Review article / Pregledni rad

A NEW FORCE IN THE DIGITAL ECONOMY: DIGITAL TWINS APPLICATIONS AND CHALLENGES

MARIJA KUŠTELEGA
University of Zagreb
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
marija.kustelega@foi.unizg.hr

RENATA MEKOVEC
University of Zagreb
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
renata.mekovec@foi.unizg.hr

AHMED SHAREEF
University of Zagreb
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
ahmed.shareef@foi.unizg.hr

ABSTRACT

Digital twin technology is revolutionizing the digital economy by merging the physical and virtual worlds, making it an essential for digitizing industries. A digital twin (DT), a virtual replica of a physical object, system, or process, is anticipated to create an intelligent, predictive, and highly efficient economy. There is an increasing demand for novel developments in DT across a variety of industries, including manufacturing, construction, oil and gas, aerospace, energy, and healthcare. Certain stakeholders are already realizing that DTs not only enhance efficiency and reduce costs but also enable the creation of new service offerings. However, the adoption of DT brings along a number of challenges, including concerns about data privacy and security. DT has become a popular topic with increasing interest in academic journal articles and solution offers from the industrial sector. This study presents a literature overview of DT in the context of privacy and security issues to gain a better understanding of the key barriers that may impact the future adoption of DT technologies. The paper presents an analysis of articles published in Scopus, Web of Science, and IEEE Xplore databases between 2019 and 2024 that examine the privacy and security problems of DT.

KEYWORDS: digital twin, digital economy, key challenges, privacy, security, The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)

1. INTRODUCTION

Digital twin (DT) technology is revolutionizing the digital economy by seamlessly offering a virtual blueprint of physical processes throughout the entire business lifecycle, enhancing the efficiency and effectiveness of processes, products, and services [Singh et al., 2023]. DT is a virtual replica of physical objects, processes, and services. It simulates the physical counterpart, enabling enhanced predictive capabilities and operational efficiency throughout various digital economies [Pervez et al., 2023]. According to Martinescu [2023], there are three different types of DT: digital model, digital shadow, and digital twin, each serving distinct functions and purposes. A digital model represents a predictive model of a physical counterpart without live updates or data exchange. Digital shadows are virtual models updated with data from the physical model, while digital twins are virtual models that communicate bidirectionally with their physical counterparts.

The global DT market is growing at a compound annual growth rate (CAGR) of 38.2% and is expected to reach a value of $26.07 billion by 2025 [Lee et al., 2020]. Market statistics indicate an increment of $48.2 billion by 2026 [Böhm et al., 2021]. It plays an important role in the digital economy by providing virtual representations of physical assets, enabling real-time monitoring, predictive analysis, and simulations [Yi, 2023; Li et al., 2022; Clementson et al., 2021]. Although it was initially developed to improve manufacturing, DT has been expanded into various domains, from traffic lights to smart cities and agriculture to healthcare [Araújo et al., 2022; Pervez et al., 2023], all of which contribute to the digital economy. DT plays a significant role in predictive maintenance in manufacturing industry [Böhm et al., 2021]. This leads to cost reduction and process optimization by allowing designers and engineers to work on deep detail of the product via a virtual model before initiation of the physical product [Chen et al., 2023]. It not only reduces cost but also improves manufacturing productivity and efficiency, leading to enhancement in designing and manufacturing processes of physical products. However, the adaptation of DT is not without challenges.

According to Yi [2023], there are unique challenges of privacy risks, for which the author demonstrates secure ways to provide services. Afzal et al. [2023] stressed the need for reliable bi-directional communication in DT to establish data integrity, required for practical decision-making, and protection of privacy against cybersecurity threats with a strong focus on security and quality, ensuring integrity and reliability. Additionally, the need for privacy-preserving networks, security protocols, and governance frameworks is stressed to protect sensitive information and ensure compliance with data regulations [Yi, 2023].

The digital economy is growing rapidly via the use of new technologies that increase connection, facilitate automation, promote data analysis, and offer new commercial opportunities. In today's industrial scene, DT has emerged as a vital innovation, redefining the operational, strategic, and economic paradigms of enterprises across several industries. This technology, which generates a virtual reproduction of actual assets, processes, or systems, has the potential to dramatically improve efficiency, save operational costs, and open up new revenue sources. The purpose of this study is to provide a comprehensive literature review on the privacy and security challenges of DT technology, aiming to identify potential barriers to their future industry adoption. The main research questions (RQs) were:

- RQ1: What are the primary application domains of DT technology?
- RQ2: Which privacy and security challenges arise most frequently when using DT technology?

This study is unique in a literature review on a wider range of privacy and security challenges, taking into account both technical and non-technical issues. The work is structured as follows: Section 2 describes the methodology used; Section 3 presents the literature review on DT applications; Section 4 shows the main results; Section 5 discusses the main privacy and security challenges; and in Section 6, the paper is concluded.

2. METHODOLOGY FOR LITERATURE REVIEW

PRISMA methodology was used to perform the literature review [Moher et al., 2009]. To identify relevant articles for the research area, a search string ("digital twin" OR "digital twins") AND ("privacy" OR "security") in the titles or abstract of the paper was utilized. A total of 438 articles were found, with 282 articles remaining after removing duplicates. All publications that dealt with privacy or security challenges in the context of DT were included; all other articles that primarily addressed subjects unrelated to the actual implementation and challenges of DT were removed. After implementing the inclusion and exclusion criteria, a total of 49 articles remained for further analysis. Only English-language articles released between 2019 and 2024 were considered. Furthermore, to better understand the concept and structure of the selected articles, keyword co-occurrence analysis was used to investigate the link between keywords in the literature. It illustrates how specific terms or keywords frequently appear together in text data, with nodes representing authors keywords identified in journal articles and linkages representing word co-occurrences [Radhakrishnan et al., 2017]. This analysis was performed using the bibliometrics library from the R tool, on 282 articles selected in the first step of the PRISMA approach.

3. DIGITAL TWIN APPLICATIONS

DT has applications in various domains where they can serve as a factor that will create a competitive advantage. Despite significant investments in Industry 4.0, industry is not yet capable of fully utilizing the new technology [Mantravadi et al., 2023].

3.1. CONSTRUCTION

In the construction, the main applications are related to smart cities development and surveillance of building projects [Waqar et al., 2023]. DTs are vital for urban planning, specifically for their visualization and simulation capabilities [Lei et al., 2023]. By incorporating the entire ecosystem in decision-making through open innovation and citizen engagement, these can produce co-innovations [D'Hauwers et al., 2021]. Weber-Lewerenz [2021] believes that DT in construction projects will have corporate digital responsibility built into them. The use of emerging technologies like blockchain and non-fungible token (NFT) standards could improve secure data sharing [Teisserenc & Sepasgozar, 2022].

3.2. INFRASTRUCTURE

Other DT applications include facility and infrastructure management also essential for preserving safety and functionality, with smart infrastructure emerging alongside traditional infrastructure assets. They could be used in civil infrastructure systems for transportation, energy, water and waste applications such as demand forecasting, emergency planning, predictive maintenance, security resilience, and so on [Callcut et al., 2021]. For example, using

bridge digital twins' models can provide effective remote management such as bridge model updating, monitoring, operational and other maintenance purposes [Ye et al., 2022]. They can be used for asset management and as a way to improve maintenance practices, service delivery, and sustainability [Fialho et al., 2022].

3.3. MANUFACTURING

In the manufacturing industry, the digital twin can be used to facilitate new business creation [Timperi et al., 2023]. An interview study with eight manufacturing companies identified barriers and challenges for fully leveraging DT benefits [Wärmefjord et al., 2020]. The study revealed a significant gap between academia and industry, with challenges primarily observed in system and work process simulation, management issues, and education. This is supported by Neto et al. [2020], who claim that standardization, technological maturity, and integration, as well as lack of people's qualifications and resistance to change impede the use of DT.

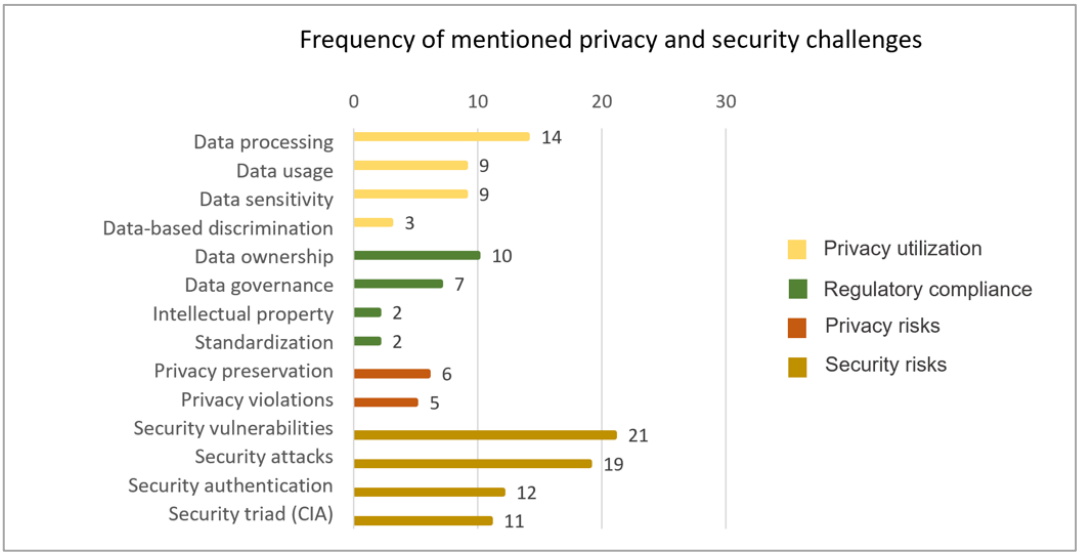
3.4. HEALTHCARE

In healthcare, DT could be an effective tool for short clinical trials and providing preventive healthcare to enable personalized medicine [De Maeyer and Markopoulos, 2021]. In his study, de Boer et al. [2022] explores the various ways in which DT can be integrated into people's lives, focusing on how potential users want to be treated and how this can be applied to the introduction of DT into care practice. Similarly, Popa et al. [2021] investigated the socio-ethical benefits and risks of DT in healthcare, focusing on the prominent risks triggered by their adoption and perceived stakeholders' benefits.

4. RESULTS

This study examined 49 articles in which challenges can roughly be divided into technical and non-technical challenges. Figure 1 depicts the frequency of identified privacy and security challenges, divided into four categories: (1) privacy utilization, (2) regulatory compliance, (3) privacy risks, and (4) security risks.

Figure 1. Frequency of mentioned privacy and security challenges

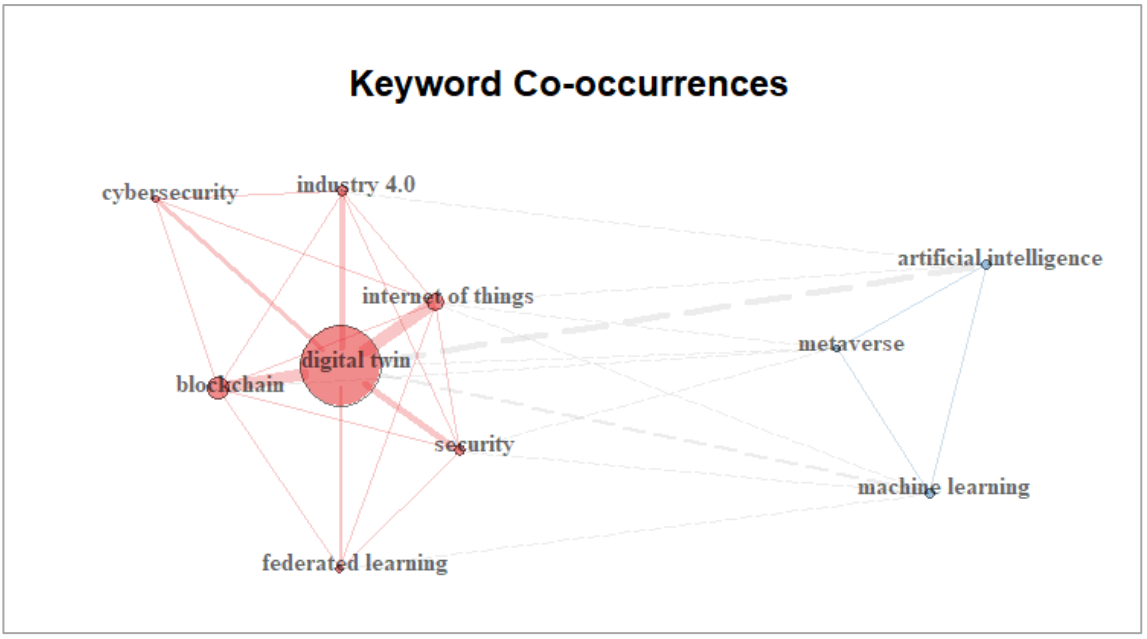


Source: Authors

Figure 1 illustrates the prevalence of security risks, including those related to system vulnerabilities, attacks, authentication, and overall threats to the data confidentiality, integrity, or availability. Next are those related to the utilization of privacy (privacy risk), such how private and sensitive information are handled and shared. Regulatory compliance-related challenges like data governance, ownership, intellectual property, and standardization are almost equally represented. When everything is taken into account, the challenges resulting from the real violation of privacy in specific attack or data breach scenarios are not that concerning.

Figure 2 depicts the co-occurrence analysis of terms performed in the R tool on 282 articles found in the IEEE Xplore, WoS and Scopus databases. With the help of keyword co-occurrence analysis, it was possible to see which terms are most often mentioned together in the literature.

Figure 2. Keyword co-occurrence network in the R tool



Source: Authors

In Figure 2, keywords are displayed using circles, while different colors indicate keyword clusters, and frequency of occurrence is indicated by the size of the circle. The two primary clusters are: digital twin and artificial intelligence. It is visible that many articles mention digital twin in the context of artificial intelligence, metaverse and machine learning. There is a strong connection between digital twin and related concepts such as the internet of things, Industry 4.0 and blockchain, although it is worth noting that terms like security and cybersecurity appears alongside these terms. This confirms the previous analysis, which found that security concerns are common when dealing with digital twin topics.

5. DISCUSSION

Our systematic review of the literature revealed four main privacy and security challenges associated with digital twins. It served as a follow up to previous literature reviews [Yao et al., 2023; Lei et al., 2023; Asad et al., 2023]. As stated, this emerging technology needs to address

challenges around the entire digital twin life cycle and their integration into current frameworks. One of the key challenges were **security risks**, most frequently mentioned in the total number of examined articles. They were mostly related to cybersecurity, such as system vulnerabilities and network communication problems, which can lead to data breaches and cyberattacks. Previous research confirms that data breaches have become a significant challenge for organizations [Seh at. Al, 2020; Wheatley et al., 2016], as they compromise the confidentiality, integrity, and availability of data, known as the security triad [Umran et al., 2022]. The majority of identified security triad issues pertain to data confidentiality and integrity, while data availability was less concerning. This category also encompassed issues related to security authentication, such as identity management, access control, and unauthorized access. A multi-user system could be a solution for protecting data from clouds by allowing owners to control access to specific data subsets [Hörandner and Prünster, 2021]. Authentication mechanisms could help maintain confidentiality in digital communication, including medical records and other operations [Qian et al., 2022].

The second category of challenges falls under the **privacy utilization category**, which includes data processing, data usage, data sensitivity and data-based discrimination. Data usage referred to general use of personal data, while data processing included the collection, storage, and data sharing. The paper highlights that most cyberattacks are linked to the process of collecting and handling large amounts of data [Bruynseels et al., 2018]. For this reason, Tao et al. [2019] suggested implementation of security and privacy tools that can achieve overall data protection. Data sensitivity included issues around control over sensitive data [Hörandner and Prünster, 2021], collection and dissemination [Qian et al., 2022], as well as confidentiality protection [Araújo et al., 2022]. It was observed various categories that need to be protected like sensitive project and asset data [Omrany et al., 2023], manufacturing data [Timperi et al., 2023], critical physical objects and systems information [Hemdan et al., 2023] and confidential patient data [Turab and Jamil, 2023]. Data-based discrimination is revealed as one of the challenges, explained as people's tendency to identify patterns in data can lead to prejudice [Bruynseels et al, 2018]. For example, it can cause patients to be diagnosed as ineligible for surgery or insurance [Popa et al., 2021]. It can widen socio-economic gaps by not being accessible in countries with lack of access to research facilities, leading to inequality and injustice [Popa et al., 2021; Winter and Chico, 2023]. The issue of uneven access is in previous research recognized as a significant obstacle that hinders the participation of stakeholders [Lei et al., 2023].

The third, **regulatory compliance** category, included: (1) data ownership, (2) governance, (3) regulatory frameworks, (4) intellectual property, and (5) standardization challenges. Our review revealed the most problems with data ownership and governance arise from poor regulatory frameworks and a lack of standards. As indicated by Kwon and Johnson [2013], fear of potential data breaches motivates organizations to comply with regulatory requirements. It is important to achieve regulatory compliance with data privacy guidelines [Cali et al., 2023]. As digital twin development includes frameworks related to specific industries, devices and artificial intelligence, compliance with each of these regulations should be achieved [Cellina et al., 2023].

Finally, the fourth category of **privacy risks** received little attention. It dealt with privacy preservation and data anonymity, while mentioning various forms of privacy violations such as personal information attacks, privacy breaches, data leaks, and misuses of private data. As wireless data transfer may contain content that can jeopardize owners' privacy, it requires the creation of secure data sharing channel [Son et al., 2022]. Private data must also be protected, as vehicle DT data, including position and transmission conditions, is vulnerable to attack when

transmitted to the cloud [Yang et al., 2022]. Detailed product information can facilitate production management, but at the same time it makes it easier for attackers to learn confidential business know-how [Holmes et al., 2021].

6. CONCLUSION

This study tackled the current state of DT implementation and the challenges that industries are facing, with a particular emphasis on privacy and security. Findings showed that DT are implemented in various domains such as construction, infrastructure, manufacturing and healthcare, which was related to the first research question (RQ1). In response to the second research question (RQ2), this study identified 4 main categories of privacy and security challenges: (1) privacy utilization, (2) regulatory compliance, (3) privacy risks, and (4) security risks. The key technical challenges were cybersecurity and attacks, as well as authentication problems caused by system vulnerabilities.

Security risks are identified as one of the major challenges that prevents successful DT implementation. Other reasons included some non-technical aspects that were primarily related to privacy challenges, such as the use of private and sensitive data, legislation, and fair data distribution. The results indicate that establishment of an appropriate security infrastructure could solve a number of non-technical challenges and reduce the possibility of privacy and security risks. Furthermore, recommendations for further research should be aimed at creating a common regulatory environment for the development of a digital twin technology. In particular, the challenges identified in this study can be used as variables or constructs that can be addressed in developing a digital twin framework. One of the limitations of this research is that focus was only on privacy and security challenges, while there are a number of other challenges that prevent its successful implementation. Some of the open questions relate to what challenges arise in certain phases of the digital twin's life cycle, so that they can be focused on during each development phase.

REFERENCES

[1] 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.

[2] 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 IGLC* (Vol. 30).

[3] Asad, U., Khan, M., Khalid, A., & Lughmani, W. A. (2023). Human-centric digital twins in industry: A comprehensive review of enabling technologies and implementation strategies. *Sensors*, *23*(8), 3938.

[4] Böhm, F., Dietz, M., Preindl, T., & Pernul, G. (2021a). Augmented Reality and the Digital Twin: State-of-the-Art and Perspectives for Cybersecurity. *Journal of Cybersecurity and Privacy, 1(3)*, 519–538. https://doi.org/10.3390/jcp1030026

[5] Bruynseels, K., Santoni de Sio, F., & Van den Hoven, J. (2018). Digital twins in health care: ethical implications of an emerging engineering paradigm. *Frontiers in genetics*, *9*, 320848.

[6] Cali, U., Dimd, B. D., Hajialigol, 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.

[7] Callcut, M., Cerceau Agliozzo, J. P., Varga, L., & McMillan, L. (2021). Digital twins in civil infrastructure systems. *Sustainability, 13(20),* 11549.

[8] Cellina, M., Cè, M., Alì, M., Irmici, G., Ibba, S., Caloro, E., ... & Papa, S. (2023). Digital Twins: The New Frontier for Personalized Medicine?. *Applied Sciences*, *13*(13), 7940.

[9] 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. https://doi.org/10.3390/app13031440

[10] Clementson, J., Teng, J., Wood, P., & Windmill, C. (2021). Legal Considerations for Using Digital Twins in Additive Manufacture – A Review of the Literature. In M. Shafik & K. Case (Eds.), *Advances in Transdisciplinary Engineering*. IOS Press.

[11] D'Hauwers, R., Walravens, N., & Ballon, P. (2021). From an inside-in towards an outside-out urban digital twin: Business models and implementation challenges. *ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *8*, 25-32.

[12] de Boer, B., Strasser, C., & Mulder, S. (2022). Imagining digital twins in healthcare. *prometheus*, 38(1), 67-81.

[13] De Maeyer, C., & Markopoulos, P. (2021, July). Future outlook on the materialisation, expectations and implementation of Digital Twins in healthcare. In *34th British HCI Conference* (pp. 180-191). BCS Learning & Development.

[14] Fialho, B. C., Codinhoto, R., Fabricio, M. M., Estrella, J. C., Ribeiro, C. M. N., Bueno, J. M. D. S., & Torrezan, J. P. D. (2022). Development of a BIM and IoT-Based Smart Lighting Maintenance System Prototype for Universities' FM Sector. *Buildings*, *12*(2), 99.

[15] 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*, *131*(3), 2193-2216.

[16] 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.

[17] 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).

[18] Kwon, J., & Johnson, M. E. (2013). Health-care security strategies for data protection and regulatory compliance. *Journal of Management Information Systems*, *30*(2), 41-66.

[19] Lee, J., Azamfar, M., Singh, J., & Siahpour, S. (2020). Integration of digital twin and deep learning in cyber-physical systems: Towards smart manufacturing. *IET Collaborative Intelligent Manufacturing, 2(1),* 34–36. https://doi.org/10.1049/iet-cim.2020.0009

[20] Lei, B., Janssen, P., Stoter, J., & Biljecki, F. (2023). Challenges of urban digital twins: A systematic review and a Delphi expert survey. *Automation in Construction*, *147*, 104716.

[21] Li, Q., Huo, D., & Jiang, L. (2022, December). A Digital Twin System for Monitoring the Security of Theatrical Stages. 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. 2224-2230). IEEE.

[22] Mantravadi, S., Srai, J. S., & Møller, C. (2023). Application of MES/MOM for Industry

4.0 supply chains: A cross-case analysis. *Computers in Industry*, 148, 103907.
[23] Martinescu, L. (2023, October 23). *Exploring the concepts of digital twin, digital shadow, and digital model*, https://oxfordinsights.com/insights/exploring-the-concepts-of-digital-twin-digital-shadow-and-digital-model/, downloaded: [Maj, 27th 2024]
[24] 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.
[25] Neto, A. A., Deschamps, F., da Silva, E. R., & de Lima, E. P. (2020). Digital twins in manufacturing: an assessment of drivers, enablers and barriers to implementation. *Procedia Cirp*, *93*, 210-215.
[26] Omrany, 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.
[27] Pervez, Z., Khan, Z., Ghafoor, A., & Soomro, K. (2023). SIGNED: Smart cIty diGital twiN vErifiable Data Framework. IEEE Access, 11, 29430–29446. https://doi.org/10.1109/ACCESS.2023.3260621
[28] 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, 1-25.
[29] 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.
[30] Radhakrishnan, S., Erbis, S., Isaacs, J. A., & Kamarthi, S. (2017). Novel keyword co-occurrence network-based methods to foster systematic reviews of scientific literature. *PloS one*, *12*(3), e0172778.
[31] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020, May). Healthcare data breaches: insights and implications. In *Healthcare* (Vol. 8, No. 2, p. 133). MDPI.
[32] Singh, A., Ali, Md. A., Balusamy, B., & Sharma, V. (2023). Potential applications of digital twin technology in virtual factory. In Digital Twin for Smart Manufacturing (pp. 221–241). Elsevier. https://doi.org/10.1016/B978-0-323-99205-3.00011-0
[33] 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.
[34] Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, *98*, 660-671.
[35] Teisserenc, B. and Sepasgozar, S. M. (2022). Software Architecture and Non-Fungible Tokens for Digital Twin Decentralized Applications in the Built Environment. *Buildings*, *12*(9), 1447
[36] Timperi, M., Kokkonen, K., Hannola, L., & Elfvengren, K. (2023). Impacts of digital twins on new business creation: insights from manufacturing industry. *Measuring Business Excellence*, (ahead-of-print).
[37] Turab, M., & Jamil, S. (2023). A comprehensive survey of digital twins in healthcare in the era of metaverse. *BioMedInformatics*, *3*(3), 563-584.
[38] Umran, S. M., Lu, S., Abduljabbar, Z. A., Lu, Z., Feng, B., & Zheng, L. (2022, December). 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.

[39] Waqar, A., Othman, I., Almujibah, H., Khan, M. B., Alotaibi, S., & Elhassan, A. A. (2023). Factors influencing adoption of digital twin advanced technologies for smart city development: Evidence from Malaysia. *Buildings*, 13(3), 775.

[40] Wärmefjord, K., Söderberg, R., Schleich, B., & Wang, H. (2020). Digital twin for variation management: A general framework and identification of industrial challenges related to the implementation. *Applied Sciences*, *10*(10), 3342.

[41] Weber-Lewerenz, B. (2021). Corporate digital responsibility (CDR) in construction engineering—et Weber-Lewerenz, B. (2021). Corporate digital responsibility (CDR) in construction engineering—ethical guidelines for the application of digital transformation and artificial intelligence (AI) in user practice. *SN Applied Sciences*, *3*, 1-25.

[42] Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, *89*, 1-12.

[43] 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.

[44] Yang, Y., Ma, W., Sun, W., Liu, Z., Xu, L., & Zhu, Y. (2022, December). 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.

[45] Yao, J. F., Yang, Y., Wang, X. C., & Zhang, X. P. (2023). Systematic review of digital twin technology and applications. *Visual Computing for Industry, Biomedicine, and Art*, *6*(1), 10.

[46] Ye, C., Kuok, S. C., Butler, L. J., & Middleton, C. R. (2022). Implementing bridge model updating for operation and maintenance purposes: Examination based on UK practitioners' views. *Structure and Infrastructure Engineering*, *18*(12), 1638-1657.

[47] Yi, H. (2023). Improving cloud storage and privacy security for digital twin based medical records. *Journal of Cloud Computing, 12(1),* 151. https://doi.org/10.1186/s13677-023-00523-6