



Privacy and security challenges of the digital twin: systematic literature review


Marija Kuštelega

(University of Zagreb Faculty of Organization and Informatics, Varazdin, Croatia
 <https://orcid.org/0009-0004-7125-5163>, marija.kustelega@foi.unizg.hr)

Renata Mekovec

(University of Zagreb Faculty of Organization and Informatics, Varazdin, Croatia
 <https://orcid.org/0000-0003-1107-4796>, renata.mekovec@foi.unizg.hr)

Ahmed Shareef

(University of Zagreb Faculty of Organization and Informatics, Varazdin, Croatia
 <https://orcid.org/0009-0000-4966-1908>, ahmed.shareef@foi.unizg.hr)

Abstract: As technology advances and becomes more extensively used, digital twins are likely to play an increasingly crucial role in defining the future of industry, trade, and society. Despite the stated advantages and potential of digital twin technology, certain research and implementation gaps exist, which have hindered the adoption and advancement of digital twins. This study investigates how current research on the digital twin implementations has been positioned in front of practical challenges focused on privacy and security issues. The research method adopted was a systematic literature review, employing the PRISMA approach. A total of 47 publications were identified and analyzed. The results indicate that the privacy and security challenges for digital twin implementation are complicated and may be divided into six primary groups: (1) data privacy, (2) data security, (3) data management, (4) data infrastructure and standardization, (5) ethical and moral issues, (6) legal and social issues.

Keywords: Digital twin, challenges, privacy, security, literature review, PRISMA

Categories: L.4, E.0, E.4, J.6

DOI: 10.3897/jucs.114607

1 Introduction

With the recent wave of digitalization, the latest trend in every industry is to develop systems and approaches that are useful not only in the conceptualization, prototyping, testing, and design optimization phases, but also in the operations phase, with the goal of using them throughout the product lifecycle and possibly far beyond [Rasheed *et al.*, 20]. Originally created to enhance production processes, digital twins are now understood to be digital replicas of both living and non-living objects. According to [Glaessgen and Stargel, 12], a digital twin is a virtual replica of a physical object or system, such as a vehicle, that is created using ultra-high-fidelity simulation and integrated with on-board sensors and historical data. Digital twins make it possible to track, comprehend, and improve the operations of all physical objects, and they also give people constant input to enhance their quality of life [El Saddik, 18].

The statistics show that the digital twin market is growing rapidly and the global market share of the digital twin business exceeded USD 5 billion in 2020 and is projected to experience a compound annual growth rate (CAGR) of 35% until 2027 [Bennett, 24]. It is clarified that this growth is mostly attributed to the increased adoption of Internet of Things (IoT) and smartphones by enterprises. Furthermore, it is mentioned how the segment encompassing product, design, and development applications had a significant portion, approximately 50%, of the total market share in China throughout 2019. This can be attributed to the increasing utilization of Industrial Internet of Things (IIoT) in sectors such as manufacturing, automotive, and aerospace & military.

According to [Grand View Research, 23] the digital twins market size in 2022 was estimated above 11 billion, where the compound annual growth rate (CAGR) is expected to grow 37.5% from 2023 to 2030. With the growth of digital twin adoption, the concern for data privacy has also been increasing. Based on a report by [Accenture, 21] from a survey conducted 73% respondents were concerned about the privacy and security risks associated with digital twin technology. Even 79% of companies consider GDPR compliance as a top priority for their digital twin projects [Upura, 23]. For the massive adoption of digital twins, building trust among users is inevitably important.

A survey on digital twins found that security and privacy are among the top challenges in the development and deployment of digital twins [Wang et al., 23]. The survey results show that digital twins can pose privacy protection concerns due to the sensitive data they contain. Therefore, they can provide cybercriminals with a new way to access and exploit sensitive data. The growing privacy concerns surrounding digital twin technology demonstrate why it is so important to ensure that data is used responsibly and in compliance with regulations [de Magalhães, 20]. When it comes to personal data, it's crucial to be truthful and transparent about purposes for the data gathering and the methods employed to safeguard collected data.

The aim of this paper is to offer diverse insights from research and industry about major digital twin challenges with emphasis on privacy and security. To achieve this, we pose the following research questions:

RQ1: What are the possible applications of the digital twin?

RQ2: What are key data-related challenges with digital twins, regarding privacy and security issues?

To answer these questions, a systematic review of the literature was performed. A thorough study allowed a more detailed understanding of the required topics, as well as proposals for future research on the concept of privacy in the digital twin.

2 Digital twin

Digital twin, initially a model that mimics reality, later incorporated into product life cycle management, then described as a bidirectional mechanism between two spaces, and finally defined by NASA as a multi-scale integrated model that simulates a flying object [Singh *et al.*, 21]. As a novel technology, it is increasingly being employed in industries such as transportation, medicine, smart cities etc. "Typically described as consisting of a physical entity, a virtual counterpart, and the data connections in between, the Digital Twin is increasingly being explored as a means of improving the performance of physical entities through leveraging computational techniques,

themselves enabled through the virtual counterpart” [Jones *et al.*, 20]. However, there is no consensus on a one definition for digital twin yet [AlBalkhy *et al.*, 2024] As such, there are many different interpretations and definitions of the term “digital twin”, depending on the context and the specific application. Some definitions of digital twin emphasize its use in manufacturing and industry, while others emphasize healthcare, urban planning, or even space exploration. And each organization or industry has different needs and objectives, which brings up different definitions for the term “digital twin”. Overall, the variety of definitions of digital twin reflects the broad and complex nature of this concept and its potential applications.

The technical aspects of how digital twins work can be divided into data collection, data integration, real-time data, homogenization of data, and simulation [AltexSoft, 21]. According to that division, data collection is the stage where a digital twin fetch updated data from the physical counterpart immediately, and the data collected from the physical object or process gets seamlessly integrated into the digital twin, enabling monitoring and analyzing it in real-time. As explains [Boyes and Watson, 22]: “simulations can be used to explore how the physical entity will perform considering changes to the entity itself or the environment in which it operates or is intended to operate”. Moreover, it allows simulation of the physical object, which can be used to predict future performance, identify areas for improvement, and test the impact of changes before implementing them.

2.1 History and evolution

Mirror Worlds is the title of a book that was written by David Gelernter and released in 2008 [Gelernter, 08]. The major metaphor of the book is the computer acting as a mirror of the world. According to Gelernter, the development of computing will inevitably result in the creation of a single enormous, distributed computer system that will include an exact mirror image of the entirety of reality. Individuals will be able to investigate reality without having to leave their homes if Gelernter's predictions of the "downloadable" world, which is the digital mirror of our reality, come to fulfillment.

Since it was first coined by Michael Grieves in 2002, the fundamental idea behind the Digital Twin model has remained relatively unchanged [Grieves and Vickers, 16]. In 2010, John Vickers from NASA named it “Digital Twin” [Zhang *et al.*, 21]. The term digital twin appeared in the most widely used definition of the NASA as an "integrated multi-physics, multiscale, probabilistic simulation of a vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its corresponding flying twin" [El Saddik, 18]. [Tao *et al.*, 19] suggested that a comprehensive digital twin should consist of five components: the physical part, the virtual portion, connectivity, data, and service.

There has been a notable rise in research papers and applications of digital twins across several industries [Enders *et al.*, 19]. The digital twin was first conceived in the aerospace industry and later in the automotive, construction, urban and healthcare [Corallo *et al.*, 22]. The Airframe Digital Twin (ADT) concept proposed by the U.S. Air Force in 2011 [Edwards, 21], which can accurately predict the future behavior of an aircraft and guide decision-makers to customize a management plan for each aircraft in order to extend its service life and reduce costs [Grieves and Vickers, 16].

The automobile industry has been significantly impacted by the introduction of various car types, models, and designs, with Tesla being a notable example of a

sophisticated model using technologies such as the IoT, Artificial Intelligence (AI), Machine Learning (ML), predictive analysis, and simulation tools in the modeling and design process of their automobiles. This approach is known as a "digital twin." A digital twin has also been recognized as a significant factor that will be essential to the long-term success of autonomous vehicles in the future. First, a digital model of the vehicle is created, and then, with the help of information gathered from actual driving conditions, the model is simulated and put through various tests to assist engineers in determining how the vehicle will operate before it is even designed. For the purposes of simulation, the data on vehicles that are required include information on aerodynamics, motors, suspensions, body designs, and materials [Zhang *et al.*, 21].

Digital twins will be more widely used in the medical field to solve the problems, such as real-time monitoring, dynamic analysis and precise treatment for diseases, which cannot be fully explained by traditional methods. It can model the perception and action of any relevant facility in the medical environment, coupling the observable state of the digital twin with the state of the physical entity [Corallo *et al.*, 22].

2.2 Hierarchical and Composable Deployment of Digital Twin

Digital twins are being used in a hierarchical/composable fashion to enhance their functionality and enable more complex and interconnected systems. This hierarchical approach allows for the creation of digital twins at various levels, from individual components to entire systems or even ecosystems [Tao *et al.*, 19]. By breaking down complex objects into smaller, interconnected components, researchers can model and simulate the behavior of each individual component and its interactions within the larger system [Xie *et al.*, 18]. When it comes to security and privacy, the hierarchical/composable fashion of digital twins presents certain challenges [Mohamed *et al.*, 23]. As digital twins become more interconnected and integrated into larger systems, there is an increased risk of security vulnerabilities and data breaches. It is essential to implement robust security measures to safeguard the interconnected digital twins and sensitive data [Elmay *et al.*, 23].

2.3 Privacy and security issues in digital twin

According to [de Magalhães, 20] when developing and implementing digital twins in manufacturing, it is important to address concerns related to data privacy and security. This may involve implementing appropriate security measures and ensuring that data is collected, stored, and used in compliance with regulations and standards. Failure to address these concerns can lead to data breaches, the loss of intellectual property, and other security risks [Crawford, 21]. Therefore, it is important to prioritize privacy and security in the development and implementation of digital twins [Shahzad *et al.*, 22].

The lack of opportunity for individuals to give meaningful consent to the processing of their personal data in a smart city environment where digital twins play a huge role can be a great challenge to privacy protection [Wernick *et al.*, 23]. Moreover, the collection of private data from public interactions as well as the "privatization" of ownership of both infrastructure and data in digital twin smart cities have been well discussed in the context of digital twin smart cities [Park *et al.*, 19].

Privacy protection is the measure taken to ensure that personal information is kept confidential and not disclosed to unauthorized parties [Lohr and Donaldson, 94].

Privacy protection involves limiting the link between personal data and external information, preventing identity theft and fraud [Sweeney, 02]. People can be harmed or debilitated if there is no restriction on the public's access to and use of personal information. Privacy protection is necessary to safeguard against such abuses. Privacy legislation can restrict government and law enforcement agencies from easily accessing private citizens' information [Malyk, 23]. Therefore, it is important to ensure that data is used responsibly and in compliance with regulations [de Magalhães, 20].

Digital twins can create an expanded attack surface, which can lead to new security threats like launch attacks [Glaessgen and Stargel, 12]. Privacy of the digital twin user can be at potential risk like any other technology connected to the network [Crawford, 21]. Digital twins, which contain sensitive data about physical objects and processes, pose privacy and security concerns. The interconnected nature of these devices creates new opportunities for cybercriminals to exploit sensitive data, leading to data breaches and misuse of information. As digital twin adoption increases, concerns about data privacy and security are growing [Enders *et al.*, 19]. Other data-related challenges include data analysis, data capture, data quality, data communication latency, availability of data storage databases and others [Ammar *et al.*, 22].

2.4 Issue of fake digital twins

To address the issue of fake digital twins, it is essential to establish robust verification and validation (V&V) processes, as well as to implement measures that ensure the authenticity and integrity of digital twins. Verification and validation activities are crucial to ascertain that a digital twin accurately represents its physical counterpart and performs its intended functions [Shao *et al.*, 23]. This includes applying Uncertainty Quantification (UQ) to measure performance and credibility [Shao *et al.*, 23]. UQ in the context of digital twins refers to the process of identifying, quantifying, and managing uncertainties inherent in the modeling and simulation of the physical system [Rahman *et al.*, 22].

Security measures are also vital. For instance, the integration of blockchain technology can provide a decentralized and transparent approach to validate digital twins and manage their configurations, thereby preventing unauthorized access and ensuring data privacy [Samaniego *et al.*, 23]. The development of trust and security analyzers can help in evaluating the trustworthiness of individual digital twins, considering criteria such as security, resilience, reliability, and dependability [Kurupparachchi *et al.*, 22].

The concept of a single point of truth, such as the digital twin of a system, can help manage networks of digital twins by ensuring that all twins are controlled and validated through a central authoritative source [Reiche *et al.*, 21]. The use of emulation systems to create high-fidelity digital twins can contribute to the detection of security vulnerabilities and automation of security policy development [Hammar *et al.*, 23].

Det Norske Veritas (DNV) is a global quality assurance and risk management services provider. Assurance of digital twins, as proposed by DNV's recommended practices, provides a systematic way to address and assess quality, thereby increasing the trustworthiness of digital twins [Bell *et al.*, 23]. This includes defining capability levels and functional elements as well as setting requirements for functionality, operations, platform, data quality, cyber security, and organizational aspects.

Handling fake digital twins requires a multifaceted approach that includes rigorous V&V processes, application of UQ, implementation of security measures such as blockchain, establishment of a single point of truth, and adherence to industry-recommended practices for assurance and quality assessment [Reiche *et al.*, 21; Kurupparachchi *et al.*, 22; Hammar *et al.*, 23; Bell *et al.*, 23; Samaniego *et al.*, 23; Shao *et al.*, 23]. These strategies collectively contribute to the creation of a secure and trustworthy digital twin ecosystem. Many well-established firms still lack a digital strategy, despite the fact that they have been using technology for a long time; it is unknown who owns the data and who controls it [Broo and Schooling, 23].

3 Methodology

For the literature review, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) technique was utilized, which was divided into three phases: identification, study selection, and data extraction [Moher *et al.*, 09].

3.1 Identification

The search phrase ("digital twin" OR "digital twins") AND ("privacy" OR "security") was used to find a wide range of articles that mentioned digital twin in the context of privacy and security. Due to the large number of results in the initial search, the search was narrowed down to only those articles that contained these terms in the title or abstract of the paper, in order to find pertinent journals that go into more detail about the subject. Scopus, WoS and IEEE Xplore databases were searched for articles, conference papers, or reviews that matched the search criteria, limited to open-access English publications published between 2018 and February 2024.

3.2 Study selection

This phase involves screening procedure with eligibility evaluation. The subsequent screening was done in two stages: (1) title and abstract screening, and (2) full-text screening. Because certain databases contained duplicate articles, duplicates were removed earlier on in the identification phase. After removing duplicates, all titles and abstracts were read first, applying to them following eligibility criteria:

Inclusion criteria: has identified challenges related to digital twin data.

Exclusion criteria: not written in English, only mentions the term digital twin without further elaboration, or be overly technical (describing functions, algorithms, etc.).

All publications that did not fulfill one or more of the inclusion or exclusion criteria were discarded. The remaining articles were subjected to full-text screening where eligibility assessment was repeated. This determined the final number of articles that will be used in the analysis.

3.3 Data extraction

Only articles that met the inclusion and exclusion criteria were extracted following a careful second examination. At the beginning, a total of 438 articles were identified in the Scopus (n=203), WoS (n=156) and IEEE Xplore (n=79) databases. After removing duplicates, 112 articles remained, primarily from the Scopus database. After the first

study selection, when reviewing titles and abstracts, publications that were not relevant to the subject were excluded, leaving 50 articles. After reading the remaining articles in entirety, a total of 47 articles were finally selected for study. Figure 1 provides a visual representation of the PRISMA search, utilizing the decision tree approach.

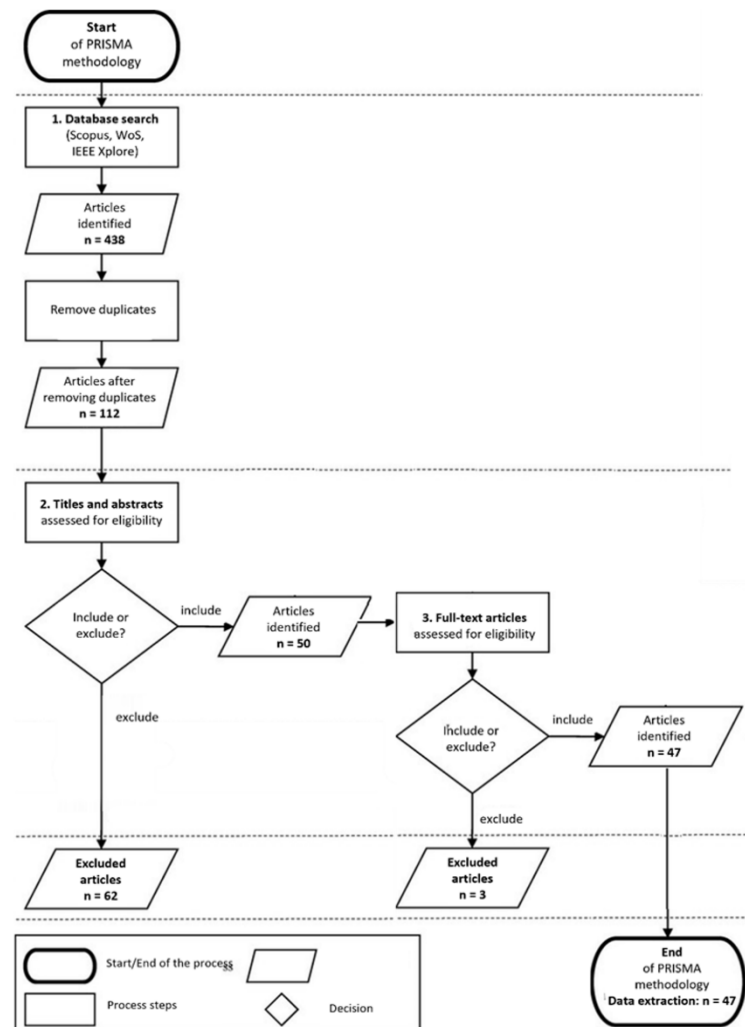


Figure 1: Decision tree based on the PRISMA methodology

Analyzing the results from Scopus, WoS, and IEEE Xplore database, it is evident that from 2018 to 2024, the number of publications related to the term digital twin has grown significantly. Given that the market for digital twins is anticipated to continue to grow over the next ten years, interest in this relatively new idea is not surprising.

4 Results

Following an assessment of the papers, 47 were found to meet the criteria (Table 1). A large part of articles (15 in total) addressed the emerging technologies like augmented reality, metaverse, automation industry, autonomous vehicles, vehicular edge computing, 6G and 5G network, wireless and cyber-physical systems, blockchain, cloud, and IoT. Articles from the construction industry (9 in total) cover topics like smart cities, building information modeling (BIM), and federated learning, while articles from healthcare (7 in total) primarily addressed ethical issues. Other articles included energy and water industry (5 articles), manufacturing (3 articles), oil and gas industry (2 articles), and other industries (6 articles) like maritime and tourism.

| Domain (s) | Author(s) |
|---------------------------|---|
| Emerging technologies | [Almeaibed <i>et al.</i> , 21; Aziz <i>et al.</i> , 23; Böhm <i>et al.</i> , 21; Gehrman and Gunnarsson, 2019; Hemdan <i>et al.</i> , 23; Holmes <i>et al.</i> , 21; Khan <i>et al.</i> , 22; Luo <i>et al.</i> , 23; Müller <i>et al.</i> , 22; Qian <i>et al.</i> , 22; Son <i>et al.</i> , 22; Suhail <i>et al.</i> , 21; Wang <i>et al.</i> , 22; Wang <i>et al.</i> , 23; Yang <i>et al.</i> , 22] |
| Construction | [Afzal <i>et al.</i> , 23; Almatared <i>et al.</i> , 23; Araújo <i>et al.</i> , 22; Kineber <i>et al.</i> , 23; Lucchi, 23; Omrany <i>et al.</i> , 23; Patwardhan <i>et al.</i> , 22; Pervez <i>et al.</i> , 23; Teisserenc and Sepasgozar, 2021] |
| Healthcare | [Cellina <i>et al.</i> , 23; Pirbhulal <i>et al.</i> , 22; Popa <i>et al.</i> , 21; Turab and Jamil, 23; Vasiliu-Feltes <i>et al.</i> , 23; Winter and Chico, 23; Yi, 23] |
| Energy and water industry | [Cali <i>et al.</i> , 23; Kumari <i>et al.</i> , 23; Sifat <i>et al.</i> , 23; Mohammed <i>et al.</i> , 23; Sheng <i>et al.</i> , 23] |
| Manufacturing | [Chen <i>et al.</i> , 23; Clementson <i>et al.</i> , 21; Timperi <i>et al.</i> , 23] |
| Oil and gas industry | [Wanasinghe <i>et al.</i> , 20; Umran <i>et al.</i> , 22] |
| Other industries | [B. Heluanya and Gkioulos, 23; Hörandner and Prünster, 21; Sharma <i>et al.</i> , 22; Siddique <i>et al.</i> , 23; Yigit <i>et al.</i> , 23; Rahmadian <i>et al.</i> , 23] |

Table 1: Summary of PISMA results for digital twin application domains

Based on reviewed articles challenges can be categorized in 6 major groups (Figure 2).

From Figure 2, the most serious data issues with digital twins are related to security and privacy. Because it is a relatively new technology, there are still significant concerns with data management, as well as the necessity for suitable infrastructure and standardization. There are also certain social, legal, and ethical issues around intellectual property and trust in digital twins.

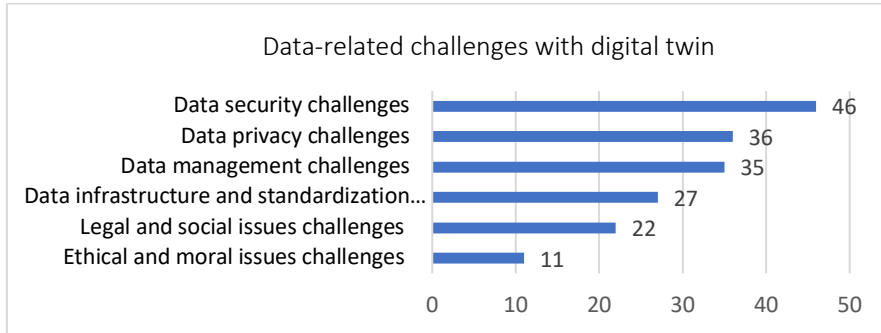


Figure 2: Data-related challenges with digital twin (number of articles).

5 Challenges of digital twin

In the following section, 47 articles will be examined in greater depth. Because some challenges, such as data security and data management were too broad, they were divided into more specific categories. Figure 3 shows a more detailed categorization of the challenges faced by digital twins in the form of a tree-like taxonomy.

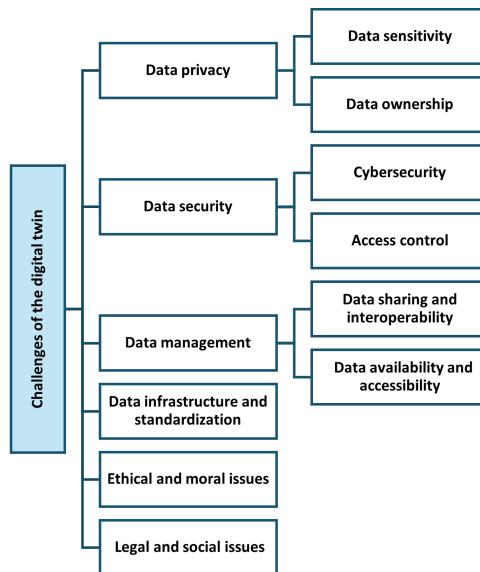


Figure 3: Tree-like taxonomy of challenges with digital twin.

By this alone, it can be seen (Figure 3) that the observed challenges cover a broad range of challenges that need to be resolved before the implementation and widespread use of digital twin technology.

5.1 Data privacy

One of the biggest challenges regarding data privacy is how to exchange real-time data and how to do so securely. Collection of large amounts of data like location, performance indicators, and private information such as medical records, autonomous car sensor data, and real-time smart grid performance data [Chen *et al.*, 23], might result in confidentiality issues like the loss or exposure of sensitive data [Qian *et al.*, 22]. The collection of personal data through IoT devices can lead to unprecedented granularity and high synchronization frequency, opening new possibilities for misuse and criminal activity [Wang *et al.*, 23; Luo *et al.*, 23].

Current methods of creating digital twins are mostly centralized and lack trusted data provenance, auditability, and traceability. This can compromise the security and integrity of data related to transactions, logs, and history [Hasan *et al.*, 20].

5.1.1 Data sensitivity

Because digital twins frequently contain confidential and sensitive data, there is a greater risk of intellectual property (IP) theft. As more and more data are used for commercial or scientific purposes, there is a risk of commodification of personal data [Winter and Chico, 23], therefore owners of the data may choose not to expose highly sensitive data to processing services [Hörandner and Prünster, 21].

The collecting and storage of large amounts of sensitive patient data increases the risk of data breaches, illegal access, and information misuse. To maintain the confidentiality strong security measures, encryption techniques, and access controls must be in place [Turab and Jamil, 23]. As the healthcare industry deals with people's private medical information, Yi [23] suggested encrypting sensitive patient data to prevent privacy leaks.

Autonomous vehicles generate significant data, primarily navigational information and routes for vehicles to follow, which is exchanged with the network and often stored in the cloud. As a result, any weakness in those systems might have devastating repercussions, especially if discovered by hackers [Almeaibed *et al.*, 21]. [Hörandner and Prünster, 21] stress that open domains provide difficulties since different organizations manage the cloud storage service, compute on the data, and own the digital twins, or the sensitive information associated with the physical object. A multi-user system is required for sensitive data in order to: (a) secure digital twin data so that the cloud cannot learn about it; and (b) provide owners control over which organizations are allowed to view which parts of their data.

5.1.2 Data ownership

Clarity about data ownership is crucial [Teisserenc and Sepasgozar, 21]. It is vital to preserve intellectual property rights, offer secure access, delegate tasks, and specify the amount of access for stakeholders while exchanging data [Wanasinghe *et al.*, 20]. Accurate data ownership issues occur due to the lack of explicit definition of who owns data [Pervez *et al.*, 23]. Because data can come from a variety of sources, it is critical

that ownership is properly verified before using it for analysis that informs applications and services. The various stakeholders must first agree on a precise definition of the ownership of the data, its scope, and procedures for granting other parties access to the data during the digital twin's life cycle. To prevent legal issues, it will also be necessary to meet national, state, and international legal requirements [Holmes *et al.*, 21]. This issue is especially significant in healthcare, as patients should understand and consent to how their data is handled [Yi, 23]. The availability of genetic information complicates these scenarios since, as the digital twin gets broader, it may be possible to identify, with alarming accuracy, what type of genetic material is best suited for survival and health [Popa *et al.*, 21].

Proper tracking and verification of data ownership is crucial for smart city applications and services, where data owners should be able to identify data elements for selective sharing [Pervez *et al.*, 23]. For example, it is difficult to determine where the information is located therefore the server ownership is a problem that may be crucial later when assigning fault for security breaches.

5.2 Data security

Due to the fact that digital twins operate in many industries and may provide threats to the entire ecosystem, data security concerns represent a significant obstacle to their usage [Sharma *et al.*, 22]. Unauthorized modification or deletion of data/operations while in processing, transport, or storage must be prevented [Holmes *et al.*, 21]. The system's integrity must be preserved [Chen *et al.*, 23] to retain trust in its reliability and safety.

Digital twin-based security concerns encompass challenges connected with security of physical device and interface security [Khan *et al.*, 22]. Cyberattacks can target IoT sensors, disabling, intercepting, or falsifying data, especially when updating physical object states in real-time through network communication [Qian *et al.*, 22].

Incorporating access controls, authentication methods, and user permissions helps to restrict data access to authorized individuals or entities, hence improving the security in general of the digital twin ecosystem. Furthermore, data governance is vital to ensuring compliance with applicable legislation and standards. This includes creating explicit policies and procedures for data collecting, storage, sharing, and retention. Organizations may demonstrate accountability and transparency in the handling of sensitive data by adhering to established data governance principles, hence increasing stakeholder trust [Omrany *et al.*, 23].

[Wang *et al.*, 22] propose 7 basic digital twin security functions: security detection (using the most recent network data gathering at that point, an analysis of the security state of the network is conducted), security simulation (simulating security threats and countermeasures), security verification (utilize a model to iteratively optimize security policies while taking security and non-security indications into account), security forecast, security decision, security planning and security optimization.

5.2.1 Cybersecurity

According to [Siddique *et al.*, 23], cybersecurity challenges in industrial applications of digital twins (IIoT) are related to: (1) data privacy, (2) cyber-physical attacks (intrusion detection), (3) supply chain risks (vendor verification), (4) authentication

issues, (5) data falsification, and (6) standardization (lack of standards, industry collaboration). Experts from the manufacturing industry highlight that cybersecurity concerns appear when sharing too much information. As a result, many businesses take extra precautions when sharing their expertise and technological know-how [Timperi *et al.*, 23].

The practical application of digital twins faces cybersecurity challenges primarily related with safeguarding networked systems and preventing malicious attacks on sensory devices [Araújo *et al.*, 22]. There is a need for establishing a synchronized cyber-physical system to resolve vulnerabilities like computational storage and infrastructural resources [Winter and Chico, 23]. Sixth generation (6G) wireless environments are anticipated to facilitate digital twin services. What prevents their realization is cybersecurity, as wireless channels are thought to be susceptible to a variety of attacks [Son *et al.*, 22]. According to [Vasiliiu-Feltes *et al.*, 23], achieving "zero-trust cybersecurity" in blockchain is a top priority. This means that everything should be verified instead of blindly trusting every user or device connected to the network, which involves multi-factor authentication, encryption, and continuous monitoring.

Digital twin establishes a cyber-physical linked environment that allows for real-time evaluation of asset performance and the generation of control demands and operational plans. The linked assets are exposed to cyber-attacks [Wanasinghe *et al.*, 20] particularly in the energy industry [Kumari *et al.*, 23; Cali *et al.*, 23] where system is vulnerable to various hardware and sensor attacks, as well as data integrity attacks, due to the large number of sensitive data circulating throughout the digital twin grid network [Sifat *et al.*, 23]. They are also significant in the maritime sector, where raising connectivity in smart ports can lead to internal and external attacks [Yigit *et al.*, 23].

Cybersecurity challenges should be considered throughout the development and deployment phases of any self-driving car, regardless of the level of autonomy. The requirement for cybersecurity features arises from the fact that numerous types of sensors in vehicle platforms might serve as entry points for any cyberattack [Almeaid *et al.*, 21].

Existing national laws governing cyberspace security and geospatial data are insufficient for policymaking and are likely impractical for some technologies [Luo *et al.*, 23]. Another point of view considers the digital twin as a technology that enhances cybersecurity. Detecting anomalies and cyberattacks, managing security patches, conducting security testing, creating autonomous systems, and enhancing risk management are just a few of the cybersecurity challenges that DT helps to solve [Pirbhulal *et al.*, 22].

5.2.2 Access control

Ensuring limits on allowed access to system resources and information is important for safeguarding the privacy of personal and commercial data [Holmes *et al.*, 21]. High-value industrial products used in crucial applications, like aerospace, necessitate full traceability from the manufacturing and testing process, protection from unauthorized and uncontrolled access (and printing), and assurance that digital files are not accidentally or intentionally modified [Clementson *et al.*, 21]. Data in transmission should be cryptographically protected, ensuring that only authorized individuals can view and modify data [Pervez *et al.*, 23].

Security and authorization in cyber-physical systems are difficult to implement when devices are controlled remotely, therefore access rights for critical services must be specified [Aziz *et al.*, 23]. It is not enough to implement an authentication mechanism for individuals, but also for machine-to-machine communication [Qian *et al.*, 22]. Blockchain-powered digital twins are being used in healthcare and pharmaceuticals to enhance patient ownership and engagement, thus enabling people to manage access to their health information [Vasiliu-Feltes *et al.*, 23]. Strong security measures and access control mechanisms are needed to maintain data confidentiality and integrity [Turab and Jamil, 23]. In multi-stakeholder environments, it is vital to provide device authentication and traceability for shared information [Patwardhan *et al.*, 22].

5.3 Data management

The development of a digital twin is primarily dependent on data. One of the key obstacles in developing digital twins is acquiring, cleaning, and processing sensor data. The broader problem of privacy and security issues is related to the proper data management, it is imperative to ensure the quality of data [Kineber *et al.*, 23]. Due to the complexity of digital twins, there is concern about the ability to manage it from the client's point of view, so it is important for clients to grasp the technology.

Data management, which includes collection, transmission, storage, and fusion, is a critical component of digital twin technology since it requires a single source of truth and good data quality [Afzal *et al.*, 23]. Data quality issues, such as missing or inaccurate data, may compromise a digital twin model's usefulness and reliability, resulting in incorrect analysis and decision-making. Inaccurate and incomplete data can be caused by a variety of factors, including human errors during data acquisition or entry, difficulties integrating data from multiple sources with inconsistencies in formats and structures, limitations or malfunctions of sensors used for real-time data capture, and gaps in information that may be unavailable or inadequately recorded [Omran *et al.*, 2023].

Healthcare systems often face significant data management challenges due to the data quality like inconsistent or incomplete data [Cellina *et al.*, 23] and presence of diverse and fragmented data sources [Turab and Jamil, 23]. In the energy sector, the electric grid digital twin faces significant challenges in data collection, management, transmission and storage. The digital twin network must quickly forward and evaluate data, which necessitates the establishment of a substantial communication and computer infrastructure [Sifat *et al.*, 23]. Major challenges of microgrid digital twins (MGDT) are acquiring, cleaning and processing of sensor data due to vast amounts of data, data diversity and data validity [Kumari *et al.*, 23]. In addition to that, the construction industry faces integration issues, requiring establishment of holistic strategies to integrate various data types and protocols used [Afzal *et al.*, 23].

5.3.1 Data sharing and interoperability

Digital twins may involve many data gathering devices that store data in different formats, resulting in fragmentation, data heterogeneity, and a lack of interoperability. These concerns may reduce the industry's readiness for digital twin adoption [Araújo *et al.*, 22]. Therefore open standards must be adopted and data exchange protocols

developed [Vasiliu-Feltes *et al.*, 23], furthermore individuals needed to understand what kinds of data could be shared in a digital twin and how they can be shared [Timperi *et al.*, 23].

Data sharing can bring enormous advantages to the entire supply chain and ecosystem [Wanasinghe *et al.* 20] and to achieve effective communication with both internal and external departments [Luo *et al.*, 23]. Achieving interoperability is particularly pronounced in healthcare, which needs to achieve compatibility between electronic health records, medical devices and other wearable sensors [Turab and Jamil, 23]. Furthermore, each healthcare system may have its own data requirements and formats, limiting communication and data sharing between organizations [Cellina *et al.*, 23]. Healthcare systems generally have fragmented data sources, making it difficult to integrate and synchronize data across platforms and devices.

The interoperability of numerous digital twin components is a difficult task. The goal is to design standardized data formats, communication protocols, and data-exchange methods that allow for the efficient flow of information between systems [Turab and Jamil, 23]. The lack of established formats and protocols might cause scalability and interoperability issues. Data exchange for digital twins must be secure throughout the life cycle of the physical object represented by the digital twin [Teisserenc *et al.*, 21].

5.3.2 Data availability and accessibility

Major challenges in IoT present server or device failures due to the large numbers of heterogeneous nodes in the IoT. This is especially evident in managing smart manufacturing services which require real-time communication and operations, thus ensuring scalability and data availability [Chen *et al.*, 23]. To guarantee that important data is available and accessible, it is critical to first determine what data each stakeholder needs, followed by excellent data management.

In industrial cyber-physical systems (ICPS) device availability is a major concern, as most embedded systems have limited resources like battery-powered sensors [Aziz *et al.*, 23]. Digital twin technology attempts to improve the maintainability and endurance of its physical counterpart, hence ensuring availability throughout its lifetime. Implementation restrictions, particularly in strongly integrated digital twins as opposed to digital models, can lead to undesired interactions that impact overall system availability. For example, if a cyber-attack compromises the digital twin, the physical twin could suffer devastating consequences. As a result, a digital twin can introduce a new vulnerability in the system that can be exploited by cybercriminals [Holmes *et al.*, 23]. A digital twin's virtual entity is made out of the same types of assets as the real entity, which may include servers, IoT devices, an operating system, software, hardware, and so on. As a result, update management is an important security precaution for keeping assets up to date with the most recent security patches [B. Heluanya and Gkioulos, 23]. To optimize availability of digital twin data, a system should be created that will allow safe data sharing with other users while protecting their privacy [Son *et al.*, 22].

5.4 Data infrastructure and standardization

While data is the foundation of digital twins, much existing field data does not adhere to a consistent data standard. Data might be unstructured, semi-structured, or organized. Furthermore, the existing data is typically not connected to a centralized database and is frequently held in many locations [Wanasinghe *et al.*, 20]. Because data comes from different sources, there should be more consistency in the flow of information globally [Timperi *et al.*, 23]. The primary causes for standardization's difficulty include a lack of standardized modeling, specific domain usage, insufficient infrastructure, and poor data quality [Omrany *et al.*, 23].

The Energy sector and smart cities domain face challenges in achieving interoperability and compatibility due to lack of standard technical specifications and protocols [Cali *et al.*, 23; [Kumari *et al.*, 23]. Data integration systems from various suppliers use different standards and methodologies to display their data [Wanasinghe *et al.*, 20]. Generally, each domain has a unique knowledge so it is not enough to use the same standards, it is necessary to ensure that all stakeholders interpret it in the same way [Afzal *et al.*, 23].

The absence of a standardized method to represent construction projects elements such as structural components, systems, and processes is a barrier to the continued development of digital twins [Omrany *et al.*, 23]. In the construction sector, the most widely used building information modeling (BIM) standard can be challenging to maintain and update due to its complexity [Afzal *et al.*, 23].

Industries with complex systems and multiple data sources cannot provide standardized format for data used to build digital twin model [Hemdan *et al.*, 23]. Yi [23] also addresses this issue, claiming that in healthcare, an interoperability standard must exist to enable integration with the existing healthcare IT infrastructure. One of the obstacles is the digital maturity of the infrastructure, legislative frameworks, and industrial practices specific to each country [Omrany *et al.*, 23].

Due to long product life cycles, vast subcontractor networks, and a lack of data sharing infrastructure, the problem of inefficient data and information flow in the manufacturing industry continues to grow [Timperi *et al.*, 23]. Also, the construction and maintenance of digital twin infrastructure can be costly, necessitating significant financial investments and expert education [Cellina *et al.*, 23].

Cali *et al.* [23] believe that without standardized components and protocols digital twins can hardly achieve their full potential. More open data sharing agreements and infrastructure are desperately needed, and everyone involved must establish common objectives and a shared vision for the development of digital twin [Timperi *et al.*, 23].

5.5 Ethical and moral issues

Digital twins have raised new socio-ethical issues, such as fears that they are unrealistic or might result in widespread data inequity and injustice, as well as anxieties about losing control and autonomy [Winter and Chico, 23]. The concept of incorporating ethical considerations into software architecture design has also evolved, necessitating that architects comprehend and analyze ethical issues [Rahmadian *et al.*, 23]. Various ethical challenges have arisen in the context of big data utilization, particularly in terms of security and privacy. The development of a big data governance framework could

resolve these challenges, enabling organizations policies and standards for managing data [Rahmadian *et al.*, 23].

Ethical issues are important in healthcare where ensuring patient data privacy and safe data handling are recognized as key challenges [Cellina *et al.*, 23; Vasiliu-Feltes *et al.*, 23]. Informed consent, data ownership, and patient autonomy are crucial issues that guarantee the responsible and ethical implementation of DTs [Turab and Jamil, 23]. Clear rules and regulations are needed to ensure ethical considerations in the use of patients' private health information for digital twin modeling, protecting their rights and maintaining data openness [Turab and Jamil, 23].

The creation of a trustworthy and transparent data ecosystem is one of the major issues [Suhail *et al.*, 21], due to unclear data ownership, access and security [Afzal *et al.*, 23]. For this purpose, it is critical to ensure that the data in the digital twin model comes from reliable and confidential sources [Pervez *et al.*, 23].

5.6 Legal and social issues

The deployment of digital twins in various sectors faces challenges due to a lack of common definition, design, framework, and appropriate tools [B. Heluanya and Gkioulos, 23]. The regulatory framework for digital twins is still developing but it should address several open challenges such as misunderstandings about digital twin data and its features, unclear data ownership, and legal responsibilities [Turab and Jamil, 23]. Protecting intellectual property rights, as well as finalizing good contractual arrangements is key for the actual implementation of DT [Clementson *et al.*, 21]. There are some ownership and traceability limitations like difficulties in proving intellectual property rights, undefined roles and responsibilities, and its feasibility [Teisserenc and Sepasgozar, 21].

Healthcare faces a lack of regulations, validation methodologies, clinical practice regulations, and regulatory authorities [Winter and Chico, 23]. Thus regulatory frameworks are essential in balancing innovation, patient rights, and responsible digital twin implementation [Turab and Jamil, 23]. For deeply intertwined systems like cyber-physical systems, governance of the devices and services should be clearly defined, including rules for device access and individuals responsible for them [Aziz *et al.*, 23]. For example, blockchain-powered DT in healthcare can be implemented with a patient-centric approach, ensuring patient rights are at the core of technology implementation [Vasiliu-Feltes *et al.*, 23]. Since health data is strictly regulated, in order for a cloud-based medical record service system to be feasible, it must comply with all applicable laws and regulations [Yi, 23].

6 Discussion

Digital twins have the potential to transform and change variety of sectors, therefore we can expect to see even more innovative applications that will advance society and individuals wellbeing. In this paper a literature analysis was conducted to identify potential digital twin applications and key data-related obstacles, including privacy and security concerns.

As concerns our research questions, in relation to RQ1 (*What are the possible applications of the digital twin?*) our findings show that upcoming technologies such as augmented reality, metaverse, the automation industry, autonomous cars, vehicular

edge computing, 6G and 5G networks, wireless and cyber-physical systems, blockchain, cloud, and IoT are the most common sectors for which digital twins are employed. The following domains include the construction sector (which includes themes such as smart cities and building information modelling), healthcare, energy and water, manufacturing, oil and gas, and other industries. These findings are in accordance with latest digital twin statistics [Bennett, 24] that show that 27% of companies plan to use digital twins as autonomous equipment, robots or vehicles. Digital twins have emerged as a game-changer in the industrial landscape, revolutionizing operations, optimizing processes, and driving innovation across diverse sectors and enabling a wide range of applications that enhance efficiency, productivity, and overall performance. Businesses may improve production scheduling, resource allocation, and supply chain management by modelling different scenarios, evaluating real-time data, and finding critical points. As this technology continues to develop, it is important to have a robust framework in place to protect privacy, security, and human rights. As concerns our RQ2 (*What are key data-related challenges with digital twins, regarding privacy and security issues?*) based on the literature review performed in this article, data-related challenges with digital twins can be separated down into six categories: (1) data privacy, (2) data security, (3) data management, (4) data infrastructure and standardization, (5) data ethics and morality and (6) legal and social problems.

The results of literature review can help us to identify and stress major challenges of digital twin in three major groups: (1) data challenges, (2) technical challenges, and (3) ethical and legal challenges.

Firstly, we can put focus on data that are drivers of whole digital twin concept where the number of data and quality of data being collected/managed are the key prerequisite of successful digital twin usage. Therefore, the primary concerns in digital twin usage should be data privacy. According to our results data privacy encompasses data sensitivity, data ownership, data sharing and interoperability, and data availability and accessibility. Data management issues, particularly in the early stages of digital twin implementation, are primarily caused by low data quality and inadequate system infrastructure, leading to security breaches and privacy concerns.

Secondly, there is need to improve technical part of digital twin where we should put emphasis on infrastructure, like sensors, network and transfer protocols. According to our results, technical challenges continue to represent a major obstacle in implementing digital twin technology where they are connected with cybersecurity, access control, data infrastructure and standardisation. Because of its linked nature, technology has the potential to communicate risks throughout a large network, offering assistance to stakeholders in making informed decisions.

Thirdly, it has been observed that recent research is increasingly focused on examining ethical challenges posed by emerging technologies. Digital twin technologies will have to consider ethical aspects, especially in the context of their integration with artificial intelligence tools. Regulatory framework should focus on these challenges and provide clear understanding of possibilities but also and responsibilities of all stakeholders involved in digital twin usage.

7 Conclusion

Digital twins, an emerging and disruptive technology, are a digital environment in which physical devices, software, firmware, and their interactions are precisely recreated in digital form. Despite the promising offers of digital twin, security and privacy concerns present significant barriers to its widespread adoption. Various security risks and privacy breaches in digital twins may occur as a result of widespread individual data collecting and extensive data sharing. By effectively handling privacy and security concerns, industries may fully realize the transformative potential of digital twin technologies, enhancing competitiveness and resilience in the face of changing digital landscapes.

Our study aimed to demonstrate the significance of developing digital twin technologies from two distinct perspective points: the academic and the business worlds.

This study contributes to the body of knowledge by categorizing essential variables in the development of digital technology for applications. This can help existing and forthcoming research efforts, as well as industry practitioners, gain a better understanding of privacy and security concerns so that they can be addressed proactively. Secure data transmission, access management, encryption, and threat detection are critical components of digital twin systems in the industrial sector. Therefore, in order to increase the usage of digital twin technology, future studies should investigate the aforementioned issues and how they could potentially be overcome.

The current study's limitations arise from the number of papers analysed in the literature review. In the future, to improve research precision, the principle might be used to a more expansive sample.

Acknowledgements

This work has been supported by the Croatian Science Foundation under the project IP-2019-04-4864.

References

- [Accenture, 21] Accenture (2021). *The power of massive, intelligent, digital twins*. Retrieved September 29, 2023, from <https://www.accenture.com/us-en/insights/health/mirrored-world>
- [Afzal *et al.*, 23] Afzal, M., Li, R. Y. M., Shoaib, M., Ayyub, M. F., Tagliabue, L. C., Bilal, M., Ghafoor, H., & Manta, O. (2023). Delving into the Digital Twin Developments and Applications in the Construction Industry: A PRISMA Approach. *Sustainability*, 15(23), 16436. <https://doi.org/10.3390/su152316436>
- [AlBalkhy *et al.*, 2024] AlBalkhy, W., Karmaoui, D., Ducoulombier, L., Lafhaj, Z., & Linner, T. (2024). Digital twins in the built environment: Definition, applications, and challenges. *Automation in Construction*, 162, 105368.

- [Almatared *et al.*, 23] Almatared, M., Liu, H., Abudayyeh, O., Hakim, O., & Sulaiman, M. (2023). Digital-Twin-Based Fire Safety Management Framework for Smart Buildings. *Buildings*, 14(1), 4.
- [Almeaibed *et al.*, 21] Almeaibed, S., Al-Rubaye, S., Tsourdos, A., & Avdelidis, N. P. (2021). Digital twin analysis to promote safety and security in autonomous vehicles. *IEEE Communications Standards Magazine*, 5(1), 40-46.
- [AltexSoft, 21] AltexSoft. (2021, September 16). *Digital Twins: Components, Use Cases, and Implementation Tips*. Retrieved September 16, 2021, from <https://www.altexsoft.com/blog/digital-twins/>
- [Ammar *et al.*, 22] Ammar, A., Nassereddine, H., AbdulBaky, N., AbouKansour, A., Tannoury, J., Urban, H., & Schranz, C. (2022). Digital twins in the construction industry: A perspective of practitioners and building authority. *Frontiers in Built Environment*, 8, 834671.
- [Araújo *et al.*, 22] Araújo, C. S., Costa, D. B., Corrêa, F. R., & Ferreira, E. D. A. M. (2022, July). Digital Twins and Lean Construction: Challenges for Future Practical Applications. In *Proceedings of the 30th Annual Conference of the International Group for Lean Construction (IGLC30)*, Edmonton, AB, Canada (pp. 6-12).
- [Aziz *et al.*, 23] Aziz, A., Schelén, O., & Bodin, U. (2023, January). Digital twin as a proxy for industrial cyber-physical systems. In *Proceedings of the 2023 10th International Conference on Wireless Communication and Sensor Networks* (pp. 85-92).
- [B. Heluanya and Gkioulos, 23] B. Heluany, J., & Gkioulos, V. (2023, August). Survey on Digital Twins: from concepts to applications. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-8).
- [Bell *et al.*, 23] Bell, C. J., Celnik, M., Devgun, J., Hansen, O., Osborn, W., & Faiz, G. (2023). Providing Assurance of Digital Twins. Day 2 Wed, September 06, 2023, D021S006R001. <https://doi.org/10.2118/215599-MS>
- [Bennett, 24] Bennett, S. (2024, June 9). *Digital Twin Statistics*. WebinarCare. <https://webinarcare.com/best-digital-twin-software/digital-twin-statistics/>
- [Böhm *et al.*, 21] Böhm, F., Dietz, M., Preindl, T., & Pernul, G. (2021). Augmented Reality and the Digital Twin: State-of-the-Art and Perspectives for Cybersecurity. *Journal of Cybersecurity and Privacy*, 1(3), 519-538.
- [Boyes and Watson, 22] Boyes and Watson (2022, December). Digital twins: An analysis framework and open issues. *Elsvier*, 143. <https://doi.org/10.1016/j.compind.2022.103763>
- [Broo and Schooling, 23] Broo, D. G. and Schooling, J. (2023). Digital twins in infrastructure: definitions, current practices, challenges and strategies. *International Journal of Construction Management*, 23(7), 1254-1263.
- [Cali *et al.*, 23] Cali, U., Dimd, B. D., Hajjaligol, P., Moazami, A., Gourisetti, S. N. G., Lobaccaro, G., & Aghaei, M. (2023, June). Digital Twins: Shaping the Future of Energy Systems and Smart Cities through Cybersecurity, Efficiency, and Sustainability. In *2023 International Conference on Future Energy Solutions (FES)* (pp. 1-6). IEEE.
- [Cellina *et al.*, 23] Cellina, M., Cè, M., Ali, M., Irmici, G., Ibba, S., Caloro, E., Fazzini, D., Oliva, G., & Papa, S. (2023). Digital Twins: The New Frontier for Personalized Medicine?. *Applied Sciences*, 13(13), 7940. <https://doi.org/10.3390/app13137940>
- [Chen *et al.*, 23] Chen, H., Jeremiah, S. R., Lee, C., & Park, J. H. (2023). A Digital Twin-Based Heuristic Multi-Cooperation Scheduling Framework for Smart Manufacturing in IIoT Environment. *Applied Sciences*, 13(3), 1440.

- [Clementson *et al.*, 21] Clementson, J., Teng, J., Wood, P., & Windmill, C. (2021). Legal considerations for using digital twins in additive manufacture—a review of the literature. *Advances in Manufacturing Technology XXXIV*, 91-96.
- [Corallo *et al.*, 22] Corallo, A., Buccoliero, F. O., Crespino, A. M., Del Vecchio, V., Spennato, A., Visone, D., & Napolitano, D. R. (2022, July 5). Internet of Things and Shop-Floor Digital Twin: an Aerospace case study. *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*. <https://doi.org/10.23919/splitech55088.2022.9854314>
- [Crawford, 21] Crawford. (2021). *Five ways to protect digital twins that probably lack cyber protection*. ASME. Retrieved September 26, 2023, from <https://www.asme.org/topics-resources/content/five-ways-to-cyber-protect-your-digital-twin>
- [de Magalhães, 20] de Magalhães, S. T. (2020, March). The European Union’s General Data Protection Regulation (GDPR). *Cyber Security Practitioner’s Guide*, 529–558. https://doi.org/10.1142/9789811204463_0015
- [Edwards, 21] Edwards, J. (2021, January 14). *6 business benefits of data protection and GDPR compliance*. Data Backup. <https://www.techtarget.com/searchdatabackup/tip/6-business-benefits-of-data-protection-and-GDPR-compliance>
- [El Saddik, 18] El Saddik, A. (2018, April). Digital Twins: The Convergence of Multimedia Technologies. *IEEE MultiMedia*, 25(2), 87–92. <https://doi.org/10.1109/mmul.2018.023121167>
- [Elmay *et al.*, 23] Elmay, F. K., Madine, M., Salah, K., & Jayaraman, R. (2023). NFTs for Trusted Traceability and Management of Digital Twins for Shipping Containers. *IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops)*, 433–438.
- [Enders *et al.*, 19] Enders, M. R., & Hoßbach, N. (2019). Dimensions of Digital Twin Applications—A Literature Review. Americas Conference on Information Systems.
- [Gehrmann and Gunnarsson, 2019] Gehrmann, C., & Gunnarsson, M. (2019). A digital twin based industrial automation and control system security architecture. *IEEE Transactions on Industrial Informatics*, 16(1), 669-680.
- [Gelernter, 08] Gelernter (2008). Mirror Worlds: The Universe in a Box? *Springer, Vienna*, 36–72. https://doi.org/10.1007/978-3-211-78539-3_3
- [Glaessgen and Stargel, 12] Glaessgen, E. and Stargel, D. (2012, April 23). The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles. *53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference≪BR≫20th AIAA/ASME/AHS Adaptive Structures Conference≪BR≫14th AIAA*. <https://doi.org/10.2514/6.2012-1818>
- [Grand View Research, 23] Grand View Research (2023). *Digital Twin Market Size, Share & Trends Analysis Report By Solution (Component, Process), By Deployment (Cloud, On-premise), By Enterprise Size, By Application, By End-use, By Region, And Segment Forecasts, 2023 - 2030*. Retrieved September 29, 2023, from <https://www.grandviewresearch.com/industry-analysis/digital-twin-market>
- [Grieves and Vickers, 16] Grieves, M. and Vickers, J. (2016, August 17). Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. *Transdisciplinary Perspectives on Complex Systems*, 85–113. https://doi.org/10.1007/978-3-319-38756-7_4
- [Hammar *et al.*, 23] Hammar, K., & Stadler, R. (2023). Digital Twins for Security Automation. NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, 1–6. <https://doi.org/10.1109/NOMS56928.2023.10154288>

- [Hasan *et al.*, 20] Hasan, H. R., Salah, K., Jayaraman, R., Omar, M., Yaqoob, I., Pesic, S., Taylor, T., & Boscovic, D. (2020). A Blockchain-Based Approach for the Creation of Digital Twins. *IEEE Access*, 8, 34113–34126. <https://doi.org/10.1109/ACCESS.2020.2974810>
- [Hawashin *et al.*, 23] Hawashin, D., Salah, K., Jayaraman, R., & Musamih, A. (2023). Using Composable NFTs for Trading and Managing Expensive Packaged Products in the Food Industry. *IEEE Access*, 11, 10587–10603. <https://doi.org/10.1109/ACCESS.2023.3241226>
- [Hemdan *et al.*, 23] Hemdan, E. E. D., El-Shafai, W., & Sayed, A. (2023). Integrating Digital Twins with IoT-Based Blockchain: Concept, Architecture, Challenges, and Future Scope. *Wireless Personal Communications*, 1-24.
- [Holmes *et al.*, 21] Holmes, D., Papathanasaki, M., Maglaras, L., Ferrag, M. A., Nepal, S., & Janicke, H. (2021, September). Digital Twins and Cyber Security—solution or challenge?. In *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)* (pp. 1-8). IEEE.
- [Hörandner and Prünster, 21] Hörandner, F., & Prünster, B. (2021). Armored Twins: Flexible Privacy Protection for Digital Twins through Conditional Proxy Re-Encryption and Multi-Party Computation. In *SECRYPT* (pp. 149-160).
- [Jones *et al.*, 20] Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020, May). Characterising the Digital Twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, 29, 36–52. <https://doi.org/10.1016/j.cirpj.2020.02.002>
- [Khan *et al.*, 22] Khan, L. U., Han, Z., Saad, W., Hossain, E., Guizani, M., & Hong, C. S. (2022). Digital twin of wireless systems: Overview, taxonomy, challenges, and opportunities. *IEEE Communications Surveys & Tutorials*.
- [Kineber *et al.*, 23] Kineber, A. F., Singh, A. K., Fazeli, A., Mohandes, S. R., Cheung, C., Arashpour, M., Ejohwomu, O., & Zayed, T. (2023). Modelling the relationship between digital twins implementation barriers and sustainability pillars: Insights from building and construction sector. *Sustainable Cities and Society*, 99, 104930. <https://doi.org/10.1016/j.scs.2023.104930>
- [Kumari *et al.*, 23] Kumari, N., Sharma, A., Tran, B., Chilamkurti, N., & Alahakoon, D. (2023). A Comprehensive Review of Digital Twin Technology for Grid-Connected Microgrid Systems: State of the Art, Potential and Challenges Faced. *Energies*, 16(14), 5525. <https://doi.org/10.3390/en16145525>
- [Kurupparachchi *et al.*, 22] Kurupparachchi, P., Rea, S., & McGibney, A. (2022). Trust and Security Analyzer for Collaborative Digital Manufacturing Ecosystems. In T. Margaria & B. Steffen (Eds.), *Leveraging Applications of Formal Methods, Verification and Validation. Practice* (Vol. 13704, pp. 208–218). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-19762-8_15
- [Lohr and Donaldson, 94] Lohr, K. N., & Donaldson, M. S. (Eds.). (1994). Health data in the information age: use, disclosure, and privacy.
- [Lucchi, 23] Lucchi, E. (2023). Digital twins for the automation of the heritage construction sector. *Automation in Construction*, 156, 105073.
- [Luo *et al.*, 23] Luo, X., Wen, J., Kang, J., Nie, J., Xiong, Z., Zhang, Y., Yang, Z., & Xie, S. (2023). Privacy attacks and defenses for digital twin migrations in vehicular metaverses. *IEEE Network*. <https://doi.org/10.1109/MNET.2023.3317320>
- [Malyk, 23] Malyk, M. (2023, February 22). *The Pros And Cons Of Privacy Laws For Consumers And Corporations*. www.easylama.com. <https://www.easylama.com/blog/pros-and-cons-of-privacy-laws/>

- [Mohamed *et al.*, 23] Mohamad, N. H., Saidin, N. B., & Zaidi, M. I. H. B. (2023). Data Security and Privacy Issues in Cloud Computing: Challenges and Solutions Review [Preprint]. Preprints. <https://doi.org/10.36227/techrxiv.170327865.59737799/v1>
- [Mohammed *et al.*, 23] Mohammed, M. A., Lakhani, A., Abdulkareem, K. H., Abd Ghani, M. K., Marhoon, H. A., Kadry, S., Nedoma, J., Martinek, R., & Zaporain, B. G. (2023). Industrial Internet of Water Things architecture for data standardization based on blockchain and digital twin technology. *Journal of advanced research*. <https://doi.org/10.1016/j.jare.2023.10.005>
- [Moher *et al.*, 09] Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & PRISMA Group*. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of internal medicine*, 151(4), 264-269.
- [Müller *et al.*, 22] Müller, K. O., von der Assen, J., Feng, C., & Stiller, B. (2022). An Overview and Ontology of Privacy to Preserve Privacy in Ultra-Wideband Networks. *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, 2317-2324.
- [Omran *et al.*, 23] Omran, H., Al-Obaidi, K. M., Husain, A., & Ghaffarianhoseini, A. (2023). Digital twins in the construction industry: a comprehensive review of current implementations, enabling technologies, and future directions. *Sustainability*, 15(14), 10908.
- [Park *et al.*, 19] Park, H., Easwaran, A., & Andalain, S. (2019). Challenges in Digital Twin Development for Cyber-Physical Production Systems. *Cyber Physical Systems. Model-Based Design*, 28–48. https://doi.org/10.1007/978-3-030-23703-5_2
- [Patwardhan *et al.*, 22] Patwardhan, A., Thaduri, A., Karim, R., & Castano, M. (2022). Federated learning for enablement of digital twin. *IFAC-PapersOnLine*, 55(2), 114-119.
- [Pervez *et al.*, 23] Pervez, Z., Khan, Z., Ghafoor, A., & Soomro, K. (2023). SIGNED: Smart city digital twin verifiable data framework. *IEEE Access*, 11, 29430-29446.
- [Pirbhulal *et al.*, 22] Pirbhulal, S., Abie, H., & Shukla, A. (2022, June). Towards a novel framework for reinforcing cybersecurity using digital twins in IoT-based healthcare applications. In *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)* (pp. 1-5). IEEE.
- [Popa *et al.*, 21] Popa, E. O., van Hilten, M., Oosterkamp, E., & Bogaardt, M. J. (2021). The use of digital twins in healthcare: socio-ethical benefits and socio-ethical risks. *Life sciences, society and policy*, 17(1), 1-25.
- [Qian *et al.*, 22] Qian, C., Liu, X., Ripley, C., Qian, M., Liang, F., & Yu, W. (2022). Digital twin—Cyber replica of physical things: Architecture, applications and future research directions. *Future Internet*, 14(2), 64.
- [Rahmadian *et al.*, 23] Rahmadian, E., Feitosa, D., & Virantina, Y. (2023). Digital twins, big data governance, and sustainable tourism. *Ethics and Information Technology*, 25(4), 61.
- [Rahman *et al.*, 22] Rahman, M., Khan, A., Anwar, S., Al-Imran, M., Verma, R., Kumar, D., Kobayashi, K., & Alam, S. (2022). Leveraging Industry 4.0—Deep Learning, Surrogate Model and Transfer Learning with Uncertainty Quantification Incorporated into Digital Twin for Nuclear System (arXiv:2210.00074). arXiv. <http://arxiv.org/abs/2210.00074>
- [Rasheed *et al.*, 20] Rasheed, A., San, O., & Kvamsdal, T. (2020). Digital Twin: Values, Challenges and Enablers From a Modeling Perspective. *IEEE Access*, 8, 21980–22012. <https://doi.org/10.1109/access.2020.2970143>

- [Reiche *et al.*, 21] Reiche, L. T., Gundlach, C. S., Mewes, G. F., & Fay, A. (2021). The Digital Twin of a System: A Structure for Networks of Digital Twins. 2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 1–8. <https://doi.org/10.1109/ETFA45728.2021.9613594>
- [Samaniego *et al.*, 23] Samaniego, M., & Deters, R. (2023). Digital Twins and Blockchain for IoT Management. Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure, 64–74. <https://doi.org/10.1145/3594556.3594611>
- [Shahzad *et al.*, 22] Shahzad, M., Shafiq, M. T., Douglas, D., & Kassem, M. (2022). Digital twins in built environments: an investigation of the characteristics, applications, and challenges. *Buildings*, 12(2), 120.
- [Shao *et al.*, 23] Shao, G., Hightower, J., & Schindel, W. (2023). Credibility consideration for digital twins in manufacturing. *Manufacturing Letters*, 35, 24–28. <https://doi.org/10.1016/j.mfglet.2022.11.009>
- [Sharma *et al.*, 22] Sharma, A., Kosasih, E., Zhang, J., Brintrup, A., & Calinescu, A. (2022). Digital twins: State of the art theory and practice, challenges, and open research questions. *Journal of Industrial Information Integration*, 100383.
- [Sheng *et al.*, 23] Sheng, D., Lou, Y., Sun, F., Xie, J., & Yu, Y. (2023). Reengineering and its reliability: An analysis of water projects and watershed management under a digital twin scheme in China. *Water*, 15(18), 3203.
- [Siddique *et al.*, 23] Siddique, S., Haque, M. A., Rifat, R. H., George, R., Shujate, K., & Gupta, K. D. (2023, December). Cyber Security issues in the industrial applications of digital twins. In *2023 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 873-878). IEEE.
- [Sifat *et al.*, 23] Sifat, M. M. H., Choudhury, S. M., Das, S. K., Ahamed, M. H., Muyeen, S. M., Hasan, M. M., Ali, M. F., Tasneem, Z., Islam, M. M., Islam, M. R., Badal, M. F. R., Abhi, S. H., Sarker, S. K., & Das, P. (2023). Towards electric digital twin grid: Technology and framework review. *Energy and AI*, 11, 100213. <https://doi.org/10.1016/j.egyai.2022.100213>
- [Singh *et al.*, 21] Singh, M., Fuenmayor, E., Hinchy, E. P., Qiao, Y., Murray, N., & Devine, D. (2021). Digital twin: Origin to future. *Applied System Innovation*, 4(2), 36.
- [Son *et al.*, 22] Son, S., Kwon, D., Lee, J., Yu, S., Jho, N. S., & Park, Y. (2022). On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain. *IEEE Access*, 10, 75365-75375.
- [Suhail *et al.*, 21] Suhail, S., Hussain, R., Jurdak, R., & Hong, C. S. (2021). Trustworthy digital twins in the industrial internet of things with blockchain. *IEEE Internet Computing*, 26(3), 58-67.
- [Sweeney, 02] Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05), 571-588. <https://doi.org/10.1142/s021848850200165x>
- [Tao *et al.*, 19] Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C. (2019). Digital Twin in Industry: State-of-the-Art. *IEEE Transactions on Industrial Informatics*, 15(4), 2405–2415. <https://doi.org/10.1109/TII.2018.2873186>
- [Teisserenc and Sepasgozar, 21] Teisserenc, B., & Sepasgozar, S. (2021). Project data categorization, adoption factors, and non-functional requirements for blockchain based digital twins in the construction industry 4.0. *Buildings*, 11(12), 626.

- [Timperi *et al.*, 23] Timperi, M., Kokkonen, K., Hannola, L., & Elfvingren, K. (2023). Impacts of digital twins on new business creation: insights from manufacturing industry. *Measuring Business Excellence*.
- [Turab and Jamil, 23] Turab, M., & Jamil, S. (2023). A comprehensive survey of digital twins in healthcare in the era of metaverse. *BioMedInformatics*, 3(3), 563-584.
- [Umran *et al.*, 22] Umran, S. M., Lu, S., Abduljabbar, Z. A., Lu, Z., Feng, B., & Zheng, L. (2022). Secure and Privacy-preserving Data-sharing Framework based on Blockchain Technology for Al-Najaf/Iraq Oil Refinery. In *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)* (pp. 2284-2292). IEEE.
- [Upura, 23] Upura (2023). Cybersecurity: Digital Twins in Automotive Industry. *Diva*. <https://www.diva-portal.org/smash/get/diva2:1776713/FULLTEXT01.pdf>
- [Vasiliu-Feltes *et al.*, 23] Vasiliu-Feltes, I., Mylrea, M., Zhang, C. Y., Wood, T. C., & Thornley, B. (2023). Impact of Blockchain-Digital Twin Technology on Precision Health, Pharmaceutical Industry, and Life Sciences: Conference Proceedings, Conv2X 2023. *Blockchain in Healthcare Today*, 6.
- [Wanasinghe *et al.*, 20] Wanasinghe, T. R., Wroblewski, L., Petersen, B. K., Gosine, R. G., James, L. A., De Silva, O., Mann, G. K. I., & Warriar, P. J. (2020). Digital twin for the oil and gas industry: Overview, research trends, opportunities, and challenges. *IEEE access*, 8, 104175-104197.
- [Wang *et al.*, 22] Wang, K., Du, H., & Su, L. (2022, October). Digital Twin Network based Network Slice Security Provision. In *2022 IEEE 2nd International Conference on Digital Twins and Parallel Intelligence (DTPI)* (pp. 1-6). IEEE.
- [Wang *et al.*, 23] Wang, Y., Su, Z., Guo, S., Dai, M., Luan, T. H., & Liu, Y. (2023). A survey on digital twins: architecture, enabling technologies, security and privacy, and future prospects. *IEEE Internet of Things Journal*.
- [Wernick *et al.*, 23] Wernick, A., Banzuzi, E., & Mörelius-Wulff, A. (2023). Do European smart city developers dream of GDPR-free countries? The pull of global megaprojects in the face of EU smart city compliance and localisation costs. *Internet policy review*, 12(1), 1-45.
- [Winter and Chico, 23] Winter, P. D., & Chico, T. J. (2023). Using the non-adoption, abandonment, scale-up, spread, and sustainability (NASSS) framework to identify barriers and facilitators for the implementation of digital twins in cardiovascular medicine. *Sensors*, 23(14), 6333.
- [Xie *et al.*, 18] Xie, B., Hou, J., Xu, Z., & Dan, M. (2018). Component-based model of fin plate connections exposed to fire-part I: Plate in bearing component. *Journal of Constructional Steel Research*. <https://api.semanticscholar.org/CorpusID:115901764>
- [Yang *et al.*, 22] Yang, Y., Ma, W., Sun, W., Liu, Z., Xu, L., & Zhu, Y. (2022). Privacy-Preserving Digital Twin for Vehicular Edge Computing Networks. In *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)* (pp. 2238-2243). IEEE.
- [Yi, 23] Yi, H. (2023). Improving cloud storage and privacy security for digital twin based medical records. *Journal of Cloud Computing*, 12(1), 151.

[Yigit *et al.*, 23] Yigit, Y., Kinaci, O. K., Duong, T. Q., & Canberk, B. (2023, May). TwinPot: Digital twin-assisted honeypot for cyber-secure smart seaports. In *2023 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 740-745). IEEE.

[Zhang *et al.*, 21] Zhang, L., Zhou, L., & Horn, B. K. (2021, April). Building a right digital twin with model engineering. *Journal of Manufacturing Systems*, 59, 151–164. <https://doi.org/10.1016/j.jmsy.2021.02.009>