International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Software Security in Digital Twins and Cyber-Physical Systems: review paper

Ms. Amna Hassan Ali Al-Shidi
IT Instructor, University of Buraimi, Oman
Email: amna.h@uob.edu.om

Abstract
Digital twins (DTs) are essential components of cyber-physical systems (CPSs), enabling monitoring, analytics, predictions, and process improvement. However, their integration and deployment into the infrastructure can pose significant security risks, potentially exposing software vulnerabilities and cyber threats and challenges. This study explains and examines the role of software in digital twin-based CPSs, focusing largely on the key security challenges and solutions. Through a literature review, the study highlights software shortcomings, such as low-quality encryption, outdated protocols that require updating, and unauthorized access that could compromise the digital domain and lead to data loss. The study also explains various security models, including zero-trust architectures and secure multiparty computing, to enhance the resilience of digital twins against cyber threats. The findings also highlight the need for continuous and ongoing development of security processes to ensure data integrity, security, reliability, and privacy in digital twin-enabled CPS environments.

Keywords: Software Security; Digital Twins.

Introduction

Digital Twins (DTs) are essential technology in modern cyber-physical systems (CPS), representing a virtual demonstration of multiple systems and processes, these digital technologies offer simultaneous tracking, monitoring, and capabilities of simulation to improve performance and security (Zhao et al., 2022). As DTs become increasingly connected to infrastructure, they pose new security risks, including cyber threats and system and software vulnerabilities that can compromise both digital and physical domains (Eckhart et al., 2019).

Software security indicates to a few actions that assist in saving software applications and digital solutions from attacks, and those developers integrate this technology into the software development and update life cycle and testing processes (Suhailet al., 2022). However, DTs are virtual exemplification of physical objects, operations, and systems that are updated continuously with real-time data and information (Wang al., 2023).

Moreover, the cyber-physical system integrates computational and physical processes, making it possible to automate manufacturing, transportation, and healthcare industries (Jaber al., 2022). These systems rely on the exchange of information and data between digital platforms, which will make them vulnerable to cyber-attacks, DT integration allows for enhancing and strengthening the security of CPS by detecting threats in real-time, assessing the level of risk and predictions (Tao et al., 2021).

In addition, data management systems (DTs) face numerous challenges in ensuring data preservation and privacy. Attackers may exploit numerous software vulnerabilities to manipulate processes and attempt to

compromise systems, leading to inaccurate system behavior and decision-making errors. Furthermore, this can lead to problems such as data integrity, unauthorized access, and significant security risks in the DTs environment. (Homaei et al., 2025).

It is imperative to develop robust security models and systems that address all aspects of software vulnerabilities and enhance their resilience. This paper explores the role of software security in cloud-based data protection systems. This study highlights the key challenges and current solutions used in advanced security technologies. The primary objective of this research is to provide a comprehensive description of software security in cloud computing, demonstrating its ability to strengthen cloud data protection systems against cyberattacks and ensure system reliability (Zhang et al., 2023).

Problem Statement

The use of digital transformation technologies (DTs) in data protection systems (CPSs) has been demonstrated, demonstrating how they can improve performance and efficiencies through monitoring, simulation capabilities, and predictive analytics. However, the comprehensive interconnectedness and integration of DTs and infrastructure can lead to significant security risks. Software vulnerabilities and cyber threats pose a significant threat in the digital realm. Security vulnerabilities, such as protocols, malicious data manipulation, and poor encryption quality, can lead to inaccurate system operational issues and CPS failures. Despite the tremendous potential of DTs, maintaining data security and privacy remains a significant challenge. Furthermore, the evolving nature of cyberattacks requires the development of robust security models and programs. This paper aims to recognize the main role of software security in the development of DTs within CPSs, and the study focuses on identifying the main security difficulties related to software vulnerabilities and attacks facing DTs in CPSs by reviewing previous studies.

Literature Review

The study by Eckhart et al. (2023) demonstrates the role of DTs as virtual copies of physical objects in developing and strengthening the Defense of CPSs. CPSs, the ability of the DT system to monitor and predict, which leads to increased efficiency in manufacturing. The researcher in this study indicates that DTs can enhance and develop the security of CPSs during their life cycle, but they face some challenges such as complexity and high costs.

Similarly, the study by Holmes et al. (2021) this paper examines the effective role of advanced DT technology, which helps in digital analysis, effective design and optimization of systems, enhancing speed and efficiency, DTs support modern models for example, Industry (4.0) and future factories while improving efficiency in domains for instance, industrialization, cultivation, building and automotive, however, the risk connected with DTs in the field of cybersecurity is still not fully understood. Therefore, this paper examines the risks involved and explores how DTs can enhance the effectiveness of cybersecurity, which may become a key component of defense-in-depth strategies.

A study by Ding et al. in 2019 explores CPSs projects and DT technologies to integrate physical and cyber-shop floors. Cyber-physical production systems operating on the DT system are developed, focusing on its configuration, operation, and real-time data-driven control.

In contrast, a research by Ulhe et al. (2023) identifies how CPSs processing and sector (4.0) are improving and evolving production through digital manufacturing principles, with a strong focus on rapid decision making and waste reduction, examining and revealing data collection via wireless sensor network (WSN), waste elimination through the use of value flow chart (VSM 4.0), and servicing predictions through total

productive maintenance (TPM) with real-time KPIs, big data analytics promote adaptable manufacturing, while CONWIP control (CSC) supports production flexibility. Through brain-inspired pattern recognition for structural and syntactic computing (BIC-SS), with MATLAB simulation optimization of Kanban parameters, digital manufacturing ultimately improves efficiency, reduces cost, and promotes innovation.
In a related study, Park (2020) explores how production mechanisms in make-to-order (MTO) environments provide a flexible supply chain to cope with dynamic changes, because the legacy cyber-physical system (CPS) faces problems and limitations in controlling SC for MTO, the study proposes a system called a comprehensive cyber-physical management system through the operator-based embedded blossoming system in the Many-layered CPS architecture, this Structure helps to enhance the flexibility and scalability of SC through a simulation process of distributed DT.
Moreover, a paper by Huang et al. (2024) aims to recognize the percentage of the ability of DTs technology rise to the challenge and difficulties within food supply chains (FSCs). The study highlights the involvement of DTs in food supply chains (FSCs), focusing on their main characteristics, including monitoring, simulation, and analysis, by taking advantage of innovation theories. This study identifies a five-step structured enforcement process across three phases and introduces two new steps, namely technology assessment and performance assessment, which are essential for the successful progress of DT integration.
Likewise, a survey done by Guo et al. (2024) investigates the function of DTs in improving and strengthening lean supply chains that include Industry 4.0, improving and developing efficiency, reducing and reducing costs, and improving the level of responsiveness. Despite their capabilities, the relationships between DTs and lean supply chains are still unclear and unexplored. This study applied the SCOR framework to classify the effects of DTs on the process of supply chain and accomplishment. The results showed that DTs are mainly used in planning and manufacturing processes. DTs enhance and strengthen lean manufacturing practices by improving information flow, reducing waste, and improving and developing logistics services.
Additionally, Park et al. (2024) This study examines the challenges of supply chain (SC) control in make-to-order (MTO) environments, where dynamic fluctuations are required for operational flexibility, through this study, it was observed that traditional CPSs face limitations in the field of supply chain control management in manufacturing conditions, in order to address this, the study proposes an agent-based cyber-physical logistics system within a multi-level CPS framework. This framework enhances the flexibility and capacity of the supply chain by arranging and coordinating the distributed DT simulation process.
Moreover, the study by Li et al. (2021) This paper introduces the field of social manufacturing as a model and framework for network manufacturing that leverages social manufacturing resources to meet individual demands through collective intelligence and collaborative architectures to create products and address challenges. The study proposes digital that supports Blockchain technology as an integrated solution.
In the realm of smart warehouses, Wu et al. (2023) proposes frameworks that rely on DT for smart warehouses, to address the challenges in digital warehouse designs, the four-step framework works to improve and develop warehouse designs, procedures, and operations, and its working mechanisms have been verified through a case study of a microprocessor manufacturing plant.
Exploring cybersecurity applications, McLaughlin (2023) highlights the mechanisms for enhancing and strengthening DTs for cybersecurity networks, which are considered a decentralized security structure

enhanced by artificial intelligence technology, in addition to working as digital copies, DTs enable real-time predictive analysis, changing cybersecurity from identifying threats to proactive forecasting.

On an urban scale, Masoumi et al. (2023) examine the level of progress of DTs of cities (CDTs), the type of data analysis, the technology used, and the levels of progress. The study highlights the gap between real-time analytics and big data.

Jiang et al. (2024) explore how the integration of CPSs into cyber-physical construction systems, can strengthen and enhance manufacturing but increase cybersecurity risks. To address this, this study proposes DT-based security model that improves asset visibility, prioritizes vulnerability mitigation, and allows for risk assessment through virtual simulation. The model has helped identify security threats without disrupting operations, and its effectiveness has been demonstrated in human-robot assemblies, demonstrating the possibility of DT technology to build up and strengthen the cybersecurity of CPPSs.

In healthcare, Zhang (2021) investigates medical digital twins (MDTs) for health prediction and clinical decision-making, integrates augmented reality and deep learning for human-cyber interactions, and proposes CodeBERT-based neural networks to mitigate security risks.

Finally, Azambuja et al. (2023) this study explores DT technologies in Industry 4.0, focusing on their advantages and cybersecurity challenges. The study focuses on the security risks associated with DT connectivity and discusses best practices for securing virtual models and protecting physical systems.

Results and Discussion of the literature survey according to the above studies:

Year	Author	Problem of Study	Proposed Method	Weakness
2023	Eckhart et al.	Cyber-physical security of systems using DTs.	The method used is by using DTs to monitor, test security and detect breaches.	High costs and complexity hinder its adoption.
2021	Holmes et al.	DTs in industrial risks and cybersecurity.	reconnoitering DTs for System Improvement and Development and Cyber Security.	Cybersecurity risks remain Undiscovered.
2019	Ding et al.	Digital Dual Integration in Smart Manufacturing	DT-based cyber-physical construction systems for smart industry	Lacks practical real-world implementation applications.
2023	Ulhe et al.	Digital lean manufacturing in Industry.	The method used is Wireless Sensor Networks (WSN) which includes several techniques such as VSM (4.0), Big Data Analytics,	High computational requirements and complexity.

			and Pattern Recognition using BIC-SS, in addition to using MATLAB simulation.	
2020	Park	Supply Chain Flexibility in On-Demand Production Environments.	Using the Electronic Physical Logistics System (CPLS) with the use of distributed DT simulation.	Implementation challenges in real-world environments.
2024	Huang et al.	DTs' working mechanisms in the chain of food supply.	Systematic literature review (SLR) theoretical framework TOE model	Limited experimental validation
2024	Guo et al.	DTs in the Enterprise (4.0) Supply network.	Systematic literature review (33 papers). SCOR framework analysis.	Very limited focus on sources and revenues.
2024	Park et al.	Supply chain monitoring in make-to-order (MTO) environments.	Cyber-Physical Logistics System (CPLS), Distributed DT Simulation.	Lacks real-world validity
2021	Li et al.	Challenges of cooperation in the field of communal manufacturing.	Blockchain-powered dual digital collaboration platform	Concerns about blockchain scalability
2023	Wu et al.	Challenges in Designing Digital Repositories.	A Four-Step Digital Framework for Smart Warehouses.	Validation is limited beyond a single case study.
2023	McLaughlin	Moving from reactive threat identification to	Using DTs to enhance and strengthen the cybersecurity	Cybersecurity systems are reactive systems that focus

		predictive cybersecurity.	network Artificial intelligence to enable prediction.	primarily on identifying threats.
2023	Masoumi et al.	Address research gaps in CDTs related to analysis, data insights, and engagement.	Leveraging City Digital Twins (CDTs) with higher-level data types and technologies.	Gaps in analytics, big data insights, and public participation in city digital twins (CDTs).
2024	Jiang et al.	CPPS systems are facing cybersecurity risks due to increased connectivity.	A DT-based security framework for assessing risks and mitigating their impact.	Implementation challenges: scalability and real-time responsiveness.
2021	Zhang	Combining Haptic-AR Navigation, Deep Learning, and Code BERT-Based Neural Network to Mitigate Security Risks.	Enhancing and strengthening health prediction and important clinical decision-making using Medical Digital Twins (MDTs).	Security risks in the systems that make medical decisions.
2023	Azambuja et al.	Explore the cybersecurity challenges and benefits of technology in manufacture 4.0.	Securing virtual models and protecting physical systems.	Security risks associated with DT communication in Industry (4.0)

Research Methodology

1. **Research Approach**

- The researcher used the qualitative research method with a comprehensive review of the literature.

2. In this research paper, researchers focused on "software security in cyber-physical systems based on the digital twin".
3. **Data Collection**

- Reviewing academic papers, reports, and reviewing studies.
- Sources from "IEEE Xplore", "Springer", and "ScienceDirect".
- The researcher selected a group of studies published in recent years to serve as references for this research paper.

4. **Data Analysis**

- Comparative analyses of current challenges, solutions and security trends.

- The researcher evaluated the evaluation of security models to enhance and strengthen the resilience of DT-based CPS systems..

5. **Ethical Considerations**

Ethical considerations were maintained by:

- Properly documenting all sources according to academic documentation.
- Not collecting any private data and avoiding bias in data collection.
- Avoiding plagiarism.
- The researcher is committed to presenting research information without misinterpretation.
- The researcher is committed to adhering to all standards and principles of academic integrity.

In addition, during the last ten years, an increasing number of scientific research papers Related to Software Security in Digital Twins and Cyber-Physical Systems have been observed. Therefore, the researcher conducted statistics to determine the percentage and number of scientific papers and research papers between the following years 2014 and 2024, as shown in table (1):

Years 2014 to 2025	number of scientific papers
2014 - 2015	100
2015-2016	179
2016-2017	402
2017-2018	848
2018-2019	1,590
2019-2020	2,740
2020-2021	4,210
2021-2022	5,690
2022-2023	7,980
2023-2024	9,670
2024-2025	6,620

Figure (1): showing the number of scientific papers published on software security in digital twins and cyber-physical systems from (2014 to 2025).

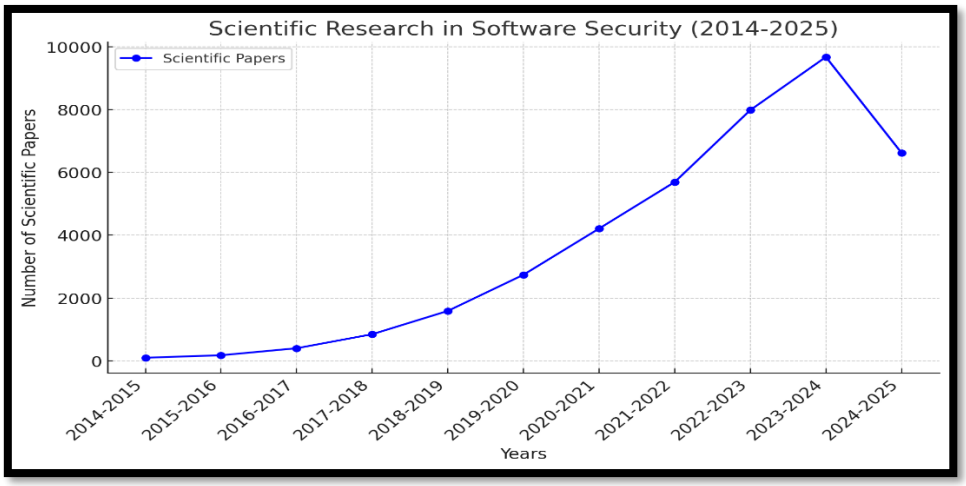

Figure 1

Source: My own preparation.

Discussion and analysis

Subject	Number of research/studies
(DTs) in Cybersecurity	4 studies
(DTs) in Manufacturing	4 studies
DTs in Supply Chains	4 studies
DTs in Smart Warehouses	1 studies
(DTs) in Healthcare	1 studies
Blockchain & (DTs)	1 studies
City Digital Twins (Urban Applications)	1 studies

Table: (2) The number of research areas in this paper:

The graph shows scientific studies on the topic of DTs in various fields. These include many fields, including cybersecurity, supply chains and manufacturing, which include the largest number of research studies (4 studies each), but other fields, such as healthcare, smart warehouses and blockchain, have only one study each, indicating that there are research gaps in these fields.

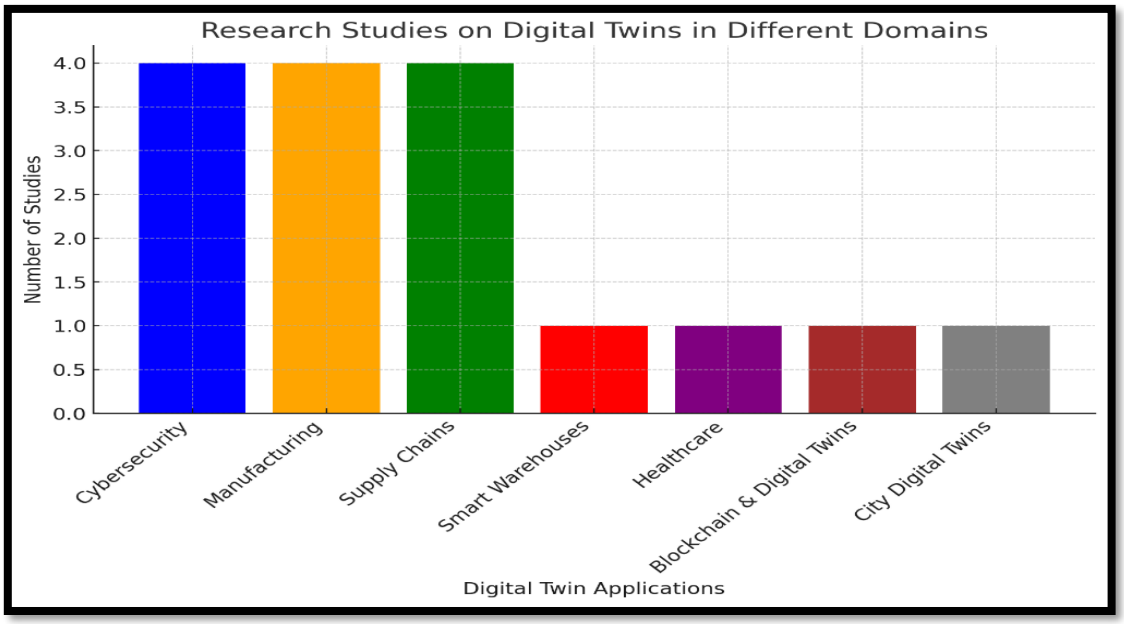

Figure 2
Source: My own preparation.

Table: (3) Below is a comprehensive summary of the number of studies that use each methodology:
The chart (3) shows the distribution of methodologies across the studies:

Methodology	Number of Studies
Systematic Literature Review (SLR)	2
Conceptual Framework/Model	4
Case Study/Simulation	3
Experimental/Implementation	2

Review/Exploratory Study	5

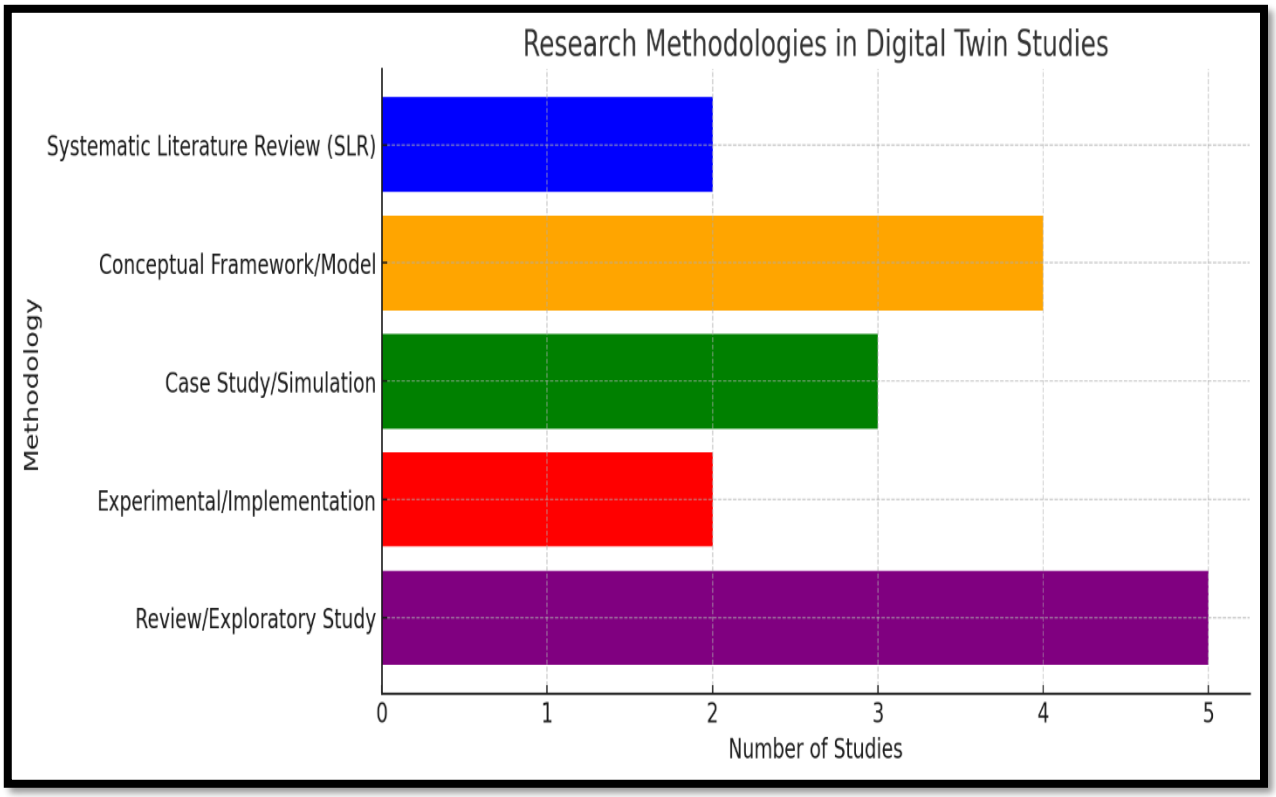

Figure 3
Source: My own preparation.

Conclusion

Previous studies included and analyzed in this paper show that DTs have great benefits but are exposed to many risks such as weak encryption, security protocols, and unauthorized access, all of which can affect and disrupt digital and physical operations. Modern solutions, including zero-trust and multi-party computing, have proven their ability to mitigate all these risks. However, there is a need for much scientific research to apply and refine these models and strengthen their implementation in applications. The main findings of this study confirmed the need to build an integrated approach to DT security that includes modern encryption methods, knowledge of current threats, and strong authentication methods. In conclusion, the security of DTs in the cyber-physical system poses ongoing challenges and requires continuous adaptation to modern threats. Through joint efforts between academia and policymakers, it is possible to develop very strong security frameworks that protect and enhance DTs.

References

1. Azambuja, A. J. G. de, Giese, T., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Opportunities and challenges related to cyber security. *Procedia CIRP, 119*, 1005–1010. https://doi.org/10.1016/j.procir.2023.09.225
2. Ding, K., Chan, F. T. S., Zhang, X., Zhou, G., & Zhang, F. (2019). Defining a digital twin-based cyber-physical production system for autonomous manufacturing in smart shop floors. *International Journal of Production Research, 57*(20), 6315–6334. https://doi.org/10.1080/00207543.2019.1566661

3. Eckhart, M., & Ekelhart, A. (2019). Digital twins for cyber-physical systems security: *Security and quality in cyber-physical systems engineering* (pp. [page range]). Springer, Cham. https://doi.org/10.1007/978-3-030-25312-7_14
4. Holmes, D., Papathanasaki, M., Maglaras, L., Ferrag, M. A., Nepal, S., & Janicke, H. (2021). 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. https://doi.org/10.1109/SEEDA-CECNSM53056.2021.9566277
5. Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J., & others. (2024). A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artificial Intelligence Review, 57*, 201. https://doi.org/10.1007/s10462-024-10805-3
6. Huang, Y., Ghadge, A., & Yates, N. (2024). Implementation of digital twins in the food supply chain: A review and conceptual framework. *International Journal of Production Research, 62*(17), 6400–6426. https://doi.org/10.1080/00207543.2024.2305804
7. Jaber, A., Koufos, I., & Christopoulou, M. (2025). A comprehensive state-of-the-art review for digital twin: Cybersecurity perspectives and open challenges. In L. Barolli (Ed.), *Advances on P2P, parallel, grid, cloud and internet computing. 3PGCIC 2024. Lecture notes on data engineering and communications technologies* (Vol. 232). Springer, Cham. https://doi.org/10.1007/978-3-031-76462-2_8
8. Jiang, Y., Wang, W., Ding, J., Lu, X., & Jing, Y. (2024). Leveraging digital twin technology for enhanced cybersecurity in cyber–physical production systems. *Future Internet, 16*(4), 134. https://doi.org/10.3390/fi16040134
9. Li, M., Fu, Y., Chen, Q., & Qu, T. (2021). Blockchain-enabled digital twin collaboration platform for heterogeneous socialized manufacturing resource management. *International Journal of Production Research, 61*(12), 3963–3983. https://doi.org/10.1080/00207543.2021.1966118
10. Masoumi, H., Shirowzhan, S., Eskandarpour, P., & Pettit, C. J. (2023). City digital twins: Their maturity level and differentiation from 3D city models. *Big Earth Data, 7*(1), 1–36. https://doi.org/10.1080/20964471.2022.2160156
11. McLaughlin, K. L. (2023). The power of digital twins in the cybersecurity mesh. *EDPACS, 68*(6), 35–39. https://doi.org/10.1080/07366981.2023.2263214
12. Park, K. T., Son, Y. H., & Noh, S. D. (2020). The architectural framework of a cyber-physical logistics system for digital-twin-based supply chain control. *International Journal of Production Research, 59*(19), 5721–5742. https://doi.org/10.1080/00207543.2020.1788738
13. Suhail, S., Malik, S. U. R., Jurdak, R., Hussain, R., Matulevičius, R., & Svetinovic, D. (2022). Towards situational aware cyber-physical systems: A security-enhancing use case of blockchain-based digital twins. *Computers in Industry, 141*, 103699. https://doi.org/10.1016/j.compind.2022.103699
14. Ulhe, P. P., Dhepe, A. D., Shevale, V. D., Warghane, Y. S., Jadhav, P. S., & Babhare, S. L. (2023). Flexibility management and decision making in cyber-physical systems utilizing digital lean principles with brain-inspired computing pattern recognition in Industry 4.0. *International Journal of Computer Integrated Manufacturing, 37*(6), 708–725. https://doi.org/10.1080/0951192X.2023.2257633
15. 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, 10*(17), 14965–14987. https://doi.org/10.1109/JIOT.2023.3263909.

16. Wu, Z., Zhou, R., Goh, M., Wang, Y., Xu, Z., & Song, W. (2023). A digital twin-based modularized design approach for smart warehouses. *International Journal of Computer Integrated Manufacturing, 37*(10–11), 1404–1425. https://doi.org/10.1080/0951192X.2023.2278100
17. Yang, Y., Li, B., Zhang, S., Zhao, W., & Zhang, H. (2021). Cooperative proactive eavesdropping based on deep reinforcement learning. *IEEE Wireless Communications Letters, 10*(9), 1857–1861. https://doi.org/10.1109/LWC.2021.3084213
18. Zhang, J., & Tai, Y. (2021). Secure medical digital twin via human-centric interaction and cyber vulnerability resilience. *Connection Science, 34*(1), 895–910. https://doi.org/10.1080/09540091.2021.2013443
19. Zhao, T., Foo, E., & Tian, H. (2022). A digital twin framework for cyber security in cyber-physical systems. *arXiv*. https://doi.org/10.48550/arXiv.2204.13859