures	Freq	References
Network layer	Denial of service	Exhaustion	Packet marking Packet tracing Traffic monitoring	14	[33,41,42,44,48,50–52,57,59,64,65,69,70]
		Jamming	Anti-jamming Active jamming Faraday cages	10	[33,41,42,48,50,52,57,59,65,69]
		Spoofing	Identity-based authentication IP security Digital signature	7	[33,42,48,52,59,65,69]
		Sinkhole attack	Intrusion detection system Rule based technology	11	[33,42,48,52,59,65,69,75,77–79]
		Unfairness	Proper security mechanism Employee education	8	[6,48,52,59,65,69,75,79]
		Selective forwarding	Monitoring neighbor node Introducing attack detection mechanism Controlling packet collection Analysis of alternate paths	13	[6,48,52,59,65,66,68,69,72,75,77–79]
		Wormhole attack	Intrusion detection system Neighbor validation Distance calculation	10	[6,41,42,48,52,59,65,66,72,77]
		Sybil attack	Cryptography Profile matching Behavior classification Channel estimation Monitoring users' mobility	12	[6,41,42,48,52,59,65,66,72,77–79]
		Flooding	Packet marking Packet tracing Link testing	10	[6,41,42,48,52,59,65,66,72,77]
		Node replication	Identity-based authentication IP security	6	[58,61,65,68,72,77]
	MITM	Eavesdropping	Adding semi-dynamic controller signature Block fake links	10	[58,61,64,65,68–70,72,76,77]
		Routing attack	Encryption	7	[58,61,64,65,72,76,77]
		Replay attack	message sequence numbers message authentication code	12	[65–70,72–77]

According to data in Tab. 3, network attacks are mainly categorized into two types of attacks, namely DoS and MITM. Both attacks have various forms of occurrence. Further, the DoS attack is launched in different ways, and it makes network resources unavailable to its intended users. Therefore, individuals and organizations need to be aware of these attacks and possible mitigation strategies.

5.3 Data Layer Security

This subsection discusses attacks that target the data/service layer of IIoT. Tab. 4 presents possible attacks, countermeasures, and their frequency of occurrence in existing literature along with referred

studies. According to the data presented in Tab. 4 and the corresponding Fig. 9, the data layer is a key target of a malicious insider. Malicious insider attacks target this layer through DoS, information extraction, and privileges execution. Individuals and organizations must implement strict security, and employees should be trained regarding security. Further, limited privileges and separation of responsibilities are inevitable to avoid the data layer from these threats. Most large organizations use cloud services for data hosting, which is also risky if proper security measures are not taken.

Table 4: CS attacks Data layer of IIoT

	Attacks	Attacks subtypes	Countermeasures	Freq	References
Data layer	Malicious Insider	DoS Extracting information Executing privileges	Periodic risk assessment Security awareness training Separation of responsibilities Strict security policy Monitoring and auditing	15	[5,7,25,33–36,40–42,44–47,51]
	CSP risks	Back door attack Social engineering Password guessing	Encrypted communication Input monitoring Employee awareness	13	[5,7,25,33–35,40–42,44,45,47,51]
	Malware	Virus Worm Botnets	Avoid suspicious opening link Use antimalware software	12	[5,7,25,33–35,40–42,44,45,47]
	Session hijacking	Active session hijacking Passive session hijacking	Intrusion detection system Monitoring MAC address Using SSL,HTTPS connection Educating users, CAPTCHA prevention	8	[5,7,25,33,35,40,42,45]

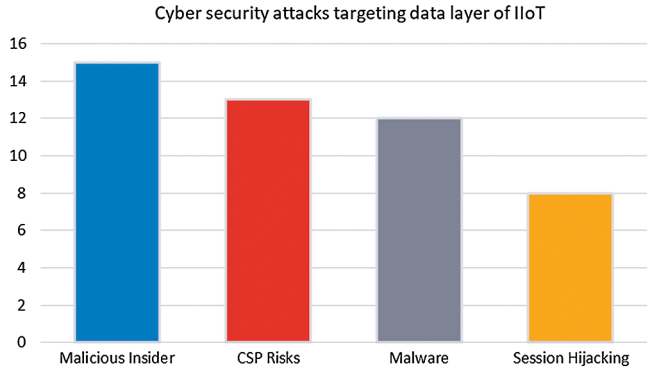

Figure 9: CS attacks targeting the Data layer of IIoT

Malware threat is a common type of attack that usually comes through auspicious links and emails. Organizations need to train their employees regarding this attack. Last but not least is session hijacking that needs to be monitored, it can be done via IDS, Monitoring MAC address, Using SSL, HTTPS connection, Educating users, and CAPTCHA prevention.

5.4 Application Layer Security

This subsection presents attacks that target the Application layer of IIoT. Tab. 5 provides an overview of CS threats targeting the application layer of IIoT along with its countermeasures and frequency of occurrence. According to the statistics of Tab. 5 and Fig. 10, DoS and malicious code injection are the key attacks targeting the application layer of IIoT. Organizations need to implement strict security policy, some preventive measures that might be adopted include firewalls and proxies, IP security, filtering, and intrusion detection systems.

Table 5: CS attacks targeting the application layer of IIoT

	Attacks	Attacks Detail	Countermeasures	Freq	References
Data layer	Phishing	Malware based phishing Social engineering	User education Authentication mechanism Network-level protection Using client-side tools Using server-side tools	19	[58–70,72–74,77–79]
	Sniffing	Active sniffing Passive sniffing	Encryption MAC filtering	14	[58–63,65,67,68,70,73,74,77,79]
	DoS	Exhaustion Flooding	Firewalls and proxies Filtering IP security	22	[5–7,33,42,45,47,51,58–63,65,67,68,70,73,74,77,79]
	Malicious code injection	Injecting node Injecting packet	Authentication Intrusion detection system	22	[5–7,33,42,45,47,51,58–63,65,66,68,70,73,74,77,79]

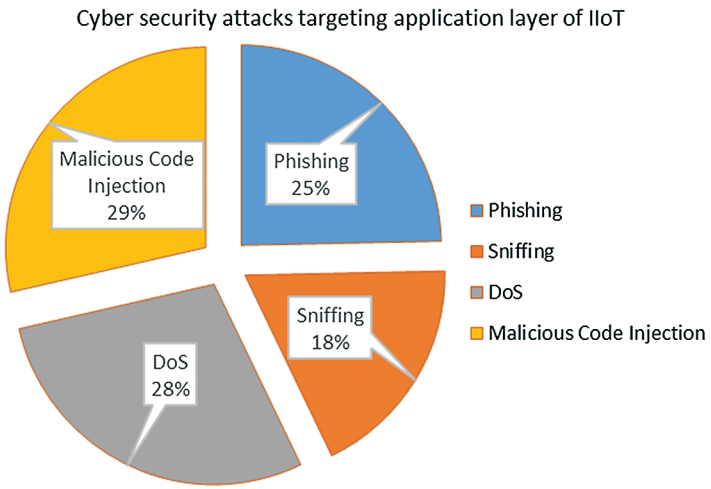

Figure 10: CS attacks targeting the application layer of IIoT

The second key attack that targets this layer of IIoT is phishing that usually comes through emails and suspicious links. This attack can somehow be prevented through user education, using client-side and server-side security tools, and by implementing a proper authentication mechanism. Last but not least is the sniffing attack that can be prevented through encryption and MAC filtering.

The above discussion provides a detailed overview of existing cybersecurity threats and challenges along with mitigation strategies to the I4.0 practitioners and researchers. Some other studies [81–84] have also discussed IIoT security challenges; however; they only targeted specific attacks instead of pinpointing existing possible attacks on various layers of IIoT.

6 Conclusion & Future Work

I4.0 has brought a great revolution in almost every field of life by connecting billions of heterogeneous devices on a real-time basis. Researchers have discussed various pillars of I4.0, including autonomous robots, simulation, cyber-security, IIoT, horizontal and vertical integration, augmented reality, etc. It was not possible to discuss cybersecurity and privacy issues confronting all the pillars of I4.0 in a single research. Therefore, in this research, we have focused on IIoT, one of the important pillars of I4.0. We have provided a detailed architecture of I4.0 that is composed of four layers. One of the key challenges faced by I4.0 is the risk of CS attacks. To overcome this problem, we have discussed all possible attacks targeting each layer of IIoT along with their consequences and possible countermeasures. This detailed analysis of the literature aims to provide a broader overview of IIoT architecture and the possible attacks targeting each layer of IIoT. It will help the IIoT researchers and practitioners in getting awareness of possible attacks and their solutions. Based on an analysis of existing cybersecurity and privacy issues targeting IIoT, a comprehensive framework is developed that provides an overview of possible security and privacy threats along with the ways of attacks and countermeasures.

In the future, we are planning to apply the proposed framework in Industry 4.0 settings to analyze the impact of the proposed approach in mitigating cyber privacy and security issues.

Funding Statement: The author(s) acknowledge Jouf University, Saudi Arabia for his funding support.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] F. Zezulka, P. Marcon, J. Arm, T. Benesel, I. Vesely *et al.,* "Communication systems for industry 4.0 and the IIoT," *IFAC-PapersOnLine*, vol. 51, no. 6, pp. 150–155, 2018.

[2] S. Munirathinam, "Industry 4.0: Industrial internet of things (IIOT)," *Advances in Computers*, vol. 117, no. 1, pp. 129–164, 2019.

[3] B. C. Ervural and B. Ervural, "Overview of cybersecurity in the industry 4.0 era," *Industry 4.0: Managing the digital transformation*, 1st ed., Vol. 1, Springer, pp. 267–284, 2018.

[4] B. Leander, A. Causevic and H. Hansson, "Applicability of the IEC 62443 standard in industry 4.0/IIoT," in *Proc. ARES*, Canterbury, CA, United Kingdom, pp. 1–8, 2019.

[5] M. Lezzi, M. Lazoi and A. Corallo, "Cybersecurity for industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103, no. 3, pp. 97–110, 2018.

[6] S. Vaidya, P. Ambad and S. Bhosle, "Industry 4.0 – A glimpse," *Procedia Manufacturing*, vol. 20, no. 1, pp. 233–238, 2018.

[7] G. Jairo, E. Sarkar, A. Cardenas, M. Maniatakos and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design & Test*, vol. 34, no. 4, pp. 7–17, 2017.

[8] M. Humayun, N. Jhanjhi and M. Alamri, "IoT-based Secure and Energy Efficient scheme for E-health applications," *Indian Journal of Science and Technology*, vol. 13, no. 28, pp. 2833–2848, 2020.

[9] B. Hugh, B. Hallaq, J. Cunningham and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, no. 8, pp. 1–12, 2018.

[10] V. S. Magomadov, "The Industrial Internet of Things as one of the main drivers of Industry 4.0," *IOP Conference Series: Materials Science and Engineering*, vol. 862, no. 3, pp. 032101–032106, 2020.

[11] M. Humayun, N. Jhanjhi, B. Hamid and G. Ahmed, "Emerging smart logistics and transportation using IoT and blockchain," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 58–62, 2020.

[12] M. Humayun, N. Jhanji and M. Alamri, "Smart secure and energy Efficient scheme for E-Health applications using IoT: A Review," *International Journal of Computer Science and Network Security*, vol. 20, no. 4, pp. 55–72, 2020.

[13] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 3171–3189, 2020.

[14] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, no. 6, pp. 97–102, 2013.

[15] R. Hill, "Dealing with cyber security threats: International cooperation, ITU, and WCIT," in *Proc. ICCC*, Tallin, Estonia, pp. 119–134, 2015.

[16] D. Craigen, N. Thibault and R. Purse, "Defining cybersecurity," *Technology Innovation Management Review*, vol. 4, no. 10, pp. 1–9, 2014.

[17] A. Humayed, J. Lin, F. Li and B. Luo, "Cyber-physical systems security–A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[18] B. Bordel, R. Alcarria, T. Robles and D. Marten, "Cyber physical systems: Extending pervasive sensing from control theory to the internet of things," *Pervasive and Mobile Computing*, vol. 40, no. 2, pp. 156–184, 2017.

[19] G. Erboz, "How to define industry 4. 0: the main pillars of industry 4.0," in *Proc ICoM 2017*, Nitra, Slovakia, pp. 1–2, 2017.

[20] M. Humayun, N. Jhanjhi, M. Alruwailli, S. Amalathas, V. Balasubramaniam *et al.,* "Privacy protection and energy optimization for 5G-aided industrial internet of things," *IEEE Access*, vol. 8, no. 1, pp. 183665–183677, 2020.

[21] S. K. Mishra, S. Mishra, A. Alsayat, N. Jhanjhi, M. Humayun *et al.,* "Energy-aware task allocation for multi-cloud networks," *IEEE Access*, vol. 8, no. 1, pp. 183825–183834, 2020.

[22] P. Radanliev, D. Roure, K. Page, J. Nurse, R. M. Montalvo *et al.,* "Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains," *Cybersecurity*, vol. 13, no. 3, pp. 1–21, 2020.

[23] M. Humayun, "Role of emerging IoT big data and cloud computing for real time application," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 4, pp. 494–506, 2020.

[24] K. Wang, Y. Wang, Y. Sun, S. Guo and J. Wu, "Green industrial internet of things architecture: An energy-efficient perspective," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 48–54, 2016.

[25] H. Holger, S. Schriegel, Ju. Jasper, H. Trsek and H. Adamczyk, "Analysis of the cyber-security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements," in *Proc ETFA*, Berlin, Germany, pp. 1–4, 2016.

[26] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Computers & Security*, vol. 68, no. 2, pp. 81–97, 2017.

[27] P. varga, S. Plosz, G. Soos and C. Hegegus, "Security threats and issues in automation IoT," in *Proc WFCS*, Trondheim, Norway, pp. 1–6, 2017.

[28] Y. Pan, J. White, D. C. Schmidt, A. Elhabashy, L. Sturm *et al.,* "Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 4, no. 3, pp. 45–54, 2017.

[29] N. Zulkipli, A. Alenezi and G. B. Wills, "IoT forensic: Bridging the challenges in digital forensic and the internet of things," in *Proc IoTBDS*, Porto, Portogal, pp. 315–324, 2017.

[30] Z. Chen, Z. Wang and C. Jia, "Semantic-integrated software watermarking with tamper-proofing," *Multimedia Tools and Applications*, vol. 77, no. 9, pp. 11159–11178, 2018.

[31] M. Ahmadvand, A. Pretschner and F. Kelbert, "A taxonomy of software integrity protection techniques," *Advances in Computers*, vol. 112, no. 1, pp. 413–486, 2019.

[32] F. Toffalini, M. Ochoa, J. Sun and J. Zhou, "Careful-Packing: A practical and scalable anti-tampering software protection enforced by trusted computing," in *Proc. CODASPY*, Dallas, Texas, USA, pp. 231–242, 2019.

[33] B. Kim and Y. Kang, "Abnormal traffic detection mechanism for protecting IIoT environments," in *Proc ICTC*, Jeju Island, Korea, pp. 943–945, 2018.

[34] L. Zhou, H. Guo and G. Deng, "A fog computing based approach to DDoS mitigation in IIoT systems," *Computers & Security*, vol. 85, no. 5, pp. 51–62, 2019.

[35] S. Z. Tajalli, M. Mardaneh, E. Fard, A. Izadian, A. F. Kavaousi *et al.,* "DoS-resilient distributed optimal scheduling in a fog supporting IIoT-based smart microgrid," *IEEE Transactions on Industry Applications*, vol. 56, no. 3, pp. 2968–2977, 2020.

[36] X. Yan, Y. Xu, X. Xing, B. Cui and Z. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6182–6192, 2020.

[37] M. Du and K. Wang, "An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 648–657, 2020.

[38] F. Lorenzo, J. Anorga and S. Arrizabalaga, "A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS," *ACM Computing Surveys*, vol. 53, no. 2, pp. 1–53, 2020.

[39] C. Jinhua, Y. Zhang, Z. Cai, A. Liu and Y. Li, "Securing display path for security-sensitive applications on mobile devices," *Computers, Materials and Continua*, vol. 55, no. 1, pp. 17–35, 2018.

[40] J. Sengupta, S. Ruj and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, no. 6, pp. 102481–102509, 2020.

[41] K. Kimani, V. Oduol and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *International Journal of Critical Infrastructure Protection*, vol. 25, no. 1, pp. 36–49, 2019.

[42] O. Dagogo and Hope Okoro, "Security challenges in IoT platforms and possible solutions," *Computing*, vol. 8, no. 1, pp. 1–7, 2020.

[43] X. Jiang, M. Lora and S. Chattopadhyay, "An experimental analysis of security vulnerabilities in industrial IoT devices," *ACM Transactions on Internet Technology*, vol. 20, no. 2, pp. 1–24, 2020.

[44] M. Shuai, L. Xiong, C. Wang and N. Yu, "A secure authentication scheme with forward secrecy for industrial internet of things using Rabin cryptosystem," *Computer Communications*, vol. 160, no. 1, pp. 215–227, 2020.

[45] W. Li and P. Wang, "Two-factor authentication in industrial internet-of-things: Attacks, evaluation and new construction," *Future Generation Computer Systems*, vol. 101, no. 1, pp. 694–708, 2019.

[46] S. Paliwal, "Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial internet of things," *IEEE Access*, vol. 7, no. 1, pp. 136073–136093, 2019.

[47] S. Madhawa, P. Balakrishnan and U. Arumugam, "Roll forward validation based decision tree classification for detecting data integrity attacks in industrial internet of things," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 3, pp. 2355–2366, 2019.

[48] H. A. Khattak, M. A. Shah, S. Khan, I. Ali and M. Imran, "Perception layer security in internet of things," *Future Generation Computer Systems*, vol. 100, no. 7, pp. 144–164, 2019.

[49] Z. A. Almusaylim, A. Alhumam and N. Jhanjhi, "Proposing a secure RPL based internet of things routing protocol: A review," *Ad Hoc Networks*, vol. 101, no. 6, pp. 102096, 2020.

[50] I. Butun, P. Osterberg and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2020.

[51] R. Ande, B. Adebisi, M. Hammoudeh and J. Saleem, "Internet of things: Evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, no. 5, pp. 101728, 2020.

[52] S. Berger, O. Burger and M. Roglinger, "Attacks on the industrial internet of things-development of a multi-layer taxonomy," *Computers & Security*, vol. 93, no. 1, pp. 101790–101809, 2020.

[53] Y. Lu and L. D. Xu, "Internet of things (IoT) cybersecurity research: a review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, 2019.

[54] L. Antao, R. Pinto, J. Reis and G. Gonccalves, "Requirements for testing and validating the industrial internet of things," in *Proc ICSTW*, Vasteras, Sweden, pp. 110–115, 2018.

[55] D. Wu, A. Ren, W. Zhang, F. Fan, P. Liu *et al.,* "Cybersecurity for digital manufacturing," *Journal of Manufacturing Systems*, vol. 48, no. 4, pp. 3–12, 2018.

[56] E. Aydogan, S. Yilmaz, S. Sen, I. Butun, S. Forsström *et al.,* "A central intrusion detection system for RPL-based industrial internet of thing," in *Proc WFCS*, Sundsvall, Sweden, pp. 1–5, 2019.

[57] K. N. Qureshi, K. Naseer, S. S. Rana, A. Ahmed and J. Gwanggil, "A novel and secure attacks detection framework for smart cities industrial internet of things," *Sustainable Cities and Society*, vol. 61, no. 1, pp. 102343–102362, 2020.

[58] T. Yadollahzadeh and Z. Mataji, "Detecting sinkhole attack in RPL-based internet of things routing protocol," *Journal of AI and Data Mining*, vol. 8, no. 1, pp. 1–15, 2020.

[59] S. Pundir, M. Wazid, A. K. Das, J. Rodrigues and Y. Park, "Designing efficient Sinkhole attack detection mechanism in edge-based IoT deployment," *Sensors*, vol. 20, no. 5, pp. 1300–1313, 2020.

[60] H. Wu, X. Lyu and H. Tian, "Online optimization of wireless powered mobile-edge computing for heterogeneous industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9880–9892, 2019.

[61] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of threats to the internet of things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019.

[62] B. Gupta and M. Quamara, "An overview of internet of things (IoT): Architectural aspects, challenges, and protocols," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 21, pp. e4946, 2018.

[63] C. Millard, W. K. Hon and J. Singh, "Internet of things ecosystems: Unpacking legal relationships and liabilities," in *Proc IC2E*, Vancouver, BC, Canada, pp. 286–291, 2017.

[64] L. Xiaomin, D. Li, J. Wan, V. Athanasios, V. Vasilakos *et al.,* "A review of industrial wireless networks in the context of industry 4. 0," *Wireless networks*, vol. 23, no. 1, pp. 23–41, 2017.

[65] I. Jamai, L. B. Azzouz and L. A. Saidane, "Security issues in industry 4.0," in *Proc IWCMC*, Limassol, Cyprus, pp. 481–488, 2020.

[66] R. Gupta, S. Tanwar, N. Kumar and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review," *Computers & Electrical Engineering*, vol. 86, no. 2, pp. 106717–106732, 2020.

[67] J. Polge, J. Robert and Y. L. Traon, "Assessing the impact of attacks on OPC-UA applications in the industry 4.0 era," in *Proc CCNC*, Las Vegas, NV, USA, pp. 1–6, 2019.

[68] T. Pereira, L. Barreto and A. Amaral, "Network and information security challenges within industry 4.0 paradigm," *Procedia Manufacturing*, vol. 13, no. 2, pp. 1253–1260, 2017.

[69] G. S. Gaba, G. Kumar, H. Monga, T. Kim, M. Liyanage *et al.,* "Robust and lightweight key exchange (LKE) protocol for industry 4. 0," *IEEE Access*, vol. 8, no. 1, pp. 132808–132824, 2020.

[70] A. Esfahani, G. Mantas, J. Ribeiro, J. Bastos, S. Mumtaz *et al.,* "An efficient web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain," *IEEE Access*, vol. 7, no. 1, pp. 58981–58989, 2019.

[71] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[72] S. R. Chhetri, N. Rashid, S. Faezi and M. A. Faruque, "Security trends and advances in manufacturing systems in the era of industry 4.0," in *Proc ICCAD*, Irvine, CA, USA, pp. 1039–1046, 2017.

[73] N. Benias and A. P. Markopoulos, "A review on the readiness level and cyber-security challenges in industry 4.0," in *Proc SEEDA-CECNSM*, Kastoria, Greece, pp. 1–5, 2017.

[74] C. Lin, D. He, X. Huang, K. Choo and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4. 0," *Journal of Network and Computer Applications*, vol. 116, no. 3, pp. 42–52, 2018.

[75] M. Whaiduzzaman and A. Gani, "Measuring security for cloud service provider: A third party approach," in *Proc EICT, KUET*, Khulna, Bangladesh, pp. 1–6, 2014.

[76] C. Tang and J. Liu, "Selecting a trusted cloud service provider for your SaaS program," *Computers & Security*, vol. 50, no. 1, pp. 60–73, 2015.

[77] J. E. Rubio, R. Roman and J. Lopez, "Analysis of cybersecurity threats in industry 4.0: The case of intrusion detection," in *Proc CIRITIS*, Lucca, Italy, pp. 119–130, 2017.

[78] S. Luthra and S. K. Mangla, "Evaluating challenges to industry 4.0 initiatives for supply chain sustainability in emerging economies," *Process Safety and Environmental Protection*, vol. 117, no. 4, pp. 168–179, 2018.

[79] N. Moustafa, E. Adi, B. Turnbull and J. Hu, "A new threat intelligence scheme for safeguarding industry 4.0 systems," *IEEE Access*, vol. 6, no. 1, pp. 32910–32924, 2018.

[80] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa, "Cyber physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, no. 1, pp. 151019–151064, 2020.

[81] T. Gebremichael, L. P. Lehlogonolo, M. H. Eldefrrawy, G. P. Hancke, N. Pereira *et al.,* "Security and privacy in the industrial internet of things: Current standards and future challenges," *IEEE Access*, vol. 8, no. 1, pp. 152351–152366, 2020.

[82] K. P. Waqas and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial internet of things," *Entropy*, vol. 22, no. 2, pp. 175, 2020.

[83] L. Tawalbeh, F. Muheidat, M. Tawalbeh and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Applied Sciences*, vol. 10, no. 12, pp. 4102–4119, 2020.

[84] P. Vikram, I. Priyadarshini, R. Kumar and L. C. Kim, "Blockchain meets IIoT: An architecture for privacy preservation and security in IIoT," in *Proc ICCSEA*, Sydney, Australia, pp. 1–7, 2020.