Cybersecurity in Distributed Industrial Digital Twins: Threats, Defenses, and Key Takeaways

Sani M. Abdullahi[a,†], Ashkan Zare[a], and Sanja Lazarova-Molnar [a,b]

[a] *Maersk Mc-Kinney Moller Institute, University of Southern Denmark, Campusvej 55, Odense 5230, Denmark*
[b] *Institute AIFB, Karlsruhe Institute of Technology, Kaiserstr. 89, Karlsruhe, 76133, Germany*

Abstract

Distributed Digital Twins are designed to enhance the intelligence, predictability, and optimization of industrial assets by actively engaging, synchronizing, and collaborating with their physical counterparts, i.e., the systems they model, in near real time. This interoperability allows for seamless connections between real systems and their virtual counterparts, thereby facilitating the flow of data while aggregating vital information for comprehensive insights across large entities. However, the constant exchange of data and dependency on the information technology and operations technology process integrations in these complex distributed systems give rise to various cyber-security challenges. These include threats to data, unauthorized accesses, as well as threats to the integrity and reliability of the digital tools and the services they offer, among others. In this paper, we discuss the relevant cyber-threats within distributed Digital Twins ecosystems, which we then analyze while outlining different strategies to mitigate such threats. As a result, we present key takeaways toward a secure and reliable Digital Twin platform. Finally, different challenges are raised to highlight the status quo on the security of Digital Twins and areas for improvement.

Keywords

Distributed ditigal twins, cybersecurity, cyberthreats, defense mechanisms, manufacturing

1. Introduction

According to the initial goals of Industry 4.0, the integration of new information technology (IT) and operation technology (OT) paradigms into manufacturing, healthcare, automation, production, and logistics is currently underway [1]. This has led to the inception of some advanced technologies such as AI, big data, IIoT, fog computing, edge computing, etc. However, one of the most notable amongst such technologies within Industry 4.0 is the Digital Twin (DT). The primary objective of a DT is to predict impacts of errors, variations, and significant deviations that could affect the inherent behavior of a system by transforming physical assets into digital data representations via specification-based methods [2-4], computational models [5, 6], and application programming interfaces (APIs) [7]. These methods operate on servers, virtual machines, virtual networks, and containers. Consequently, these servers establish connections with physical elements so that they can engage in interaction with real-world assets [8]. As a result, Grieves [9] identifies a DT with three primary spaces, including physical, digital, and communication, while Kritsinger et al. [10] identify three different types of mirroring systems, including digital model, digital shadow, and Digital Twin. All mirroring systems depict the in-depth characterization of DTs through their integration with algorithms, networked systems, and different technologies to make decisions that enable autonomous actions on physical entities.

Up to this point, the practical usefulness of DTs has been demonstrated in several situations, such as industry [11, 12], military field [13], smart cities [14], and disaster management [15]. Such usefulness

DiDiT 2024: 1st International Workshop on Distributed Digital Twins, June 17, 2024, Groningen, the Netherlands
†Corresponding author
saa@mmmi.sdu.dk (S.M. Abdullahi); zare@mmmi.sdu.dk (A. Zare); slmo@sdu.dk (S. Lazarova-Molnar)
0000-0003-4962-2794 (S. M. Abdullahi); 0000-0002-7351-709X (A. Zare); 0000-0002-6052-0863 (S. Lazarova-Molnar)

of DTs in different application domains has attracted a plethora of private and public economic sectors, as well as researchers and experts. However, insufficient investigation into cybersecurity concerns persists, posing a dilemma for two primary reasons: i) Due to the involvement of DTs in automation processes [9], they are regarded as critical systems; and ii) DTs harbor private intellectual property that serves as a digital replica of the physical real-world systems [16]. An attacker seeking to compromise an industry's model will end up tarnishing its prestige or inflicting irreversible harm, especially with regard to critical infrastructure. To seize control of the fundamental infrastructure and its physical assets, an adversary may also cause damage to the DT from the digital space, as is evident when contemplating a general DT scenario [8]. This is a result of the DT paradigm's interconnectedness and reliance on algorithms, cloud, and communication systems from the IT realm and cyber physical technologies from the OT realm, which ends up linking the two and exposing it to more cyberthreats. Moreover, this obviously suggests that the attack surface within the DT ecosystem is extremely diverse. As such, the importance of cybersecurity for industrial Digital Twin cannot be overlooked.

To shed more light on possible solutions regarding the plethora of cyberthreats that can inflict irreparable damage to DTs, in this paper, we analyze the different cyberthreats within the DT ecosystem while outlining some recent mitigation strategies. Moreover, we itemize key takeaways from our exploration to ensure a secure and hitch-free deployment of DTs. In light of this, the remaining sections of the paper are organized as follows: Section 2 provides background on the use of DT in industrial domains as well as the role of cybersecurity in such DT in industrial environments. Section 3 discusses the potential cybersecurity threats in industrial DT while delineating the recent strategies put forward to mitigate such threats. Section 4 provides key takeaways from this overview to pave the way for future research. In addition, different challenges will be given in Section 5, while Section 6 finally draws the conclusion.

2. Background

2.1. Distributed DTs and their use in industry

Since the Second World War, when computer simulation was first used [17], it has developed and become a powerful tool and a key enabler in productivity, safety, optimization, and decision making in industry today. In the early 2000s, Grieves introduced the concept of digital DT, a more complex near real-time simulation model, representing the actual physical system in the virtual world throughout its lifecycle [18]. From the time when Digital Twin was first defined, it has taken different definitions depending on the application and the specific use cases. The three essential characteristics in these definitions are: the physical object in the real world, the virtual representation of the object, and the bidirectional exchange of data between the two objects [19]. In general, a Digital Twin can be defined as “a virtual representation of a physical system (and its associated environment and processes) that is updated through the exchange of information between the physical and virtual systems” [20]. Moreover, depending on the automation level of data exchange between the two systems, DTs can also be further categorized as digital models (manual data flow), digital shadows (one-way automatic data flow), and Digital Twins (complete automatic data flow) [10].

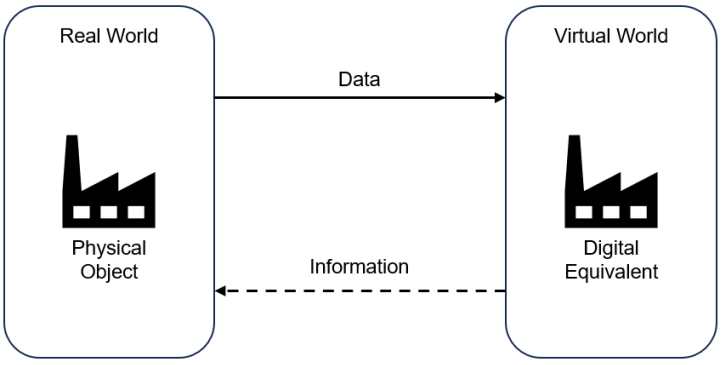

Figure 1: Digital Twin concept proposed by Grieves

Technological advancements, especially in Internet of Things (IoT) and sensor technologies, have aided in realization of DT with automatic data flow as evident by the rapid growth in research and application of DTs during the past decade [21]. Today, many industries benefit from the implementation of DTs such as: aerospace, energy, agriculture, and manufacturing [22, 23]. The aerospace field, driven by NASA, was the first industry to use DTs in performance optimization [24]. Energy and healthcare industries have also utilized the capabilities of DTs for maintenance monitoring [25], and productivity improvements [26]. More significantly, the vast applications of DTs in manufacturing industry show DTs‘ pivotal role as a key catalyst in moving the industry towards smart manufacturing and Industry 4.0 [27]. DTs facilitate manufacturing testing and validation [28], as well as automation integration [29] leading to production optimization and reliability improvements. Figure 1 illustrates DT’s concept.

2.2. Cybersecurity in industry

As increasing number of industries transition to the digital environment and integrate their operations online, cybersecurity is expanding into a more comprehensive and broader discipline. This indicates that, apart from cybersecurity representing an industry on its own, there are cybersecurity requirements in virtually every industrial sector. The notion of security has evolved beyond the typical hacker symbolism of constantly crafting malicious code and breaking into systems; cybersecurity as a discipline now incorporates a vast range of interdependent skills that collaborate harmoniously. These skills include information security, network security, digital forensics, cloud security, critical infrastructure security, and application security, among others.

With the growing interconnectedness of IT-OT paradigms in industry, the potential vulnerabilities to cyberattacks also expands. It is worth noting that such IT-OT integration is exacerbated by the transformation of traditional industrial manufacturing systems into contemporary industrial cyber-physical systems, which consequently necessitates the adoption of new technologies such as Digital Twins that are complex and distributed in nature. Reports on industrial risk evaluations indicate that this transformation has resulted in the emergence of several novel threats [30], which has further been proven by the recent analysis on the distribution of cyberattacks across industries worldwide [31]. According to the study, manufacturing sector experienced the greatest proportion of cyberattacks among the world's leading industries in 2022, with cyberattacks targeting manufacturing industries comprising approximately 25% of the overall attacks during the year under study, with a total global market size expected to project at an annual compound growth rate of 12.3% from 2023 to 2030 [32].
To establish an intelligent manufacturing setting based on automated decision making and problem solving according to Industry 4.0 requirements, it is necessary to use innovative technologies that can provide spontaneous connections between all industrial tools and devices within a manufacturing ecosystem and the web, such as distributed DT, AI, IIoT, CPS, big data, etc. Moreover, Industry 4.0 promotes the use of these technologies to facilitate decentralized communication between systems rather than just depending on conventional cloud servers or other centralized frameworks [1, 33]. Incorporating this diverse range of technologies within industrial cyberspace necessitates the prioritization of cybersecurity issues in their design approach. While Industry 4.0 has proven to enhance manufacturing efficacy and productivity, intrusions and breaches through cyberattacks can have severe consequences for industrial operations, thus leading to the loss of sensitive information and credibility [34]. Figure 2 depicts the interoperability between different novel technologies within the I4.0 ecosystem that are vulnerable to cyberthreats.

Recent works on cybersecurity vulnerabilities in various industries and their possible defense mechanisms include the works of Aoun et al. [35], where the authors explore the future prospects of blockchain technology as a means of strengthening I4.0 industrialization. With the addition of novel functionalities, they determine which domains of blockchain technology can enhance the implementation and efficiency of I4.0, especially in terms of cybersecurity. In [36], the authors elucidate the need for adopting a dynamic cybersecurity approach in response to the demands of Industry 4.0. They analyze the limitations of present techniques and highlight the growing significance of integrating novel approaches.

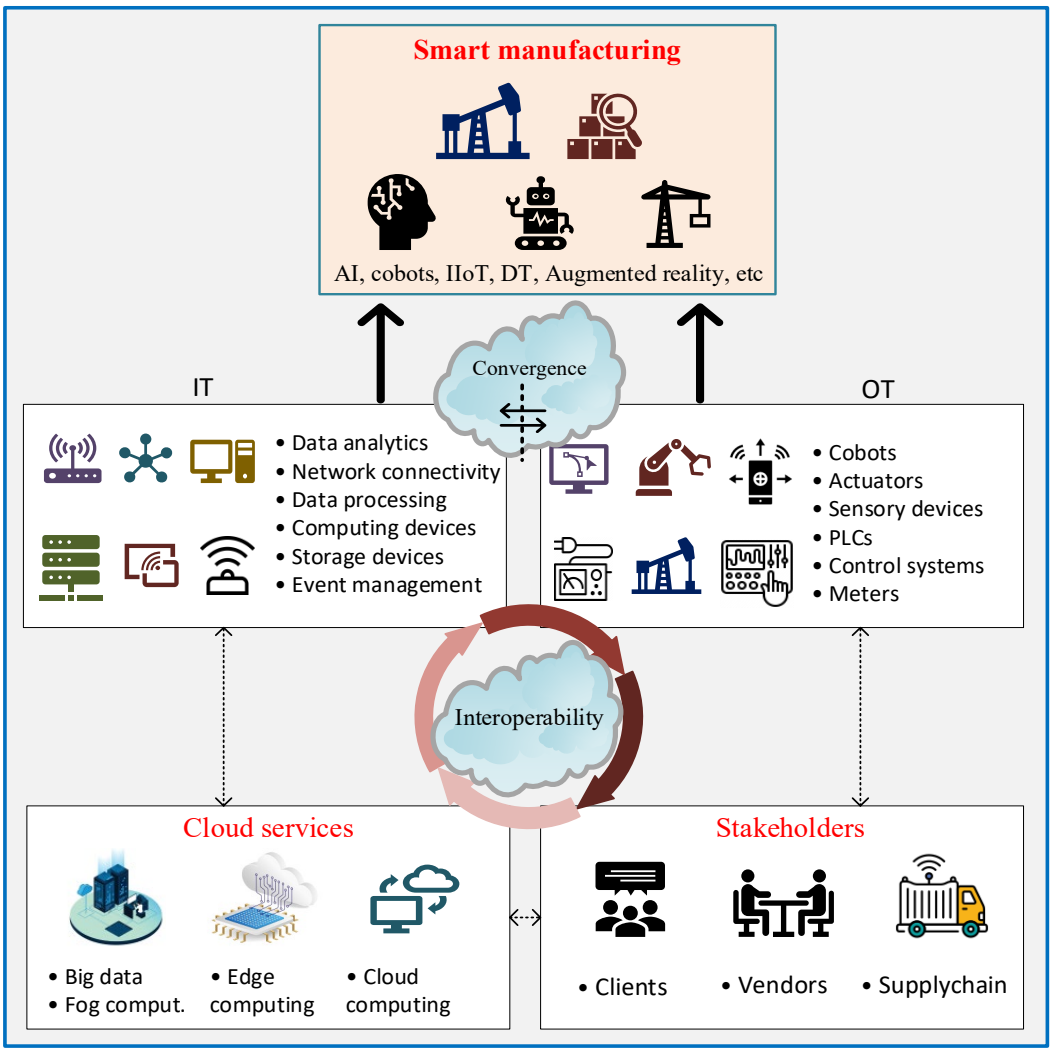

Figure 2: Interoperability between different vulnerable technologies within industry 4.0

Laghari et al. [37] present a security system that utilizes digital signatures to provide authentication, integrity, and defense against cyber breaches. The method is evaluated based on industrial Semiconductor Equipment Communication Standard/Generic Equipment Model (SECS/GEM) design and implementation protocols [36] against cyberattacks. The findings suggest that SECS/GEM successfully blocked unauthorized organizations from initiating connections with legitimate industrial devices while also ensuring the integrity of communications by rejecting fake signals. Likewise, attacks such as replay, Denial-of-Service, and False-Data-Injection are mitigated by the SECS/GEM. In [38], Ghimire et al. adopt a federated learning framework for cybersecurity within the IoT, with a main emphasis on security. They also provide different advances to tackle performance concerns in terms of accuracy, resource constraints, and latency. Latino et al. [39] proposed a cybersecurity reference framework for the food and beverage industry. They compare the progress made in cybersecurity within the food and beverage sector with suggested advancements in the I4.0 framework. Given the fact that I4.0 has diverse implementations in the food and beverage supply chain, it also establishes unique circumstances that necessitate ad hoc cybersecurity solutions. As such, the authors proposed future directions to mitigate these challenges. Peña Zarzuelo [40] highlights some crucial cybersecurity challenges in the ports and maritime industry. The author stressed the recent smart transformation of the port sector (smart port) due to the increasing adoption of I4.0 and emphasized the importance of ensuring its security as a critical infrastructure. Other proposed frameworks for different cybersecurity application domains include space [41], automated vehicles [42, 43], process control and operations [44], FinTech [45], energy [46], construction [47], railway [48], smart electric vehicle charging [49], unmanned aerial systems [50], bioprinting [51], SMEs [52], medical devices, [53] etc.

In [54], the authors combined deep learning and blockchain to secure critical health care data in CPS. The authors present a secure pattern-proof malware validation technique that was developed specifically for ICPS using blockchain and reinforcement learning techniques on the LSTM deep learning model. The method is able to improve system performance, mitigate cyber threats, and detect known and unknown attacks. Other applications of blockchain-based techniques for industrial cybersecurity include the works on blockchain-secured smart manufacturing [55], blockchain in internet of things [56], blockchain in industrial context [57], blockchain-enabled smart operations [58], blockchain and DT empowered self-healing [59], and blockchain-based data-driven control system [60].

3. Cybersecurity in distributed industrial DTs

The advancements brought by DTs in industry are undeniably huge. However, the interactions, interconnectedness, and incorporation of DTs with other novel technologies, such as AI, big data, IIoT, CPS, and enhanced visualization, present a variety of cybersecurity challenges. Moreover, given its huge dependency on data, DTs are also vulnerable to multifaceted threats due to lack of data protection, confidentiality, integrity, availability, and privacy.

Hence, as we progressively embrace and incorporate distributed DTs in various industrial sectors and everyday routines, it is crucial to fully understand and investigate their cybersecurity impacts. By acquiring this insight, we will be able to fully utilize the advantages of DTs while averting the related cybersecurity vulnerabilities. The main objective of this section is to examine the potential cybersecurity threats in distributed DTs and outline methods to reduce them, with a specific emphasis on the manufacturing sector.

3.1. Potential cyberthreats in distributed DTs

Distributed DT ecosystems may, in fact, be more susceptible to cybersecurity breaches and threats than conventional systems. This is due to the fact that platforms containing distributed DTs generally exhibit different attributes, which include.

- The infrastructure is characterized by extensive network connectivity and redistribution.
- Distributed DT allows for remote management and exchange of vital information.
- Distributed DT connects to cloud, edge, and fog devices located at the perimeter that require a highly secure system setting.
- Distributed DT platforms make use of open standards of operation.

Additionally, security is a critical concern that needs to be taken into account within the distributed DT platform. An important factor contributing to this is the expansion of the DTs to encompass a variety of applications, such as data analytics, predictive maintenance, monitoring, etc., a significant number of which are considered crucial. Moreover, each of these services is highly dependent on software components including algorithms, models, and applications, which are frequently vulnerable to various threats stemming from defects. Also, these services depend on numerous interfaces, interconnections, and frameworks [8]. The intricate nature of these nuances has the potential to introduce inaccuracies into the DT, which could subsequently impact the operation of the underlying system via erroneous conclusions.

Furthermore, under the assumption that DTs can be modified to function in critical settings such as the manufacturing industry, it becomes obligatory to provide additional protection for industrial systems in conjunction with their DTs. Nevertheless, this requirement also prompts an investigation into whether the integration of security protocols into the DT could subsequently introduce additional hardware and software intricacies that could impact the functioning of the DT. One potential drawback is that the integration of security measures may impede critical functions in DTs that encounter substantial challenges in generating and analyzing models and data without having the choice to transfer resources to more powerful platforms [8]. Then, operational efficiency must take precedence in simulations conducted on systems where security is a prerequisite but not a primary concern, provided that it does not significantly impede tasks related to modeling and simulation [8].

Clearly, inadequate security setup within the distributed DT paradigm can also present a crucial threat. Given that DTs are regarded as reflections of the real-physical world, they contain duplicate confidential data from the whole IT-OT paradigm [61]. This data might comprise sensitive information such as the operational procedures of OT components, the functional attributes of confidential processes, the particulars of the operational setting and its connections, or the crucial security credentials required to access vital resources. Consequently, DTs also encompass vital information, enabling malicious actors to extract and generate a mapping of the complete system or a specific component thereof, in addition to deriving confidential data or identifying patterns through the analysis of databases, system structures, and resources [8]. Furthermore, deliberate manipulation of digital assets can have catastrophic consequences for their real-physical equivalents, as they are capable of automatic decision-making. As a result, DTs must be regarded as critical platforms that need careful consideration with respect to every security requirement, including confidentiality, integrity, availability, and privacy of data and resources.

In line with this, it is imperative that every security evaluation of DTs considers the four featured functional layers [8] in terms of their enabling technologies and the conceptualization provided in [7, 62]. This is primarily due to the fact that DTs predominantly depend on data processing and digital assets, which necessitates the utilization of the four layers. Figure 3 depicts the range of cyberattacks that the DT platform can be susceptible to based on the four functional layers. It can be seen that the attack surface is extremely vast. Distributed DTs can be vulnerable to adversaries that exploit the physical attack surface, which includes Layer 1 and Layers 2-4. However, physical assets might also be vulnerable whenever DTs are targeted, specifically from Layers 4–2 and down to Layer 1. In this scenario, both internal and external attackers might enhance their understanding and methods of attack by gathering vital information directly from the DT source [8]. This consequently leads to a devastating attack sequence that could be detrimental to not just the DT but the entire industrial chain. All attacks covered in Figure 3 emanate due to a variety of threats that clearly do not respect the security requirement on confidentiality, integrity, availability, and privacy of data within the DT paradigm. Below, we itemize such threats and their impact on the DT.

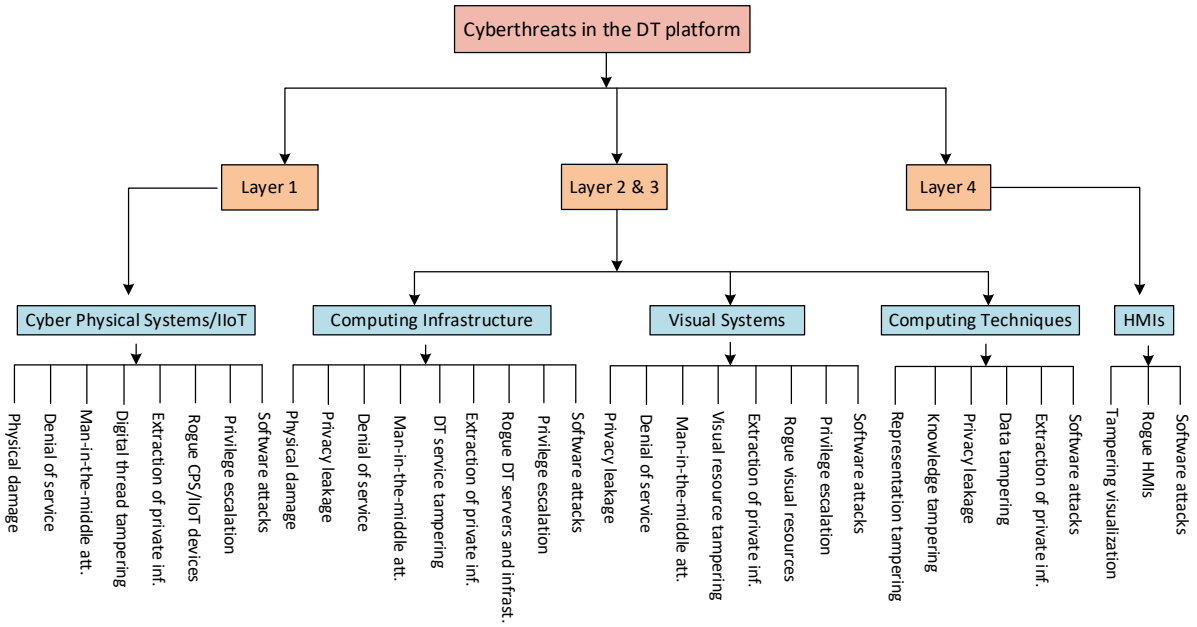

Figure 3: Cyberthreats in the distributed DT paradigm based on the four functional layers [8].

3.1.1. Threats to data integrity

The vulnerability of data poses a greater risk to the reliability and accuracy of DT. This can compromise the integrity of the data it gets from the real physical system. Any tampering or distortion of this data can result in inaccurate modeling and analysis, which in turn leads to flawed conclusions.

Data integrity-focused cyberattacks, such as tampering, sniffing, and manipulation through different software attacks, present a substantial risk to distributed DTs [63] as they cover a large number of attack surfaces that can be initiated at any of the four layers in Figure 3.

3.1.2. Threats to data confidentiality

Data confidentiality pertains to securing data from illicit access, disclosure, or unauthorized intrusion, exposure, and misappropriation. An unsecure DT ecosystem will certainly fall short of achieving the required confidentiality due to the huge attack surface. The significance of confidentiality in distributed DTs cannot be overstated, particularly in ensuring the preservation of information and data privacy. In essence, when establishing connections between DTs, particular confidentiality threats from Layers 1 to 4 that the current security measures might not be able to adequately handle can arise [64]. Therefore, a lot of considerations, such as architectural requirements, standard risk control, and other novel security measures and policies from credible institutions, must be put in place [64].

3.1.3. Threats to data privacy

Data privacy in distributed DTs is one of the most alarming threats. The DT paradigm presents a significant security concern regarding data privacy, primarily due to its emphasis on safeguarding the proprietary information stored within its servers. Entities capable of infiltrating breached servers or associated infrastructures may extricate sensitive data, including but not limited to login information, setups, services, and other processes. They can harvest data for the purpose of industrial cyber espionage or discover primary weaknesses in DTs to enhance data penetration or other components. Threats related to software attacks and privacy leakage are some of the vulnerabilities surrounding data privacy. In Figure 3, Layers 2 and 3 depict such threats within the DT platform.

3.1.4. Threats via authentication and access control

DTs generally handle sensitive and confidential data, which makes them a desirable target for attackers with the intent of gaining illegal access to the systems. This action may also be undertaken with the purpose of covertly acquiring data for other malicious intents, such as withholding critical data for financial reasons and impersonation [65]. Consequently, the use of weak access restrictions or the lack of authentication and access control mechanisms in distributed DT will lead to several other vulnerabilities, including software attacks, privilege escalation, and different tampering scenarios. These threats also cover a large attack surface in Figure 3, particularly from Layer 1, Layer 2 (computing infrastructure), and Layer 4 (HMIs). Figure 4 depicts the threat landscape in a distributed DT paradigm.

3.1.5. Threats to digital tools and services

The IT and OT realms provide the backbone through which data exchange between different tools and services is carried out within the DT paradigm. This brings yet another large attack surface to the DT. Any form of threat that intercepts the edge connecting both realms will be devastating. Moreover, ensuring the physical security of OT devices is crucial since they are susceptible to potential harm, destruction, or theft by adversaries. The real physical replica of the DT also utilizes various technologies, such as tamper-proof and tamper-resistant hardware, to safeguard their data against unauthorized manipulation [66]. However, it still remains feasible for attackers to penetrate and modify the data via rogue CPS/IIoT, digital threat tampering, man-in-the-middle and poisoning attacks, or by leveraging other flaws within the infrastructure, applications, and communication channels. By monitoring and assessing various physical traits, such as processing times, supply flow, and various production channels, the attacker can also exploit confidential information through a physical device. This threat also exhibits a large attack surface, especially in Layers 1, 2, and 4, indicated to Figure 3.

3.1.6. Threats via network connectivity

Given that the distributed DT logic is distributed across a whole network of computing ecosystems through clouds, fog, and at the edge, rogue DT servers and devices can function as an attack surface [67], allowing DT communication to flow through. Similarly, such servers whose nodes carry a portion of the logic have the potential to introduce inaccuracies within the information under processing, modify or breach the storage systems under monitoring, and alter the generated knowledge or representation meant for the end user [8]. Common vulnerabilities to network infrastructures due to the high interconnectivity include software attacks, man-in-the-middle attacks, and manipulation-based attacks (DoS and DDoS). Figure 3 delineates the presence of these threats in all layers of the DT platform. Additionally, Figure 5 depicts the information flow characterization between cyberspace, DT, and cyberthreats.

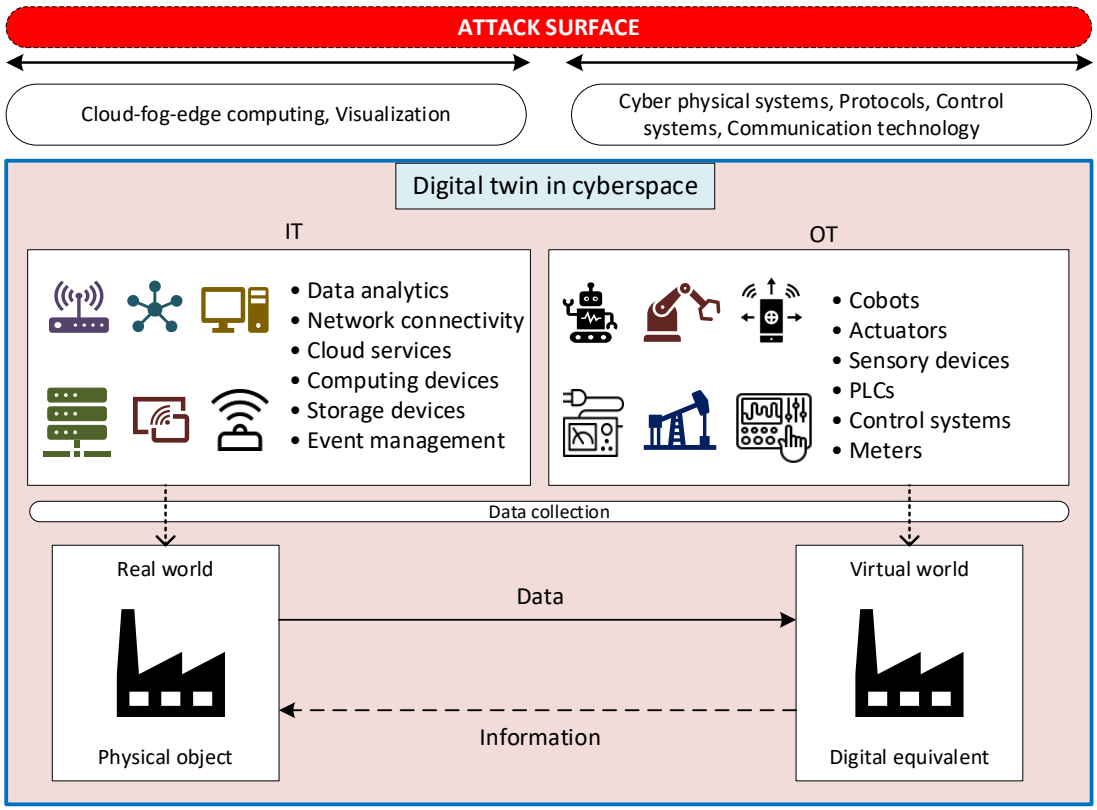

Figure 4: Threat landscape within the distributed DT paradigm. **Note:** The entire threat landscape is indicated in light brown.

3.2. Strategies for mitigating cyberthreats in distributed DT

Similar to other new technologies and infrastructures, distributed DTs face the same cybersecurity-related risks. They need to effectively tackle the various types of cyberthreats mentioned earlier and establish strong security regulations and frameworks. A complete cybersecurity strategy and plan should include security measures in several facets, including secure network connectivity, software security, hardware security, secure communication channels, etc. All with the aim of ensuring data protection, network protection, access control, identity control and authentication, cloud protection, databases and cloud infrastructure protection, mobile protection, endpoint protection, and training of personnels/OT systems.

In the following, we provide defense mechanisms against cyberthreats that DTs are susceptible to. These mechanisms are based on recent novel techniques put forward by researchers and cybersecurity experts to mitigate different cyberthreats in DT.

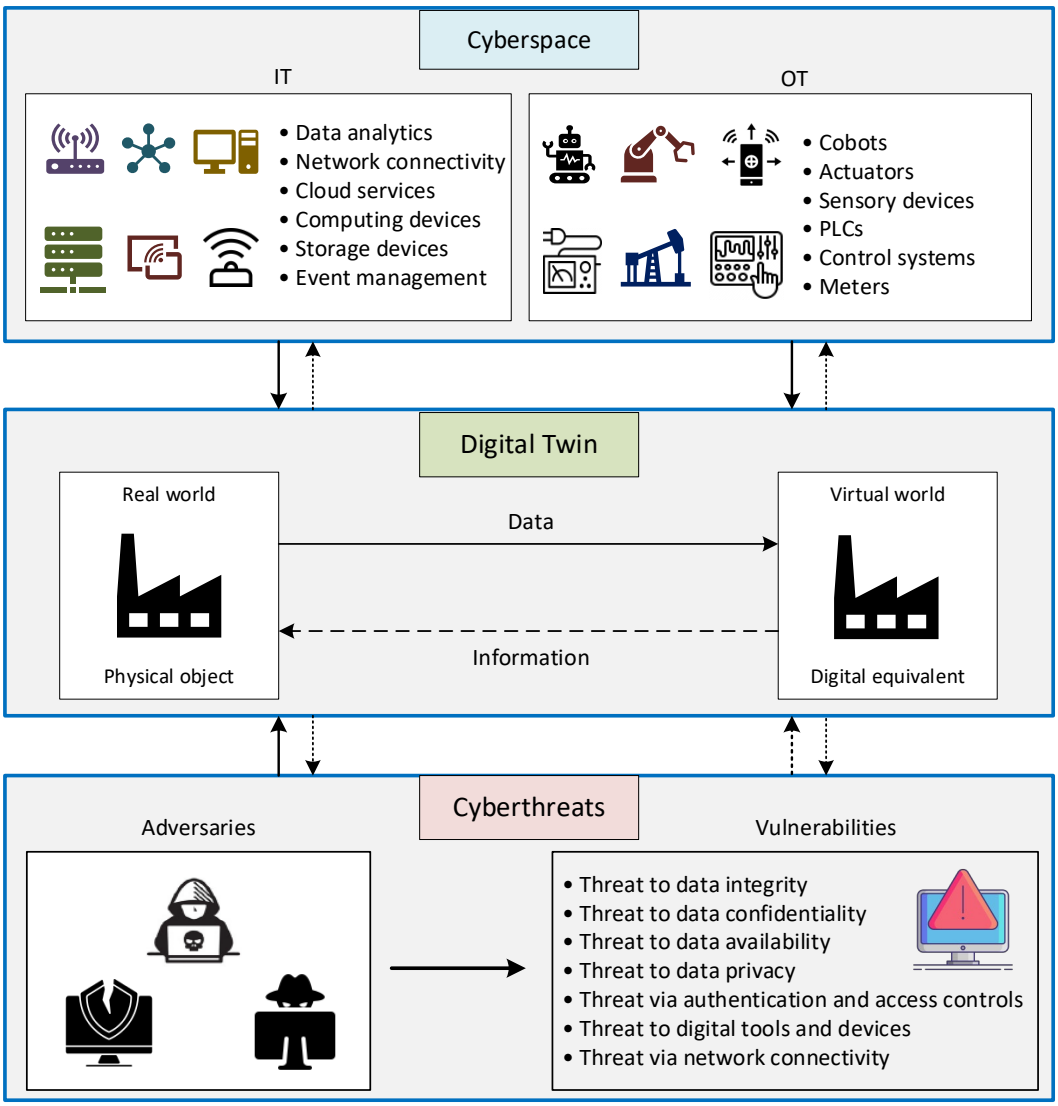

Figure 5: Information flow characterization between cyberspace, DT, and cyberthreats

3.2.1. Recent defense mechanisms

1. **Authentication and access control:** Strong authentication and access control mechanisms are essential in the DT to ensure that access is only granted to authorized entities. Through the implementation of authentication, users will have the ability to safely access various data processing services within the DT paradigm through secure login credentials. Also, considering the complex nature of distributed DTs in terms of their heterogeneous interconnectivity with other technologies, authentication and access control will provide a secure and seamless DT interaction with other interfaces and processes. Some novel state-of-the-art data authentication mechanisms in the communication space of DT in different manufacturing sectors include the works in [68-72]. The authors mainly emphasize privacy-preserving authentication between different communication scenarios. Pervez et al. [69] specifically adopt the concept of 'Verifiable Credentials' in their proposed framework to ensure the verifiable authenticity of Digital Twin data by encompassing provenance, transparency, and dependability via the use of verifiable representation. Likewise, Chen et al. [68] and Jiang et al. [73] utilize framework models at different layers of their architecture, which provide flexible support for internal expansion of the DT and enable multi-DT connectivity to more accurately represent intricate systems within the digital realm. This also ensures the proper management of many internal and external interfaces within the ecosystem. In

terms of access control, techniques such as [74] and [75] provide frameworks for preventing unauthorized access to multiple systems that exist together within the DT paradigm. Other access control-based blockchain schemes include [76, 77]. Both techniques ensure the secure exchange of DT data while preserving privacy. This gives adequate protection and access to resources by granting the right privileges to the right parties involved.

2. **Real-time monitoring and incidence response:** The real-time virtualization and monitoring of security-related events generated by DTs and the prompt response to incidents are essential steps in ensuring the optimal functionality and security of the DT platform. This is to guarantee early detection of potential threats, exploits, and vulnerabilities within the entire ecosystem. The security operation center (SOC) [78] is the centralized entity responsible for the real-time monitoring and detection of cyberthreats on IIoT platforms. Security Information and Event Management systems (SIEM) are crucial tools utilized in SOCs. They gather critical events from various sources within the entire DT network, standardize the events to a uniform format, and store the standardized events to promptly detect illicit activity [78]. To enhance proactive security measures and improve situational awareness in DTs, SIEMs and SOCs can additionally include Cyber Threat Intelligence (CTI) protocols [8] to monitor and control the exchange of critical security information. Moreover, the efficacy of these monitoring methods also relies on the ability of their data analytics approach in terms of collection, analysis, and providing prompt and reliable feedback to reactive systems [78].

3. **Network security:** The network interconnectivity between distributed DT layers and other IIoT devices within the DT ecosystem is considered crucial as it comprises a large attack surface and vulnerabilities. Therefore, it is imperative to adopt efficient network defense mechanisms and incorporate them into all associated technologies within the ecosystem. Some of these technologies are covered in [79, 80], where priority is given to architectural design that supports network security by design. In addition, as good practices and preventive measures, techniques such as network segmentation [73, 81] and network configuration [82, 83] should be adopted and implemented within the ecosystem. All of these will serve as the first line of defense in the event of cyberthreats within the network infrastructure.

4. **Data security:** Data serves as the core basis on which other platforms, services, and technologies operate in the digital domain, let alone in distributed DT. As such, data security should be an integral part of every DT platform, given that DT's entire functionality revolves around data use. In fact, without sufficient data availability, the concept of DT would not have existed. With this in mind, researchers and cybersecurity experts have proposed different frameworks [69, 84, 85] with the aim of securing data in various DT scenarios. Consequently, encryption techniques [86] also provide efficient protection to data against malicious manipulations, which should be adopted in all DT platforms. Moreover, all the other security measures and defense mechanisms, such as authentication, access controls on specific data, periodic real-time monitoring audits and incidence response, as well as network security, also provide protection for the DT data.

5. **Privacy-preservation:** Data privacy is another important requirement of DT data protection. It primarily concerns the rights and privileges of users in relation to their critical data and personal information. Therefore, considering the massive processing and analysis of data performed in DT, it is paramount to ensure all crucial data within the DT ecosystem is given the utmost privacy-preserving protection. Recently, technologies such as federated learning [87, 88], blockchain [76], secure multi-party computation [89], and pseudo anonymization and differential privacy [90] have been proposed to mitigate privacy risks in distributed DT. The combination of federated learning and blockchain empowered technologies [91, 92] has also seen a progressive surge. Li et al. [92]

leverage access point model learning and directed acyclic graph (DAG) to exploit blockchain for secure model updates. This ensures efficient DT architectural design while preserving data privacy.

6. **Training of personnels:** Personnel training on how and what to do in case of cyber-attack is a crucial aspect to protecting IT and OT systems against cyber threats. Extensive cybersecurity training should be given to personnel who are responsible for the development, operation, and maintenance of IT and OT tools and systems. This guarantees a workforce that is both vigilant and well-informed. Moreover, personnel in the IT realm should be familiar with all tools and technologies used by their OT counterparts and vice versa. Also, when creating the training programs, it is advisable to employ activity monitoring rules to assess the level of expertise, competency, and abilities in the proper use of the IT and OT tools and technologies, as well as the corresponding cyber threats. This ensures synergy in both their activities and knowledge of cyber threats.

4. Key takeaways

Generally, our review yields the following findings that are worth further research: (a) The security of OT systems is not sufficiently investigated in both academia and industry. (b) Security guidelines, policies, and preventive methods are often ignored. (c) Inadequately adaptive security measures lose their efficacy over time. (d) DTs for cybersecurity and (e) Cyber-immune systems for DTs are worth exploring.

a) **OT systems security needs more research:** Considering the security of OT is not as mature as that of IT [30], present security measures [34] are insufficient in providing the required protection due to the integration of OT systems with diverse characteristics and interconnectivity with the IT industrial systems. Therefore, OT security solutions are worth investigating in both academia and industry.

b) **Security policies and preventive measures are often ignored:** Implementing security policies is the first and most viable approach to mitigating attacks and human errors. Recent research, however, indicates that academia places a strong emphasis on intrusion detection systems after an attack occurs, but lacks focus on studies based on security policies before an attack occurs [30]. Therefore, it is important that the research community also focus on preventive measures through security policies before an attack happens.

c) **Cybersecurity solutions that are not adaptable become invalid:** Traditional industrial systems were constructed with a fixed architecture that consisted of modules designed to operate reliably for a specific period of time without substantial modifications. Nevertheless, the IIoT architectures exhibit dynamism since they include different technologies, and such dynamism comes with a plethora of solutions, some of which are novel and efficient [5, 76, 88, 93]. However, as the race between adversaries and cybersecurity experts continues, all solutions that are not adaptable become invalid over time. Therefore, it is important to incorporate recent solutions to emerging technologies such as DT.

d) **DTs for cybersecurity:** Recently, researchers have started exploring the notion of using DT for cybersecurity, coined the Cyber Digital Twin [93-96], which is gaining momentum. This concept highlights that industries can use DTs to identify and eliminate vulnerabilities in their systems by generating virtual replicas for the purpose of conducting security assessments, thereby enhancing cybersecurity by responding to cyberthreats in a manner that closely resembles a real secure system. To this end, we believe that establishing a novel research direction focused on investigating the potential of DTs to serve as mechanisms for bolstering the security of different critical infrastructures is imperative.

e) **Cyber-immune system for DT:** As the integration of OT and IT exposes industrial technologies to more vulnerability and increases the attack surface, the implementation of a robust cybersecurity system that aims to replicate the adaptive immune system of humans is an effective approach to

safeguarding against existing and emerging cyberthreats [97]. Cyber-immune systems can survive various types of attacks, particularly those caused by novel malware and viruses that cannot be detected by traditional cybersecurity solutions [98, 99]. As a result, using cyber-immune systems could be the key to making sure that data processing on the DT platforms is more secure than ever, considering the immense vulnerability and large attack surface of DTs.

5. Challenges

a) **Expansive attack surface:** Due to the expansive interconnectivity landscape covered by distributed DT, its attack surface happens to be one of the largest (if not the largest) among the recent novel technologies. Also, the creation of a DT visual replica essentially multiplies the potential attack surface, as adversaries can target either the physical system or its digital counterpart. This poses a huge challenge to researchers and cybersecurity experts in reaching the required protection, considering the immense performance-security tradeoff this expansive attack surface could lead to.

b) **Lack of standardized assessment criteria:** Cybersecurity research for distributed DT and other novel technologies lacks a standard framework for assessing vulnerabilities. Most proposals and security measures focus on adopting conventional security solutions. However, evaluating the framework implementation of DT through the modeling of attacks and defenses while studying the system for a certain duration may provide the most accurate assessment. The major drawback, however, is that it is not permissible to interfere with the real system owing to the crucial nature of its activities and the need for constant supervision. Even though some solutions [8, 70, 86] are suggested to overcome this limitation, their effectiveness is uncertain owing to the absence of an assessment framework [86].

c) **Lack of trained personnels:** Considering the expansive nature of cybersecurity due to its integration with other security domains, it is difficult for a single expert to tackle the plethora of security challenges. Therefore, a unanimous collaboration of experts in various security domains is imperative. In addition, the OT stakeholders also lack the relevant training and security awareness for managing the new IT technologies integrated within the OT systems due to their acquaintance with the traditional OT tools and systems [7]. Therefore, it is important to establish training programs that integrate both domains. An effective approach to promoting learning in both IT and OT might include implementing frequent training programs that use tailored and integrated instructional methods, specifically using cyber-range concepts [100-102].

d) **Interoperability:** The interoperability of distributed DTs is the ability of technologies to efficiently communicate information without restrictions across different DTs and their integrated systems, both in physical and virtual spaces [103]. Such interoperability encompasses several elements, including hardware, software, algorithms, interfaces, operating systems, etc., and one major research obstacle towards interoperable DTs is achieving comprehensive cross-chain interoperable processes [86]. Therefore, a collaborative effort from both industries and academics is required to establish regulations and standards toward streamlined distributed DT operability.

6. Conclusion

A distributed DT is built upon the integration of several technologies, including CPS, IIoT, AI, edge computing, big data, etc. The convergence of these novel technologies, in tandem with the inherent DT interconnections and data sharing with its corresponding physical counterpart, gives rise to several security concerns that have not been adequately investigated. To propose efficient solutions, this paper provides an in-depth discussion and analysis of the impact and significance of cybersecurity in distributed industrial DTs. The work first examined the importance of DT and cybersecurity in industry, followed by potential cyberthreats in industrial DTs. The analysis of threats within the large attack surface of the DT platform is covered in terms of the four functional layers of the DT. Additionally, the

defense mechanisms for mitigating such threats are discussed in terms of recent technical approaches. Finally, we provide important key takeaways toward the realization of a secure and privacy-preserving industrial DT as well as challenges to existing DT security. Future work will focus on exploring the key takeaways of our findings to uncover efficient methods of securing key architectures for distributed DTs in the industrial domain.

7. Acknowledgements

The authors extend their thanks for the funding received from the ONE4ALL project funded by the European Commission, Horizon Europe Programme under the Grant Agreement No. 101091877.

8. References

[1] V. Mullet, P. Sondi, and E. Ramat, "A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0," IEEE Access, vol. 9, pp. 23235-23263, 2021, doi: 10.1109/ACCESS.2021.3056650.

[2] M. Eckhart and A. Ekelhart, "Towards Security-Aware Virtual Environments for Digital Twins," presented at the Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Incheon, Republic of Korea, 2018, doi: 10.1145/3198458.3198464.

[3] R. Bitton et al., "Deriving a Cost-Effective Digital Twin of an ICS to Facilitate Security Evaluation," in Computer Security, Cham, J. Lopez, J. Zhou, and M. Soriano, Eds., 2018: Springer International Publishing, pp. 533-554.

[4] M. Eckhart and A. Ekelhart, "A Specification-based State Replication Approach for Digital Twins," presented at the Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy, Toronto, Canada, 2018, doi: 10.1145/3264888.3264892.

[5] A. Saad, S. Faddel, T. Youssef, and O. A. Mohammed, "On the Implementation of IoT-Based Digital Twin for Networked Microgrids Resiliency Against Cyber Attacks," IEEE Transactions on Smart Grid, vol. 11, no. 6, pp. 5138-5150, 2020, doi: 10.1109/TSG.2020.3000958.

[6] J. Friederich, D. P. Francis, S. Lazarova-Molnar, and N. Mohamed, "A framework for data-driven digital twins of smart manufacturing systems," Computers in Industry, vol. 136, p. 103586, 2022.

[7] R. Minerva, G. M. Lee, and N. Crespi, "Digital Twin in the IoT Context: A Survey on Technical Features, Scenarios, and Architectural Models," Proceedings of the IEEE, vol. 108, no. 10, pp. 1785-1824, 2020, doi: 10.1109/JPROC.2020.2998530.

[8] C. Alcaraz and J. Lopez, "Digital Twin: A Comprehensive Survey of Security Threats," IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1475-1503, 2022, doi: 10.1109/COMST.2022.3171465.

[9] M. Grieves and J. Vickers, "Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems," in Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches, F.-J. Kahlen, S. Flumerfelt, and A. Alves Eds. Cham: Springer International Publishing, 2017, pp. 85-113.

[10] W. Kritzinger, M. Karner, G. Traar, J. Henjes, and W. Sihn, "Digital Twin in manufacturing: A categorical literature review and classification," IFAC-PapersOnLine, vol. 51, no. 11, pp. 1016-1022, 2018, doi: 10.1016/j.ifacol.2018.08.474.

[11] M. Liu, S. Fang, H. Dong, and C. Xu, "Review of digital twin about concepts, technologies, and industrial applications," Journal of Manufacturing Systems, vol. 58, pp. 346-361, 2021, doi: 10.1016/j.jmsy.2020.06.017.

[12] N. Mohamed, S. Lazarova-Molnar, and J. Al-Jaroodi, "Digital Twins for Energy-Efficient Manufacturing," in 2023 IEEE International Systems Conference (SysCon), 2023: IEEE, pp. 1-7.

[13] A. F. Mendi, T. Erol, and D. Dogan. (2022) Digital Twin in the Military Field. 33-40. URL: https://doi.ieeecomputersociety.org/10.1109/MIC.2021.3055153

[14] T. Ruohomäki, E. Airaksinen, P. Huuska, O. Kesäniemi, M. Martikka, and J. Suomisto, "Smart City Platform Enabling Digital Twin," in 2018 International Conference on Intelligent Systems (IS), 25-27 Sept. 2018, pp. 155-161, doi: 10.1109/IS.2018.8710517.
[15] C. Fan, C. Zhang, A. Yahja, and A. Mostafavi, "Disaster City Digital Twin: A vision for integrating artificial and human intelligence for disaster management," International Journal of Information Management, vol. 56, p. 102049, 2021, doi: 10.1016/j.ijinfomgt.2019.102049.
[16] M. Hearn and S. Rix, "Cybersecurity Considerations for Digital Twin Implementations," in "Industrial Internet Consortium," 2019. URL: https://www.iiconsortium.org/news-pdf/joi-articles/2019-November-JoI-Cybersecurity-Considerations-for-Digital-Twin Implementations.pdf
[17] D. Goldsman, R. E. Nance, and J. R. Wilson, "A brief history of simulation revisited," in Proceedings of the 2010 Winter Simulation Conference, 2010: IEEE, pp. 567-574.
[18] M. Grieves, "Digital twin: manufacturing excellence through virtual factory replication," White paper, vol. 1, no. 2014, pp. 1-7, 2014.
[19] M. Singh, E. Fuenmayor, E. P. Hinchy, Y. Qiao, N. Murray, and D. Devine, "Digital twin: Origin to future," Applied System Innovation, vol. 4, no. 2, p. 36, 2021.
[20] E. VanDerHorn and S. Mahadevan, "Digital Twin: Generalization, characterization and implementation," Decision support systems, vol. 145, p. 113524, 2021.
[21] F. Tao, H. Zhang, A. Liu, and A. Y. Nee, "Digital twin in industry: State-of-the-art," IEEE Transactions on industrial informatics, vol. 15, no. 4, pp. 2405-2415, 2018.
[22] M. R. Enders and N. Hoßbach, "Dimensions of digital twin applications-a literature review," 2019.
[23] A. Khodadadi and S. Lazarova-Molnar, "Essential Data Requirements for Industrial Energy Efficiency with Digital Twins: A Case Study Analysis," in The 7th International Conference on Emerging Data and Industry, 2024.
[24] M. Shafto et al., "Draft modeling, simulation, information technology & processing roadmap," Technology area, vol. 11, pp. 1-32, 2010.
[25] A. Rassõlkin et al., "Implementation of Digital Twins for electrical energy conversion systems in selected case studies," Proceedings of the Estonian Academy of Sciences, vol. 70, no. 1, 2021.
[26] J. Monteiro, J. Barata, M. Veloso, L. Veloso, and J. Nunes, "Towards sustainable digital twins for vertical farming," in 2018 Thirteenth International Conference on Digital Information Management (ICDIM), 2018: IEEE, pp. 234-239.
[27] M. Singh et al., "Applications of digital twin across industries: A review," Applied Sciences, vol. 12, no. 11, p. 5727, 2022.
[28] S. Huang, G. Wang, D. Lei, and Y. Yan, "Toward digital validation for rapid product development based on digital twin: a framework," The International Journal of Advanced Manufacturing Technology, pp. 1-15, 2022.
[29] Q. Qi and F. Tao, "Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison," Ieee Access, vol. 6, pp. 3585-3593, 2018.
[30] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, "Cybersecurity of Industrial Cyber-Physical Systems: A Review," ACM Comput. Surv., vol. 54, no. 11s, p. Article 229, 2022, doi: 10.1145/3510410.
[31] A. Petrosyan. "Distribution of cyber attacks across worldwide industries in 2022." statista. URL: https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/#:~:text=Share%20of%20cyber%20attacks%20in%20global%20industries%20worldwide%202022&text=In%202022%2C%20manufacturing%20had%20the,of%20the%20total%20cyber%20attacks.
[32] G. V. Research. "Cyber Security Market Size, Share & Trends Analysis Report " URL: https://www.grandviewresearch.com/industry-analysis/cyber-security-market#:~:text=The%20global%20cyber%20security%20market,12.3%25%20from%202023%20to%202030.
[33] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories," IEEE Access, vol. 7, pp. 45201-45218, 2019, doi: 10.1109/ACCESS.2019.2908780.

[34] M. Dawson, "Cyber Security in Industry 4.0: The Pitfalls of Having Hyperconnected Systems," Journal of Strategic Management Studies, vol. 10, no. 1, pp. 19-28, 2018, doi: 10.24760/iasme.10.1_19.
[35] A. Aoun, A. Ilinca, M. Ghandour, and H. Ibrahim, "A review of Industry 4.0 characteristics and challenges, with potential improvements using blockchain technology," Computers & Industrial Engineering, vol. 162, p. 107746,2021, doi: 10.1016/j.cie.2021.107746.
[36] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, "Addressing Industry 4.0 Cybersecurity Challenges," IEEE Engineering Management Review, vol. 47, no. 3, pp. 79-86, 2019, doi: 10.1109/EMR.2019.2927559.
[37] S. U. A. Laghari, S. Manickam, A. K. Al-Ani, S. U. Rehman, and S. Karuppayah, "SECS/GEMsec: A Mechanism for Detection and Prevention of Cyber-Attacks on SECS/GEM Communications in Industry 4.0 Landscape," IEEE Access, vol. 9, pp. 154380-154394, 2021, doi: 10.1109/ACCESS.2021.3127515.
[38] B. Ghimire and D. B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8229-8249, 2022, doi: 10.1109/JIOT.2022.3150363.
[39] M. E. Latino and M. Menegoli, "Cybersecurity in the food and beverage industry: A reference framework," Computers in Industry, vol. 141, p. 103702, 2022, doi: https://doi.org/10.1016/j.compind.2022.103702.
[40] I. d. l. Peña Zarzuelo, "Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue," Transport Policy, vol. 100, pp. 1-4, 2021, doi: 10.1016/j.tranpol.2020.10.001.
[41] A. Carlo et al., "The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications," Journal of Space Safety Engineering, vol. 10, no. 4, pp. 474-482, 2023, doi: 10.1016/j.jsse.2023.08.002.
[42] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Cybersecurity regulatory challenges for connected and automated vehicles – State-of-the-art and future directions," Transport Policy, vol. 143, pp. 58-71, 2023, doi: 10.1016/j.tranpol.2023.09.001.
[43] S. Khalid Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Modelling cybersecurity regulations for automated vehicles," Accident Analysis & Prevention, vol. 186, p. 107054, 2023, doi: 10.1016/j.aap.2023.107054.
[44] S. Parker, Z. Wu, and P. D. Christofides, "Cybersecurity in process control, operations, and supply chain," Computers & Chemical Engineering, vol. 171, p. 108169, 2023, doi: 10.1016/j.compchemeng.2023.108169.
[45] D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, "Cybersecurity threats in FinTech: A systematic review," Expert Systems with Applications, vol. 241, p. 122697, 2024, doi: 10.1016/j.eswa.2023.122697.
[46] P. Sanders, C. Bronk, and M. D. Bazilian, "Critical energy infrastructure and the evolution of cybersecurity," The Electricity Journal, vol. 35, no. 10, p. 107224, 2022, doi: 10.1016/j.tej.2022.107224.
[47] Ž. Turk, B. García de Soto, B. R. K. Mantha, A. Maciel, and A. Georgescu, "A systemic framework for addressing cybersecurity in construction," Automation in Construction, vol. 133, p. 103988, 2022, doi: 10.1016/j.autcon.2021.103988.
[48] S. Soderi, D. Masti, and Y. Z. Lun, "Railway Cyber-Security in the Era of Interconnected Systems: A Survey," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 7, pp. 6764-6779, 2023, doi: 10.1109/TITS.2023.3254442.
[49] S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, "Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective," IEEE Access, vol. 8, pp. 214434-214453, 2020, doi: 10.1109/ACCESS.2020.3041074.
[50] Z. Wang et al., "A survey on cybersecurity attacks and defenses for unmanned aerial systems," Journal of Systems Architecture, vol. 138, p. 102870, 2023, doi: 10.1016/j.sysarc.2023.102870.
[51] J. C. Isichei, S. Khorsandroo, and S. Desai, "Cybersecurity and privacy in smart bioprinting," Bioprinting, vol. 36, p. e00321, 2023, doi: 10.1016/j.bprint.2023.e00321.

[52] M. Kappe, R.-C. Härting, C. Karg, and D. Deffner, "Cybersecurity in SMEs – Drivers of Cybercrime, Insufficient Equipment and Prevention," Procedia Computer Science, vol. 225, pp. 3631-3640, 2023, doi: 10.1016/j.procs.2023.10.358.
[53] E. Wreh, "Chapter 13 - Cybersecurity in medical devices," in Medical Device Regulation, E. Wreh Ed.: Academic Press, 2023, pp. 345-368.
[54] M. A. Mohammed et al., "Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology," Engineering Applications of Artificial Intelligence, vol. 129, p. 107612, 2024, doi: 10.1016/j.engappai.2023.107612.
[55] J. Leng et al., "Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 1, pp. 237-252, 2021, doi: 10.1109/TSMC.2020.3040789.
[56] H. Pourrahmani, A. Yavarinasab, A. M. H. Monazzah, and J. Van herle, "A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain," Internet of Things, vol. 23, p. 100888, 2023, doi: 10.1016/j.iot.2023.100888.
[57] P. Seiler, E. Brandt, and F. Brandt, "Systematic mapping study on the security and efficiency of blockchain in industrial context," Procedia Computer Science, vol. 217, pp. 1497-1505, 2023, doi: 10.1016/j.procs.2022.12.349.
[58] L. Fu et al., "Blockchain-enabled device command operation security for Industrial Internet of Things," Future Generation Computer Systems, vol. 148, pp. 280-297, 2023, doi: 10.1016/j.future.2023.06.004.
[59] X. Feng, J. Wu, Y. Wu, J. Li, and W. Yang, "Blockchain and digital twin empowered trustworthy self-healing for edge-AI enabled industrial Internet of things," Information Sciences, vol. 642, p. 119169, 2023, doi: 10.1016/j.ins.2023.119169.
[60] A. B. Masood, A. Hasan, V. Vassiliou, and M. Lestas, "A Blockchain-Based Data-Driven Fault-Tolerant Control System for Smart Factories in Industry 4.0," Computer Communications, vol. 204, pp. 158-171, 2023, doi: 10.1016/j.comcom.2023.03.017.
[61] M. Hearn, "Digital twins, the Industrial Internet of Things and cyber security threats in connected industry," Cyber Security: A Peer Reviewed Journal, vol. 3, no. 2, pp. 116-123, 2019.
[62] D. Manufacturing, "Digital Twin Framework for Manufacturing" ISO TC184/SC4/WG15, Standard AP238, 2020, vol. 2023. URL: http://ap238.org/iso23247/
[63] A. R. Al-Ali, R. Gupta, T. Zaman Batool, T. Landolsi, F. Aloul, and A. Al Nabulsi, "Digital Twin Conceptual Model within the Context of Internet of Things," Future Internet, vol. 12, no. 10, doi: 10.3390/fi12100163.
[64] A. Kismul, H. Al-Khateeb, and H. Jahankhani, "A Critical Review of Digital Twin Confidentiality in a Smart City," in Cybersecurity in the Age of Smart Societies, Cham, H. Jahankhani, Ed., 2023: Springer International Publishing, pp. 437-450.
[65] G. Sirigu, B. Carminati, and E. Ferrari, "Privacy and Security Issues for Human Digital Twins," in 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), 14-17, 2022, pp. 1-9, doi: 10.1109/TPS-ISA56441.2022.00011.
[66] A. De Benedictis, C. Esposito, and A. Somma, "Toward the Adoption of Secure Cyber Digital Twins to Enhance Cyber-Physical Systems Security," in Quality of Information and Communications Technology, Cham, A. Vallecillo, J. Visser, and R. Pérez-Castillo, Eds., 2022: Springer International Publishing, pp. 307-321.
[67] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues," IEEE Access, vol. 6, pp. 18209-18237, 2018, doi: 10.1109/ACCESS.2018.2820162.
[68] C.-M. Chen, Q. Miao, S. Kumar, and T.-Y. Wu, "Privacy-preserving authentication scheme for digital twin-enabled autonomous vehicle environments," Transactions on Emerging Telecommunications Technologies, vol. 34, no. 11, p. e4751, 2023, doi: https://doi.org/10.1002/ett.4751.
[69] Z. Pervez, Z. Khan, A. Ghafoor, and K. Soomro, "SIGNED: Smart cIty diGital twiN vErifiable Data Framework," IEEE Access, vol. 11, pp. 29430-29446, 2023, doi: 10.1109/ACCESS.2023.3260621.

[70] J. Xu, C. He, and T. H. Luan, "Efficient Authentication for Vehicular Digital Twin Communications," in 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), 27-30 Sept. 2021, pp. 1-5, doi: 10.1109/VTC2021-Fall52928.2021.9625518.
[71] C. Lai, M. Li, G. Li, and D. Zheng, "Efficient Group Authentication and Key Agreement Scheme for Vehicular Digital Twin," in IEEE/CIC International Conference on Communications in China (ICCC), 10-12 Aug. 2023, pp. 1-6, doi: 10.1109/ICCC57788.2023.10233652.
[72] Z. Hóu, Q. Li, E. Foo, J. S. Dong, and P. d. Souza, "A Digital Twin Runtime Verification Framework for Protecting Satellites Systems from Cyber Attacks," in 2022 26th International Conference on Engineering of Complex Computer Systems (ICECCS), 26-30 March 2022, pp. 117-122, doi: 10.1109/ICECCS54210.2022.00022.
[73] Z. Jiang, Y. Guo, and Z. Wang, "Digital twin to improve the virtual-real integration of industrial IoT," Journal of Industrial Information Integration, vol. 22, p. 100196, 2021, doi: https://doi.org/10.1016/j.jii.2020.100196.
[74] J. Lopez and J. E. Rubio, "Access control for cyber-physical systems interconnected to the cloud," Computer Networks, vol. 134, pp. 46-54, 2018, doi: 10.1016/j.comnet.2018.01.037.
[75] R. Trabelsi, G. Fersi, and M. Jmaiel, "Access control in Internet of Things: A survey," Computers & Security, vol. 135, p. 103472, 2023, doi: 10.1016/j.cose.2023.103472.
[76] S. Son, D. Kwon, J. Lee, S. Yu, N. S. Jho, and Y. Park, "On the Design of a Privacy-Preserving Communication Scheme for Cloud-Based Digital Twin Environments Using Blockchain," IEEE Access, vol. 10, pp. 75365-75375, 2022, doi: 10.1109/ACCESS.2022.3191414.
[77] V. Divya, S. Arunarani, U. Hemamalini, and A. Bharathi, "Blockchain Based Digital Twins for Authorization and Remote Resource Sharing," in 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), 15-17, 2023, pp. 382-385.
[78] S. Bhatt, P. K. Manadhata, and L. Zomlot, "The Operational Role of Security Information and Event Management Systems," IEEE Security & Privacy, vol. 12, no. 5, pp. 35-41, 2014, doi: 10.1109/MSP.2014.103.
[79] W. Park, S. Park, D. Lee, T. Yang, and S. H. Kim, "Inter-Twin Connectivity for Digital Twin Networks in Secure Contactless Delivery Service Scenarios," in 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), 20-23 June, 2023, pp. 1-5, doi: 10.1109/VTC2023-Spring57618.2023.10200211.
[80] K. Wang, H. Du, and L. Su, "Digital Twin Network based Network Slice Security Provision," in IEEE 2nd International Conference on Digital Twins and Parallel Intelligence (DTPI), 24-28 Oct. 2022, pp. 1-6, doi: 10.1109/DTPI55838.2022.9998964.
[81] C. He, T. H. Luan, R. Lu, Z. Su, and M. Dong, "Security and Privacy in Vehicular Digital Twin Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 30, no. 4, pp. 154-160, 2023, doi: 10.1109/MWC.002.2200015.
[82] G. Pék, L. Buttyán, and B. Bencsáth, "A survey of security issues in hardware virtualization," ACM Comput. Surv., vol. 45, no. 3, p. Article 40, 2013, doi: 10.1145/2480741.2480757.
[83] J. Lopez, J. E. Rubio, and C. Alcaraz, "Digital Twins for Intelligent Authorization in the B5G-Enabled Smart Grid," IEEE Wireless Communications, vol. 28, no. 2, pp. 48-55, 2021, doi: 10.1109/MWC.001.2000336.
[84] W. Dong, B. Yang, K. Wang, J. Yan, and S. He, "A Dual Blockchain Framework to Enhance Data Trustworthiness in Digital Twin Network," in 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI), 15 July-15, 2021, pp. 144-147, doi: 10.1109/DTPI52967.2021.9540185.
[85] I. Anda, R. Mishra, and A. M. Aliyu, "Data Security Management Framework for Digital Twins of Industrial Pipeline," in 2021 International Conference on Maintenance and Intelligent Asset Management (ICMIAM), 12-15 Dec. 2021, pp. 1-5, doi: 10.1109/ICMIAM54662.2021.9715199.
[86] Y. Wang, Z. Su, S. Guo, M. Dai, T. H. Luan, and Y. Liu, "A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects," IEEE Internet of Things Journal, vol. 10, no. 17, pp. 14965-14987, 2023, doi: 10.1109/JIOT.2023.3263909.
[87] D. Chen, D. Wang, Y. Zhu, and Z. Han, "Digital Twin for Federated Analytics Using a Bayesian Approach," IEEE Internet of Things Journal, vol. 8, no. 22, pp. 16301-16312, 2021, doi: 10.1109/JIOT.2021.3098692.

[88] W. Sun, S. Lian, H. Zhang, and Y. Zhang, "Lightweight Digital Twin and Federated Learning With Distributed Incentive in Air-Ground 6G Networks," IEEE Transactions on Network Science and Engineering, vol. 10, no. 3, pp. 1214-1227, 2023, doi: 10.1109/TNSE.2022.3217923.
[89] G. Li et al., "Breaking Down Data Sharing Barrier of Smart City: A Digital Twin Approach," IEEE Network, vol. 38, no. 1, pp. 238-246, 2024, doi: 10.1109/MNET.140.2200512.
[90] G. Ahmadi-Assalemi, H. Al-Khateeb, and A. Aggoun, "Privacy-enhancing technologies in the design of digital twins for smart cities," Network Security, vol. 2022, no. 7, p. null, 2022, doi: 10.12968/s1353-4858(22)70046-3.
[91] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-Latency Federated Learning and Blockchain for Edge Association in Digital Twin Empowered 6G Networks," IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 5098-5107, 2021, doi: 10.1109/TII.2020.3017668.
[92] L. Jiang, H. Zheng, H. Tian, S. Xie, and Y. Zhang, "Cooperative Federated Learning and Model Update Verification in Blockchain-Empowered Digital Twin Edge Networks," IEEE Internet of Things Journal, vol. 9, no. 13, pp. 11154-11167, 2022, doi: 10.1109/JIOT.2021.3126207.
[93] G. P. Sellitto, M. Masi, T. Pavleska, and H. Aranha, "A Cyber Security Digital Twin for Critical Infrastructure Protection: The Intelligent Transport System Use Case," in The Practice of Enterprise Modeling, Cham, E. Serral, J. Stirna, J. Ralyté, and J. Grabis, Eds., 2021: Springer International Publishing, pp. 230-244.
[94] M. Masi, G. P. Sellitto, H. Aranha, and T. Pavleska, "Securing critical infrastructures with a cybersecurity digital twin," Software and Systems Modeling, vol. 22, no. 2, pp. 689-707, 2023, doi: 10.1007/s10270-022-01075-0.
[95] R. Faleiro, L. Pan, S. R. Pokhrel, and R. Doss, "Digital Twin for Cybersecurity: Towards Enhancing Cyber Resilience," in Broadband Communications, Networks, and Systems, Cham, W. Xiang, F. Han, and T. K. Phan, Eds., 2022: Springer International Publishing, pp. 57-76.
[96] S. Pirbhulal, H. Abie, and A. Shukla, "Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications," in 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), 19-22, 2022, pp. 1-5, doi: 10.1109/VTC2022-Spring54318.2022.9860581.
[97] P. Sergei, "Developing a Cybersecurity Immune System for Industry 4.0," in Developing a Cybersecurity Immune System for Industry 4.0: River Publishers, 2020, pp. i-xlvi.
[98] T. Menze. "From Cybersecurity to Cyber Immunity in IIoT." ARC Advisory group. URL: https://www.arcweb.com/industry-best-practices/cybersecurity-cyber-immunity-iiot.
[99] M. Mylrea, M. Nielsen, J. John, and M. Abbaszadeh, "Digital Twin Industrial Immune System: AI-driven Cybersecurity for Critical Infrastructures," in Systems Engineering and Artificial Intelligence, W. F. Lawless, R. Mittu, D. A. Sofge, T. Shortell, and T. A. McDermott Eds. Cham: Springer International Publishing, 2021, pp. 197-212.
[100] I. T. S. I. Data, "Automation Systems and Integration—Digital Twin Framework for Manufacturing: Part 4," in "Information Exchange, ISO/DIS Standard 23247-4:2021 ", 2021. URL: https://www.iso.org/standard/78745.html
[101] NIST, "The NIST Cybersecurity Framework 2.0," URL: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd, 2023.
[102] ISO/IEC, "Cybersecurity," in " IoT security and privacy — Guidelines," URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27400:ed-1:v1:en, 2022.
[103] Y. Wu, K. Zhang, and Y. Zhang, "Digital Twin Networks: A Survey," IEEE Internet of Things Journal, vol. 8, no. 18, pp. 13789-13804, 2021, doi: 10.1109/JIOT.2021.3079510.