ISSN 2744-1741
Review Article

Defense and Security Studies
Vol. 3, August 2022, pp.32-49
https://doi.org/10.37868/dss.v3.id188

Cybersecurity challenges in Industry 4.0: A state of the art review

Elmedina Avdibasic[1], Amanzholova Saule Toksanovna[2], Benjamin Durakovic[1*]
[1] International University of Sarajevo, Bosnia
[2] International Information Technology University, Kazakhstan

*Corresponding author E-mail: bdurakovic@ius.edu.ba

Received Jul. 22, 2021
Revised Aug. 27, 2022
Accepted Aug. 13, 2022

Abstract

Cybersecurity is an important topic for Industry 4.0, which will face a lot of non-traditional challenges before it can be fully implemented to help society. The objective of the study is to recognize recent cybersecurity trends, newly occurring threats and challenges as well as their potential solutions. The articles reviewed in the paper are found through science direct, Scopus, Semantic scholar and google scholar. After reviewing them, ideas from articles were grouped together to show how different articles had similar thoughts. Through the analysis of 70 articles, it was found that cybersecurity still needs a lot of improvement in order to efficiently implement Industrial Internet of Things (IIoT), especially since many articles underline the need for security-by-design approach, followed by regular updating. Key challenges are lack of awareness and security experts, increased cybercriminal and the fact that the chain is as only as strong as its weakest point. Some of the most important solutions include incorporating security into design, stronger encryption, regular updates to patch vulnerabilities and good prevention and detection mechanisms. Once cybersecurity challenges are overcome, Industry 4.0 will be able to bloom to its full extent.

Keywords: Cybersecurity, Industry 4.0, Internet of Things (IoT), Artificial intelligence

1. Introduction

As humanity progressed throughout the time, the focus was always on developing better technologies. Purpose of industry revolutions is to improve production. The first industrial revolution brought us mechanization, second one introduced mass production, and third one was about automatization. Next in line is fourth industrial revolution, or as some like to call it, Industry 4.0. Some of the concepts of industry 4.0 is to make the machines smarter by introducing machine learning, and then interconnecting those machines so that the data can be exchanged between them. Therefore, the following core components of Industry 4.0 can be recognized [1]:

1. Cyber-physical systems.
   Purpose is to combine networks and computers-which are cyber part, with manufacturing- which is physical-systems part. The idea is to have manufacturing processes under the surveillance of computers.
2. Smart factory.
   A background system that manages the virtual and physical systems, gives almost real time feedback about manufacturing. It's basically a self-sustaining factory that does not need intervention of humans.
3. Internet of things.

Cooperation and communication of devices that are part of one cyber-physical system is provided through internet of things. They can share the data and help each other with problem solving.

4. Internet of services.
   All the services that are needed are accessible through the Internet.

There are few questions that arise when it comes to the challenges of Industry 4.0. The articles that are written about the Industry 4.0 and its challenges discuss these questions and their possible answers, ways to overcome these challenges. Do the companies have enough competent staff needed to shift to this new technology? Do they have the right infrastructure needed to make this change? Another very important question is regarding the data privacy, whether the shared data is safe. How to protect the consumer and consumers' data? How secure are the clouds where the data will be uploaded, and how exactly is the data going to be manipulated? Cybersecurity surely is one of the biggest challenges that 4.0 will face [1]. Figure 1 shows the context of cybersecurity in the big picture of Industry 4.0 and Industrial Internet of Things (IIoT).

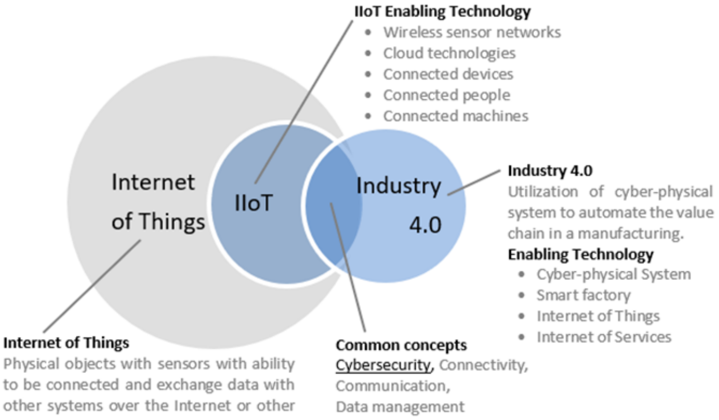
IIoT Enabling Technology
• Wireless sensor networks
• Cloud technologies
• Connected devices
• Connected people
• Connected machines
Internet of Things
IIoT
Industry 4.0
Industry 4.0
Utilization of cyber-physical system to automate the value chain in a manufacturing.
Enabling Technology
• Cyber-physical System
• Smart factory
• Internet of Things
• Internet of Services
Internet of Things
Physical objects with sensors with ability to be connected and exchange data with other systems over the Internet or other
Common concepts
Cybersecurity, Connectivity, Communication, Data management

Figure 1. Industry 4.0, IIoT and cybersecurity context

Security needs to be integrated into the design. After releasing the initial product, its software needs to be updated regularly to patch up new vulnerabilities. Data encryption will need to be improved in order to keep data safe, and employees will need to be trained to keep up with new security measures. Lack of awareness could be a problem, so both users and employees will need to be educated about the importance of cybersecurity.

Since the cybersecurity represent one of the biggest Industry 4.0 challenges thus, the purpose of this paper is to provide most recent advancement in cybersecurity for Industry 4.0. Therefore, the paper is structured as follow: Section 1.2.2 Section 2 explains methods that were used to choose the articles to be reviewed for this paper. Section 3 Results and Discussion, contains literature review with tables and diagrams with the actual article analysis. Ideas from the articles are grouped and combined into following topics: general information about Industry 4.0, hyperphysical systems, smart manufacturing, Internet of Things and cybersecurity for health system in Industry 4.0. At the end in section 4 conclusion is made.

2. Method applied in study

First database that was used to obtain sources used in this paper was sciencedirect.com. The key terms for search were "cybersecurity industry 4.0". The total number of results were 344. Among the article types that had these keywords were editorials, review articles, book chapters and research articles. After filtering the search results, two different diagrams were created in Excel to visually present the popularity of the topic and areas of research where the topic was present. To choose among the huge number of articles and decide which articles will be used in the paper, the relevancy "test" was performed. Relevancy was determined in the following way: the article had to have words "cybersecurity" and "industry 4.0" in its title, and it had to be written over the period of past few years.

Second part of the articles was found through Google Scholar, by searching the keywords "cybersecurity industry 4.0" and alternative version "security industry 4.0". Among many articles that passed relevancy test on google scholar, 16 of them were chosen.

Third database that was used for finding articles was Semantic Scholar, and it has turned out to be the one with the largest number of relevant recent studies.

Another way of finding articles was through the references of already chosen articles – if the article chosen was of good quality, it probably cited reliable, quality sources, so those were taken into the consideration as well, as long as they were written from 2015 onward.

Since the topic of the paper is focused on *current literature,* the spotlight was on the papers written in the period from 2015 to present, since the papers written before that period are most likely not relevant anymore, or not as relevant as the ones written in the past few years.

The first part of the actual research was to read the abstracts of articles, as well as summary/conclusion part of the article if it was available, since in many cases it provided information that was helpful in deciding whether the article was relevant to the topic and if it contained information that was worth including. After choosing the articles that would be reviewed for this paper, second step was to read full articles to gain better understanding of the topic. After that, main ideas were compared between different articles and important points in the articles were summarized. Information from articles were then grouped by similar topics.

3. Results and discussion

As found in the literature, topic of Cybersecurity for Industry 4.0 has been discussed/mentioned in 332 articles available there. Popularity of this topic has certainly increased over the years, as can be seen from Figure 2 below. Results from the first initial search are included in the diagram.

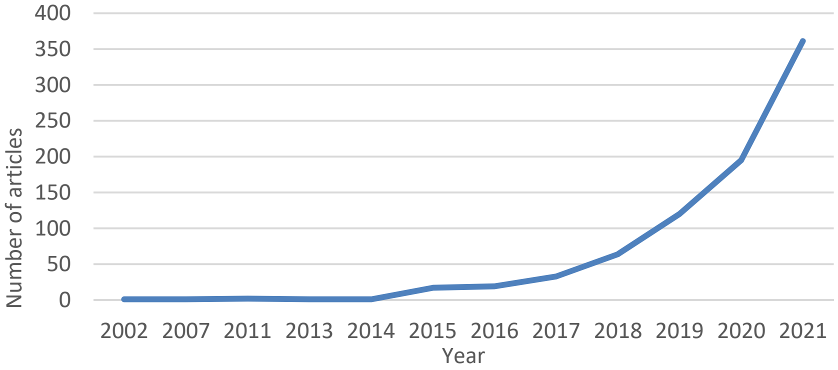

Figure 2. Topic popularity

Referring to Figure 2, it is observed that this research field is pretty young. The first paper publish was in 2002 but since 2016 the number of publications is gradually increasing from year to year.

Referring to Figure 2, it is observed that this field of research is quite new and emerging. The first work was published in 2002, but until 2015 there was no noticeable increase in the number of publications. Since 2016, the number of publications has been increasing significantly from year to year. Which is an indicator that the topic attracts more and more researchers from all over the world. Second diagram in

Figure 3 shows the research areas where this topic was mentioned/written about. As expected, Computer science, Engineering and Decision Science are most frequent scientific areas in which articles appeared.

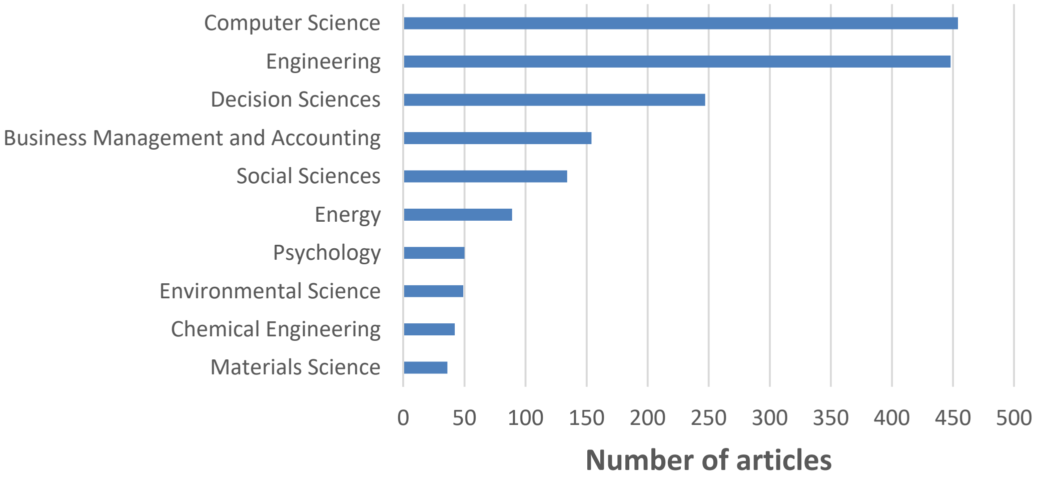

Figure 3. Areas of research

Below are shown tables that contain categorized research papers used in this review. Table 1 shows articles sorted by topic they were used for.

Table 1. Division by topic

Industry 4.0	Cyber-physical systems	Smart manufacturing	Internet of Things	Healthcare
Published article	[56] [32] [26] [17]	[59] [58] [57] [50] [33] [27] [25] [24] [18]	[65] [64] [63] [62] [61] [60] [37] [35] [34] [22] [21] [20] [19] [13] [12] [11] [9] [8] [6] [5]	[36] [66] [67] [68] [69] [70]

Results obtained from articles, threats that would cause problems and possible solutions are specified in the tables down below, together with the references where those were mentioned.

Table 2. Threats mentioned in articles

Threats and challenges	**References**
Lack of awareness	[45] [46] [47]
Lack of experts	[48][58]
Companies are unprepared	[60]
Large attack surface due to many entry points	[12][27][30] [68]
Vulnerable device connected to a network	[6][16][27][22]
Weak link in a supply chain	[25][59]
Unsafe data exchange	[23][26][49]
Stealing sensitive data for private benefit	[5][16][31][69][50][53][66][40][68] [70]
Blackmailing	[5][24]
DoS attacks	[13] [23] [61][6]
Harming safety of people	[51][16] [36][67] [68]
Financial harm	[5][16][52][69]
Default passwords	[21][34]
Unsafe updates, or lack of	[63] [12][35]
Interruption in providing services due to connection being lost	[11] [8]

Table 3. Solutions mentioned in articles

Solutions	**References**
Training employees, educating people	[48] [58] [15] [7] [3]
Security-by-design	[24] [15]
Security embedded in layers	[2] [3]
Identifying most vulnerable spots and putting extra protection there	[54] [17] [65] [41]
Prevention and detection techniques	[24] [15] [25]
Additional authorization and authentication	[4] [18]

Direct-to-machine data transfer	[18]
Computational and cyber threat intelligence	[54] [24]
Stronger encryption	[3] [63] [26]
Blockchain technology	[55]
High availability through redundancy	[8]
Controlled areas	[53] [40]
Ditching default passwords	[3] [62]
Encouraging reporting vulnerabilities	[3] [62]
Regular updates	[3] [64] [62]
Certifying cybersecurity technologies	[64]

1.1 Article analysis

It is worth noting that throughout the paper, terms “Industry 4.0”, “industrial internet of things (IIoT)” and “digital manufacturing” will be used interchangeably. “Industrial internet of things” is the same as “Industry 4.0” or the term “Smart manufacturing”, but it needs to be stated that industry 4.0 is a broader term than smart manufacturing is [38]. Even though cybersecurity is widely used word, the universal, standard definition for it doesn’t exist. It’s definitions vary and they can be subjective [44]. With that in mind, a couple of definitions are provided down below. The purpose of that is to show what meaning cybersecurity has in the further sections of this paper.

1. Definition by Public safety Canada: “The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability [10].”
2. Definition by Kaspersky, which is one of the leading companies that are taking care of cybersecurity: “Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security [42].”
3. Definition by US government: “Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information [43].”

Since vulnerability is mentioned very often throughout this paper, the definition of vulnerability is quoted as well. Vulnerability is: “Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [71].” Defense Advanced Research Projects Agency has stated that “Security Shield for Internet of Things” is among the 4 programs that are predicted to have impact bigger than the Internet had. This is probably due to the fact that IIoT connectivity will bring cybersecurity to another level because of the many non-traditional challenges it will face [28].

Among all the other challenges that Industry 4.0 will be facing, cybersecurity is one of the most serious ones. Since 4.0 introduces a lot of new concepts, it will not only have to deal with usual security problems that occur when certain system is connected to the internet, but it will also have to deal with security and privacy issues that will be unique and characteristic for Industry 4.0. That is what may make it harder to troubleshoot these problems, and unless these issues are properly taken care of, Industry 4.0 may not achieve its full potential [14]

In one of the surveys about digital manufacturing, companies were asked about largest challenge they are facing while implementing digital manufacturing. Only 18% stated they were concerned about data security [45]. Annual WEF report regarding global risks stated for year 2019 that unfortunately a lot of tech companies didn’t see “security by design” as their primary interest, but as something secondary-their main goal was, expectedly, to put their goods on the market. For 2019, cyber-attacks were listed as the 5th in the list of the "top 10 risks" by likelihood, and 7th by the impact it would have [46]. As for the 2020 report, cyber-attacks were ranked 8 by impact and 7 by likelihood [39].

It is important to raise the awareness of the importance of cybersecurity. If the idea of Industry 4.0 is implemented and the machines and different phases of the production are connected, then it is also necessary for all the workers who are involved in the process of production to be trained to understand and practice security requirements [15]. Right now in, in some environments cybersecurity is underestimated and is seen only as a "technical" problem, and many companies see it only as an additional, maybe even unnecessary cost that they are not eager to pay [47].

In one of the articles, it was mentioned how the security had the image of being a "trouble-maker" in traditional manufacturing environments [29]. However, cybersecurity in the Industry 4.0 has the opportunity to be seen as an enabler, something that could provide additional valuable services. Another article mentioned the same idea- cybersecurity produced opportunity for providing "additional services" in following way: due to cyber threats that come with new technologies, companies that are able to provide protection, security and reliability within their products can profit from that through "selling" those three promised features. However, developing technologies that would ensure the highest percentage of security may be pretty expensive, and if the awareness of importance of cybersecurity is not present, then the question is whether the customers would be willing to pay for such product [47].

Raising awareness is something that comes up whenever cybersecurity is mentioned. People will have to be trained to think of the cybersecurity intuitively. Just like a person checks left and right before crossing the street, it needs to become intuitive to check if the IoT device is secure enough, and that paying more for a secure device is worth it [7]. Another roadblock for adopting the Industry 4.0 security procedures beside lack of awareness is lack of security experts. People who already work in OT or IT security are experts in that area, but for Industry 4.0 they will need to be trained to work in new environments that Industry 4.0 brings with itself. There will also be need to raise awareness about security issues of new technologies, that are unlike any traditional security issues that they may have been facing. An ENISA recommendation for this is to raise awareness through training the employees and helping them transition, as well as educating the students through their courses about the importance of security in Industry 4.0, which would help with raising awareness and understanding [48]. Interconnecting different objects comes with a certain risk. In one of the articles, they give an example of business partners who are exchanging sensitive data [23]. Industry 4.0 should provide them with a safe space for the data exchange, however this space can be reached and attacked by outsiders, via DoS attacks that can interrupt the data flow and cause integrity issues.

Compared to systems that are not interconnected, systems in the IoT environment pose a bigger threat due to the larger surface for cyber-attacks [30]. Up to the recent days, number of entry points was rather restricted. This made cybersecurity a lot easier to deal with, but still there were a lot of cyber-attacks happening. With IIoT happening any time now, traditional security measures that were in practice until now will need to be changed and improved to correspond to the huge scale of IIoT. Companies will now be in need of security measures that cover the whole system and all of the many entry points they have, so security will need to be implemented among many layers [2]. Another article supports the layered security approach and gives its suggestions. The security measures for each layer that the article is recommending are following [3]:

- network layer: using firewalls, antiviruses, use more secured wireless network like WPA2 and not WEP, using encryption when transferring data to the cloud, using many SSID-s.
- Application layer: checking for CSRF vulnerabilities, as well as vulnerabilities in the versions of open-source libraries and third parties that an application is using, changing default password if an app is a service provided by some other company; using https, encryption, setting normal behavior which will help to later identify any abnormalities.
- Device layer: updating firmware on time, changing any default passwords and configurations, testing the device regularly.
- Physical layer: limiting access to certain areas by using secure keys/badges, using security cameras.
- Human layer: training employees regularly, educating users on how to secure their devices, encourage employees and users to report any vulnerabilities they may find, and reward them for doing so.

Among "the top ten privacy risks" are Information transfers that aren't secure enough, collecting information unrelated to the main function, and possibly forwarding that and other information to the third parties [49]. There are different types of sensitive data that could be stolen. One of the worst scenarios mentioned in one of the articles was attackers stealing the information that is crucial for product design- basically stealing ideas for new products, as well as the instructions for manufacturing that product. This could also lead to the emerging of more counterfeit products [50]. A threat can come from the inside as well. Employees who have access to the sensitive data can steal it and sell it to the outsider with the highest bid [31].

Cybersecurity is especially important when it comes to the idea of smart cities and buildings. Each building needs to be designed with security in mind, since all the systems will be connected. Control systems, security cameras, fire detectors, elevators, even electricity, and many other services that are provided could be compromised. The damages that could be done is interrupt in providing these services, which could harm safety of people and safety of sensitive information in the banks or other organizations. A way into the smart building could be hacking the most vulnerable spot, like smart TV, which wouldn't be hard since up to date there aren't any anti-virus/malware software for smart TVs [16]. As for the attacks on cars, they won't need to be physical- a connected vehicle will have connections to the cloud, wireless and Bluetooth connections that could be compromised, and through these connections an outsider could meddle with car controls. The center of attention for security and protection will need to be transitioned from the physical aspect to the cyber-attacks [51].

Cybersecurity attacks leave a mark on the financial state as well. Kaspersky lab conducted a worldwide survey in 2017, and reported that among the companies that endured cyber-attacks, 20% of them stated that harm on their finances has increased due to these attacks, and that lead them to increase their fund for cyber security systems [52]. To achieve a healthy and strong system that has effective cybersecurity, it is important to have cyber-attack prevention tactics, as well as detection methods and response procedures [25]. One of the solutions for physical control and data protection that was mentioned in two different articles was "controlled areas", also called protected areas [40] [53]. Rooms where sensitive information is spoken so it can be heard need to be protected so that no outsider could get access to the data. To prevent third partied from hearing sensitive data, sound insulation can be implemented for those rooms. To prevent radio and electromagnetic signals that contain sensitive data from getting beyond the walls of protected rooms, the electromagnetic shielding for the rooms could be implemented as well.

In order for the company to be ready to deal with cybercrime and defend from it, there are a couple of things they can do to ensure effective cybersecurity. A company needs to analyze what their most important assets are and then invest in protecting them. Cyber threat intelligence helps to prepare by analyzing when and where the threats could occur. There needs to be a constant improvement of cybersecurity. Topic of security needs to be a recurring element, a regular part of meetings and discussions [54].

General solution for protecting the system as whole would be to estimate in advance what are the most vulnerable and the most critical parts of the network that need to be protected [41]. They say that earlier systems did not give much thought to the cybersecurity during their design phase. And now a different approach is needed, where the security would be integrated in the design. Instead of focusing on responsive actions that would need to be taken after a cyber-attack, they propose focusing on preventive policies that would provide security from the start [15]. Some of the measures that can help with assuring security would be authorization of the software on the connected devices, authenticating the device prior to the data transfer to/from the cloud, and using firewalls [4]. A new approach to cybersecurity is using blockchain technology. It is famous for being used in bitcoin, and with its help, the transactions are more secure and safe. Users on the different ends of transaction don't have to trust each other, and after the transaction is confirmed, it isn't possible to reverse it. Due to its decentralized nature, blockchain is basically impossible to hack, which makes it safe and perfect to use in cybersecurity for Industry 4.0 [55].

3.1. Cyber – physical systems

Industrial Control Systems (ICS) is a part of cyber-physical systems. Well performing ICS present a solid foundation for the success of Industry 4.0. ICS are category of control systems that are used for handling and automatization of industrial processes. With bigger connectivity comes a bigger risk of cyber-attacks, which means that ICS will need better security. As one article noted, South-east Asia had the largest percentage of ICS infections in 2018-61% of their devices were attacked in H1 of 2018, and 57.8% in H2 of 2018 [56].

Number of articles suggest using CAD (computer aided design) in the process of creating cyber-physical model [32]. Together with offering a lot of amazing features, CAD model also comes with its own cybersecurity risks. One of the inevitable things regarding industry 4.0 is collaboration via cloud when developing new products. However, it is going to be a challenge to protect sensitive data about the model of a new product, if it is shared via cloud. One of the articles suggested using customized encryption for cloud-shared CAD models. There would be two different types of users, owner of the model and its collaborators.

The way that the encryption would work is the owner of the model would upload to the cloud CAD model in encrypted form, and then collaborators can download the encrypted model from the cloud and decrypt it [26].

Another article offers the steps for managing the cybersecurity risks. First thing is to identify those risks, by identifying weaknesses, as well as possible threats. Second is analyzing those risks, by determining how likely is it for such situation to happen, as well as determining the possible impact of the risk. Third would be evaluating risks. What would the magnitude of the risk be, is the risk acceptable? Last step are risk controls, and it would be performed by implementing controls for the risk [17].

3.2. Smart factory

The idea behind smart factory is to get more from the manufacturing by transitioning from the traditional way to the industry 4.0 way – creating a network of suppliers and a connected system that uses real-time data and adjusts the manufacturing so that the new demands can be met. That results with a system that is overall more efficient and that could rank better than the other competitors in market [57].

Smart factory, just like other parts of industry 4.0, will face certain challenges. Types of jobs that people will have in factory will evolve into something more complex, as the automation takes over the repetitive and dull jobs. Some may argue that automation presents a threat to the current job positions in manufacturing. However, the jobs will still remain, but the tasks that workers will do will change. Companies will need workers who will operate on new technologies that industry 4.0 will bring. Right now, they say that it’s hard to start implementing new digital technologies because there aren’t enough workers that have skills that are required to be able to run those technologies. Companies will eventually have to invest in training their employees and equipping them with skills needed to operate the new technologies. Apart from this challenge, another one will be dealing with cybersecurity [58]. Table presents summary of results on key cybersecurity challenges for cyber-physical system and smart factory.

Table 4. Key cybersecurity challenges for cyber-physical system and smart factory

Challenge	Result	Reference
Manufacturing processes as potential risk.	• Multiple connected suppliers may not have the same security levels. Probably smaller suppliers, will have weaker cybersecurity which will cause a threat to the rest of the connected suppliers. • An outside attacker could identify the weakest link and use it to get access to the rest of the suppliers. • 92% of overall cyber-attacks for a year happened in a smaller organization. This would be a scenario likely to happen with Smart manufacturing supply chains where outsiders would attack smaller companies because of their vulnerability, • interconnections come with a certain risk but solution maybe to limit the communication between the machines or separate the machines that are used for production from the personal computers that are on the same network.	[18], [25], [33], [50], [59].
Industrial Control Systems (ICS).	• South-east Asia had the largest percentage of ICS infections in 2018-61% of their devices were attacked in H1 of 2018, and 57.8% in H2 of 2018 • Collaboration via cloud when developing new products is challenge to protect sensitive data about the model of a new product • There would be two different types of users, owner of the model and its collaborators and the encryption would work CAD files uploaded to the cloud, and then collaborators can	[17], [26], [56].

Challenge	Result	Reference
	download the encrypted model from the cloud and decrypt it. • Risk identification, analysis, evaluation and control are necessarily phased of the risk management.	
Smart factory challenges.	• Companies have to be prepared for cybersecurity challenges such as: detection of viruses and malware before they get into system, and using computational intelligence for spotting and tracing threats like viruses and hackers that could lead to data manipulation, cyber stalking, blackmailing, executing terroristic acts, and other actions that may harm the system or parts of the system. • Industry 4.0 depends on data that is transmitted from sensors in real-time, which puts security at risk due to number of entry points that each network has and increases the potential number of weaknesses in the system and vulnerabilities that hackers may use. • Types of jobs that people will have in factory will evolve into something more complex, the jobs will still remain, but the tasks that workers will do will change. • Companies will need new talents who will operate on new digital technologies that industry 4.0 will bring. • Companies have to invest in training their employees and equipping them with skills needed to operate the new technologies.	[24], [27]., [58],

One of the articles says that security-by-design is mandatory for securing smart factories. It includes detection of viruses and malware before they get into system, and using computational intelligence for spotting and tracing threats like viruses and hackers that could lead to data manipulation, cyber stalking, blackmailing, executing terroristic acts, and other actions that may harm the system or parts of the system [24]. Industry 4.0 depends massively on data that is transmitted from sensors in real-time. That puts security at risk because of many entry points that each network has, and then all of those networks are interconnected as well. This increases the potential number of weaknesses in the system and vulnerabilities that hackers may want to take advantage of [27].

An example of a possible risk would be the connection of suppliers and their manufacturing processes [25]. Multiple suppliers are connected in a supply chain, and they probably will not have the same security levels-some of them, probably the smaller suppliers, will have weaker cybersecurity which will cause a threat to the rest of the suppliers that are connected to that chain. An outside attacker could identify the weakest link in the chain and use their weak security in order to get access to the rest of the suppliers. In one of the reports, it was stated that 92% of overall cyber-attacks for that year happened to the smaller organizations. This would be a scenario likely to happen with Smart manufacturing supply chains (unless the security is better taken care of than it is now), where outsiders would attack smaller companies because of their vulnerability, and since they represent the easiest entry into the chain, that would lead them to bigger companies that are their actual target.

These small companies would represent a risk for the bigger organizations since they could be easily attacked through them, despite the cybersecurity measures that they have accomplished in their own company [59]. Since interconnections come with a certain risk, one of the articles suggested that a solution would be to limit the communication between the machines, and limit the machines that can communicate with each other. Additionally, they could also separate the machines that are used for production from the personal computers that are on the same network, that way limiting the access [50].

Several solutions for protecting critical data are offered throughout these articles. One of the solutions discussed the situation when certain data would need to be transferred through different layers, until it finally reaches the machine that executes it. Solution would be to skip all the unnecessary carriers of that data, and transfer it directly to the machine, with help of authentication and authorization. It would also strip off any non-essential data – only the information that is required for the execution would be given to the machine [18]. Also it is important to remove the walls between information technology sector and operations technology sector, and have them share the information with each other, since these two are the sectors that will be crucial for effective defense of Industry 4.0. Focal point for IT is CIA-confidentiality, integrity and availability, and OT mostly puts focus on availability. Issue with OT is that they lack room for adding cybersecurity into the equation in a way that wouldn't have disadvantageous impact on production [33].

3.3. Internet of things

One of the articles argues that the security is the number one challenge of IIoT [19]. One of the surveys that was conducted among 400 experts from four countries UK, Germany, US and Japan, concluded the following:

- Regarding the IoT security, 75% stated it was important, however just 16% stated that the company they were working for is ready for it.
- Companies were generally not prepared for each part of the security ensuring action, which consists of predicting, preventing, detecting and reacting.
- Regarding the strategies for cybersecurity that can be applied to IoT as well, less than two thirds stated that they have one ready [60].

Another article notes that systems that are part of IoT should from the very beginning be designed with possibility of integrating it with the other systems [20]. Protection measures need to be taken regarding protecting 3 things: device security, data security and privacy of the user. To protect the security of device, it needs to be saved from engaging in Distributed Denial-of-Service (DDoS) attacks and harming devices that are connected to the same network as that device. Protecting data means taking care of Confidentiality, Integrity and Availability (CIA) of information on the IoT device, ensuring its security while its being transferred and analyzed. Protecting users' privacy means protecting the personally identifiable information that could possibly impact the user, either directly or indirectly [61].

Accountability is important when implementing security procedures since it distributes responsibilities and holds objects accountable for their actions. Accountability isn't enough to prevent cyber-attacks from happening on its own, but it does help to make sure that the rest of security methods, such as confidentiality or integrity are functioning well [9]. As availability is one of the key features that cybersecurity keeps safe, availability for the crucial devices needs to be as close to the 100% as possible. A very high percentage of availability at all times can be accomplished through redundancy, which in essence means that in case that one part fails to provide service, then there exists a backup of that same part that can provide service instead [8]. Possibility of losing connectivity could interfere with proper functioning of IoT device, and potentially reduce its security. Extreme case would be inability of the device to function without the connection to the Internet. Solution that BITAG proposes is to configure device in a way that it can still fulfill its main purpose even in case of losing the connectivity [11]. Table 5 shows summary of results related to IoT device cybersecurity.

Table 5. Review of key IoT device cybersecurity results

Challenge	Result	Reference
IoT devices mass production.	• Cost of producing IoT devices will decrease but update feature may be costly / impossible due to limited resources. • Updates of IoT devices are one of the possible places for the outsiders to attack. Updates need to be secured especially since they are usually arranged for a specific time slot and executed throughout the downtime. • More IoT devices means more entry points that can be hacked.	[12], [35], [37], [63], [65].

Challenge	Result	Reference
Unpreparedness for IIoT security.	• IIoT security is the number one challenge. • Protection measures have to include: device security, data security and privacy of the user. • Protecting data means taking care of Confidentiality, Integrity and Availability (CIA) of information on the IoT device,	[19], [20], [61].
Unpreparedness for IIoT security.	• 400 experts from UK, Germany, US and Japan concluded that 75% stated it was important, 16% stated they were working on it. • Companies were generally not prepared for each part of the security ensuring action, which consists of predicting, preventing, detecting and reacting • Regarding the strategies for cybersecurity that can be applied to IoT as well, less than two thirds stated that they have one ready.	[60].
Employees smart devices (shadow devices) connected to organization's network, without knowing of IT department.	• These shadow devices are a door for hackers for entering the organization's network. • 46% of organizations found shadow devices connected to their corporate network. • Only 25% of organizations haven't discovered any shadow devices connected to their network. • It will be possible to turn many IoT devices into botnets and use a massive army of modems, controllers, routers and other devices to execute a DDoS attack.	[13], [21], [22].
Default passwords.	• Default passwords for commercial IoT devices could usually be found online in less than half an hour. • Most users want to buy a new technology, but they are too lazy to read the user manual and check how to change password or restrict access.	[21], [34].
Home automation controllers and remote controllers for garage doors.	• Hackers use that data from these devices identify perfect timing for executing robberies. • Criminals from these data when the user is at home and when the garage doors are opened / closed.	[5].
Healthcare IoT devices.	• Healthcare infrastructure is among the most frequently targeted industries for cyber-attacks. • Hackers can attack IoT medical devices and send commands to the device and to stop them working. • These devices are vulnerable harming patient's privacy and breaking physician-patient confidentiality, and harming patients and possibly causing more health problems. • Medical information is attractive to attackers to be used to get	[36], [66], [67], [68], [69].

Challenge	Result	Reference
	prescription medication and drugs that can be sold on Darknet, or occasionally contains the data that can be used for opening new bank accounts or taking out loans.	
Insufficient law regulations regarding IoT devices.	IoT devices rules in UK law: • IoT devices passwords cannot be rosetted to the default factory settings. • IoT device manufacturer must come up with an easy and accessible way to contact them so that any new-found vulnerabilities and weaknesses in their products can be reported, and they have to respond in an appropriate amount of time. • IoT device manufacturer must declare minimum time before the device software becomes outdated and needs to be updated.	[62].
Certification of IoT technologies.	• European cybersecurity organization came up with the idea to certificate • IoT devices are always changing and in need of regular updates that would fix new-found vulnerabilities. • A one-time security certificate is not sufficient thus it has to be adjusted to implement an agile procedure for certificating such systems, that would make sure that its cybersecurity is updated and suited for the system at each point throughout its lifespan.	[64].

Veracode conducted a study where it inspected six new always-on household IoT devices, most of them being controller device for home automation, and remote controllers for switches, garage doors and outlets. They found many vulnerabilities in the devices. One of the results said that hacking the data from home automation controllers and remote controllers for garage doors, criminals could know the pattern of when the user is at home or when the garage doors are opened and closed, and they could use that data to find perfect timing for executing robberies. Hacking into a central control device would enable them to set the microphone on so they can hear sensitive information that they can steal, or information they can later use for blackmailing [5].

One of the threats for the IoT, that is already happening at this time are shadow devices. Basically, employees of a company bring their smart watches or fitness trackers which are IoT devices with themselves to the work, and then connect them to the organization's network, without IT department knowing about it. They are usually not aware that those products pose a threat by being unregistered IoT device connected to the network. These devices can be used by hackers as a door for entering the network and committing cyber-crimes. Infoblox reported that in the previous year 46% of organizations found these shadow devices connected to their corporate network. Only 25% haven't discovered any shadow devices to be connected to their network [22]. If one device has weak points in its security, then it could put the whole network that it is connected to at risk. If that device is hacked, it can be used for DDoS attacks. Since IoT will enable a lot of devices connected to a network, it would mean that hacker would get the opportunity to recruit a big number of targets from one network and use them for attacks [6]. Another article claims the same thing, it will be possible to turn many IoT devices into botnets and use the massive army of modems, controllers, routers and other devices to execute a DDoS attack [13].

Another issue are passwords. Users are not aware of importance of the security of their devices. Most of them just want to buy and use the new technology, but are too lazy to read the user manual and check how to change password or restrict access [21]. Researchers have found that default passwords for commercial IoT devices could usually be found online in less than half an hour. The intention behind that was probably to make it easier for the user to set up their device, however the issue here is that the hackers can easily find this password too, and since users aren't too keen on changing the default password, hackers have even more chance to easily take advantage of this "password protected" device. Another problem that was found was that devices that were produced by same companies had the same default passwords. The worst scenario is if it is impossible to change the password, because then the whole idea of password doesn't make any sense [34]. Law regulations in UK will make it mandatory for IoT devices sold in UK to oblige to these 3 rules:

1. All of the devices will need to have one-of-a-kind passwords that cannot be rosetted to the default factory settings.
2. Producers of these devices have to come up with an easy and accessible way to contact them so that any new-found vulnerabilities and weaknesses in their products can be reported, and they have to respond in an appropriate amount of time.
3. Producers have to declare minimum time before the device's software becomes outdated and needs to be updated [62].

One article notes that cost of producing IoT devices will decrease, and huge number of the devices will be produced, and more IoT devices means more entry points that can be hacked. Since update feature can be costly, or impossible due to the resource restrictions, new-found vulnerabilities will not be possible to fix. And if update is obtainable, some companies do not seem to be using encryption when downloading them to the devices, and all of these things pose a serious threat to the security of these devices [12].

Another article agrees that it would be a huge threat to the security of device if it cannot receive an update once a vulnerability is identified. Another threat is if the data is in the clear text form while being transferred across the cloud, apps and networks. There needs to be a secure encryption for the data transfer to eliminate the possible threats of data stealing and manipulation [63]. One more article agrees that updates for IoT devices are one of the possible places for the outsiders to attack, especially since they are very different from the traditional updates that we have now. These updates need to be secured especially since they are usually arranged for a specific time slot and executed throughout the downtime [35].

European cybersecurity organization came up with the idea to certificate IoT cybersecurity technologies. IoT devices and systems are dynamic, always changing and in need of regular updates that would fix new-found vulnerabilities. Due to these characteristics, a one-time security certificate could be of short lifetime, so strategy would be to adjust the certification to these characteristics and implement an agile procedure for certificating such systems, that would make sure that its cybersecurity is updated and suited for the system at each point throughout its lifespan [64].

One of the researchers claims that many household devices will become IoT devices, even though they would not need to be. The cost of producing a smart device using a chip will be only a dime. Since the cost will be so low, manufacturers will try to turn as many of these devices into smart ones, not for the benefits of users, but so that they can collect data with those chips [37]. Some argue that certain types of IoT devices should have increased security. Such devices are high risk IoT devices like ones made for children. Vulnerable people like children would not know how to deal with compromised devices, and they probably would not realize that they should report it. Another example of high-risk devices would be ovens and thermostats. If attacked, these devices could make more harm than other devices that are not high-risk [65].

3.4. Healthcare

IoT devices can do a lot of good in healthcare by providing a more efficient diagnosing of the patients and collecting accurate data on patients' status. However, these devices are also vulnerable to potential cyber-attacks which would lead to harming patient's privacy and breaking physician-patient confidentiality [66]. One of the threats that healthcare faces are attacks on their medical devices, services they provide and their infrastructure, that could affect safety and well-being of their patients, indirectly harming them and possibly causing more health problems, and in worst case scenario, even death [67]. Reports have shown that healthcare infrastructure is among the most frequently targeted industries for cyber-attacks. Right now, each bed in a hospital is connected to up to 15 different medical devices that can be furtherly interconnected, which is already a relatively big number of entry points. Hackers exploit these points to get access to the data, and potentially to harm the patients. When the IIoT time comes, the surface available for cyber-attacks will only grow bigger, so healthcare is one of the industries that are going to need cybersecurity the most [68]. One of the reasons why hackers may attack healthcare systems is for financial benefit. It may be generally unknown, but data from the healthcare has bigger worth than other type of data. These illegally obtained medical identities are later utilized to get prescription medication and drugs that can be sold on Darknet. Medical information occasionally contains the data that can be used for opening new bank accounts or taking out loans [69].

One of the parts of Industry 4.0 will be Smart Connected Health. It would lower the price of medical treatments, help to identify any abnormal changes in the patient through analysis of collected data, and generally boost the efficiency of the whole system. However, using IoT medical devices can also be dangerous since it could be possible for hackers to attack them and send commands to the device to stop working. This can be very harmful since certain devices, like cardiac devices are crucial for keeping a patient alive [36]. One of the studies has shown that during the period of time 2013-2017, 1512 data breaches happened in the USA, which affected records of 154 415 257 patients. Even though the percentage of data breaches caused by hacking incidents was below 25%, it was found that hacking was accountable for almost 85% of the records that were affected. And this happened in the time when IoT was not there yet. As healthcare gets to implement the IoT technologies in the future, the incidents may get worse, unless the healthcare implements very strong cybersecurity technologies [70].

4. Conclusions

Development of new technologies is what led to the Industry 4.0. Through making machines smarter, interconnecting them and combining cyber and physical systems, industry 4.0 will soon face its blooming phase. It will also face some challenges like cybersecurity that will force it to furtherly improve.

This paper reviewed selected articles that discuss the cyber threats that Industry 4.0 will most likely face, as well as the possible solutions. Some of the threats for cybersecurity include lack of awareness, security not being incorporated into the design, poor encryption, default passwords and over-the-air updates. Major problems that Industry 4.0 will probably face are lack of experts on cybersecurity areas, stealing and manipulation of sensitive data, vulnerable points in the network chain that put the whole network at risk, DDoS attacks, as well as other types of cyber-attacks.

Healthcare may face one of the more serious problems, where the health and safety of the patients might be compromised, beside their data that may be stolen. Apart from these challenges, there are also some good news and solutions for some of these problems. Some of them are layered security approach, stronger encryption, more frequent authentication and authorization of devices, as well as prevention, detection and response mechanisms regarding cyber-attacks. Suggestions include analyzing the system and detecting its vulnerable points and adding extra security around those. Through creating cyber-attack scenarios, companies will be able to identify possible breaches and find a way to stop them before they happen. And lastly, implementing law regulations that would guard the satisfactory security levels in the devices and certificating the cybersecurity software.

One of the possible directions for the future research would be investigating how blockchain technology can be used for implementing better cybersecurity. Hyper connectivity is a double-edged sword – it will put many things at hand and help with efficiency of manufacturing and living in general, but it will also increase safety risks. As the Industry 4.0 is a growing industry, many more problems will emerge and new solutions will need to be found.

Declaration of competing interest

The authors declare that they have no any known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

References

[1] D. Mukerji, "Industry 4.0 Defined: 4 Core Components," 2018. [Online]. Available: https://kingstar.com/industry-4-0-defined-4-core-components/. [Accessed: 24-May-2020].

[2] "Industry Agenda In collaboration with Accenture Industrial Internet of Things: Unleashing the Potential of Connected Products and Services," 2015.

[3] B. Russell *et al.*, "Security Guidance for Early Adopters of the Internet of Things (IoT)," *Mob. Work. Gr. Peer Rev. Doc.*, no. April, pp. 1–54, 2015.

[4] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, 2016, pp. 336–341, doi: 10.1109/ICITST.2015.7412116.

[5] O. Charlie, "Internet of Things devices lack fundamental security, study finds," *ZDNet*, 2015. [Online]. Available: http://www.zdnet.com/article/internet-of-things-devices-lack-fundamental-security-study-finds/.

[6] "Privacy & Security in a Connected World FTC Staa Report," 2015.

[7] D. Palmer, "IoT security: Why it will get worse before it gets better," *ZDNet*, 2018. [Online]. Available: https://www.zdnet.com/article/iot-security-why-it-will-get-worse-before-it-gets-better/.

[8] J. P. Nzabahimana, "Analysis of security and privacy challenges in Internet of Things," in *Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018*, 2018, pp. 175–178, doi: 10.1109/DESSERT.2018.8409122.

[9] S. Aouad, A. Maizate, and A. Zakari, "Cyber Security and the Internet of Things : vulnerabilities and Security requirements," *Aouad Cyber Secur. Internet Things 1 Mediterr. Telecommun. J.*, vol. 9, no. 2, 2019.

[10] "Security and Prosperity in the Digital Age: Consulting on Canada's Approach to Cyber Security." [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/index-en.aspx. [Accessed: 01-Jun-2020].

[11] "Internet of Things (IoT) Security and Privacy Recommendations," 2016.

[12] R. H. Weber and E. Studer, "Cybersecurity in the Internet of Things: Legal aspects," *Comput. Law Secur. Rev.*, vol. 32, no. 5, pp. 715–728, Oct. 2016, doi: 10.1016/j.clsr.2016.07.002.

[13] D. Palmer, "History repeating: How the IoT is failing to learn the security lessons of the past," *ZDNet*, 2016. [Online]. Available: https://www.zdnet.com/article/history-repeating-how-the-internet-of-things-failed-to-learn-the-security-lessons-of-the-past/.

[14] L. Thames and D. Schaefer, "Cybersecurity for Industry 4.0," no. May, pp. 1–33, Apr. 2017, doi: 10.1007/978-3-319-50660-9.

[15] T. Pereira, L. Barreto, and A. Amaral, "Network and information security challenges within Industry 4.0 paradigm," *Procedia Manuf.*, vol. 13, pp. 1253–1260, 2017, doi: 10.1016/j.promfg.2017.09.047.

[16] R. Khatoun and S. Zeadally, "Cybersecurity and privacy solutions in smart cities," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 51–59, Mar. 2017, doi: 10.1109/MCOM.2017.1600297CM.

[17] D. Glavach, J. LaSalle-DeSantis, and S. Zimmerman, "Applying and Assessing Cybersecurity Controls for Direct Digital Manufacturing (DDM) Systems," 2017, pp. 173–194.

[18] A. Wegner, J. Graham, and E. Ribble, "A New Approach to Cyberphysical Security in Industry 4.0," 2017, pp. 59–72.

[19] L. Thames and D. Schaefer, "Industry 4.0: An Overview of Key Benefits, Technologies, and Challenges," 2017, pp. 1–33.

[20] J. Mehnen *et al.*, "Practical Security Aspects of the Internet of Things," 2017, doi: 10.1007/978-3-319-50660-9_9.

[21] D. Palmer, "Internet of Things security: What happens when every device is smart and you don't even know it?," *ZDNet*, 2017. [Online]. Available: https://www.zdnet.com/article/internet-of-things-security-what-happens-when-every-device-is-smart-and-you-dont-even-know-it/.

[22] D. Palmer, "Rogue IoT devices are putting your network at risk from hackers | ZDNet," *ZDNet*, 2020. [Online]. Available: https://www.zdnet.com/article/rogue-iot-devices-are-putting-your-network-at-risk-from-hackers/. [Accessed: 06-Feb-2020].

[23] J. E. Rubio, R. Roman, and J. Lopez, "Analysis of cybersecurity threats in Industry 4.0: the case of intrusion detection," 2018.

[24] H. He *et al.*, "The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence," in *2016 IEEE Congress on Evolutionary*

Computation, CEC 2016, 2016, pp. 1015–1021, doi: 10.1109/CEC.2016.7743900.

[25] L. Thames and D. Schaefer, *Cybersecurity for Industry 4.0*, no. May. Cham: Springer International Publishing, 2017.

[26] X. T. Cai, S. Wang, X. Lu, and W. D. Li, “Customized Encryption of CAD Models for Cloud-Enabled Collaborative Product Development,” 2017, pp. 35–57.

[27] P. Eden *et al.*, “SCADA System Forensic Analysis Within IIoT,” 2017, pp. 73–101.

[28] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” *Digit. Commun. Networks*, vol. 4, no. 2, pp. 118–137, Apr. 2018, doi: 10.1016/j.dcan.2017.04.003.

[29] A. Becue *et al.*, “CyberFactory#1 — Securing the industry 4.0 with cyber-ranges and digital twins,” in *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2018, vol. 2018-June, pp. 1–4, doi: 10.1109/WFCS.2018.8402377.

[30] M. L, M. E, and M. A, “Cybersecurity Management for (Industrial) Internet of Things: Challenges and Opportunities,” *J. Inf. Technol. Softw. Eng.*, vol. 08, no. 05, 2018, doi: 10.4172/2165-7866.1000250.

[31] L. Urquhart and D. McAuley, “Avoiding the Internet of Insecure Industrial Things,” 2018, doi: 10.1109/TII.2014.2300753.

[32] J. Sini, M. Violante, and R. Dessi, “Computer-Aided Design of Multi-Agent Cyber-Physical Systems,” in *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, 2018, vol. 2018-September, pp. 677–684, doi: 10.1109/ETFA.2018.8502448.

[33] S. J. Shackelford, “Smart Factories, Dumb Policy?: Managing Cybersecurity and Data Privacy Risks in the Industrial Internet of Things,” *SSRN Electron. J.*, Oct. 2018, doi: 10.2139/ssrn.3252498.

[34] O. Shwartz, Y. Mathov, M. Bohadana, Y. Elovici, and Y. Oren, “Opening Pandora’s box: Effective techniques for reverse engineering IoT devices,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, vol. 10728 LNCS, pp. 1–21, doi: 10.1007/978-3-319-75208-2_1.

[35] European Union Agency for Network and Information Security, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, no. November. 2018.

[36] K. Sha, W. Wei, T. Andrew Yang, Z. Wang, and W. Shi, “On security challenges and open issues in Internet of Things,” *Futur. Gener. Comput. Syst.*, vol. 83, pp. 326–337, Jun. 2018, doi: 10.1016/j.future.2018.01.059.

[37] Danny Palmer, “Internet of Things security: What happens when every device is smart and you don’t even know it? | ZDNet,” *March 20, 2017*, 2017. [Online]. Available: https://www.zdnet.com/article/internet-of-things-security-what-happens-when-every-device-is-smart-and-you-dont-even-know-it/.

[38] V. Sklyar and V. Kharchenko, “ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios,” in *Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*, 2019, vol. 2, pp. 1046–1049, doi: 10.1109/IDAACS.2019.8924452.

[39] “The Global Risks Report 2020 Insight Report 15th Edition.”

[40] G. Breda and M. Kiss, “Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas &amp; Industrial Security,” *Procedia Manuf.*, vol. 46, pp. 580–590, 2020, doi: 10.1016/j.promfg.2020.03.084.

[41] A. Corallo, M. Lazoi, and M. Lezzi, “Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts,” *Computers in Industry*, vol. 114. Elsevier B.V., p. 103165, 01-Jan-2020, doi: 10.1016/j.compind.2019.103165.

[42] “What is Cyber Security? | Definition, Types, and User Protection | Kaspersky.” [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Accessed: 01-Jun-2020].

[43] “What is Cybersecurity? | CISA,” 2019. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-001. [Accessed: 01-Jun-2020].

[44] R. Purse, D. Craigen, and N. Diakun-Thibault, “Defining Cybersecurity.” .

[45] “How to achieve and sustain the impact of digital manufacturing at scale | McKinsey,” 2017. [Online]. Available: https://www.mckinsey.com/business-functions/operations/our-insights/how-to-achieve-and-sustain-the-impact-of-digital-manufacturing-at-scale. [Accessed: 03-Jun-2020].

[46] *The Global Risks Report 2019 14th Edition Insight Report*. 2019.

[47] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, “Addressing Industry 4.0 Cybersecurity Challenges,”

IEEE Eng. Manag. Rev., vol. 47, no. 3, pp. 79–86, Sep. 2019, doi: 10.1109/EMR.2019.2927559.

[48] ENISA, “Enisa Lists High-Level Recommendations To Different Stakeholder Groups in Order To Promote Industry 4.0 Cybersecurity and Facilitate Wider Take-Up of Relevant Innovations in a Secure Manner. 2 Industry 4.0 Cybersecurity: Challenges & Recommendations,” 2019.

[49] “OWASP Top 10 Privacy Risks.” [Online]. Available: https://owasp.org/www-project-top-10-privacy-risks/. [Accessed: 01-Jun-2020].

[50] I. Heritage, “Protecting Industry 4.0: challenges and solutions as IT, OT and IP converge,” *Netw. Secur.*, vol. 2019, no. 10, pp. 6–9, Oct. 2019, doi: 10.1016/S1353-4858(19)30120-5.

[51] H. He, “Security Challenges on the Way Towards Smart Manufacturing – IoT Security Foundation,” 2015. [Online]. Available: https://www.iotsecurityfoundation.org/security-challenges-on-the-way-towards-smart-manufacturing/. [Accessed: 01-Jun-2020].

[52] “Worried about IoT, but hit by malware: Kaspersky Lab reveals industrial organization pain points | Kaspersky,” 2018. [Online]. Available: https://www.kaspersky.com/about/press-releases/2018_ics-cybersecurity. [Accessed: 01-Jun-2020].

[53] M. Kiss, G. Breda, and L. Muha, “Information security aspects of Industry 4.0,” *Procedia Manuf.*, vol. 32, pp. 848–855, 2019, doi: 10.1016/j.promfg.2019.02.293.

[54] “EY Cybersecurity and the Internet of Things,” 2015.

[55] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, “Internet of things security: A top-down survey,” pp. 199–221, 2018, doi: 10.1016/j.comnet.2018.03.012ï.

[56] Y. S. Tiong, “The Need For Better ICS Cybersecurity - IAA - Industrial Automation,” 2019. [Online]. Available: https://www.iaasiaonline.com/the-need-for-better-isc-cybersecurity-2/. [Accessed: 28-May-2020].

[57] “The smart factory Responsive, adaptive, connected manufacturing A Deloitte series on Industry 4.0, digital manufacturing enterprises, and digital supply networks,” 2017.

[58] “What is the Smart Factory and its Impact on Manufacturing?,” 2019. [Online]. Available: https://ottomotors.com/blog/what-is-the-smart-factory-manufacturing. [Accessed: 27-May-2020].

[59] T. White, “Cyber-security risks in the supply chain,” 2019.

[60] “Six ways CEOs can promote cybersecurity in the IoT age | McKinsey,” 2017. [Online]. Available: https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age#. [Accessed: 03-Jun-2020].

[61] K. Boeckl *et al.*, “NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,” 2019, doi: 10.6028/NIST.IR.8228.

[62] D. Palmer, “IoT security: Your smart devices must have these three features to be secure,” *ZDNet*, 2020. [Online]. Available: https://www.zdnet.com/article/iot-security-your-smart-devices-must-have-these-three-features-to-be-secure/.

[63] “Data Security Threats to the Internet of Things,” 2015. [Online]. Available: https://www.parksassociates.com/blog/article/data-security-threats-to-the-internet-of-things. [Accessed: 01-Jun-2020].

[64] S. N. Matheu, J. L. Hernandez-Ramos, and A. F. Skarmeta, “Toward a Cybersecurity Certification Framework for the Internet of Things,” *IEEE Secur. Priv.*, vol. 17, no. 3, pp. 66–76, May 2019, doi: 10.1109/MSEC.2019.2904475.

[65] “(5) (PDF) Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age | Charlotte A Tschider - Academia.edu,” 2018. [Online]. Available: https://www.academia.edu/36014158/Regulating_the_IoT_Discrimination_Privacy_and_Cybersecurity_in_the_Artificial_Intelligence_Age. [Accessed: 02-Jun-2020].

[66] A. Razaque *et al.*, “Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain,” *IEEE Access*, vol. 7, pp. 168774–168797, 2019, doi: 10.1109/ACCESS.2019.2950849.

[67] Y. Ahmed, S. Naqvi, and M. Josephs, “Cybersecurity Metrics for Enhanced Protection of Healthcare IT Systems,” 2019.

[68] A. Alsuwaidi, A. Hassan, F. Alkhatri, H. Ali, M. QbeaaH, and S. Alrabaee, “Security Vulnerabilities Detected in Medical Devices,” in *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, 2020, pp. 1–6, doi: 10.1109/URC49805.2020.9099192.

[69] P. Lynne Coventry and D. Branley, “Cybersecurity in healthcare: a narrative review of trends, threats and ways forward,” doi: 10.1016/j.maturitas.2018.04.008.

[70] J. G. Ronquillo *et al.*, “Brief Communication Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information,” doi: 10.1093/jamiaopen/ooy019.

[71] R. M. Blank *et al.*, “Information Security Continuous Monitoring (ISCM) for federal information systems and organizations,” 2011.