Journal of Systems Architecture 151 (2024) 103120

Contents lists available at ScienceDirect

Journal of Systems Architecture

journal homepage: www.elsevier.com/locate/sysarc

A comprehensive survey of digital twins: Applications, technologies and security challenges

Sekione Reward Jeremiah [a], Abir El Azzaoui [b], Neal N. Xiong [c], Jong Hyuk Park [b,*]

[a] Department of Electrical and Information Engineering, Seoul National University of Science and Technology, 232 Gongneung-ro, Nowon-gu, Seoul, 01811, South Korea
[b] Department of Computer Science and Engineering, Seoul National University of Science and Technology, 232 Gongneung-ro, Nowon-gu, Seoul, 01811, South Korea
[c] School of Resources Engineering, Xi'an University of Architecture and Technology, Xi'an, Shaanxi, China

ARTICLE INFO

Keywords:
Digital twin
Virtual twin
Digital twin security
Digital twin network
Digital twin modeling
DT enabling technologies

ABSTRACT

Alongside advancements in Artificial Intelligence (AI), significant progress has been made in big data processing, edge/cloud computing, and ubiquitous computing in the past two decades. These advancements catalyzed the development and adoption of Digital Twins (DT) across various domains, serving as virtual replicas of Physical Objects (POs). DTs provide advanced visualization and simulation capabilities, enabling effective estimation, optimization, and forecasting of PO's behaviors. However, the widespread adoption of DTs has introduced various security threats, vulnerabilities, and attacks. Despite ongoing research in DT applications and security, there is a lack of systematic review of the DT security literature across domains and architectural layers. This study fills this gap by systematically reviewing DT research, focusing on three interrelated aspects: DT applications, architectural layers, and security. We explore DT's architectural layers, functional requirements, application, and creation software to identify potential threats, attacks, and vulnerabilities specific to DT layers and application domains. We then systematize our findings under a unified security framework and pinpoint countermeasures against identified security challenges. Furthermore, our study explores DT's role in mitigating existing cyber threats, and we conclude our work by identifying open challenges and potential research directions.

1. Introduction

A Digital Twin (DT) is a virtual representation of a Physical Object (PO), capable of simulating and analyzing the PO's performance in the real world. Digital twins use mathematical models [1,2], application programming interfaces (APIs), and specification-based technologies [3,4] to characterize physical assets. DTs run on containers, virtual machines (VM), or servers to enable the storage of digital assets. The primary objective of having DT in place is to foresee variations, errors, and other abnormalities that can alter a system's natural or default behavior. Digital twins can be used on the Internet of Things (IoT) and Cyber-Physical Systems (CPS) to improve the design, operation, and maintenance of physical assets, such as buildings, machines, and infrastructure.

Digital twin solutions have already been explored and deployed in several domains, particularly the industrial sector. In the oil and gas industry, digital twins monitor and optimize drilling operations, predict equipment failure, and improve safety [5–7]. Transportation companies use digital twins to simulate traffic flow, optimize logistics, and enhance the passenger experience [6,7]. Similarly, for Automated Guided Vehicles (AGVs), DTs are applied to simulate and optimize their movements and operations, enhance safety protocols, predict maintenance needs, and improve overall system efficiency [8]. Water management organizations use DTs to model water distribution networks, predict water usage, and detect leaks [9]. In the electrical energy sector, DTs are used to monitor and control power generation [10], transmission [11], and distribution [12–15].

In the chemical and petrochemical industry, digital twins simulate chemical reactions, optimize production processes, and reduce emissions [16,17]. Manufacturing companies use digital twins to simulate production lines, optimize product design, and improve quality control [18–20]. In the automotive industry, digital twins simulate vehicle performance, test new features, and improve safety [21–23]. In healthcare, DTs are used to model patient anatomy and simulate medical

This research was supported by the National Research Foundation of Korea(NRF) funded by the Ministry of Science and ICT (2022K1A3A1A61014825)
* Corresponding author.
E-mail address: jhpark1@seoultech.ac.kr (J.H. Park).

https://doi.org/10.1016/j.sysarc.2024.103120
Received 31 May 2023; Received in revised form 7 January 2024; Accepted 21 March 2024
Available online 27 March 2024

procedures [24,25], enabling personalized treatments and reducing risk.

Given the widespread adoption of DTs in industries ranging from chemical and petrochemical to healthcare, their role in optimizing processes, enhancing safety, and personalizing treatments is undeniably significant. However, this growing dependence on DTs raises critical questions about their security, especially given their integration with sensitive data and IoT devices. The features that make DTs invaluable - their real-time integration with sensitive data and IoT devices also make them vulnerable to cyber threats. Addressing DTs' security concerns becomes paramount, especially as their complexity grows, necessitating a robust security framework to safeguard them against potential cyber threats and data breaches [26].

The importance of addressing security issues in DTs becomes evident when considering incidents like the February 2022 cyber-attack on Toyota's supplier, Kojima Industries Corp [27]. This incident led to the loss of around 13,000 cars of output and highlighted the significant impact of cyber-attacks on industrial operations. Another notable instance is the May 2021 ransomware attack on the Colonial Pipeline, which caused fuel distribution disruptions along the U.S. East Coast [28,29]. Though not a DT system, this incident explains the cascading repercussions of cyber vulnerabilities in such critical infrastructure and the heightened risks as DTs gain traction in managing such infrastructures.

Moreover, the variability of DT building blocks is among the fundamental problems constituting DT security issues. Several hardware components are deployed on DTs, including embedded systems, actuators, and sensors equipped with several proprietaries and commercial software products. DTs are also made up of layers where each layer creates a collection of critical services (i.e., data collecting and dissemination, synchronization, modeling, simulation, and representation) offered by various interfaces, technologies, and computer systems. Therefore, it is crucial to examine DT security based on its layers [30,31].

Furthermore, the DTs' layered architecture and diverse components deployed on each layer underscore the complexity of their security landscape. This structural complexity necessitates a thorough understanding of DT architecture for effective security solutions. Recognizing each layer's distinct roles and vulnerabilities allows for a more targeted approach to identifying and mitigating security threats. Therefore, in this study, we categorize the security issues according to DT layers and their accompanying technologies since integrating these technologies and computing systems also results in substantial security issues [32–34].

This comprehensive categorization of security risks based on the layered structure of DTs paves the way for identifying vulnerabilities specific to layers. Our study also proposes effective strategies to prevent attacks by pinpointing these weak points. In doing so, we extensively survey the latest advancements in DTs, covering DT's categories, definitions, applications, software, architecture, and security challenges. We propose a detailed three-dimensional security framework, as depicted in Fig. 1, which systematically addresses the security challenges across different DT layers and application domains, expanded in subsequent sections.

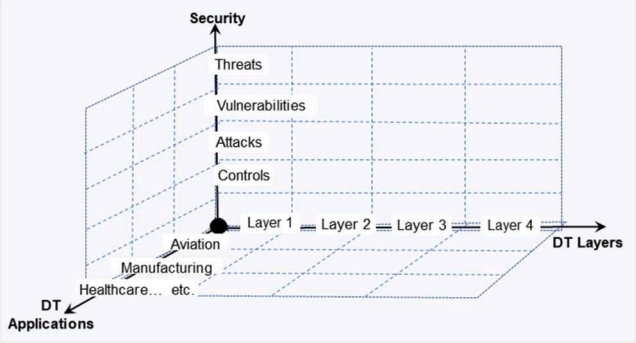

Fig. 1. DT Security Framework.

1.1. Our contribution

To supplement prior efforts in DT surveys focusing on applications and security challenges, we comprehensively study DT technologies, security and privacy threats, and their technical countermeasures. Furthermore, our work also sheds light on other DT aspects, including application domains, categories, definitions, software, and tools. Our study's main contributions are outlined as follows:

- Our research identifies DT categories and definitions, application domains, and the relevant software and tools for DT creation/modeling.
- We propose a detailed digital twins security framework consolidating prior research. Following a well-known taxonomy of threats, attacks, controls, and vulnerabilities, we make understanding and analyzing DT security issues across domains and architectural layers easier. Additionally, we investigate potential sources of threats to digital twins and the motivations behind them with actual examples.
- We survey and analyze various attack methods on digital twins, including manipulating normal behavior and exploiting real-time conditions to compromise security.
- We provide approaches to secure DTs from the identified attacks and illustrate this with a blockchain-based case scenario. We also identify ways DT can solve security challenges across different application domains.
- We provide recommendations and best practices to improve DT's security, and lastly, we identify unsolved issues and challenges.

1.2. Paper organization

Fig. 2 provides an overview of our paper's organization, which unfolds as follows: Section 2 presents background and related research, and Section 3 focuses on DT technical aspects such as architecture, functional requirements, technologies, and tools. Section 4 elaborates on DT threats, vulnerabilities, attacks, countermeasures, solutions to security issues employing DTs, and a blockchain-based case scenario. Section 5 presents security-related and general challenges facing digital twins, our recommendations, open research challenges, and future directions. We conclude our study in Section 6.

2. Research background

This section analyzes the scientific literature on digital twins to explore the current research and advancements in developing and using them. We provide an overview of the recent trends in digital twin technology (digital twin evolution) and DT categories and definitions based on different perspectives, such as functionalities and characteristics. The section also comprehensively compares our work and existing surveys on digital twin applications and security challenges.

2.1. Key considerations and methodology

To identify and understand the digital twin's characteristics, categories, definitions, requirements, and security challenges, we chose the following general research questions at the start of our study to guide our research:

1) RQ1: What are the common/shared definitions for DT published literature? Are there any common attributes for the available definitions, and can they be categorized?

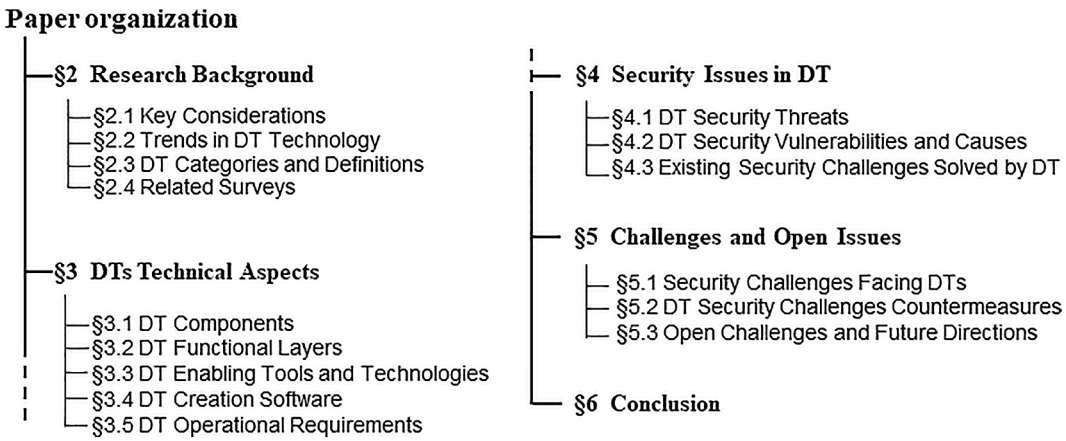

Fig. 2. Overview of the paper.

2) RQ2: In what domains is the DT being applied? What significant situations and scenarios might fully benefit from leveraging digital twins?
3) RQ3: What are DT's characteristics and technological requirements? What technology and tools are available to support DT communication, data handling, modeling, visualization, and security? Are there any commercial or free platforms that can assist in implementing DT?
4) RQ4: What are the challenges and solutions to DT security? Can DT solve existing cybersecurity challenges?

2.2. Trends in DT technology

Over the past five years, there has been a notable surge in interest and research surrounding digital twin technology, its security concerns, and the development of specialized software for its creation and implementation. The normalized number of Google searches for the words "Digital Twin," "Digital Twin Security," and "Digital Twin Software" over the previous five years is shown in Fig. 3. The value shown on the Y-axis represents the user's interest, varying from 0 to 100, where 100 represents the highest level of popularity the search term gained within the designated time window, and 0 means the lowest. This growing trend, as evidenced by increasing search queries and academic focus (See Fig. 4), underscores DT technology's rapidly expanding role in various industries, including manufacturing, healthcare, and urban planning.

Moreover, for this study, we searched Google scholar for digital twin-related keywords between 2010 and 2023 to obtain the literature on DT's applications and security. Our search was restricted to Google scholar to avoid bias [35] and favor specific publishers. This search was aimed at finding answers to our RQ2. We searched using the query {intitle: "Digital Twin"}, which returns results where "Digital Twin" appears in the paper's title. While our search query is designed to focus on the title and potentially capture instances where "Digital Twin" is a keyword, Google Scholar does not provide a way to strictly limit the search to only the keywords section. However, there's a good chance that papers with the term "Digital Twin" in the title will also have it listed as a keyword, given its relevance.

Fig. 4 illustrates the annual scientific publications of DT-related studies from 2010 to 2023. Notably, there has been a significant publication surge since 2018, peaking in 2023. From the DT publication statistics shown in that exact figure, approximately 92.3% of the papers were published between 2020 and 2023. The substantial escalation in the volume of DT scholarly publications from 2020 to 2023 signifies a robust and expanding academic and industrial engagement with DT technologies. This trend reflects the convergence of advanced computational capacities and intensified research interest, which collectively boosts the application of DT across various sectors. Moreover, the COVID-19 pandemic breakout has accelerated digital innovation, encouraging DT adoption in remote operations and system management.

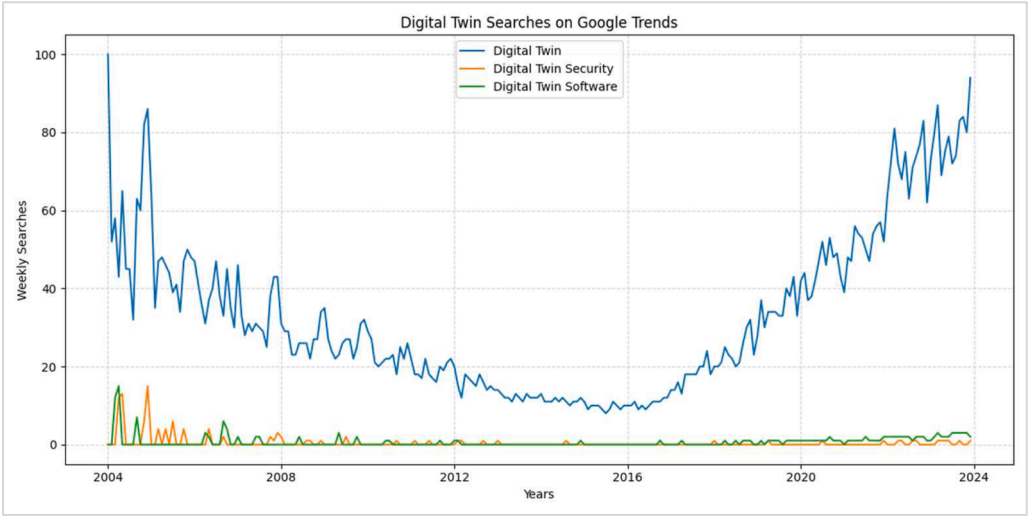

Fig. 3. DT technology, security, and software interest trend as seen through Google searches.

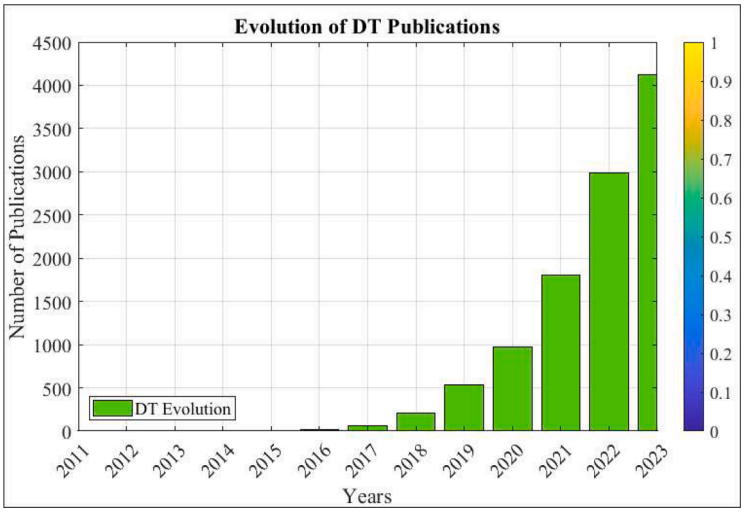

Fig. 4. Analyzed articles timeline.

2.3. DT categories and definitions

A universally agreed upon definition of digital twin does not exist. However, it is commonly understood as a virtual copy of a real-world entity enhanced by Artificial intelligence (AI) capabilities [36,37]. The concept behind DT was first proposed in 2002 in a presentation on "Conceptual Ideal for Product Life-cycle Management" by Michael Grieves [38]. At that early stage, many of the critical features we now associate with digital twins, such as the connection between the physical and virtual worlds and the data flow between them, were already present.

The concept of a digital twin (DT) has evolved and can be interpreted in various ways depending on the context. Generally, digital twins are digital replicas of physical entities, but the depth and scope of these replicas can vary [39]. To address our first research question (RQ1), we summarized common categories of DTs for grouping definitions provided in the existing literature we analyzed as follows:

1. **Product Digital Twins:** These are digital representations of physical products. They are often used in manufacturing and product design to simulate, analyze, and test products in a virtual environment before they are built. A standard definition from the existing literature that fits this category is that of a DT as a clone or a digital counterpart [18,39]. From this definition, the authors imply that DTs are computerized clones of physical assets or the virtual counterpart of a physical system. This definition is closely related to product DTs, as it involves creating a digital replica of a physical product that can be used for various analyses and optimizations [1].

Furthermore, some studies define DTs as mirrors or replicas of their physical counterparts [30,40–44]. Again, this definition emphasizes the creation of a digital counterpart or replica of a PO or system that mirrors the object's real-world state. Based on this definition, DTs are typically used for monitoring, diagnosing, and simulating their physical counterpart using real-world data. This can help in various ways, such as improving product design, predicting equipment failure, or optimizing maintenance schedules [45].

1. **System Digital Twins:** These represent larger systems, such as factories, buildings, or cities. They integrate multiple products and process twins, providing a more holistic view. This type helps understand how different components interact and optimize overall system performance. A standard DT definition encountered from the literature that falls under this category is that of a DT as an "Integrated system" [46–48]. Existing studies define a DT as an integrated system for comprehensive, multi-scale simulations integrating PO and virtual products, data, and services [49,50].
2. **Process Digital Twins:** This DT category involves the simulation of processes. It's common in industries involving complex processes, such as manufacturing or logistics. Process DTs help optimize workflows, identify bottlenecks, and virtually test process changes. Some of the literature defines DT as a "simulation, or prediction" mechanism where the authors stress the use of DT to simulate processes, test various scenarios, and predict outcomes [22,36,51,52]. This definition emphasizes using DTs in understanding and forecasting the performance of systems under different conditions without the need to physically test them, which saves time and resources and reduces the risk of damage or downtime.
3. **IoT-Enabled Digital Twins:** In this category, digital twins are closely integrated with IoT technology. Sensors on physical objects collect data to update and refine the DT in real-time, making the twin a dynamic and constantly evolving representation of its physical counterpart. Some studies define a DT regarding ties and links, focusing on the connections between data and the real products they represent [53–55]. This definition signifies that DTs use data from IoT devices to create a link between the physical entity and its digital representation. In most cases, it happens in real time.
4. **Human Digital Twins:** This is an emerging category in which the digital twin concept is applied to human health and biology [57]. It involves creating a digital replica of an individual's health profile for personalized medicine, health monitoring, and health outcome prediction [56,57].
5. **Service Digital Twins:** This category of DTs focuses on the services aspect, often used in service operations and maintenance. For example, a service operation's DT might help predict maintenance needs or train service personnel [58–60].

Each of these categories focuses on different aspects and applications of digital twins, highlighting the versatility and broad applicability of the DT technology across various domains.

2.4. Related surveys

DT research has recently become the focus of several publications in literature. Scholarly research has extensively examined the progress and advancements in digital twin technology and applications, highlighting potential areas for further study, future innovation, and open research questions. These studies also indicate potential areas where DT

technology could provide significant business benefits in specific industries. This section offers a comprehensive overview of the recent DT surveys.

In [61], Tao et al. analyzed 50 publications and eight patents for DTs. The authors address the DT concept through DT services, simulation, and modeling. The study also covers the DTs application in manufacturing, the most dominant application domain for DTs, covering product design and production. This study draws from similar publications that are mainly concerned with state-of-the-art DT applications. Pires et al. [62] briefly outlined digital twins' fundamental concepts, technologies, and applications. The study presents a real-world example of DT use and discusses the challenges that must be overcome to become widely adopted across industries. Moreover, the study highlights ongoing research in creating a digital twin for a collaborative robot.

He et al. [63] conducted a study that primarily concentrated on DT's capabilities to control and monitor various industrial settings. However, the study does not stress DT definitions and applications outside the previously identified domain. The authors present technologies capable of transforming the digital twin into a cutting-edge method for some surveillance applications.

Biesinger et al. [64] conducted a study to determine the importance of integration DTs in the planning processes of the automobile sector. Unlike the other articles, which focused on evaluating scholarly publications, this research interviewed 22 participants from diverse industries, including automotive manufacturing. The study aimed to answer the demand for a simple and adaptable DT for a particular use case, mainly related to integration planning. This study is a good indicator of DT's industrial market potential. However, the study does not provide tools, technologies, and solutions that may help DT deployment per their guidelines.

The DT's definitions, applications, and design implications are the subject of research by Barricelli et al. [65]. This study covers the detailed evolution of the DTs. The authors answer questions concerning DT definitions, key characteristics, and the application domains, including healthcare, aviation, and manufacturing. The authors discuss several DT implementations and the design implications and challenges programmers should consider while creating such a system. In contrast, our study aims to extend ideas in this work by delving into further depth on the DT's categories, security issues, tools, and technologies that enable DTs.

Fuller et al. [66] evaluated DT, emphasizing how it integrates with IoT and data analytics technology. The research also highlights the need for a consistent DT definition encompassing every aspect of DT. The study further examined DT-supporting technologies and applications focusing on manufacturing, healthcare, and smart cities. Building on Fuller's work and similar studies, our study aims to complement these studies by providing an in-depth analysis of the DT, including tools and software for DT design, creation, and visualization.

Huang et al. investigated the application of AI-driven DTs in intelligent manufacturing and cutting-edge robotics [67]. The study details the benefits of implementing a DT in production planning and management, quality control, predictive maintenance, and other services to achieve sustainability in manufacturing and robotics. They also elaborate on how AI technology enables the use of DTs in these industries. Rasheed et al. [68] evaluate DT's value, the technology behind it, its use cases, and the obstacles it faces. The study also investigates the potential socioeconomic impacts of DT technology and compiles research from various industries where it has been implemented and evaluated.

Löcklin et al. [69] published a work focusing on DT applications in verification and validation use cases. In this study, DT is primarily used to monitor, verify, and validate physical assets to provide meaningful feedback based on the acquired data. This research also discusses how the DT may be used for verification and validation. The survey is devoted to researching the DT application possibilities for validation and verification purposes across various industrial fields.

Minerva et al. [70] examine numerous DT applications highlighted in research on various technical and industrial areas, including manufacturing, multiagent systems, virtualization, and IoT. In addition, the authors demonstrated several crucial DT qualities and attributes that were frequently ignored in other studies. Such attributes include data ownership, contextualization, augmentation, etc. Before identifying specific DT applications, the paper analyzes DT market potential. While the survey covers DTs-supporting technologies and applications, the particular tools and technologies (software) that can create DTs for such applications are not covered in depth, and our study bridges that gap.

Holmes et al. [71] explore the potential dangers of DT and examine ways it can be utilized to reduce cyber-security risks. The paper investigates how DTs can be part of a robust defense system by understanding the cyber-security risks that may arise from their integration with physical systems. The study concludes that DT can enhance system security by providing an additional defense against cyber-security risks. However, given the rapid evolution of DTs, there are still many unknowns regarding the potential vulnerabilities arising from their integration into existing systems. Additionally, with the rapid evolution of cyber-security threats, there is a need for additional investigation to comprehend the extent of the danger associated with DTs, as presented in this paper.

Vukovic et al. [72] conducted a survey study providing design guidelines and standards for creating DTs in the Industrial Internet of Things (IIoT). Their study focused on understanding what protocols should be used when connecting a DT with its corresponding PO so it can communicate effectively. It also looks at how computational power available on IIoT edge devices can help reduce latency and improve scalability when developing a DT model. However, this study's focus was surveying the design guidelines for creating DTs in IIoT.

The study by Alcaraz et al. [73] examined the existing state of DT and its dangers. Their analysis considered DT's functionality layers and operational requirements for a complete classification. The study provides an initial set of security recommendations for ensuring the responsible use of DTs. The study concludes that there needs to be an increased focus on risks involved with DT deployment due to potential security threats. This paper also classifies these potential threats based on DT's functionality layers and operational requirements and provides preliminary security recommendations for ensuring the responsible use of DTs.

In [74], the authors systematically analyzed DTs within the energy sector. They provide the DT landscape through a Systematic Literature Review (SLR), searching through academic databases to extract significant insights and observable patterns from the publications. This study reveals DTs' diverse energy generation, storage, transmission, and consumption functions, underscoring DTs' prevalent application in the energy sector. The paper's methodology and content greatly support our survey by shedding light on critical applications and difficulties, which we then critically evaluate to pinpoint new ground and advance the conversation.

In another recent review of DT applications within the Architecture, Engineering, and Construction (AEC) industry, Zhang et al. [75] discuss the applications and enabling technologies during the operation and maintenance stages. Their systematic analysis of existing publications from 2016 to 2023 maps out the prevalent DT technologies and identifies critical gaps and opportunities for future research. This review sets a foundational understanding for our study, highlighting the significance of integrating DT at the maintenance phase to enhance efficiency and safety.

Moreover, the survey by Liu et al. [76] examines the integration of DTs in smart manufacturing, presenting a thorough analysis of 117 articles from 2017 to 2022. The paper defines DTs, elaborates on their core elements, and explains their applications across various domains. Through their analysis, the authors underscore the significance of virtual models and twin data. Another review study by Liu et al. [77] comprehensively analyzes DTs in machining. The study examined the evolution of DT-driven machining. The key findings include identifying

various DT models, their operational processes, and the services they offer in the machining system.

Nica et al. [76] present a review focusing on DT technologies in urban governance. It integrates diverse research and examines how DT simulation, spatial cognition algorithms, and multi-sensor fusion technology contribute to sustainable urban governance. The paper stands out for its systematic analysis, encompassing recent literature and employing tools like PRISMA and bibliometric mapping for a comprehensive review. These insights are valuable for our study, offering a broad perspective on applying DT in urban governance and paving the way for further exploration.

The review study presented in [78] explores the integration of DT technology in energy storage systems. The paper analyses existing literature, identifying critical technological advancements and applications of DT in this domain. It offers an overview of DT definitions and their application across various energy storage domains. A different study on DTs by Attaran and Celik [80] surveys DT technologies and applications across diverse industries. The paper offers DT's definition, explains their enabling technologies, and presents an overview of their application domains, ranging from manufacturing to healthcare.

The study by Weil et al. [81] focused on Urban DT (UDT) challenges and presented a systematic review examining critical issues in implementing UDTs for sustainable smart cities. It identifies key challenges across categories like interoperability, infrastructure, data acquisition, and quality while addressing planning, prediction, and ethical aspects. The study highlights the evolving understanding of UDTs in urban management and planning. This paper's findings underscore the multifaceted nature of UDT challenges, emphasizing data and model semantics, infrastructure constraints, and the need for more effective data harmonization.

Yin et al. [82] compiled and analyzed works focusing on integrating Augmented Reality (AR) with DTs, highlighting its transformative impact on various industrial sectors. The work categorizes AR-assisted DT applications throughout the engineering lifecycle, emphasizing their role in enhancing human-machine interactions and optimizing processes. Key findings include identifying emerging trends, technological advancements, and potential challenges. The study evaluates the current state and points towards future directions, forming a seamless transition to other works in domains related to digital twins.

Based on the abovementioned studies, Table 1 highlights our study's novelty by comparing its contributions with those of previous surveys. This study thoroughly analyses DT concepts to supplement earlier publications in application domains, enabling technologies and tools, and architectural and functional requirements. It also provides an in-depth analysis of security challenges solved by DTs and security challenges facing DTs across various application domains.

3. DTs technical aspects

In addressing our third research question (RQ3), we present our findings on the characteristics and technological requirements necessary for deploying DTs. This section also offers technologies, tools, and software that facilitate DT communication, data handling, modeling, visualization, and security. Our conceptual model is rooted in the framework provided by [15,31,39,71,74] to abstract the DT functional layers discussed in our study. Building upon these foundational studies, we have dedicated Section 3 of this paper to comprehensively examining the DT technical landscape.

Table 1
Paper's contribution in contrast to existing publications.

Contribution References	Publication Year	DT Definitions	DT Enabling Technologies	DT Application Domains	Software (Tools)	DT Security Challenges	Security Challenges Solved by DT	DT Security Framework
Tao et al. [61]	2018	✓✓	✓✓	✓✓	×	✓	×	✓
He et al. [63]	2018	✓	✓	✓	×	✓	×	×
Pires et al. [62]	2019	✓✓	✓	✓	×	✓	×	×
Biesinger et al. [64]	2019	✓	×	×	×	✓	×	×
Barricelli et al. [65]	2019	✓✓	✓	✓	✓	✓	×	×
Rasheed et al. [68]	2020	✓✓	✓	✓	×	✓	×	×
Fuller et al. [66]	2020	✓	✓	✓✓	×	✓	×	×
Löcklin et al. [69]	2020	✓	✓	✓	×	✓	×	×
Minerva et al. [70]	2020	✓	✓	✓	×	✓✓	×	×
Huang et al. [67]	2021	✓	✓	✓	×	✓	×	×
Holmes et al. [71]	2021	✓	×	×	×	✓	✓✓	✓
Vukovic et al. [72]	2021	✓	✓	✓	×	✓	×	×
Alcaraz et al. [73]	2022	✓	✓	✓	×	✓	×	×
Doamaral et al. [74]	2023	✓	×	✓	✓	✓	×	×
Zhang et al. [75]	2023	✓	✓	×	✓	✓	×	×
Liu et al. [76]	2023	✓✓	✓	✓✓	✓	✓	×	×
Liu et al. [77]	2023	✓	✓✓	✓	×	×	×	×
Semeraro et al. [78]	2023	✓	✓✓	✓	×	✓	×	×
Nica et al. [79]	2023	✓	✓✓	✓✓	×	✓	×	×
Attaran et al. [80]	2023	✓✓	✓	✓	✓	✓	×	×
Weil et al. [81]	2023	✓✓	✓	✓✓	×	×	×	×
Yin et al. [82]	2023	✓✓	✓	✓✓	×	×	×	×
This study	2024	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓

✓✓: Extensively Covered ✓: Extensively Covered ×: Not discussed.

We divide the DT framework into four functional layers, describing each layer's role within the broader DT architecture. This structural partition is visually represented in Fig. 5 and explained in detail in the following sections. Herein, we explore both commercial and free platforms, assessing their capabilities and limitations in supporting the operational requirements of DTs. This section offers the DT ecosystem's characteristics, tools, technologies, and components, providing substantial insight into RQ3.

3.1. DT components

According to the literature, DTs have three essential components: the physical object in real space, the virtual product in virtual space, and the information or data that links the virtual and physical objects together [44,83]. While the prior components are the most common, some existing studies put the DT component from five-dimension perspectives. From the five dimensions point of view, DT comprises physical entities, virtual models, data, services, and connections [84]. Notably, the components of a DT can vary depending on the application and the industry. However, these are the essential components commonly found in most DT implementations. In this section, we have expanded these critical components and discussed each of them in detail below:

A. **A digital representation** of a system or a PO can include detailed information about its design, manufacturing, and operational characteristics.
B. **Sensors and other data collection devices** gather data about the physical object or system, such as its location, performance, and condition.
C. **A software platform** that can process and analyze the data collected from the sensors and other data collection devices to create a detailed and accurate representation of the PO or system.
D. **A user interface** is an essential component of a digital twin system, allowing users to interact with the DT and access its information. A user interface enables users to interact with the digital twin to view its status, run simulations, or change its configuration. A user interface typically includes a visual display of the DT, such as a 3D model or dashboard, and interaction tools like buttons, sliders, and other controls [42]. A user interface can also run simulations or change the DT's configuration by adjusting parameters or testing different scenarios. This helps users understand how the physical twin would behave in other conditions and identify potential issues or opportunities for improvement.
E. **Communication** allows the DT to be connected to other systems, such as enterprise systems, cloud-based services, or other DTs [85]. The communication procedures that must be developed for DT fall into three main categories: between the domain user experts who interact with the DT through Human-Machine Interface (HMI), between the DT and the physical twin, and between DTs within the same virtual environment or in nearby settings [65].
F. **Data Storage and Processing:** Data is the backbone of digital twins. Some experts have expanded the original digital twin concept to include data and services [46,83]. All data that is exchanged must be stored in a data repository accessible to DT, which results in a significant storage demand [72]. This data can include historical data, metadata, and derived data [42]. To manage high-dimensional data effectively, digital twins employ advanced techniques for handling, analyzing, and decoding high-dimensional data and algorithms for merging multiple data sources to produce more accurate and valuable information [43,86,87].
G. **Statistical and AI algorithms** can analyze data and provide insights, predictions, and recommendations. Digital twins also depend on AI to adapt and improve as new data is generated. To reduce the cost of storage and computation, the preferred AI techniques should be able to minimize data dimensionality while still preserving the

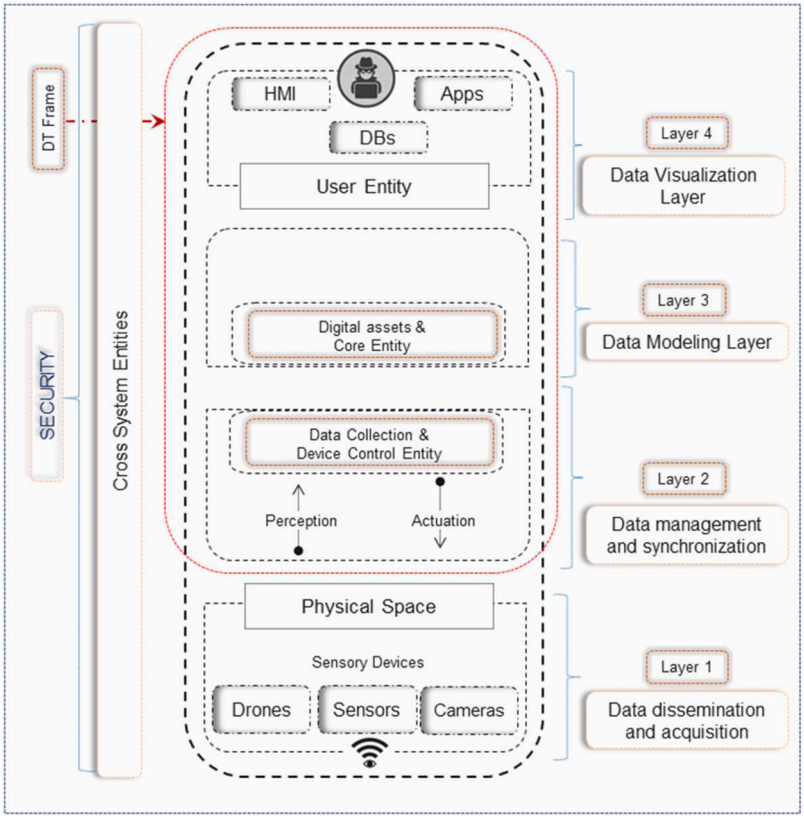

Fig. 5. Simplified DT Architecture ([15,31,39,71,74]).

most valuable data for the DT [44,88]. DTs use statistical applications, pattern recognition, and unsupervised/supervised learning to process and analyze data from the physical twin and its surrounding environment. It enables the detection of changes and the identification of patterns and trends [42].

The DT's ability to adapt and adjust its parameters closely mirrors its physical twin throughout its lifecycle. Implementing a modular and parameterized DT can make this process more efficient. Modularity ensures that changes to one module do not affect the others. Parameterization allows quick and easy adjustments to the DT's status. Algorithms such as stochastic optimization or evolutionary algorithms can be used to determine the best parameter values for matching the DT to its physical counterpart [43].

H. **Security and access control components** are essential to ensure the integrity and confidentiality of the data and the design [89,90]. Security and access controls ensure the data and system integrity and confidentiality. Some examples of security and access control components in the DT system include authentication and authorization elements, intrusion detection and prevention components, and data leakage prevention components [91–93].

3.2. DT functional layers

Digital twin technology can have multiple layers [94], depending on the specific application and the level of detail required [95,96]. A DT typically includes a physical, data, and model layer. The physical layer represents the actual physical asset or system being monitored. The data layer collects and stores data obtained from the physical asset. The model layer uses this data to create a digital asset representation, which can be used for simulations, analysis, and forecasting. Additional layers, such as a knowledge layer, can also be added to provide more advanced capabilities. Similar to [15,31,65,70,73], we identify four functional layers of digital twins based on data acquisition to the visualization stage, depicted in Fig. 5 and explained in detail in the following subsections. It is also worth noting that the simplified architecture provided here is specific to the "IoT-enabled digital twins" category, as was elaborated in Section 2.1.

1. **Layer 01 - Data Acquisition Layer**

This is the lowest DT layer responsible for data acquisition and dissemination. The data acquisition layer for a DT is responsible for collecting and storing data from the physical system being modeled. This can include sensor data, performance metrics, and other relevant information. The data is then used to update the different layers of the digital twin, such as the physical, functional, and behavioral layers, to ensure that the digital twin accurately represents the system [73]. The Data Acquisition Layer also includes data validation and quality assurance methods to provide accurate and reliable data [97]. This layer also enables data sharing and integration with other systems, allowing the digital twin to be used in various applications and workflows.

2. **Layer 02 – Data Synchronization Layer**

This layer is concerned with data synchronization and management, providing layer 3 with essential services and data that it needs. The Data synchronization layer in DT offers a mechanism by which data is transferred and shared between the PO and its digital representation. This layer guarantees that the digital replica precisely reflects the current state of the PO or system by continuously synchronizing data between the two. This can include data such as sensor readings, status updates, and configuration changes. The data synchronization layer also allows for bidirectional communication, enabling the digital twin to control and interact with the physical system.

3. **Layer 03 - Data Modeling Layer**

The digital twin entity is the third layer, and data modeling occurs at this layer. This layer uses digital models to specify behavior, states, and geometric forms, allowing for monitoring, diagnosing, and maintaining cybersecurity issues. The modeling layer provides a way to structure and organize the data representing the physical object or system. This layer provides a logical representation of the physical system and its components, functions, properties, and relationships, which can be used to make predictions, analyze data, and identify patterns. It also allows for integrating data from multiple sources, such as sensor readings, historical data, and simulations. This layer is vital to understanding and analyzing the data from the physical system. It is often used to generate insights, perform simulations, and make decisions that can improve the performance or maintenance of the physical system [98,99].

4. **Layer 04 – Data Visualization Layer**

This layer is concerned with data accessibility and visualization. This layer provides a way to present the data representing the PO or systems [100,101]. It provides a graphical representation of the data, making it easy to understand and interact with 2D/3D visualizations, interactive dashboards, and virtual and augmented reality (VR/AR) interfaces. The data visualization layer allows users to monitor the status of the physical system easily, identify patterns, and make decisions. It also enables users to interact with the digital twin and control the physical system, providing a seamless experience across the digital and physical worlds. The data visualization layer is also used for training, testing, and debugging [98], allowing developers to test different scenarios and improve the physical system's performance [99].

3.3. DT enabling technologies

The complexity of the DT is reflected in the combination of technologies required for its implementation. Table 2 represents the most frequent Industry 4.0 DT enabling technologies and tools we identified

Table 2
DT Enabling Technologies and Tools.

Tools	Technologies
Layer 04 – Data Visualization and Access Layer	
• HMI (Visualization Software) • Dashboarding Tools • Reporting Tools	• VR/AR Technologies • Web Portals • Mobile Apps
Layer 03 - Data Modeling Layer (Modeling, Representation)	
• Agent-Based Simulation • Discrete System Dynamics • Event Simulation • Petri-Nets, CAD	• IronCAD, Anylogic, FlexSim, Simio, Arena • Enterprise SolidWorks • AutoCAD, Dynamics • FreeCAD, AutoMod
Data Analytics	
• AI Models (K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN) • TensorFlow, Keras	• Artificial Intelligence • Machine Learning • Deep Learning
Layer 02 – Data Synchronization and Management Layer	
• Databases (e.g., SQL, NoSQL) • Data Warehouses • ETL Tools	• Cloud Services (e.g., AWS, Azure) • Data Lakes • Middleware
Layer 01 - Data Acquisition and Dissemination Layer	
• Arduino • Eclipse IoT Project • NodeRED, Kinoma • Modbus Examiner • IoT Sensors • Smart Meters • Wearable Devices	• Modbus • MQTT • Smart sensors • TCP-IP • OPC-UA • SAGIN Networking (Space-Air-Ground Integrated Network)

in articles we reviewed in our work. Tools are specific software or hardware used to accomplish DT-related tasks. For instance, using Computer-Aided Design (CAD) software for modeling or Arduino for data acquisition. Technologies are broader concepts or frameworks that can be applied in various ways. For example, machine learning technology can be implemented using tools like TensorFlow or Keras. Consistent with [102], CPS is the most frequently used technology, followed by AI-related technologies, VR, AR, Big Data (BD), and IoT technologies.

Incorporating big data strategies is vital in managing large amounts of data DTs collect. To effectively process and analyze this data, simulation, and AI techniques are crucial for monitoring, diagnosis, forecasting, and optimization tasks. Deep Learning (DL) algorithms, which can be executed on cloud-based platforms, are frequently utilized. VR, AR, and Mixed Reality (MR) technologies are often employed to enhance user engagement. IoT and networking solutions can establish the connection between the PO and DT.

Different data processing and storage technologies are also deployed for layers 2–4. For computing, edge fog, and cloud computing [104] are the most deployed to support the computation of large amounts of data and provide connections to nearby surroundings [103]. Data management requires BD techniques and AI approaches. In [52], Qi and Tao explore the challenges of incorporating big data into digital twin-based industrial environments. The complex procedures and regulations for converting, cleaning, merging, and maintaining data consistency add to the difficulties. Furthermore, the varying data structures in industrial settings can exacerbate these challenges.

Another enlightening discovery is that techniques and technologies employed in DT are not just those emerging from Industry 4.0 but are also heavily influenced by its applications. Building a model for a DT can involve using formal mathematical foundations such as Petri-Nets or visual model creation tools like CAD. Depending on the system or equipment for which the twin is being generated, intelligent sensors and communication protocols to allow data connection can be used for data collecting. The authors of [104] identified MQTT and OPC-UA as two of the most often utilized data collection communication protocols. DL algorithms are today's most used data analytics technologies. Finally, data processing may be done via edge, fog, and cloud computing technologies.

3.4. DT creation software

Based on the DT software market analysis we've conducted, fierce competition exists among the market leaders as they try to introduce novel features and cutting-edge technologies. Table 3 is a list of major players in the DT twin industry software, including Amazon, Siemens, Bosch, Microsoft, IBM, and Oracle Corporation. However, the difference between simulation and digital twins must be clarified before highlighting the representative software used in creating digital twins. Virtual model-based simulations are used by both digital twin technology and simulation; however, they differ. Digital twins have better simulation capabilities than traditional CAD and computer-aided design and engineering (CAE) software, even if CAD-CAE is appropriate for product design applications [105]. It is worth noting that, in this section, we provide a list of software tools for digital twins and not merely simulation tools. Moreover, despite the diversity and complexity of digital twins, they can be categorized into five distinct categories, as elaborated in Section 2.3. We consider those categories to identify software relevant to digital twins' creation, i.e., products, processes, services, systems, IoT-enabled, people, and places digital twins.

3.5. DT operational requirement

Digital twins have transformed how we interact with physical assets, necessitating stringent operational requirements for dependable and trustworthy DTs. Fig. 6 illustrates the main DT functional requirements

Table 3
Representative digital twin creation software.

Software	Software Description	Applicability
Commercial Software		
Simiio	When a PO's DT, or software model, is to be developed, Simio Simulation Software can be employed. Processes, people, locations, systems, and gadgets may be a part of the entity [106].	Creating a virtual copy of places, processes, procedures, or devices
Azure DT (Microsoft)	Azure DTs IoT platform constructs digital representations of things, locations, business processes, and people in the real world. This allows creators to gain knowledge to improve goods, streamline processes, and cut costs while delivering ground-breaking consumer experiences [107,108].	Use IoT spatial intelligence to create models of physical environments.
Akselos	Akselos's cutting-edge engineering simulation software is 1000 times faster than other methods, opening a wide range of opportunities throughout the product lifecycle. This software performs condition-based monitoring and preventive maintenance programs, optimizing designs and safely increasing assets' lifespans [109].	Creating a virtual copy (DTs) of products, processes, and real-world systems.
AWS IoT Twin Maker (Amazon)	AWS IoT TwinMaker simplifies the creation of DTs of real-world systems, including structures, factories, machinery, and production lines. It allows developers to mix 3D models with real-world data, utilize existing data from different sources, and generate virtual representations of any physical environment [110, 111].	Creating digital twins of real-world systems, e.g., factories.
Siemens NX software	Siemens NX software helps deliver better products faster and more effectively. With NX's next-generation design, simulation, and production solutions, companies can realize the advantages of the digital twin [112].	Creating a virtual copy of products and processes.
Oracle IoT DT	Oracle IoT production monitoring cloud gives a comprehensive view of operations by gathering data at the manufacturing machine level and basing it on the production line [113].	Creating a virtual copy of products and processes.
Open-Source Platforms		
Ditto Project (Bosch)	"Eclipse Ditto is an open-source framework that helps users build DTs of devices connected to the Internet" [114]. Because it is design-domain neutral, it can be utilized in industrial, domestic, agricultural, and many other IoT domains.	It concentrates on data modeling and connectivity.
iTwin.js (Bentley)	"A starter kit for developing web applications for infrastructure digital twins" [114]. iTwin.js uses a standard web browser to visualize and evaluate engineering change in 3D and 4D.	Focuses on infrastructure modeling.

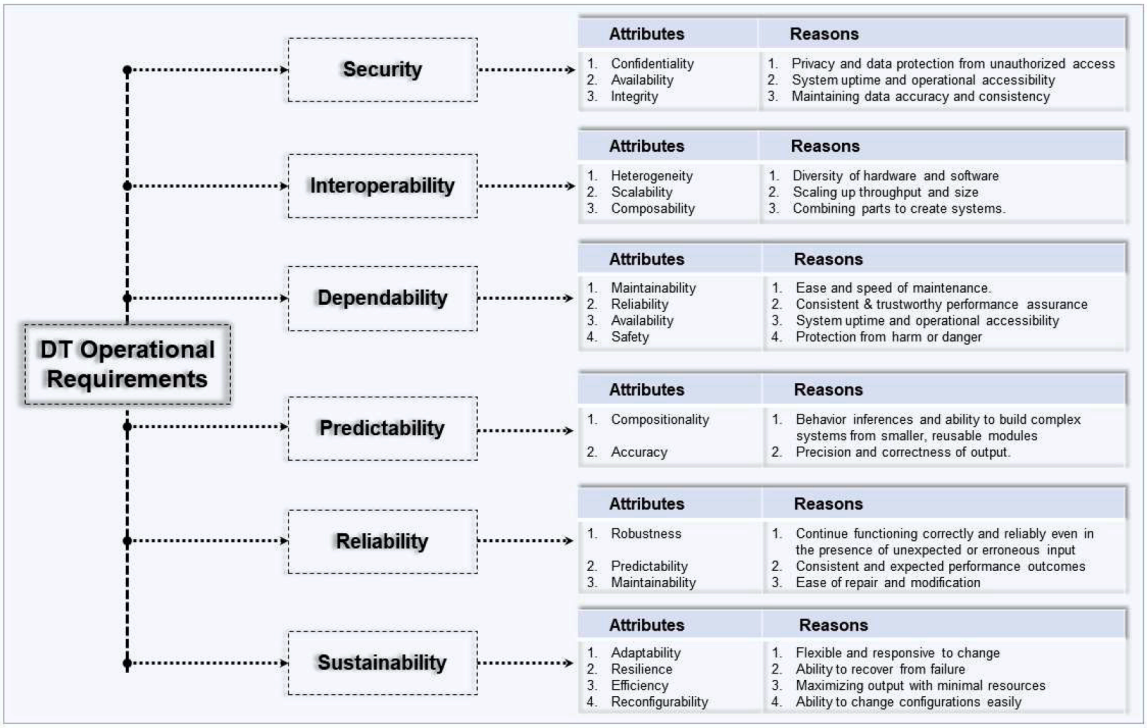

Fig. 6. Digital Twins' operational requirements and challenges ([15,31,39,71,74]).

and highlights challenges associated with their implementation. Building on previous scholarly work, such as Bächle and Gregorzik's [115] emphasis on IIoT interoperability and Durão et al.'s [116] and Moyne et al.'s [117] industry-focused insights, we synthesize their findings with additional functional requirements. The result is an expansive view of DT operational requirements and their challenges, where overlapping requirements are addressed once to streamline our discussion.

The functional requirements for dependable DT systems should be met, ensuring DT's integrity and utility in real-world applications. Moreover, the challenges chosen for discussion represent fundamental challenges facing DT's deployment and functioning. They encompass aspects like security and interoperability, which are critical for the trustworthiness and utility of DT systems, as well as dependability and predictability, which ensure that DTs can perform their intended functions reliably. Reliability and sustainability are also crucial for long-term operation, particularly in dynamic environments where conditions and requirements may change over time. Addressing these challenges is essential to advance DT technology and broaden its application across various domains.

3.5.1. *DT security*

Controlling access to resources and safeguarding sensitive information from unauthorized disclosure in DTs is essential. A secure DT system should feature mechanisms to prevent unauthorized data modification and disclosure of sensitive information. Due to their complex and scalable nature, DTs and their physical counterparts are subject to failures and attacks. Malicious attacks, such as eavesdropping, man-in-the-middle attacks, denial-of-service attacks, injection of fake sensor measurements, or actuation requests, can target the DT infrastructure to disrupt operations or steal sensitive information.

In addition, factors like the use of insecure communication protocols, the deployment of legacy systems, and the rapid adoption of commercial off-the-shelf technologies can heighten DT systems' vulnerability to security threats. Therefore, implementing robust security measures must be a top priority when designing and deploying DT systems to ensure data and resources' confidentiality, integrity, and availability. We discuss DT security requirements i.e., confidentiality, integrity, and availability (CIA).

A. **Confidentiality**: A highly confidential system uses secure protection mechanisms to prevent unauthorized access to information, disclosure, or tampering. Data confidentiality is essential in digital twin applications, where attacks targeting data transmitted can degrade system efficiency. Unsecured data transmission channels can result in critical data being eavesdropped on, injection of malicious data into the network, or the data flow being redirected over compromised sensors. Encryption, access control mechanisms, and intrusion detection systems can help maintain data confidentiality reasonably across all DT application domains.
B. **Integrity** is a critical property of a DT, implying its ability to protect itself and its data from unauthorized modification or manipulation to maintain accuracy and correctness. A DT with high integrity must have robust authorization and consistency check mechanisms [118]. To achieve that, various integrity check mechanisms must be incorporated into the DT architecture. These mechanisms include regular checks on network packet integrity, active monitoring of false data injection to identify malicious behaviors, or identification of compromised actuator or sensor components.
C. **Availability** refers to the ability of a DT system to remain accessible and operational even in the presence of faults. A DT with high availability is designed to isolate any malfunctioning components or services from the rest of the system and continue functioning without them. Cyber-attacks, such as denial-of-service (DoS) attacks, can significantly disrupt the availability of a system's services. For example, in the digital twin of medical systems, the availability of medical data is critical for timely and accurate decision-making that could save a patient's life. Attacks or malfunctioning of such a system can render data and services inaccessible. This, in turn, can jeopardize a patient's well-being and harm the patient's health.

Fault-tolerant mechanisms must be incorporated into the DT system design to ensure high availability during its operations. These

mechanisms may include backup systems and fail-over procedures that maintain system operation despite failures or attacks. Overall, availability is critical for a digital twin, particularly those working with safety-critical systems. Maintaining continuous access to essential data and services is necessary for the system's success and the safety of the people it serves.

3.5.2. Interoperability

Interoperability in DT environments refers to the seamless collaboration and information exchange among various components, systems, or devices to deliver desired services or functionalities [118]. In a manufacturing plant's DT, interoperability would mean that various sensors, controllers, machines, and software systems can communicate and exchange data, enabling seamless monitoring and control of the entire plant.

A highly interoperable digital twin system should be designed to enable effective communication and collaboration among its various components, including machines, software applications, and databases. Ensuring the system operates effectively and provides the desired services is critical, even in complex and dynamic environments. For example, in the case of unmanned air vehicles (UAVs) monitored through real-time DTs, the lack of interoperability standards can lead to the failure of critical missions. UAVs necessitate uninterrupted communication among themselves and multiple ground stations to undertake extensive military or civilian operations. Developing and testing dynamic standards for devices, systems, and processes used in UAV DT deployments is critical to ensuring interoperability under realistic operating conditions. Interoperability is comprised of the following aspects:

A. **Compossibility** refers to the ability of digital twin components to be combined and integrated to form larger, more complex systems. Digital twin components should be designed to be modular and flexible, allowing them to be quickly composed into larger systems without requiring extensive modification. Composability enables digital twin components to exchange information and seamlessly provide specified services.
B. **Heterogeneity** refers to the diversity of digital twin components with different hardware, software, or communication protocols. Digital twin systems should be designed to be heterogeneous, allowing components from various vendors and platforms to integrate seamlessly. Heterogeneity requires the development of interoperability standards and protocols that will enable components to communicate and exchange information effectively.
C. **Scalability** refers to the ability of digital twin systems to expand and accommodate increasing numbers of components and users without compromising their performance or functionality. DT systems should be designed to be scalable, allowing them to handle growing volumes of data, users, and processes. This requires using distributed architectures, cloud computing, and other scalable technologies to ensure that they can accommodate future growth [119,120].

3.5.3. Dependability

Dependability is another critical factor in establishing trust in DT and the data it produces. A highly dependable DT should operate seamlessly, deliver accurate and timely insights, and not encounter critical errors or issues during operation [121]. DT should be able to perform required functionalities and tasks without significantly degrading performance and accuracy. Assessing dependability in a DT before its actual operation is challenging. Factors like delayed actuation and uncertain or incorrect sensor readings may affect dependability, leading to unanticipated consequences after implementation. Moreover, digital twins and their physical counterparts are interdependent. Their interactions during the operation make dependability analysis challenging. DT's dependability attributes are the following:

A. **Maintainability** is a DT requirement that allows it to be repaired quickly, easily, and at a minimum expense in case of failure [118]. This can be achieved through autonomous predictive and corrective diagnostic mechanisms that continuously monitor and test the infrastructure, helping to identify which units need to be repaired. Recurrent failures can be addressed by redesigning or replacing the better-quality components. Real-time data collected from DTs can be used to schedule maintenance activities, including repairs and component replacements. By prioritizing maintenance activities and reducing downtime, maintainability is critical in maximizing DT system availability and performance [43,87].
B. **Safety** allows DT to operate without causing damage, hazard, or risk, both within and outside its boundaries. Ensuring high safety standards requires adherence to general and application-specific safety regulations and deploying safety assurance mechanisms to mitigate contingencies. For instance, real-time monitoring of sustainable production and process management across the factory in smart manufacturing can improve safety measures. Integrating embedded control systems and data collection frameworks comprising sensors can facilitate automated process control and substantially improve manufacturing plant safety. By leveraging smart networked sensors, operational anomalies or failures can be swiftly detected and prevented, averting potential catastrophic incidents that may arise from such anomalies or failures.

Safety is a critical property of a DT, particularly in safety-critical systems such as smart manufacturing. The ability to operate without causing harm or risk is essential for the system's success and the safety of the people it serves. DT's safety depends on identifying potential hazards and risks during the design stage and developing appropriate safety mechanisms to mitigate them. Safety mechanisms may include fail-safe mechanisms and emergency stop systems to prevent or minimize the impact of any safety-related incidents.

3.5.4. Predictability

A DT should be able to interpret its state, behavior, and functionality quantitatively and qualitatively. To achieve a high level of predictability, a DT should effectively deliver the intended results regarding system behavior and functionality while fulfilling all the requirements. For instance, the DT of a medical system, coupled with advanced control technologies and intelligent medical devices, must be tailored to suit the patient's unique requirements. To effectively respond to patients' actions in a healthcare environment, the digital twin should possess situational awareness and adapt accordingly. However, medical devices operate in real time and are susceptible to timing constraints and uncertainties, such as jitters and delays. To ensure accurate prediction of end-to-end timing, it is essential to develop novel programming and networking abstractions, scheduling mechanisms, and resource allocation policies. These advancements are crucial for enabling precise timing management within the healthcare system.

To ensure predictability, it is necessary to understand the behavior of the system components, including the physical counterpart and DT aspects and their interactions. Analyzing the system's performance makes it possible to identify potential issues and develop appropriate mechanisms to ensure predictability. These mechanisms may include scheduling policies, resource allocation techniques, and predictive modeling to anticipate the system's state and behavior. The following are the key attributes of the digital twin's predictability requirement:

A. **Compositionality** in DT ensures that the behaviors of its components can provide insight into the overall system. Developing a highly compositional DT requires a deep comprehension of the workings of each constituent digital and physical subsystems and components. This entails creating a digital-physical methodology for piecing together the DT from individual components. Accomplishing

compositionality is challenging due to the physical subsystems' inherent unpredictability.

To achieve compositional DTs, accurate property classifications, official measurements, and standard trial environments for assessing them must be created [122]. Additionally, well-defined mathematical models must be developed for the complete system and its components. This is essential to ensure the DT's reliability, predictability, and other vital properties.

B. **Accuracy** is crucial as it denotes how closely a system's observed or measured outcome aligns with its actual or calculated effect. A system that exhibits high accuracy should be able to approach the exact outcome as closely as possible. High accuracy is critical in digital twin applications where even minor imprecision can result in catastrophic failures. For instance, consider a digital twin of an object-tracking system based on motion. If the system receives incorrect object position estimation due to a poor sensor condition, it may initiate untimely control actions that may cause the system to fail.

3.5.5. Reliability

Reliability is the level of correctness and accuracy with which a digital twin performs its intended function. To ensure the dependable performance of digital twins within dynamic and uncertain environments, it becomes imperative to quantify uncertainties during the initial design phase. Merely certifying the capabilities of a system does not guarantee that it will function correctly. A highly reliable DT ensures its functions are performed accurately and precisely. Uncertainty analysis can help to effectively characterize DT reliability by identifying potential control flow, design errors, limitations in cross-domain network connections, and accuracy of PO and digital components.

Furthermore, timing attributes, potential design or control flow errors, and network connections affect a DT's reliability. Therefore, it is crucial to consider all these factors during the design stage and develop appropriate reliability measures to ensure the DT operates accurately and correctly. The following attributes make the DT reliable:

A. **Robustness** implies the DT's ability to maintain its stable configuration and operate despite failures. A highly robust DT should withstand failures without fundamentally changing its original configuration, ensuring its operation remains uninterrupted. The presence of disturbances, including sensor noise, actuator inaccuracies, faulty communication channels, hardware errors, or software bugs, can degrade the overall robustness of a digital twin. The lack of modeling integrated system dynamics, such as actual ambient conditions in which DTs operate, the evolved operational environment, or unforeseen events, can also affect its robustness. Such factors may be unavoidable in runtime, highlighting the need for robust digital twin designs.

3.5.6. Sustainability

The digital twins should be able to endure and operate effectively without compromising their requirements while efficiently renewing their resources. A highly sustainable DT should have dynamic tuning and self-healing capabilities to adapt to unprecedented circumstances and achieve long-lasting operations. DTs must be able to support sustainable practices in various industries, such as manufacturing, construction, and energy. By using DTs, organizations must be able to reduce waste, improve efficiency, and minimize the environmental impact of their operations. DT can support sustainability in different ways, including energy efficiency, sustainable manufacturing, and predictive maintenance.

A. **Adaptability** requires a DT to be highly adaptable and adjust its configuration and state to operate effectively under varying environmental conditions. Adaptable DTs are essential to ensure the simulation accurately reflects real-world behavior and conditions, which improves decision-making, operational efficiency, and overall performance. An adaptable DT should be able to respond quickly to changing needs and circumstances.

For example, adaptability is a critical aspect of the next-generation transportation systems in the transportation industry. The DT for transportation systems should enhance performance by enabling vehicles to adjust immediately to changing operational conditions such as traffic congestion, security threats, weather conditions, flight trajectory patterns over satellites, and air vehicle routing. This high level of adaptability ensures safe and efficient travel while addressing evolving operational challenges.

B. **Resilience:** the DT should be able to continue functioning and providing accurate and reliable services even when facing challenging situations that do not exceed its capacity to endure, such as sudden defects, malfunctioning components, or increased workload. An effective DT must possess self-repair capabilities and incorporate early warning and swift restoration mechanisms. These capabilities are crucial in mitigating disruptions and ensuring uninterrupted service delivery to its users.

Resilience is especially vital in mission-critical applications, such as automated control systems in automobiles or medical devices. Understanding potential failures and disruptions is paramount in designing a highly resilient DT system. The system's resilience properties and how DT will evolve in response to changes in the physical system it represents should also be known beforehand.

C. **Efficiency** pertains to the resources the DT requires to provide specific functions, including energy, cost, time, etc. An efficient DT must operate effectively under the optimal necessary resources. In the DT paradigm, efficiency is critical in energy management since it is expected to work continually and in real-time with its physical counterpart. For example, a smart building's digital replica can detect when there are no individuals inside and deactivate the Heating, Ventilation, and Air Conditioning) units to save energy (HVAC), and systems to conserve energy. Moreover, with the implementation of forecasting methods for occupancy, the DT can initiate automatic pre-heating or pre-cooling services, thereby boosting energy efficiency.

D. **Reconfigurability** is the ability of a DT to alter its configurations in response to failures or requests. DTs should be able to reconfigure upon request and autonomously based on the insights and data collected from their physical counterparts. DTs must be self-configurable; thus, they can adjust dynamically and manage components' operation at a finer level. Remote monitoring and control mechanisms might be necessary for DT applications, such as predictive maintenance and real-time process optimization. Operational needs, such as changing safety regulations or energy efficiency targets, may require significant reconfiguration of the digital twin model or the entire system to ensure optimal performance and resource utilization.

4. Security issues in DT

Given the sensitive nature of digital twin technology, it is crucial to consider the security concerns that may arise. These include ensuring the protection of data and resources in terms of confidentiality, integrity, and accessibility. These are essential factors to consider when working with digital twin systems, as they can significantly impact the system's functionality and effectiveness. Due to that, it's crucial to consider how potential security and privacy issues might directly or indirectly influence DT's operating requirements. One of the essential questions many ask is whether DT is a solution or a challenge to cyber

security. In this section, we answer that crucial question where we discuss DT security issues, focusing on security challenges resulting from DT implementation, cybersecurity challenges facing DT, and existing security challenges that digital twins can solve.

4.1. DT security threats

Understanding possible attacks is one of the issues associated with protecting DTs [123]. Understanding who/what DTs should be protected from is equally important as knowing the vulnerabilities from which we should defend DTs. Traditionally, a system must meet the three security standards of confidentiality, integrity, and availability to be considered secure. Safety concerns are also crucial because of how distinct DTs are from other systems and how they interact directly with their physical world counterparts. To begin with, we must clarify what we mean by a threat. A combination of conditions potentially resulting in loss or damage to a DT is considered a security threat [124]. The damage suggests injuring people, the environment, or systems, whereas the loss might be in security precautions, confidentiality, integrity, or resource availability.

Moreover, we group threat factors into the source, motive, target, attack vector, and consequences. The attack source initiates an attack, while the target, in this case, is the DT system. The motive for starting attacks on DT varies with the attackers. However, according to [125–127], the most prominent ones are terroristic, spying, cyber war, political or criminal. Moreover, several mechanisms are involved in a successful attack, including modification, interception, fabrication, or interruption. The consequences of any DT attacks involve compromising information security and privacy. While there may be more potential threats to DT, we identified four main types. We also determine specific applications more susceptible to these threats per our security framework shown in Fig 1, and the following are the threats facing DTs:

A. *Physical Threats:*

Physical threats involve spoofing DT sensors or sabotaging system components, disrupting service, or undesired system functioning. In some cases, attackers can reach physically sensitive components of DT systems and tamper with them to install tracking and malicious devices and software external to the DT system. Smart grids, medical, and transport (smart cars) domains are highly susceptible to physical threats.

B. *Privacy Threats:*

By intercepting the communications made by the DT system using wireless hacking tools, a hacker (source) may attempt to divulge information that an organization (target) considers private, resulting in violating the privacy and confidentiality (consequence) of the organization or company and its users. Such attacks affect several DT domains and may be more severe in the healthcare sector, smart grid, and smart cars. For instance, smart cars that fully rely on global positioning (GPS) systems to guide drivers or self-driving car attackers can intercept GPS communications, resulting in privacy violations and compromising navigation systems.

C. *Criminal Threats:*

Attackers may exploit the DT system's networking and have remote control over it. In this situation, attackers can disrupt normal DT operations and perform various activities, including robbery. Furthermore, attackers can re-transmit data, capture various system commands, and jam wireless signals. Such undertakings may result in complete system failure or service unavailability. Again, smart grids, transport systems, and medical DTs are highly susceptible to criminal threats.

D. *Political and Financial Threats:*

Cyberwar may happen among hostile nations. For such reasons, one country may attempt to attack its enemy remotely to either seize the entire DT system or render it unfunctional. This is much more severe in situations like a city DT when the DTs monitor the whole city or municipality. In such attacks, nuclear plants and gas pipelines may be the primary targets, where the attacking country can sabotage components, resulting in plant shutdown or environmental pollution [126,128]. On the other hand, financial burdens may be a good reason for capable customers (attackers) trying to tamper with DT systems, especially in smart grids and other utility services, to inject false data to avoid bills.

4.2. DT security vulnerabilities

This section first identifies the root causes of current vulnerabilities in digital twins. Next, we locate vulnerabilities particular to specific layers and specify their root causes. For instance, not all layer one vulnerabilities are present in other DT layers, and vice versa. To develop appropriate solutions, it is necessary to distinguish between generic and layer-specific vulnerabilities. Moreover, it's worth noting that different

Table 4
DT Vulnerabilities Summary.

Layers	Vulnerability	Causes
Layer 1. Data Acquisition Layer	1. Power blackouts 2. Equipment physical sabotage 3. Physical unprotected components 4. Jamming and noise 5. Insecure protocols 6. Exposed interconnected field devices. 7. Insecure Access Points (APs) 8. Insecure operating systems and software	1. Heterogeneity, connectivity, and isolation assumption 2. Isolation assumption 3. Isolation assumption 4. Real-time connectivity 5. Realtime connectivity and isolation assumption 6. Realtime connectivity and isolation assumption 7. Realtime connectivity and isolation assumption 8. Realtime connectivity and isolation assumption
Layer 2–3. Data Synchronization and Modeling Layers	1. Wired and wireless communications 2. Insecure communication protocols 3. Web-based attacks 4. Open communication protocols 5. Insecure secondary access points (APs) 6. Insecure operating systems and software	1. Real-time connectivity 2. Realtime connectivity and isolation assumption 3. Realtime connectivity and isolation assumption 4. Openness, real-time connectivity, and isolation assumption 5. Realtime connectivity and isolation assumption 6. Heterogeneity, connectivity, and isolation assumption
Layer 4 Data Visualization Layer	1. Web-based attacks 2. Software attacks 3. Rogues' human-machine interfaces 4. Visualization tempering 5. Media players exploitations 6. Communication software flaws 7. Replay attacks. 8. Location traceability, e.g., Transport DTs 9. Insecure software	1. Heterogeneity and connectivity 2. Heterogeneity and connectivity 3. Isolation assumption and heterogeneity 4. Realtime connectivity and heterogeneity 5. Heterogeneity 6. Real-time connectivity 7. Realtime connectivity and isolation assumption 8. Heterogeneity 9. Heterogeneity, connectivity, and isolation assumption

layers may have similar vulnerabilities. Table 4 lists the vulnerabilities, and this section discusses the causes of vulnerabilities in DT.

Furthermore, the recurring causes of vulnerabilities in DTs, as illustrated in Table 4 (causes column), is essential to note that this overlap reflects the inherent complexities and interconnectedness of DT systems. The repetition of specific causes across different layers underscores the multifaceted nature of security challenges in these systems. It highlights that while specific vulnerabilities may be unique to particular layers, their root causes often have broader implications, affecting multiple aspects of the digital twin architecture. This understanding is crucial for developing more holistic and effective security strategies that are layer-specific and address the fundamental vulnerabilities common throughout the digital twin architectural layers.

4.2.1. Causes of vulnerabilities in DT

A. *Increased connectivity (real-time connectivity)*

DTs and their physical counterparts continuously communicate in real time, which can create new vulnerabilities. For example, a digital twin of a smart city may be connected to various sensors and devices that provide real-time data on traffic, weather, and air quality [129–131]. However, if the digital twin is not adequately secured, an attacker could potentially manipulate the data and cause chaos in the real world. Real-time connectivity can also create new attack surfaces, as digital twins may be exposed to the Internet or other networks that were not originally intended. For example, a digital twin of an industrial machine may be connected to a local network for maintenance purposes [132–135]. In the event of a network compromise, an unauthorized party can access the digital twin and alter its operations to its advantage.

B. *DT Isolation Assumption*

Digital twins are sometimes designed with the assumption that they will operate in isolation from other systems [136], which can lead to vulnerabilities. For example, a digital twin of a manufacturing plant may be designed to operate independently from different systems, such as the enterprise resource planning (ERP) system. However, if the digital twin is compromised, it can impact the entire manufacturing process, including the ERP system. Furthermore, the isolation assumption can lead to a false sense of security. Organizations may assume their DTs are secure simply because they are not directly connected to the Internet or other systems. However, attackers can still access DTs through various means, such as physical access, social engineering, or compromised third-party systems [137].

C. *Heterogeneity*

Digital twins often incorporate various technologies and components, creating new vulnerabilities. For example, a digital twin of a smart building may include multiple sensors, HVAC systems, and security cameras, all of which may be running different software and hardware. This heterogeneity can make it challenging to ensure that all components are adequately secured and updated with the latest security patches [138]. Furthermore, integrating different elements can create new attack surfaces, as attackers may exploit vulnerabilities in one part to gain access to others. To address these vulnerabilities, organizations must take a holistic approach to the digital twin's security, considering all aspects of the system, from the individual components to the more extensive network architecture [139]. This includes implementing strong access controls, conducting regular security assessments, and ensuring all components are appropriately updated and secured [140].

4.3. Existing security challenges solved by DT

DT technology, particularly cyber digital twin (CDT), can secure physical systems to avoid cyber-attacks by providing capabilities to model, predict, and enhance the visibility of their physical assets. An example of how CDT can be helpful is in its ability to conduct security analysis and monitoring that would be impossible in the physical space without causing interruptions. This feature enables security experts to conduct assessments by simulating security breaches and defense scenarios that would be difficult to execute in the actual physical environment. The advantage of CDT is that it gives them the benefits of a testing environment free of disruptions [71]. This section discusses several ways DTs can address existing cybersecurity challenges.

A. *Patch Management Improvement*

Operational Technology (OT) systems owners often encounter significant hurdles in managing and implementing software updates. These hurdles are primarily attributed to inadequate inventory management and system designs that do not allow regular maintenance. The integration of DTs offers a strategic solution to overcome these issues, although it may require higher initial expenses for development and implementation.

Another challenge for updating OT infrastructure is determining the effect of software updates or configuration changes on the entire system's security. Testing a single device in isolation is often expensive, time-consuming, or does not address system-wide consequences. These issues can be addressed by simulating the OT system with DTs, allowing patch deployment to be examined without affecting the current infrastructure or needing a separate expensive system for testing, particularly for safety-critical applications.

B. *Security Testing and Validation*

CDTs help operations management detect and respond to cybersecurity threats, enabling organizations to analyze vulnerabilities and potential attack pathways before they happen. DT implementation can be used for system and security testing to check system accuracy and penetration testing to check the system's security. Furthermore, digital twins allow for continuous security validation and other features earlier in development, leading to more efficient security testing and increased stakeholder confidence.

C. *Risk Management*

Digital twins can be used for risk management by providing a virtual representation of systems, networks, and industrial control systems (ICS) that can simulate and analyze the system's behavior in different scenarios. This allows organizations to identify potential risks and vulnerabilities before they occur in the real world [141]. It can also test various scenarios and determine the best risk management strategies. By using DTs for risk management, organizations can proactively mitigate risks and improve the overall resilience of the systems. Effective risk management allows for the automated evaluation of new system components, which reduces potential risks to human safety, facilities, or the environment. Additionally, leveraging DT's big data analytic capabilities, the system can automatically analyze logs and reports to identify and address failures quickly. It enables prompt action and minimizes potential risks [142,143].

D. *Active Cyber Defense*

Cyber-digital twin technology can aid incident responders in understanding the impact of sophisticated cyber-attacks on legacy industrial systems by reducing attack vectors and improving incident preparation. It also allows advanced training and incident response capabilities using digital twin cyber-range environments for skill development and practical engagement. Moreover, digital twins can be used for active cyber defense by simulating and analyzing the behavior of

systems and networks in different scenarios to identify vulnerabilities. DT can evaluate incident response plans, provide virtual training environments, create cyber-deception, and continuously monitor and analyze systems for anomalous activities and potential cyber threats.

E. *Virtual Commissioning*

DT improves efficiency in various industrial processes by predicting faults, scheduling maintenance, and virtually commissioning products. The information collected during the commissioning phase can be utilized to set product performance benchmarks, schedule maintenance, build training sets, and create defense plans against operational issues and cyber-attacks. Using DT's physical emulation abilities, the time for product commissioning can be shortened, and the chances of costly redesigns can be reduced [135,136].

DTs allow engineers and technicians to simulate and test the performance of a system or network before it is deployed in the field. It allows for identifying and resolving issues or malfunctions before they occur in the real world, thus reducing the need for costly on-site commissioning and the risk of expensive downtime. Virtual commissioning also optimizes the system's performance and configuration and tests various scenarios, improving the system's overall design and functionality. Using DT in virtual commissioning results in a more efficient, cost-effective, and dependable system implementation [144,145].

F. *Autonomy and Predictive Analytics*

DTs must be able to adjust to changes and developments quickly to be effective. This requires the use of autonomous systems that can respond without the need for human intervention. This allows immediate response to system anomalies, errors, faults, and attempted cybersecurity breaches. This level of autonomy ensures that digital twins can react promptly and efficiently to protect the system from potential risks. Digital twin technology supports predictive analytics by providing real-time data and simulations of systems, networks, or ICS. This data can be used to create predictive models that identify potential issues or malfunctions before they occur in the real world. By using DT for predictive analytics, organizations can improve the overall performance and reliability of the systems, reducing downtime and maintenance costs.

5. DT challenges, countermeasures and open issues

This section discusses RQ3, which probes into the technical, operational, and security challenges inherent in DT deployment and management. Moreover, the section also covers general challenges facing DT, potential limitations and drawbacks of DTs, and the research opportunities to overcome these challenges and enhance their performance and security. Overall, this section concludes by providing insights into future research directions and potential solutions that could help overcome the challenges and open issues facing the digital twin's landscape.

5.1. Security challenges facing DT

Digital twins share and store valuable data for their underlying system. DTs heavily rely on digital assets, such as algorithms, models, visualization platforms, and networks, to execute their functions. These assets can be a target for cyber attackers looking to exploit vulnerabilities and gain unauthorized access to data. This risks DT systems for data breaches and other malicious activities. It is, therefore, essential to understand all the possible security challenges facing DT and appropriate defense measures against them [146,147].

Moreover, adherence and compliance with "best practices" for cybersecurity should be mandated when DT is integrated into different applications. Furthermore, cybersecurity is one of Industry 4.0 pillars; therefore, it should be a top priority in DT implementation. The increased production efficiency brought on by DTs may cause commercial pressures to rush product launching, promoting poor and hurried decisions and disregarding best cybersecurity procedures in favor of quick financial gains. Security risks must be identified and analyzed by security experts before implementation. Below are some challenges related to DT usage.

A. *Confidentiality*

It is critical to ensure authorized access limitations to system facilities and data to maintain the confidentiality of personal and corporate data and information. Continuous monitoring is necessary to minimize system vulnerabilities as DTs constantly improve. With the use of DT, it has become much easier for business competitors to learn their counterparts' commercial and trade secrets. While DT does not create new confidentiality issues, it can worsen existing ones. An attacker with experience and expertise could interrogate a DT and obtain confidential information without the organization's knowledge or ability to prevent it.

Implementing a DT may store security settings of PO components, which should be kept secure from attackers. If an attacker gains control of these settings, they can launch a cyber-attack by exploiting known or unknown vulnerabilities. Many attacks exploit security misconfigurations and vulnerabilities arising from default or insecure setups, exposing the system to cyberattacks. When building DTs, it's essential to transport security settings securely to prevent outsiders from accessing them.

B. *Integrity*

It is essential to prevent unauthorized changes or damage to data or processes to ensure DT's safety, stability, and ability to respond to incidents. This necessitates secure communication between the physical counterpart and its digital twin. However, achieving this in real time can be difficult. An attacker targeting a digital twin or its physical representation can cause variations in the behavior or state of the DT. The bidirectional relationship and real-time communications between the two make it possible for an attacker's alterations in one to affect both. If the digital twin is used to guide and control system updates and maintenance, any malicious changes made to the DT could be replicated in the physical system. However, if implemented with cybersecurity in mind, DT can also help detect harmful alterations in both DT and PO.

DTs can enhance the PO's integrity by improving monitoring and testing capabilities. However, if an attacker can infiltrate the DT, it could lead to misleading information being provided to operators and potentially corrupting the physical system. As such, it is crucial to ensure that DTs have the same level of security protection as the physical systems they represent. One way to enhance security is using a cyber-digital twin, which simulates potential attacks on the DT to identify security vulnerabilities in the physical system. The insights from CDT simulations can then be applied to the physical system to strengthen its security.

C. *Availability*

DT availability ensures timely and reliable access to data and information that a DT must provide to authorized users. For cybersecurity, availability is crucial for maintaining the functionality and efficiency of DT systems, preventing interruptions that could lead to operational delays, data loss, or other critical impacts on an organization's functionality and reputation. In DT security, availability is particularly pertinent due to the critical nature of real-time data and simulations that digital twins provide. DTs rely heavily on continuous data flow and access to ensure accuracy and utility. This uninterrupted access is vital for making informed decisions, optimizing operations, and predicting system behaviors.

For instance, a medical device DT that simulates and monitors patient condition requires uninterrupted real-time data flow. This allows healthcare professionals to predict failures, plan maintenance, and ensure the device's optimal performance without interrupting patient care. Ensuring the DT's data and operational integrity is crucial. A breach in availability, e.g., disrupts access to device readings, could delay critical maintenance decisions or the deployment of firmware updates, potentially compromising patient safety and device efficacy.

D. *Safety*

From a cybersecurity perspective, the CDT is a double-edged sword. It is designed to replicate various cybersecurity attack scenarios to assess the system's possible vulnerabilities. If an attack against the digital twin is successful, it will likely succeed in the entire system [148]. This raises concerns about what happens if an attacker gains access to the digital twin. The attacker can detect flaws in the physical entity, test the attack's potential success, and launch the attack with greater confidence of success in the actual system. Therefore, it is crucial to carefully assess the security implications of digital twin use, especially when safety is a concern.

E. *Intellectual Property Theft and Leakage Issues*

DTs store valuable data that can be used financially and practically. For that reason, they are bound by the same intellectual property (IP) and export limitations as their physical equivalent. The data entered and stored in the DT can be easily replicated and identified. Using DTs to create a virtual model of a physical system before incorporating new PO components raises the potential for technology transfer and IP leakage.

In DT implementation, hardware and software components rely on APIs to overcome interoperability challenges between various system parts. These APIs are usually standardized and communicate by sending messages, often used to encode business logic. If the information is available, reverse engineering can decipher the organization's business logic. If this information is disclosed, it may result in financial loss and violation of legal statutes. Intellectual property theft via the digital twins is also possible if not properly secured.

5.2. DT security challenges countermeasures

Several research studies concentrated on securing DTs [122,134,147,149,150]. Based on these earlier studies and with inspiration from the comprehensive taxonomy and defensive mechanisms in DT provided by [146,147], this section looks at the various security measures necessary to enhance DTS protection, mainly when it is utilized in crucial industries such as healthcare, manufacturing, energy, and transportation. These measures are critical in ensuring that DTs are deployed securely, safeguarding sensitive data and resources from potential threats.

5.2.1. Blockchain-based DTs (A case scenario)

To rely entirely on processes and PO states represented by DTs, the DTs must be supplied with valid input data [146]. The utilization of blockchain technology within this context facilitates the communication of DTs, enabling enterprises to oversee data on a decentralized ledger while ensuring dependable coordination of DTs information across numerous stakeholders. Following that, we explore blockchain's potential for mitigating attacks on DTs. Blockchain technology has the potential to enhance the security and trustworthiness of digital twins' systems by providing a decentralized, immutable, and transparent mechanism for recording and verifying transactions. With blockchain, DTs can establish a tamper-proof audit trail for all activities related to their creation, management, and operation, including data inputs, simulations, and updates. In addition, infrastructure vulnerabilities, like deficient authentication or credentials, can abuse DT process knowledge, particularly during decommissioning, typically when DTs are archived for future use.

As indicated in Fig. 7, blockchain-based smart contracts can facilitate automated, self-executing transactions between DTs and their physical counterparts, enabling real-time monitoring and control of physical assets. Additionally, blockchain can provide a secure and scalable framework for sharing DT data among multiple parties while ensuring data privacy and confidentiality. Below are the roles of DTs in securing DTs:

A. *Authorization Using Smart Contracts*

Smart contracts may be used to maintain permission information for all involved entities [144], track data-sharing mechanisms [145], and represent twin-creation transactions [146,147] when used on DTs. Smart contracts allow code to be executed within a blockchain to automate application-specific scenarios. Furthermore, smart contracts aligned with preset conditions are preferred for scenarios that need automation induced by a change in state. In such scenarios, actions might include the activation of safety and security protocols, the execution of functions within Programmable Logic Controllers (PLC), adjustments to the physical process conditions, or alterations to the simulation setup parameters. Auditing DTs actively or retrospectively monitoring smart contract transactions can add to the rationale for deploying smart contracts in DTs.

B. *Orchestrating DT Processes*

The automated configuration, administration, and coordination of automatic configuration, administration, and coordination of computer applications, systems, and services are known as orchestration. Orchestrating DT processes administration and coordination enables the IT personnel to manage challenging activities and workflows more efficiently. Digital twin blockchain-based solutions allow tracking of changes in the digital twin's process over time, making it easier to identify outliers and modifications. Moreover, incorporating access control rules during the DT design and development stages diminishes security risks. It limits the expenses of responding to security incidents, resulting in greater efficiency during subsequent phases of the DT's lifecycle, including operation and decommissioning [146,147].

C. *Secure Lifecycle Data*

The DT usage by many parties impacts confidentiality, integrity, availability, and access control [151,152]. Blockchain solves the crucial challenge of data transmission among various participating entities by providing a distributed infrastructure. Only authorized organization representatives may access, read, and write to the DT's data. It allows blockchain to manage company regulations and policies. Moreover, the blockchain may help minimize the threats and challenges related to data integrity, leading to more informed judgments by the underlying systems.

5.2.2. DT gamification

The gamification method in cybersecurity attempts to offer security analysts a regulated, supportive virtual training environment. Although DTs function digitally in an environment different from the existing system, they are vulnerable to cyber-attacks. One potential strategy for preventing attacks on DTs is to initiate attacks on them to test their security level. However, such testing must be done in a controlled environment that does not interfere with the operation of DTs modes (especially replication). To that aim, Suhail et al. [146,147] offered a gamification strategy that provides security analysts with both evaluation and a learning environment. Their study examines how the gamification method might assist in evaluating the security of DTs against the threats related to victimizing the physical systems or their digital twins.

To improve the resilience of physical processes against possible

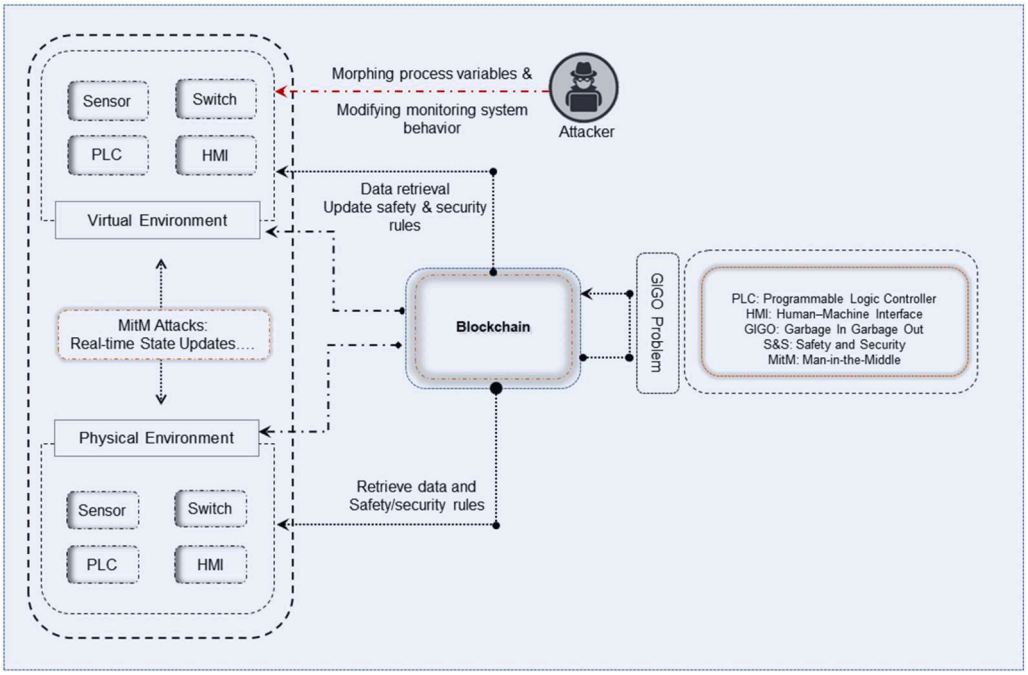

Fig. 7. Blockchain for DT Security.

attacks, calculating potential losses such as service disruption or machinery malfunction might be gamified. It is worth noting that works in the literature [152], use a similar methodology and provide a framework and environment for training security analysts. By modeling attack and defensive scenarios without jeopardizing essential infrastructure, such systems get the following benefits:

- DT's safety and, eventually, the physical assets can be assessed. Gamification for security awareness training can supplement automated security testing of DTs through incident response, which may enhance lateral mobility.
- Security analysts can be trained to obtain practical knowledge and skills based on specified learning objectives, environments, and settings through digital twin's gamification.

5.3. DT open challenges

A. *High Development Costs*

Creating a digital twin necessitates rethinking and reconfiguring the underlying software platform, production machines' hardware, and physical/cloud interface. This involves enormous expenditures and may limit the development of DTs to corporations with enough capital and personnel capabilities. Most businesses cannot afford to hire enough competent engineers to construct specialized digital twins for their specific and unique requirements. Fortunately, a few experimental and open-source DTs have been developed in recent years (as shown in Table 3) and deployed in various domains, including medical and manufacturing. However, they are insufficient and difficult to customize to organizations' business and functional needs.

On the other hand, studies have already been published for academic researchers, and the DT projects are offered as open-source software and repositories for research purposes. Without these repositories, the adaptation of digital twins may be limited to an industrial oligopoly, and more open-source projects for research purposes are needed.

On the contrary, developing a cloud-based, common open-source platform would enable small businesses and researchers to participate in the development process by designing modules, allowing easier access and collaboration. Additionally, a modular structure would allow for easier customization and integration of different components, making it more accessible to researchers and small businesses with limited resources. This approach would allow for more rapid innovation and experimentation, as developers could build on existing modules rather than start from scratch. Ultimately, this would enable more participation and collaboration among researchers and small businesses, creating more advanced and innovative digital twin applications.

B. *Realtime Interaction Challenges*

The immediate high-speed Internet connection requirement is another technological challenge affecting DT technology's development and deployment. DTs require reliable two-way real-time communication to receive data and operate real-world objects. The dynamic network environment makes transferring such massive amounts of data in real time challenging. Due to the wireless nature of the connection, the wireless channel's inherent stochastic nature may provide a poor transmission link and a proportionally longer service latency, resulting in poor quality of service. Moreover, DT's processing power, storage, communication bandwidth, and energy consumption can impact real-time two-way communication. Both the model's ongoing updating and AI prediction need significant computational work. These might affect the connectivity and relationship between digital and physical objects.

C. *Complexity and Technical Limitations*

As DT models become more complex, protecting them from attacks and breaches becomes more difficult. Various technological limitations and implementation differences concern the DT industry. Such restrictions and differences can be seen in digital twins' representations of humans and other PO. Both DTs (human and object digital twins) have similar properties but communicate differently. A DT attached to non-living things can maintain a continuous real-time connection with its physical twin, which may not be appropriate for human DTs.

Moreover, continuous communication between human DTs and their physical twin is made possible through third-party devices such as sensors or software applications, which may not always provide a

reliable connection or high data transfer rate. One example would be a DT implementation of the human body, which enables patients to continuously gather data about their health, like blood pressure, weight, etc. However, this is currently not viable due to technical and ethical limitations. This can be a limitation as it allows for a constant, intelligent, and continuous connection between the DT and the human being, enhancing its knowledge and enabling it to respond quickly to unexpected changes.

D. *Lack of Standardization in Government Policies and Regulations*

As DT technology is still evolving, the industry lacks standardization, making it harder to secure DT systems. The government must establish guidelines to validate and approve predictive physiological and biological digital twin models. Physicians must have trust in a diagnosis generated by a machine, and patients must believe in the diagnostic evaluation of experts who analyze simulations on a virtual model. Government-defined policies, rules, and regulations must be in place for these evaluations to be accepted [153]. In addition, guidelines should be established to determine humans' virtualization levels. Expressly, validation procedures for computer models in medicine and biology must be set to ensure their effectiveness.

E. *HCI and Design Issues*

Computer scientists and developers must design DTs so that non-informatic specialists in other disciplines (e.g., doctors and engineers) can engage with them efficiently without having technical skills. DTs must have well-designed, useable, and accessible interfaces to allow such requirements. Developers should prioritize developing and utilizing digital twins and emphasize the design process and end-user role. Incorporating a human work interaction design approach in all stages of DT's concept, design, and development can aid all parties involved in effectively understanding and utilizing the digital twins.

F. *Insider threats*

DTs are highly collaborative, making them vulnerable to insider threats, who can misuse or steal data. Individuals within an organization, such as employees, contractors, or third-party vendors, who have legitimate access to the system can cause insider threats and security breaches. Insider threats can include individuals who misuse or steal data or who intentionally or unintentionally cause harm to the digital twin or its physical representation [154]. Insider threats can be particularly challenging to prevent and detect because the individuals involved have legitimate access to the system. For example, an employee with access to the DT of a manufacturing system may intentionally or unintentionally change its parameters, which could cause the physical system to malfunction or produce defective products. Similarly, employees with access to DTs' sensitive data may steal or share it with unauthorized parties. To mitigate the risk of insider threats, organizations should implement strict access controls and monitoring systems and regular security training for employees. Additionally, organizations should have incident response plans to detect and respond to security breaches quickly.

6. Conclusion

DT is an emerging technology that accurately models physical objects and their interactions. Recent advancements in areas such as big data, AI, cloud computing, sensor technologies, data coding, and IoT have contributed to the DT growth over the past decade, resulting in the creation, adoption, and implementation of DTs in various fields, including robotics, manufacturing, aviation, healthcare, and system engineering. This study's contribution concentrated primarily on DT's categories, definitions, applications, requirements, technologies, and software, and more emphasis was placed on DT security aspects. For DT security, we studied and analyzed security issues inherent to DT across different domains and architectural layers. We have examined enabling technologies and tools, software, functional requirements, the security advantages and disadvantages of DTs, and some of the significant issues that need to be resolved by practitioners and researchers if the full potential of DT technology is to be realized. Moreover, it is worth noting that the applications, tools, and technologies identified in our work may not be the exhaustive list; we believe there may be many other possible applications and tools. In the context of Industry 4.0, this paper will promote debate and thoughts on the advantages and difficulties (especially in security and usability) when deploying and securing DTs.

CRediT authorship contribution statement

Sekione Reward Jeremiah: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Software, Validation, Visualization, Writing – original draft, Writing – review & editing. **Abir El Azzaoui:** Methodology, Visualization, Writing – original draft, Writing – review & editing. **Neal N. Xiong:** Methodology, Validation, Visualization, Writing – review & editing. **Jong Hyuk Park:** Funding acquisition, Project administration, Resources, Supervision, Validation, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research was supported by the National Research Foundation of Korea (NRF), funded by the Ministry of Science and ICT (2022K1A3A1A61014825).

References

[1] E. Negri, L. Fumagalli, M. Macchi, A review of the roles of digital twin in CPS-based production systems, Procedia Manuf. 11 (2017) 939–948, https://doi.org/10.1016/j.promfg.2017.07.198.
[2] A. Saad, S. Faddel, T. Youssef, O.A. Mohammed, On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks, IEEe Trans. Smart. Grid. 11 (2020) 5138–5150, https://doi.org/10.1109/TSG.2020.3000958.
[3] M. Eckhart, A. Ekelhart, Digital twins for cyber-physical systems security: state of the art and outlook, Secur. Qual. Cyber-Phys. Syst. Eng. (2019) 383–412, https://doi.org/10.1007/978-3-030-25312-7_14/COVER.
[4] M. Eckhart, A. Ekelhart, Towards security-aware virtual environments for digital twins, in: CPSS 2018 - Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Co-Located with ASIA CCS 2018, Association for Computing Machinery, Inc, 2018, pp. 61–72, https://doi.org/10.1145/3198458.3198464.
[5] Siemens, Siemens Process Systems Engineering, (n.d.). https://www.psenterprise.com/.
[6] M. Sprinzen, Digital Twins Will Drive the Future of Digital Transformation White Paper, 2020.
[7] ATOM: digital Twin of Siemens Gas Turbine Fleet Operations – AnyLogic Simulation Software, (n.d.). https://www.anylogic.com/resources/case-studies/.
[8] M.A. Javed, F.U. Muram, S. Punnekkat, H. Hansson, Safe and secure platooning of Automated Guided Vehicles in Industry 4.0, J. Syst. Arch. 121 (2021) 102309, https://doi.org/10.1016/J.SYSARC.2021.102309.
[9] A.F. Murillo, R. Taormina, N.O. Tippenhauer, S. Galelli, Co-simulating physical processes and network data for high-fidelity cyber-security experiments; co-simulating physical processes and network data for high-fidelity cyber-security experiments, Sixth Ann. Ind. Control Syst. Secur. (ICSS) Workshop (2020), https://doi.org/10.1145/3442144.
[10] M. Milton, C.O. De La, H.L. Ginn, A. Benigni, Controller-embeddable probabilistic real-time digital twins for power electronic converter diagnostics, IEEe Trans. Power. Electron. 35 (2020) 9852–9866, https://doi.org/10.1109/TPEL.2020.2971775.
[11] G.E. Research, Digital Twin Creation | GE Research, (n.d.). https://www.ge.com/research/offering/digital-twin-creation.
[12] A. Kummerow, C. Monsalve, D. Rosch, K. Schafer, S. Nicolai, Cyber-physical data stream assessment incorporating Digital Twins in future power systems, in: SEST

2020 - 3rd International Conference on Smart Energy Systems and Technologies, 2020, https://doi.org/10.1109/SEST48500.2020.9203270.
[13] W. Danilczyk, Y. Sun, H. He, ANGEL: an intelligent digital twin framework for microgrid security, 51st North American Power Symposium, NAPS 2019 (2019), https://doi.org/10.1109/NAPS46351.2019.9000371.
[14] J.C. Olivaresrojas, E. Reyes-Archundia, J.A. Gutierrez-Gnecchi, I. Molina-Moreno, J. Cerda-Jacobo, A. Mendez-Patino, Towards cybersecurity of the smart grid using digital twins, IEEe Internet. Comput. (2021), https://doi.org/10.1109/MIC.2021.3063674.
[15] M. Atalay, P. Angin, A digital twins approach to smart grid security testing and standardization, in: 2020 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2020 - Proceedings, 2020, pp. 435–440, https://doi.org/10.1109/METROIND4.0IOT48571.2020.9138264.
[16] E. Ors, R. Schmidt, M. Mighani, M. Shalaby, A conceptual framework for AI-based operational digital twin in chemical process engineering, in: Proceedings - 2020 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2020, 2020, https://doi.org/10.1109/ICE/ITMC49519.2020.9198575.
[17] Q. Min, Y. Lu, Z. Liu, C. Su, B. Wang, Machine learning based digital twin framework for production optimization in petrochemical industry, Int. J. Inf. Manage. 49 (2019) 502–519, https://doi.org/10.1016/J.IJINFOMGT.2019.05.020.
[18] J. Vachalek, L. Bartalsky, O. Rovny, D. Sismisova, M. Morhac, M. Loksik, The digital twin of an industrial production line within the industry 4.0 concept, in: Proceedings of the 2017 21st International Conference on Process Control, PC 2017, 2017, pp. 258–262, https://doi.org/10.1109/PC.2017.7976223.
[19] K. Semenkov, V. Promyslov, A. Poletykin, N. Mengazetdinov, Validation of complex control systems with heterogeneous digital models in industry 4.0 framework, Machines 9 (2021) 62, https://doi.org/10.3390/MACHINES9030062, 2021Page 62 9.
[20] L.U. Khan, Z. Han, W. Saad, E. Hossain, M. Guizani, C.S. Hong, Digital twin of wireless systems: overview, taxonomy, challenges, and opportunities, IEEE Commun. Surv. Tutor. 24 (2022) 2230–2254, https://doi.org/10.1109/COMST.2022.3198273.
[21] O. Veledar, V. Damjanovic-Behrendt, G. Macher, Digital twins for dependability improvement of autonomous driving, Commun. Comput. Inf. Sci. 1060 (2019) 415–426, https://doi.org/10.1007/978-3-030-28005-5_32.
[22] R.S. Magargle, L. Johnson, P. Mandloi, P. Davoudabadi, O. Kesarkar, S. Krishnaswamy, J. Batteh, A. Pitchaikani, A simulation-based digital twin for model-driven health monitoring and predictive maintenance of an automotive braking system, in: International Modelica Conference, 2017. https://api.semanticscholar.org/CorpusID:5753286.
[23] S. Almeaibed, S. Al-Rubaye, A. Tsourdos, N.P. Avdelidis, Digital twin analysis to promote safety and security in autonomous vehicles, IEEE Commun. Stand. Mag. 5 (2021) 40–46, https://doi.org/10.1109/MCOMSTD.011.2100004.
[24] Philips, The Rise of the Digital Twin: How Healthcare Can Benefit - Blog, Philips, 2018. |.
[25] H. Laaki, Y. Miche, K. Tammi, Prototyping a digital twin for real time remote control over mobile networks: application of remote surgery, IEEe Access. 7 (2019) 20235–20336, https://doi.org/10.1109/ACCESS.2019.2897018.
[26] V. Damjanovic-Behrendt, A digital twin-based privacy enhancement mechanism for the automotive industry, in: 9th International Conference on Intelligent Systems 2018: Theory, Research and Innovation in Applications, IS 2018 - Proceedings, 2018, pp. 272–279, https://doi.org/10.1109/IS.2018.8710526.
[27] S. Sugiyama, T. Kelly, M. Shiraki, Toyota suspends domestic factory operations after suspected cyber attack | Reuters, Reuters (2022) 1. https://www.reuters.com/business/autos-transportation/toyota-suspends-all-domestic-factory-operations-after-suspected-cyber-attack-2022-02-28/. accessed January 7, 2024.
[28] S.M. Kerner, Colonial Pipeline hack explained: everything you need to know, TechTarget (2022) 1. –1, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know. accessed January 7, 2024.
[29] J. Robertson, W. Turton, Colonial Hackers Stole Data Thursday Ahead of Shutdown, Bloomberg News, 2021. https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown. accessed January 7, 2024.
[30] K.M. Alam, A. El Saddik, C2PS: a digital twin architecture reference model for the cloud-based cyber-physical systems, IEEe Access. 5 (2017) 2050–2062, https://doi.org/10.1109/ACCESS.2017.2657006.
[31] ISO - ISO 23247-2:2021 - Automation systems and integration — Digital twin framework for manufacturing — Part 2: reference architecture, (n.d.). https://www.iso.org/standard/78743.html.
[32] The Digital Twin: compressing Time to Value for Digital Industrial Companies | GE Digital, (n.d.). https://www.ge.com/digital/lp/digital-twin-compressing.
[33] M. Antonakakis, T. April, M. Bernhard, M. Bailey, E. Bursztein, J. Cochran, A. Halderman, Understanding the Mirai Botnet, in: 26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, 2017, pp. 541–556. August 16-18, 2017, http://ipads.se.sjtu.edu.cn/lib/exe/fetch.php?media=publications:vtz.pdf%0Ahttps://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/hua. accessed July 22, 2022.
[34] M. Yar, K.F. Steinmetz, Cybercrime and the Internet: An introduction, 3rd ed., Sage, 2019. Sage.
[35] C. Wohlin, Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering, in: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, Association for Computing Machinery, New York, NY, USA, 2014, https://doi.org/10.1145/2601248.2601268.
[36] M. Grieves, J. Vickers, Digital twin: mitigating unpredictable, undesirable emergent behavior in complex systems, Transdiscip. Perspect. Complex Syst. (2016) 85–113, https://doi.org/10.1007/978-3-319-38756-7_4/COVER.
[37] Digital Twin Consortium, Glossary - Digital Twin Consortium, 2021.
[38] A. Sharma, E. Kosasih, J. Zhang, A. Brintrup, A. Calinescu, Digital Twins: state of the art theory and practice, challenges, and open research questions, J. Ind. Inf. Integr. 30 (2022), https://doi.org/10.1016/J.JII.2022.100383.
[39] A. Banerjee, R. Dalal, S. Mittal, K.P. Joshi, Generating Digital Twin Models Using Knowledge Graphs for Industrial Production Lines, in: Proceedings of the 2017 ACM on Web Science Conference, Association for Computing Machinery, New York, NY, USA, 2017, pp. 425–430, https://doi.org/10.1145/3091478.3162383.
[40] M.M. Mabkhot, A.M. Al-Ahmari, B. Salah, H. Alkhalefah, Requirements of the Smart Factory System: a Survey and Perspective, Machines 6 (2018), https://doi.org/10.3390/machines6020023.
[41] A.M. Madni, C.C. Madni, S.D. Lucero, Leveraging digital twin technology in model-based systems engineering, Systems 7 (2019) 7.
[42] Rajratna Kharat, V. Bavane, S.J.Prof.R. Marode, Digital twin: Manufacturing Excellence Through Virtual Factory Replication, 2018, https://doi.org/10.5281/ZENODO.1493930.
[43] B.A. Talkhestani, N. Jazdi, W. Schloegl, M. Weyrich, Consistency check to synchronize the Digital Twin of manufacturing automation based on anchor points, Procedia CIRP. 72 (2018) 159–164.
[44] K. Wärmefjord, R. Söderberg, L. Lindkvist, B. Lindau, J.S. Carlson, Inspection Data to Support a Digital Twin For Geometry Assurance, ASME International Mechanical Engineering Congress and Exposition, 2017. V002T02A101.
[45] G.N. Schroeder, C. Steinmetz, R.N. Rodrigues, R.V.B. Henriques, A. Rettberg, C. E. Pereira, A methodology for digital twin modeling and deployment for industry 4.0, Proc. IEEE 109 (2020) 556–567.
[46] F. Tao, M. Zhang, Digital twin shop-floor: a new shop-floor paradigm towards smart manufacturing, IEEe Access. 5 (2017) 20418–20427.
[47] F. Tao, J. Cheng, Q. Qi, M. Zhang, H. Zhang, F. Sui, Digital twin-driven product design, manufacturing and service with big data, Int. J. Adv. Manuf. Technol. 94 (2018) 3563–3576, https://doi.org/10.1007/s00170-017-0233-1.
[48] F. Tao, M. Zhang, Y. Liu, A.Y.C. Nee, Digital twin driven prognostics and health management for complex equipment, Cirp Ann. 67 (2018) 169–172.
[49] J. Lee, E. Lapira, B. Bagheri, H. Kao, Recent advances and trends in predictive manufacturing systems in big data environment, Manuf. Lett. 1 (2013) 38–41, https://doi.org/10.1016/j.mfglet.2013.09.005.
[50] R. Rosen, G. Von Wichert, G. Lo, K.D. Bettenhausen, About The Importance of Autonomy and Digital Twins for the Future of Manufacturing, IFAC-PapersOnLine 48 (2015) 567–572, https://doi.org/10.1016/J.IFACOL.2015.06.141.
[51] T. Gabor, L. Belzner, M. Kiermeier, M.T. Beck, A. Neitz, A Simulation-Based Architecture for Smart Cyber-Physical Systems, in: 2016 IEEE International Conference on Autonomic Computing (ICAC), 2016, pp. 374–379, https://doi.org/10.1109/ICAC.2016.29.
[52] Q. Qi, F. Tao, Digital Twin and Big Data Towards Smart Manufacturing and Industry 4.0: 360 Degree Comparison, IEEe Access. 6 (2018) 3585–3593, https://doi.org/10.1109/ACCESS.2018.2793265.
[53] A. Canedo, Industrial IoT Lifecycle via Digital Twins, in: Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, Association for Computing Machinery, New York, NY, USA, 2016, https://doi.org/10.1145/2968456.2974007.
[54] M. Grieves, Digital Twin: Manufacturing Excellence through Virtual Factory Replication - PDF Free Download, 2014. Florida, https://docplayer.net/37776975-Digital-twin-manufacturing-excellence-through-virtual-factory-replication.html. accessed October 23, 2023.
[55] R. Ala-Laurinaho, J. Autiosalo, A. Nikander, J. Mattila, K. Tammi, Data link for the creation of digital twins, IEEe Access. 8 (2020) 228675–228684, https://doi.org/10.1109/ACCESS.2020.3045856.
[56] H, M. C, E. G, A.Z. A, A. S, A.D. Ahmadi-Assalemi Gabriela, Al-Khateeb, Digital Twins for Precision Healthcare, in: S, C. N, I.J. Jahankhani Hamid, Kendzierskyj (Eds.), Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity, Springer International Publishing, Cham, 2020, pp. 133–158, https://doi.org/10.1007/978-3-030-35746-7_8.
[57] K. Bruynseels, F. de Sio, J. den Hoven, Digital twins in health care: ethical implications of an emerging engineering paradigm, Front. Genet. 9 (2018) 31.
[58] K. Shubenkova, A. Valiev, V. Shepelev, S. Tsiulin, K.H. Reinau, Possibility of Digital Twins Technology for Improving Efficiency of the Branded Service System, in: 2018 Global Smart Industry Conference (GloSIC), 2018, pp. 1–7, https://doi.org/10.1109/GloSIC.2018.8570075.
[59] R. Stark, C. Fresemann, K. Lindow, Development and operation of Digital Twins for technical systems and services, CIRP Ann. 68 (2019) 129–132, https://doi.org/10.1016/j.cirp.2019.04.024.
[60] T. Catarci, D. Firmani, F. Leotta, F. Mandreoli, M. Mecella, F. Sapio, A conceptual architecture and model for smart manufacturing relying on service-based digital twins, in: 2019 IEEE International Conference on Web Services (ICWS), 2019, pp. 229–236, https://doi.org/10.1109/ICWS.2019.00047.
[61] F. Tao, H. Zhang, A. Liu, A.Y.C. Nee, Digital twin in industry: state-of-the-art, IEEe Trans. Industr. Inform. 15 (2018) 2405–2415.
[62] F. Pires, A. Cachada, J. Barbosa, A.P. Moreira, P. Leitao, Digital twin in industry 4.0: technologies, applications and challenges, in: IEEE International Conference on Industrial Informatics (INDIN) 2019-July, 2019, pp. 721–726, https://doi.org/10.1109/INDIN41052.2019.8972134.
[63] Y. He, J. Guo, X. Zheng, From surveillance to digital twin: challenges and recent advances of signal processing for industrial internet of things, IEEe Signal. Process. Mag. 35 (2018) 120–129.

[64] F. Biesinger, B. Kraß, M. Weyrich, A survey on the necessity for a digital twin of production in the automotive industry, in: 2019 23rd International Conference on Mechatronics Technology, ICMT 2019, 2019, https://doi.org/10.1109/ICMECT.2019.8932144.

[65] B.R. Barricelli, E. Casiraghi, D. Fogli, A survey on digital twin: definitions, characteristics, applications, and design implications, IEEe Access. 7 (2019) 167653–167671.

[66] A. Fuller, Z. Fan, C. Day, C. Barlow, Digital twin: enabling technologies, challenges and open research, IEEe Access. 8 (2020) 108952–108971, https://doi.org/10.1109/ACCESS.2020.2998358.

[67] Z. Huang, Y. Shen, J. Li, M. Fey, C. Brecher, A survey on AI-driven digital twins in industry 4.0: smart manufacturing and advanced robotics, Sensors 21 (2021) 6340.

[68] A. Rasheed, O. San, T. Kvamsdal, Digital twin: values, challenges and enablers from a modeling perspective, IEEe Access. 8 (2020) 21980–22012, https://doi.org/10.1109/ACCESS.2020.2970143.

[69] A. Löcklin, M. Müller, T. Jung, N. Jazdi, D. White, M. Weyrich, Digital twin for verification and validation of industrial automation systems–a survey, in: 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2020, pp. 851–858.

[70] R. Minerva, G.M. Lee, N. Crespi, Digital Twin in the IoT Context: a survey on technical features, scenarios, and architectural models, Proc. IEEE 108 (2020) 1785–1824, https://doi.org/10.1109/JPROC.2020.2998530.

[71] D. Holmes, M. Papathanasaki, L. Maglaras, M.A. Ferrag, S. Nepal, H. Janicke, Digital Twins and Cyber Security - solution or challenge?, in: 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference, SEEDA-CECNSM 2021, 2021, https://doi.org/10.1109/SEEDA-CECNSM53056.2021.9566277.

[72] M. Vukovic, D. Mazzei, S. Chessa, G. Fantoni, Digital Twins in Industrial IoT: a survey of the state of the art and of relevant standards, in: 2021 IEEE International Conference on Communications Workshops, ICC Workshops 2021 - Proceedings, 2021, https://doi.org/10.1109/ICCWorkshops50388.2021.9473889.

[73] C. Alcaraz, J. Lopez, Digital twin: a comprehensive survey of security threats, IEEE Commun. Surv. Tutor. 24 (2022) 1475–1503.

[74] J.V.S. do Amaral, C.H. dos Santos, J.A.B. Montevechi, A.R. de Queiroz, Energy Digital Twin applications: a review, Renew. Sustain. Energy Rev. 188 (2023) 113891, https://doi.org/10.1016/j.rser.2023.113891.

[75] A. Zhang, J. Yang, F. Wang, Application and enabling digital twin technologies in the operation and maintenance stage of the AEC industry: a literature review, J. Build. Eng. 80 (2023) 107859, https://doi.org/10.1016/j.jobe.2023.107859.

[76] X. Liu, D. Jiang, B. Tao, F. Xiang, G. Jiang, Y. Sun, J. Kong, G. Li, A systematic review of digital twin about physical entities, virtual models, twin data, and applications, Adv. Eng. Inf. 55 (2023) 101876, https://doi.org/10.1016/j.aei.2023.101876.

[77] S. Liu, J. Bao, P. Zheng, A review of digital twin-driven machining: from digitization to intellectualization, J. Manuf. Syst. 67 (2023) 361–378, https://doi.org/10.1016/j.jmsy.2023.02.010.

[78] C. Semeraro, A.G. Olabi, H. Aljaghoub, A.H. Alami, M. Al Radi, M. Dassisti, M. A. Abdelkareem, Digital twin application in energy storage: trends and challenges, J. Energy Storage 58 (2023) 106347, https://doi.org/10.1016/j.est.2022.106347.

[79] E. Nica, G.H. Popescu, M. Poliak, T. Kliestik, O.-M. Sabie, Digital twin simulation tools, spatial cognition algorithms, and multi-sensor fusion technology in sustainable urban governance networks, Mathematics 11 (2023), https://doi.org/10.3390/math11091981.

[80] M. Attaran, B.G. Celik, Digital Twin: benefits, use cases, challenges, and opportunities, Decis. Anal. J. 6 (2023) 100165, https://doi.org/10.1016/j.dajour.2023.100165.

[81] C. Weil, S.E. Bibri, R. Longchamp, F. Golay, A. Alahi, Urban digital twin challenges: a systematic review and perspectives for sustainable smart cities, Sustain. Cities. Soc. 99 (2023) 104862, https://doi.org/10.1016/j.scs.2023.104862.

[82] Y. Yin, P. Zheng, C. Li, L. Wang, A state-of-the-art survey on Augmented Reality-assisted Digital Twin for futuristic human-centric industry transformation, Robot. Comput. Integr. Manuf. 81 (2023) 102515, https://doi.org/10.1016/j.rcim.2022.102515.

[83] Z. Jiang, Y. Guo, Z. Wang, Digital twin to improve the virtual-real integration of industrial IoT, J. Ind. Inf. Integr. 22 (2021) 100196, https://doi.org/10.1016/j.jii.2020.100196.

[84] F. Tao, Innovations in digital twin research, Nature (2021). https://www.nature.com/articles/d42473-021-00325-x.

[85] B. Schleich, N. Anwer, L. Mathieu, S. Wartzack, Shaping the digital twin for design and production engineering, CIRP Ann. 66 (2017) 141–144, https://doi.org/10.1016/j.cirp.2017.04.040.

[86] Z. Liu, N. Meyendorf, N. Mrad, The role of data fusion in predictive maintenance using digital twin, in: AIP Conf Proc, American Institute of Physics Inc., 2018, p. 20023, https://doi.org/10.1063/1.5031520.

[87] B.A. Talkhestani, T. Jung, B. Lindemann, N. Sahlab, N. Jazdi, W. Schloegl, M. Weyrich, An architecture of an Intelligent Digital Twin in a Cyber-Physical Production System, At - Automatisierungstechnik 67 (2019) 762–782, https://doi.org/10.1515/auto-2019-0039.

[88] R. Söderberg, K. Wärmefjord, J.S. Carlson, L. Lindkvist, Toward a Digital Twin for real-time geometry assurance in individualized production, CIRP. Ann. Manuf. Technol. 66 (2017) 137–140, https://doi.org/10.1016/j.cirp.2017.04.038.

[89] F. Akbarian, E. Fitzgerald, M. Kihl, Intrusion Detection in Digital Twins for Industrial Control Systems, in: 2020 28th International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2020, 2020, https://doi.org/10.23919/SOFTCOM50211.2020.9238162.

[90] L. Hu, N.-T. Nguyen, W. Tao, M.C. Leu, X.F. Liu, M.R. Shahriar, S.M.N. Al Sunny, Modeling of cloud-based digital twins for smart manufacturing with MT connect, Procedia Manuf. 26 (2018) 1193–1203.

[91] T. Hoebert, W. Lepuschitz, E. List, M. Merdan, Cloud-based digital twin for industrial robotics, in: Industrial Applications of Holonic and Multi-Agent Systems: 9th International Conference, HoloMAS 2019, Linz, Austria, 2019, pp. 105–116. August 26–29, 2019, Proceedings 9.

[92] J. Leng, Z. Chen, W. Sha, Z. Lin, J. Lin, Q. Liu, Digital twins-based flexible operating of open architecture production line for individualized manufacturing, Adv. Eng. Inf. 53 (2022) 101676.

[93] J. Leng, D. Yan, Q. Liu, H. Zhang, G. Zhao, L. Wei, D. Zhang, A. Yu, X. Chen, Digital twin-driven joint optimisation of packing and storage assignment in large-scale automated high-rise warehouse product-service system, Int. J. Comput. Integr. Manuf. 34 (2021) 783–800.

[94] V. Souza, R. Cruz, W. Silva, S. Lins, V. Lucena, A digital twin architecture based on the industrial internet of things technologies, in: 2019 IEEE International Conference on Consumer Electronics (ICCE), 2019, pp. 1–2.

[95] A.-R. Al-Ali, R. Gupta, T. Zaman Batool, T. Landolsi, F. Aloul, A. Al Nabulsi, Digital twin conceptual model within the context of internet of things, Future Internet. 12 (2020) 163.

[96] A.J.H. Redelinghuys, K. Kruger, A. Basson, A six-layer architecture for digital twins with aggregation, in: service Oriented, Holonic and Multi-Agent Manufacturing Systems for Industry of the Future, in: Proceedings of SOHOMA 2019 9, 2020, pp. 171–182.

[97] T.H.-J. Uhlemann, C. Schock, C. Lehmann, S. Freiberger, R. Steinhilper, The Digital Twin: demonstrating the Potential of Real Time Data Acquisition in Production Systems, Procedia Manuf. 9 (2017) 113–120, https://doi.org/10.1016/j.promfg.2017.04.043.

[98] Y. Xu, Y. Sun, X. Liu, Y. Zheng, A digital-twin-assisted fault diagnosis using deep transfer learning, IEEe Access. 7 (2019) 19990–19999.

[99] Z. Liu, W. Bai, X. Du, A. Zhang, Z. Xing, A. Jiang, Digital twin-based safety evaluation of prestressed steel structure, Adv. Civ. Eng. 2020 (2020) 1–10, https://doi.org/10.1155/2020/8888876.

[100] R. Martinez-Velazquez, R. Gamez, A. El Saddik, Cardio Twin, A Digital Twin of the human heart running on the edge, in: 2019 IEEE International Symposium on Medical Measurements and Applications (MeMeA), 2019, pp. 1–6.

[101] M.D. Anis, S. Taghipour, C.-G. Lee, Optimal RUL estimation: a state-of-art digital twin application, in: 2020 Annual Reliability and Maintainability Symposium (RAMS), 2020, pp. 1–7.

[102] C. Greer, M. Burns, D. Wollman, E. Griffor, Cyber-physical Systems and Internet of Things, 2019.

[103] WIN Systems, Cloud, Fog and Edge Computing – What's the Difference?, 2018.

[104] W. Kritzinger, M. Karner, G. Traar, J. Henjes, W. Sihn, Digital Twin in manufacturing: a categorical literature review and classification, IFAC-PapersOnLine 51 (2018) 1016–1022, https://doi.org/10.1016/j.ifacol.2018.08.474.

[105] TWI, Simulation Vs Digital Twin (What is the Difference Between Them?), 2021.

[106] Siimio, Simio Digital Twin Software, 2020.

[107] Microsoft, Service Limits - Azure Digital Twins | Microsoft Docs, 2022, p. 1. https://docs.microsoft.com/en-us/azure/digital-twins/reference-service-limits.

[108] Microsoft, Digital Twins – Modeling and Simulations | Microsoft Azures, 2021.

[109] Akselos, Akselos - The Fastest Engineering Simulation Technology, 2021.

[110] Amazon Web Service, Digital Twins Made Easy | AWS IoT TwinMaker, Amazon Web Services, 2021. |.

[111] Amazon Web Service, AWS IoT TwinMaker endpoints and Quotas - AWS General Reference, 2022.

[112] Siemens, NX | Siemens Software, NX | Siemens Software, 2023. https://www.plm.automation.siemens.com/global/en/products/nx/. accessed July 11, 2022.

[113] Oracle, Oracle Production Monitoring - Get Started, 2021.

[114] T.M. Ditto, iTwin.js - Don't get left behind, Get Twinning! (2022).

[115] K. Bächle, S. Gregorzik, Digital twins in industrial applications-requirements to a comprehensive data model, IIC J. Innov.-1 (2019).

[116] L. Durão, S. Haag, R. Anderl, K. Schützer, E. Zancul, L.C. Fernando S Durão, Digital Twin Require-ments in the Context of Industry 4.0, in: 15th IFIP International Conference on Product Lifecycle Man-Agement (PLM), HAL - Open Science, Turin, 2019, pp. 204–214, https://doi.org/10.1007/978-3-030-01614-2_19ï.

[117] J. Moyne, Y. Qamsane, E.C. Balta, I. Kovalenko, J. Faris, K. Barton, D.M. Tilbury, A requirements driven digital twin framework: specification and opportunities, IEEe Access. 8 (2020) 107781–107801, https://doi.org/10.1109/ACCESS.2020.3000437.

[118] IEEE Standard Glossary of Software Engineering Terminology, (1990). http://www.informatik.htw-dresden.de/~hauptman/SEI/IEEE_Standard_Glossary_of_Software_Engineering_Terminology.pdf.

[119] D. Jones, C. Snider, A. Nassehi, J. Yon, B. Hicks, Characterising the Digital Twin: a systematic literature review, CIRP. J. Manuf. Sci. Technol. 29 (2020) 36–52, https://doi.org/10.1016/j.cirpj.2020.02.002.

[120] J. Leng, Q. Liu, S. Ye, J. Jing, Y. Wang, C. Zhang, D. Zhang, X. Chen, Digital twin-driven rapid reconfiguration of the automated manufacturing system via an open architecture model, Robot. Comput. Integr. Manuf. 63 (2020) 101895, https://doi.org/10.1016/j.rcim.2019.101895.

[121] Y. Han, D. Niyato, C. Leung, D.I. Kim, K. Zhu, S. Feng, X. Shen, C. Miao, A Dynamic Hierarchical Framework for IoT-Assisted Digital Twin Synchronization in the Metaverse, IEEe Internet. Things. J. 10 (2023) 268–284, https://doi.org/10.1109/JIOT.2022.3201082.
[122] M. Hearn, S. Rix, Cybersecurity considerations for digital twin implementations, IIC J. Innov. (2019). https://www.iiconsortium.org/news-pdf/joi-articles/2019-November-JoI-Cybersecurity-Considerations-for-Digital-Twin-Implementations.pdf.
[123] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, others, Challenges for securing cyber physical systems. Workshop On Future Directions in Cyber-Physical Systems Security, 2009.
[124] C.P. Pfleeger, S.L. Pfleeger, J. Margulies, Security in Computing, 5th ed., Prentice Hall, 2015. https://eopcw.com/assets/stores/Computer%20Security/lecturenote_1704978481security-in-computing-5-e.pdf.
[125] CISA - Cybersecurity, I.S. Agency, Cyber Threats and Advisories, 2022. https://www.cisa.gov/topics/cyber-threats-and-advisories.
[126] M. Alanazi, A. Mahmood, M.J.M. Chowdhury, SCADA vulnerabilities and attacks: a review of the state-of-the-art and open issues, Comput. Secur. 125 (2023) 103028, https://doi.org/10.1016/j.cose.2022.103028.
[127] Forcepoint, What is SCADA Network Security?, 2023.
[128] D.H. Ryu, H. Kim, K. Um, Reducing security vulnerabilities for critical infrastructure, J. Loss. Prev. Process. Ind. 22 (2009) 1020–1024, https://doi.org/10.1016/j.jlp.2009.07.015.
[129] G. White, A. Zink, L. Codecá, S. Clarke, A digital twin smart city for citizen feedback, Cities. 110 (2021) 103064, https://doi.org/10.1016/j.cities.2020.103064.
[130] A. Francisco, N. Mohammadi, J.E. Taylor, Smart city digital twin–enabled energy management: toward real-time urban building energy benchmarking, J. Manag. Eng. 36 (2020) 4019045, https://doi.org/10.1061/(ASCE)ME.1943-5479.0000741.
[131] E. Shahat, C.T. Hyun, C. Yeom, City Digital Twin Potentials: a Review and Research Agenda, Sustainability. 13 (2021), https://doi.org/10.3390/su13063386.
[132] H. Chen, S.R. Jeremiah, C. Lee, J.H. Park, A Digital Twin-Based Heuristic Multi-Cooperation Scheduling Framework for Smart Manufacturing in IIoT Environment, Appl. Sci. 13 (2023) 1440, https://doi.org/10.3390/APP13031440, 2023, Vol. 13, Page 1440.
[133] S.R. Jeremiah, L.T. Yang, J.H. Park, Digital twin-assisted resource allocation framework based on edge collaboration for vehicular edge computing, Fut. Gener. Comput. Syst. 150 (2024) 243–254, https://doi.org/10.1016/J.FUTURE.2023.09.001.
[134] A. El Azzaoui, S.R. Jeremiah, N.N. Xiong, J.H. Park, A digital twin-based edge intelligence framework for decentralized decision in IoV system, Inf. Sci. (N Y) 649 (2023) 119595, https://doi.org/10.1016/J.INS.2023.119595.
[135] T.Y. Melesse, V. Di Pasquale, S. Riemma, Digital Twin Models in Industrial Operations: a Systematic Literature Review, Procedia Manuf. 42 (2020) 267–272, https://doi.org/10.1016/j.promfg.2020.02.084.
[136] Netskope, The Security Implications of A Digital Twin, 2023.
[137] Y. Gao, Y. Peng, F. Xie, W. Zhao, D. Wang, X. Han, T. Lu, Z. Li, Analysis of security threats and vulnerability for cyber-physical systems, in: Proceedings of 2013 3rd International Conference on Computer Science and Network Technology, 2013, pp. 50–55, https://doi.org/10.1109/ICCSNT.2013.6967062.
[138] M. Frustaci, P. Pace, G. Aloi, G. Fortino, Evaluating Critical Security Issues of the IoT World: present and Future Challenges, IEEe Internet. Things. J. 5 (2018) 2483–2495, https://doi.org/10.1109/JIOT.2017.2767291.
[139] S. Ksibi, F. Jaidi, A. Bouhoula, A comprehensive study of security and cyber-security risk management within e-health systems: synthesis, analysis and a novel quantified approach, Mobile Netw. Applic. 28 (2023) 107–127, https://doi.org/10.1007/s11036-022-02042-1.
[140] M.A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, J. Brown, A Comprehensive and Systematic Survey on the Internet of Things: security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures, Computers 9 (2020), https://doi.org/10.3390/computers9020044.
[141] Z. Liu, X. Meng, Z. Xing, A. Jiang, Digital Twin-Based Safety Risk Coupling of Prefabricated Building Hoisting, Sensors 21 (2021), https://doi.org/10.3390/s21113583.
[142] Z. Liu, A. Li, Z. Sun, G. Shi, X. Meng, Digital Twin-Based Risk Control during Prefabricated Building Hoisting Operations, Sensors 22 (2022), https://doi.org/10.3390/s22072522.
[143] L. Hou, S. Wu, G.(Kevin) Zhang, Y. Tan, X. Wang, Literature Review of Digital Twins Applications in Construction Workforce Safety, Appl. Sci. 11 (2021), https://doi.org/10.3390/app11010339.
[144] G. Barbieri, A. Bertuzzi, A. Capriotti, L. Ragazzini, D. Gutierrez, E. Negri, L. Fumagalli, A virtual commissioning based methodology to integrate digital twins into manufacturing systems, Prod. Eng. 15 (2021) 397–412, https://doi.org/10.1007/s11740-021-01037-3.
[145] D. Orive, N. Iriondo, A. Burgos, I. Saráchaga, M.L. Álvarez, M. Marcos, Fault injection in Digital Twin as a means to test the response to process faults at virtual commissioning, in: 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp. 1230–1234, https://doi.org/10.1109/ETFA.2019.8869334.
[146] S. Suhail, R. Jurdak, S. Member, Towards Trusted and Intelligent Cyber-Physical Systems: A Security-By-Design Approach, 2021. https://arxiv.org/abs/2105.08886v3.
[147] S. Suhail, R. Jurdak, R. Hussain, D. Svetinovic, Security Attacks and Solutions for Digital Twins, 2022.
[148] M.H. Homaei, A.C. Lindo, J.A. Daz, The role of Artificial Intelligence in Digital Twin's Cybersecurity, XVII Reunión Española Sobre Criptolog\'\ia y Seguridad de La Información, RECSI 265 (2022) 133, 2022.
[149] V. P, M.P. Kaur, M. Jeet, Mishra, The Convergence of Digital Twin, IoT, and Machine Learning: transforming Data into Action, in: A, H.-F. A, J.H. Farsi Maryam, Daneshkhah (Eds.), Digital Twin Technologies and Smart Cities, Springer International Publishing, Cham, 2020, pp. 3–17, https://doi.org/10.1007/978-3-030-18732-3_1.
[150] C. Gehrmann, M. Gunnarsson, A digital twin based industrial automation and control system security architecture, IEEe Trans. Industr. Inform. 16 (2020) 669–680, https://doi.org/10.1109/TII.2019.2938885.
[151] M, D. M, K. S, M. E, P.G. Vielberth Manfred, Glas, A Digital Twin-Based Cyber Range for SOC Analysts, in: K. Barker Ken, Ghazinour (Eds.), Data and Applications Security and Privacy XXXV, Springer International Publishing, Cham, 2021, pp. 293–311.
[152] M. Dietz, M. Vielberth, G. Pernul, Integrating digital twin security simulations in the security operations center, in: ACM International Conference Proceeding Series, 2020, https://doi.org/10.1145/3407023.3407039.
[153] E.A. Patterson, M.P. Whelan, A framework to establish credibility of computational models in biology, Prog. Biophys. Mol. Biol. 129 (2017) 13–19, https://doi.org/10.1016/j.pbiomolbio.2016.08.007.
[154] E. Karaarslan, M. Babiker, Digital Twin Security Threats and Countermeasures: an Introduction, in: 2021 International Conference on Information Security and Cryptology (ISCTURKEY), 2021, pp. 7–11, https://doi.org/10.1109/ISCTURKEY53027.2021.9654360.