STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Risk auditing for Digital Twins in cyber physical systems: A systematic review

Shahed Otoom [1]

[1] *Cybersecurity Program, King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan*

ARTICLE INFO

Article History

Received 07 Jan 2025
Accepted 23 Jan 2025
Published 29 Jan 2025

Academic Editor:

Mohammed Almaiah

Vol.2025, No.1

DOI:

https://doi.org/10.63180/jcsra.thestap.2025.1.3

ABSTRACT

Digital Twins are emerging as a transformative technology within Cyber-Physical Systems (CPS), offering enhanced optimization, predictive maintenance, and real-time monitoring. However, their integration also introduces significant security challenges. These include vulnerabilities such as data breaches, unauthorized access, and cyber-attacks that disrupt real-time data flow between their physical and digital components. The involvement of IoT devices, sensors, and complex networked environments expands the attack surface, making Digital Twins susceptible to threats like Distributed Denial-of-Service (DDoS) attacks, malware infiltration, and insider sabotage. Effective risk management and assessment are crucial in identifying vulnerabilities, evaluating risks, and implementing mitigation strategies. Securing Digital Twins ensures data integrity, system reliability, and the continued functionality of the physical assets they represent. This paper aims to classify the various security threats associated with Digital Twins and propose structured risk management approaches to enhance their security within CPS. By addressing these challenges, organizations can ensure the dependability and trustworthiness of Digital Twin implementations across industries such as manufacturing, healthcare, smart cities, and IoT ecosystems.

Keywords: Digital Twins; Cybersecurity; Risk Auditing; Vvulnerabilities; Risk Mmanagement.

How to cite the article

Otoom, S. (2025). Risk auditing for Digital Twins in cyber physical systems: A systematic review. Journal of Cyber Security and Risk Auditing, 2025(1), 22–35. https://doi.org/10.63180/jcsra.thestap.2025.1.3

1. Introduction

Digital Twins are an exciting prospect within Cyber Physical Systems (CPSs), but they also compromise much of the security concerns. They carry vulnerabilities in terms of data breaches, unauthorized access, and cyber-attacks that target and disturb the real-time data flow between their physical and digital components [1]. IoT devices, sensor involvement, and complex networked environments enlarge the attack surface and expose them to threats such as DDoS attacks, malware, or insider sabotage [2]. This turns risk management and assessment into crucial practices, as they help in the identification of weak points, evaluation of risks, and in implementing measures to prevent or respond swiftly to occurrence. Securing Digital Twins ensures that not only are the data handled kept safe, but also the dependability and functionality of the physical assets represented are preserved [3]. The main goal of this paper is to classify these risks and develop strategies for mitigation through thorough research and a structured risk management approach to finally strengthen the security of Digital Twins within CPS [4]. Digital Twins, which are virtual representations of physical systems or processes, are increasingly being adopted across industries such as manufacturing, healthcare, smart cities, and IoT. While they offer significant benefits in terms of optimization, predictive maintenance, and real-time monitoring, they also introduce a range of security challenges. These issues stem from their reliance on interconnected systems, real-time data, and advanced technologies, making them vulnerable to various threats. Addressing these security concerns is critical to ensuring the reliability, safety, and trustworthiness of Digital Twin implementations [5].

The implementation of Digital Twins in CPS offers numerous benefits. They improve operational efficiency through real-time monitoring and process optimization [7]. Decision-making is enhanced with predictive insights powered by AI-driven analytics. Digital Twins help reduce maintenance costs and prevent unexpected downtimes, ensuring better cost efficiency. Moreover, they strengthen security by identifying cyber threats and vulnerabilities before they affect physical systems. Increased reliability is another advantage, as Digital Twins enhance fault detection and failure prediction capabilities [8].

Despite their advantages, Digital Twins face several challenges. High computational requirements for real-time simulations demand significant processing power [9]. Data privacy and security concerns must be addressed to protect sensitive information from cyber threats. Integration complexity remains a challenge, requiring seamless interoperability between digital and physical systems. Additionally, scalability issues arise in large-scale CPS deployments, necessitating efficient data management strategies. Future advancements will focus on leveraging AI, blockchain, and edge computing to enhance the scalability, security, and intelligence of Digital Twins in CPS. As Industry 4.0 and IoT continue to evolve, Digital Twins will play a crucial role in shaping next-generation CPS solutions [10]. Based on above discussion, the main goal of this paper is to classify these risks and develop strategies for mitigation through thorough research and a structured risk management approach to finally strengthen the security of Digital Twins within CPS.

2. Security issues in Digital Twins

One of the primary security issues in Digital Twins is data integrity and authenticity [6]. Digital Twins depend on accurate and reliable data from sensors, IoT devices, and other sources to function effectively. If this data is tampered with or falsified, the Digital Twin may produce incorrect outputs, leading to flawed decision-making and potentially catastrophic consequences. For example, in a manufacturing setting, manipulated data could cause a Digital Twin to misinterpret the condition of machinery, resulting in equipment failure or safety hazards. To mitigate this risk, organizations must implement robust data validation mechanisms, encryption, and digital signatures to ensure the authenticity and integrity of the data being used.

Another significant concern is the vulnerability of Digital Twins to cybersecurity attacks, such as Distributed Denial of Service (DDoS), ransomware, and malware [7]. These attacks can disrupt the functionality of Digital Twins, causing operational downtime or even physical damage to the systems they represent. For instance, a ransomware attack on a Digital Twin controlling a smart grid could lead to widespread power outages. To combat such threats, organizations should deploy advanced cybersecurity measures, including firewalls, intrusion detection systems (IDS), and regular security audits, to identify and address vulnerabilities proactively. Privacy concerns also pose a major challenge for Digital Twins, particularly in industries like healthcare and smart cities, where sensitive personal data is often collected and processed. Unauthorized access to this data could result in privacy breaches, identity theft, or the exposure of proprietary information. For example, a Digital Twin used in a hospital to monitor patient health could become a target for hackers seeking to steal medical records. To protect sensitive data, organizations should employ encryption, access control mechanisms, and anonymization techniques, ensuring that only authorized users can access critical information [8]. The interoperability of Digital Twins with multiple systems, devices, and platforms introduces additional security risks. Since these interconnected systems may have varying security standards, weaknesses in one component could be exploited to compromise the entire Digital Twin ecosystem. For example, a vulnerability in a third-party IoT device connected to a Digital Twin could serve as an entry point for attackers. To address this issue, organizations should adopt standardized protocols and conduct regular security assessments of all connected systems to ensure a consistent level of protection [9].

Physical security risks are another critical concern, as Digital Twins are often linked to physical assets. Compromising a Digital Twin could lead to physical damage or safety hazards in the real world [10]. For instance, an attacker manipulating a Digital Twin controlling an industrial plant could cause machinery to malfunction, resulting in accidents or equipment damage. To mitigate these risks, organizations should implement fail-safes and physical security measures to prevent unauthorized access to both the Digital Twin and the physical systems it represents. The lack of standardization in Digital Twin security practices further exacerbates these challenges. Without universal security standards, organizations may adopt inconsistent or inadequate measures, leaving gaps that attackers can exploit. Developing and adhering to industry-wide security frameworks tailored to Digital Twins is essential to ensuring consistent and robust protection across different implementations [11].

Finally, insider threats and third-party risks also pose significant security challenges. Malicious or negligent actions by employees, contractors, or third-party vendors with access to the Digital Twin system can compromise its integrity. For example, an insider with access to a Digital Twin controlling a smart city's traffic management system could intentionally disrupt operations. To address these risks, organizations should implement strict access controls, conduct regular employee training, and perform thorough security assessments of third-party providers [12].

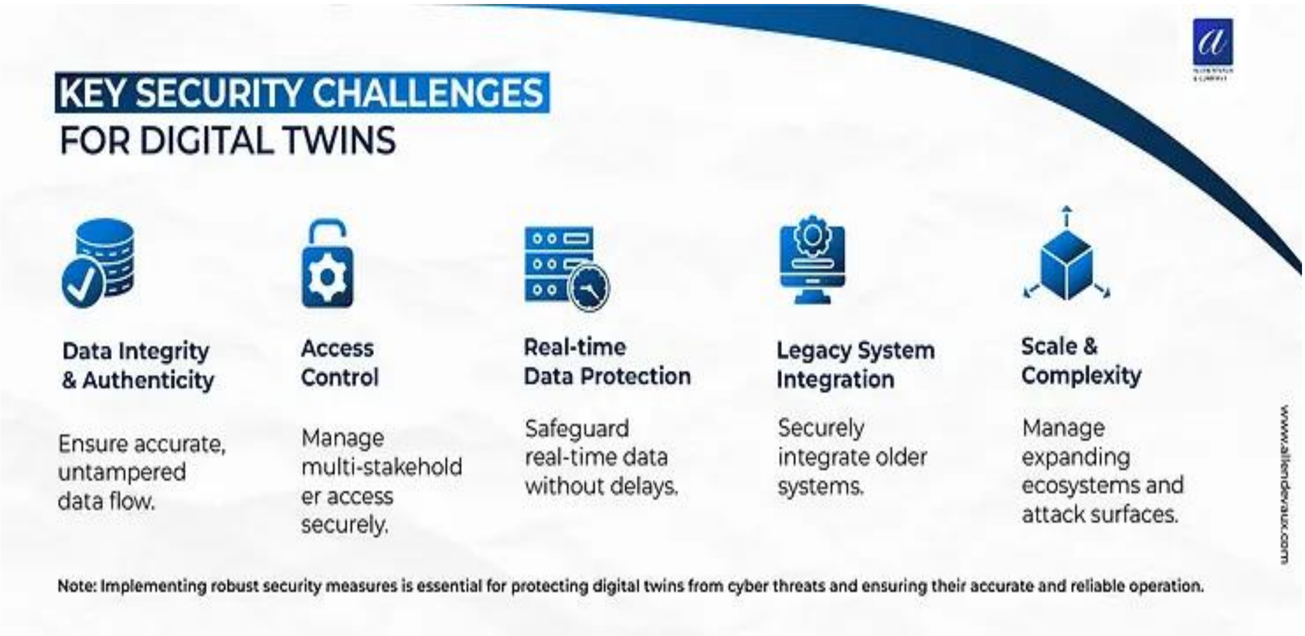

KEY SECURITY CHALLENGES
FOR DIGITAL TWINS
Data Integrity & Authenticity
Ensure accurate, untampered data flow.
Access Control
Manage multi-stakeholder access securely.
Real-time Data Protection
Safeguard real-time data without delays.
Legacy System Integration
Securely integrate older systems.
Scale & Complexity
Manage expanding ecosystems and attack surfaces.
www.allendevaux.com
Note: Implementing robust security measures is essential for protecting digital twins from cyber threats and ensuring their accurate and reliable operation.

Figure 1. Security challenges in Digital Twins.

3. Related Works

Several studies in the literature of cyber physical security systems have been investigated the current security issues related to Digital Twins. For instance, in a study conducted by Alcaraz et al., [1] that provides an in-depth analysis of DT technology in the context of Industry 4.0 and its benefits with a view of associated cybersecurity challenges. DTs are virtual representations of physical assets, used to optimize and simulate processes dependent on interconnected technologies such as IIoT, cyber-physical systems, and edge computing. The very nature of being interconnected exposes them to many vulnerabilities, including software flaws, privilege escalations, insider threats, data manipulations, and attacks such as denial of service (DoS). In this paper, a systematic classification of the risks along the four functional layers of DTs is presented, and a multi-faceted approach to security is emphasized, ensuring data integrity, availability, and confidentiality. Given DTs' critical role in automation and optimization, securing them is essential to prevent disruptions and data breaches that could severely impact industries. Suhail et al., [2], investigate the vulnerabilities of digital twins (DTs), virtual clones of physical systems, in cyber- physical systems (CPS). This work addresses how DTs—that form an integral part of Industry 4.0 and 5.0—can become targets for sophisticated cyberattacks, including reconnaissance, lateral movement, and direct system manipulation. Key vulnerabilities include weak authentication, inadequate data security during lifecycle phases, and low-fidelity simulations—qualities that attackers find lucrative to exploit in the disruption of operations or unauthorized access. To counter these threats, this paper has laid much emphasis on blockchain-based solutions for traceability, role-based access control, gamification for simulated security testing, and intelligent incident response systems for attack detection and mitigation. These measures taken together increase the resilience of digital twins and their physical counterparts against evolving cyber threats.

A study by Varghese [3] explores the utilization of digital twins for the reinforcement of cybersecurity in Industrial Control Systems. It brings forth how DTs, an imitation of physical systems executed in real time, can offer a secure platform for intrusion detection and security testing. The work presented here extends an already existing open-source DT framework by adding an ML-based IDS using a stacked ensemble classifier. This IDS outperformed the standalone ML models regarding accuracy and F1-score and was able to discern efficiently the primary four classes of cyber-attacks: command injection, network Denial of Service (DoS), calculated measurement modification, and naive measurement modification. These scenarios were realized within the DT environment, therefore proving that such an approach will be capable of detecting intrusions in near real time and providing robust cybersecurity solutions without disturbing real operations. In the same way, Carr et al., [4] in their study analyzed the vulnerability of digital twin systems of robotic cyber-physical systems, with a focus on those using the Robot Operating System (ROS). It highlights how Person-In-The-Middle attacks can be performed to intercept and modify the information flow from DT to CPS, resulting in unsafe and unexpected behavior of the robot. Two case studies are presented using an autonomous TurtleBot 3 robot and an industrial Universal Robot 10, demonstrating that such attacks can cause severe safety issues for human operators and surrounding equipment. This paper clearly shows how the current situation also calls for better security strategies for DTS-CPS deployments, more so in safety-critical environments where the introduced measures are insufficient and require further development to safeguard these cyber threats.

On the other hand, Wang et al., [5] investigates an in-depth look at the architecture and enabling technologies of the Internet of Digital Twins (IoDT), a network in which virtual representations synchronize and interact with physical systems to enable advanced data sharing and intelligent operations. It outlines key enabling technologies such as AI, blockchain, and semantic communication, which are most crucial to the growth of IoDT. The big security and privacy issues of data tampering, desynchronization, semantic adversarial attacks, and rogue IoDT devices are discussed, with a focus on potential threats to critical infrastructure. The existing defensive measures, such as blockchain for data integrity, advanced communication protocols, and AI-driven security, are explored in some detail, while future research directions such as decentralization and explainable AI are discussed to improve the security and trustworthiness of IoDT systems. This serves, therefore, as a comprehensive review of proactive security strategies of importance as IoDT evolves to support complex cyber- physical interactions. In addition, Khan et al., [6] explores the application of DT technology in wireless systems, mainly for optimizing their operations based on the analysis of real-time data and proactive management. This paper outlines the high-level architecture of DTs, elaborating on the physical interaction layers and twin layers, and explores deployment strategies like edge-based and cloud-based approaches, which can be done to meet the requirements of latency and resources. The crucial challenges identified are synchronization, data exchange security, and efficient resources management. This study will also present machine learning, blockchain, and federated learning as some of the tools for improving DT performance and security. It concludes with open issues like twin object migration, interoperability across networks, and designing an effective incentive mechanism that will give impetus to the integration of DTs into wireless systems.

A study by Sarker et al., [7], addressed the application of XAI in improving cybersecurity in DT environments. It has been pointed out that DTs, by their very nature—attempts to replicate physical systems for monitoring and predictive analytics, remain vulnerable to threats because of the interconnection of components. AI technologies are crucial for the automation of threat detection and response, but XAI is instrumental in explaining the decisions made by AI and thereby attaining transparency to earn trust. The paper provides the taxonomy of AI/XAI methods, their practical applications in the fields of anomaly detection and incident response and covers the challenges existing between effective automation and human interpretability. It will only close with a call for more research toward the problems of bias in AI models, data quality, and trust in automated cybersecurity decisions within DT ecosystems. In the same way, Jeremiah [8] conducted a review study to explore an in-depth review of how digital twin (DT) technology is revolutionizing such industries as manufacturing, healthcare, energy, and smart city management. DTs are virtual representations of physical objects, integrated with IoT systems that can offer real-time insight and predictive analysis. While it opens many opportunities, it also brings great security risks in the form of breaches of privacy, physical threats, and cyberattacks that can be driven by criminal or political motives. The authors indicate that vulnerabilities often arise from DT's complex and multi-layered architecture. In fighting these issues, the authors find the use of DTs helpful to simulate possible attacks in a system to strengthen defenses. They conclude by emphasizing current research gaps and calling for the development of targeted, layer-specific security measures to make DTs more secure and reliable.

Psaltikidis [9] addressed the complex digital twins' world in cybersecurity and points out the huge risks they are facing, from hardware and firmware issues to software and network attacks. It points out how strong the defense must be in using IDS, anomaly detection tools, firewalls, and network segmentation for keeping DT systems secure. The paper also discusses some innovative solutions, such as digital twin versions of honeypots for gathering intelligence on possible threats and the concept of a "Digital Ghost" that constantly monitors and reacts to anomalies. The authors make clear that while some good mechanisms are already in place, there is a continued need for research collaboration toward developing lightweight and efficient security strategies that will be able to keep pace with new threats. Finally, the paper calls for proactive, tailored approaches to ensure DT systems remain resilient and secure in an increasingly connected world. Sifat et al., [10] establishes how DT technology will be able to shape the management of electrical grids. Combining historical data with real-time information, DTs can strengthen monitoring, support better decision-making, and even predict potential problems before they lead to serious issues. This will provide a procedure for reducing power losses and possibly even preventing blackouts due to automated self-healing procedures. The paper also addresses the additional layer of cybersecurity that blockchain can bring to these DT grids, enabling data sharing in a more secure and transparent way. While advantages such as enhanced grid reliability and efficiency are clear, the study identifies challenges including handling the complexity of real-time data and communication hurdles. In other words, DTs can be the key to a more stable, efficient, and secure way of distributing energy.

3. Analysis and Findings

3.1 Classification of the main threats in the Digital Twins

According to the analysis results for this study in Table 1, the results indicated that Digital Twins affected by many types of threats such as Denial of Service (DoS), reconnaissance attacks, rogue devices attack, command injection attacks and others that should be addressed in order to enhance the security of Digital Twins in cyber physical systems.

Table1. Classification of the main threats in the Digital Twins.

Ref	Type of threats	Place of threats	Description of threats	Impact of threats
Article 1	Software (SW) Attacks	Layer 1 (Physical Space)	Exploiting vulnerabilities in OT device software through bugs and malware.	Operational overhead, data corruption, system inefficiency.
Article 1	Rogue Devices	Layer 1 (Physical Space)	Insertion or tampering of malicious devices to Intercept/manipulate the data.	Data leaks, disruption in data flow, potential data exfiltration.
Article 1	Denial of Service (DoS)	Layer 1 (Physical Space)	Overloading systems to disrupt data flow and operations.	Downtime, operational inefficiency, loss of availability.
Article 2	Reconnaissance Attacks	IT/OT Networks, ICS Environments	Involves gathering intelligence through network scans, exploiting vulnerabilities, and mapping systems.	Allows attackers to identify weak points for deeper attacks.
Article 2	Lateral Movement	Internal Networks, Connected Systems	Attackers move within the system to access sensitive data or control valuable assets.	Leads to compromised assets, prolonged undetected access.
Article 2	Exploitation of Digital Twins	Digital Twin Models	Manipulating digital twins by altering simulation parameters or intercepting updates.	Can cause real- world operational disruptions and data errors.
Article 3	Command Injection Attacks	PLC Interfaces, ICS Network	Exploits the lack of authentication in communication protocols to inject malicious commands that control devices.	Leads to unauthorized changes in operations, affecting process control and potentially causing safety risks.

Article 3	Calculated Measurement Modification	Sensor Data Streams, Network Traffic	An attack that alters sensor data reaching the PLC by scaling values to disrupt operations without detection.	Results in subtle but significant operational errors and compromised decision-making, impacting overall system stability.
Article 3	Naive Measurement Modification	Data Streams in ICS Network	Modifies sensor measurements to random or constant values within operational ranges.	Causes operational inconsistencies and inaccurate monitoring, affecting system reliability and output.
Article 4	Person-In-The-Middle (PitM) Attacks	Communication Channels between DTS and CPS	Interception and modification of data flow from the digital twin to the cyber-physical system.	Leads to altered behavior of the CPS, resulting in potential safety hazards for human operators and nearby facilities.
Article 5	Data Tampering Attack	IoDT Data Lifecycle (Collection, Transmission, Storage)	Manipulation of data streams during collection, transmission, or storage to alter the information processed by digital twins.	Leads to erroneous decision-making by digital twins, impacting physical operations and data integrity.
Article 5	Desynchronization of Digital Twins	Synchronization Channels between Physical Entities (PEs) and Twins	Adversaries interfere with synchronization, causing the digital twin to lose alignment with its physical counterpart.	Results in operational discrepancies and potential safety risks due to unsynchronized data representations.
Article 6	Resource Exhaustion Attacks	Edge and Cloud-Based DT Infrastructure	Attacks that target the resource allocation systems of DTs, leading to depletion of computational or network resources.	Results in reduced performance, delayed data processing, and potential DT unavailability.
Article 6	Synchronization Delay Exploits	DT and Physical Layer Interfaces	Exploiting latency issues in synchronization to create discrepancies between the real system and its DT.	Causes operational misalignment, leading to potential safety hazards and suboptimal performance.
Article 7	Bias Exploitation Attacks	AI Models in DT Cybersecurity Systems	Attacks that exploit inherent biases in AI models to manipulate the outcome of security decisions.	Leads to flawed detection or response processes, resulting in overlooked vulnerabilities and increased susceptibility to attacks.

Article 8	Physical Threats to Infrastructure	Physical and Cyber-Physical Interfaces	Direct attacks targeting the physical components that interact with the DT system to disrupt operations or compromise data flow.	Leads to operational downtime, damage to physical assets, and potential safety hazards.
Article 9	Firmware Manipulation Attacks	Embedded Systems within DT Components	Involves modifying the firmware of DT components to introduce malicious functions or backdoors.	Leads to compromised system integrity, potential data theft, and unauthorized control of DT operations.
Article 9	Honeypot Evasion Techniques	Threat Intelligence Systems	Attackers develop techniques to bypass or avoid detection by DT-based honeypots meant for gathering threat data.	Limits the effectiveness of honeypot-based threat intelligence, leading to undetected infiltration and delayed response.
Article 10	Grid Data Spoofing	Data Transmission Channels	Involves inserting false or misleading data into communication channels to create incorrect grid status updates.	Leads to flawed decision-making, potentially triggering unnecessary or incorrect automated grid responses.

3.2 Classification the main vulnerabilities in the digital twins

According to the analysis results for this study in Table 2, the results indicated that Digital Twins have many types of vulnerabilities such as software bugs and weaknesses, authentication and access control, lack of encryption, vulnerable network architecture and others that should be addressed in order to enhance the security of Digital Twins in cyber physical systems.

Table 2. Classification of the main vulnerabilities in the Digital Twins.

Ref	**Type of vulnerabilities**	**Place of vulnerabilities**	**Description of vulnerabilities**	**Impact of vulnerabilities**
Article 1	Software Bugs and Weaknesses	Layer 1 (Physical Space)	Flaws in the code of OT devices, including legacy software with known issues.	Allows attackers to exploit systems for unauthorized access or control.
Article 1	Authentication and Access Control	Layers 1-3, Communication Space	Weak or outdated authentication mechanisms enabling unauthorized entry.	Leads to privilege escalation, data tampering, and configuration changes.
Article 1	Lack of Encryption	Communication Space	Absence of secure communication protocols, especially in industrial settings.	Data interception and man-in-the- middle (MitM) attacks become easier.

Article 2	Improper Disposal Practices	Decommissioning Phase	Failure to securely dispose of or sanitize digital twin data when no longer needed.	Allows attackers to access archived data and use it for future attacks.
Article 2	Low Fidelity in Digital Twins	DT Simulation and Replication Modes	Digital twins that do not accurately represent their physical counterparts.	Facilitates attacker understanding of system behavior and manipulation.
Article 2	Vulnerable Network Architecture	Internal Networks, Communication Channels	Weak network segmentation or security measures that allow lateral movement.	Enables attackers to spread within the network undetected.
Article 3	Lack of Intrusion Detection Mechanisms	PLC and ICS Network Layers	The absence of inadequacy of mechanisms to detect and respond to cyberattacks in real-time.	Allows attackers to execute process- aware attacks unnoticed, leading to prolonged system compromise.
Article 3	Insufficient Data Validation	Sensor Data Streams and Processing Units	Failing to validate incoming data accurately, allowing modified or false data to be accepted as genuine.	Leads to incorrect system responses and potentially harmful operational decisions.
Article 3	Protocol Vulnerabilities	Communication Protocols in ICS (e.g., ENIP)	Inherent weaknesses in industrial communication protocols that lack built-in security features, such as authentication or encryption.	Enables attackers to manipulate or intercept data, leading to command injections and data tampering.
Article 4	Interception-Prone Communication	Data Transfer Pathways (DTS to CPS)	The communication between the digital twin and CPS can be easily intercepted and modified due to unsecured transfer protocols.	Enables attackers to alter control commands or data, leading to unsafe and unexpected robot actions.
Article 5	Desynchronization Issues	Synchronization Channels in IoDT	Vulnerabilities that allow attackers to interfere with synchronization processes, leading to discrepancies between the physical and virtual representations	Causes misalignment, leading to incorrect system behavior and decision-making in critical operations.
Article 5	Cache Poisoning Attack Vulnerabilities	Information- Centric Caching Systems	Weaknesses that enable attackers to introduce or manipulate cache contents, resulting in polluted or malicious data being stored.	Leads to reduced performance and possible data retrieval issues, impacting the integrity and availability of data.
Article 6	Resource Management Vulnerabilities	Edge and Cloud Infrastructure	Inefficient allocation and management of computational and network resources that can be exploited by attackers.	Can lead to resource exhaustion, reducing system performance and availability.

Article 6	Interoperability Weaknesses	Multi-Vendor and Cross- Network DT Systems	Challenges in ensuring consistent communication and data exchange across heterogeneous systems and vendors.	Creates security gaps that attackers can exploit to introduce malicious data or disrupt operations.
Article 7	Data Quality and Integrity Issues	Data Input and Processing Stages in DTs	Poor data quality or integrity in the datasets used to train or inform AI models, leading to unreliable or compromised outputs.	Reduces the effectiveness of predictive and defensive measures, potentially causing false negatives or false positives in threat detection.
Article 8	Insufficient Monitoring of Digital- Physical Interactions	Cyber-Physical Interfaces	Lack of real-time monitoring of interactions between the DT and its physical counterpart, allowing malicious actions to go unnoticed.	Can result in subtle manipulations that impact physical processes, leading to safety hazards or incorrect outputs.
Article 9	Firmware Integrity Vulnerabilities	Embedded Systems within DT Components	Weak or nonexistent checks for firmware integrity, allowing malicious modifications to go undetected.	Enables attackers to compromise the system at a foundational level, resulting in data theft, loss of control, or unauthorized operations.
Article 9	Inefficient Anomaly Detection Tuning	Anomaly Detection Systems	Poorly configured or under-optimized anomaly detection systems, which can lead to either excessive false positives or missed true threats.	Reduces trust in security systems, leading to potential delays in response and ineffective threat mitigation.
Article 10	Insufficient Redundancy Mechanisms	Backup and Fallback Systems within DTs	A lack of redundant systems to maintain operations during primary system failures or cyberattacks.	Increases the risk of prolonged downtimes or complete system failures when the main system is compromised or disrupted.

3.3 Classification the main countermeasures/security controls for the Digital Twins

Based on the analysis results for this study in Table 3, the results indicated that there types of security controls that should be implemented in the Digital Twins in order to solve the main threats such as software patching and updates, robust authentication mechanisms, encryption and secure protocols, provenance-aware Blockchain solutions, Role-Based Access Control (RBAC), ML-based IDS and others.

Table 3. Classification of the main security controls for the Digital Twins.

Ref	Type of countermeasures	Place of countermeasures	Description of countermeasures	Impact of countermeasures
Article 1	Software Patching and Updates	Layer 1 and Layers 2-3	Regularly updating and patching OT devices, DT servers, and related software.	Reduces vulnerability to exploits and ensures software reliability.
Article 1	Robust Authentication Mechanisms	Layers 1-3, Communication Space	Implementing multi- factor authentication (MFA) and strong access controls.	Enhances access security, reducing the risk of privilege escalation.
Article 1	Encryption and Secure Protocols	Communication Space	Using secure communication protocols (e.g., TLS, HTTPS) for data transfer.	Protects data integrity and confidentiality, mitigating MitM attacks.
Article 2	Provenance- Aware Blockchain Solutions	Digital Twin Lifecycle Phases	Implementing blockchain to create an immutable record for data interactions to ensure traceability.	Enhances data integrity and trustworthiness; helps detect unauthorized changes.
Article 2	Role-Based Access Control (RBAC)	Access Points and Data Management Layers	Assigning permissions based on user roles to restrict access to system components and data.	Reduces unauthorized access and privilege escalation; improves system security.
Article 2	Gamification-Based Security Testing	Testing and Simulation Environments	Using gamified cybersecurity exercises to simulate attack/defense scenarios for evaluating system resilience.	Trains analysts, identifies vulnerabilities, and strengthens response capabilities without affecting live systems.
Article 3	ML-based Intrusion Detection Systems (IDS)	Digital Twin Modules, ICS Network	Implementing machine learning algorithms to detect process-aware attacks in real-time by analyzing system data and identifying anomalies.	Enhances the ability to identify and mitigate a wide range of attacks, improving the overall security posture and response times.
Article 3	Simulation of Attack Scenarios	Digital Twin Environments	Using digital twins to simulate various attack types, such as command injection and data modification, to understand vulnerabilities and test defenses.	Helps in developing effective defense mechanisms and training security teams without risking the actual ICS.

Article 4	Network Traffic Monitoring Tools	DTS-CPS Data Transfer Pathways	Implementing continuous monitoring and analysis tools to detect and prevent malicious activities in real-time.	Improves the detection of anomalies and potential attacks, allowing for rapid response and mitigation.
Article 5	Cache Management Protocols	Information- Centric Caching Systems	Utilizing advanced cache management protocols to prevent cache pollution and poisoning by verifying cache entries.	Enhances data accuracy and availability, mitigating risks of data manipulation and performance degradation.
Article 5	Decentralized Consensus Mechanisms	IoDT Data Management and Governance	Deploying decentralized consensus methods (e.g., blockchain variants) to ensure the integrity of data synchronization and decision-making across twins.	Strengthens data consistency and trustworthiness, preventing data tampering and ensuring resilient operations.
Article 6	Federated Learning for Security	Distributed DT Systems	Implementing federated learning to enhance DT security by training models across distributed nodes without sharing raw data.	Improves privacy and resilience to data breaches, enhancing the overall security of distributed DT systems.
Article 6	Energy-Efficient Resource Allocation	Edge and Cloud Infrastructure	Adopting resource allocation strategies that optimize energy use while maintaining system performance and security.	Reduces vulnerability to resource exhaustion attacks and enhances operational stability and sustainability.
Article 7	Bias Detection and Mitigation Tools	AI Model Training and Deployment Stages	Using specialized tools and frameworks to identify and reduce biases in AI algorithms to enhance fairness and accuracy.	Reduces vulnerabilities that attackers might exploit and ensures more reliable and equitable security decision-making.
Article 8	Incident Response Simulations	DT Security Testing and Training Environments	Conducting real- world incident response drills and simulations within a DT framework to test and improve reaction protocols.	Increases preparedness for actual security incidents, minimizing response time and impact on operations.
Article 9	Firmware Verification Mechanisms	Embedded System Firmware Layers	Utilizing firmware verification protocols that check for authenticity and integrity before any updates or operations.	Ensures that firmware has not been tampered with, protecting against unauthorized changes and enhancing overall system security.

Article 9	Honeypot Digital Twins	Threat Intelligence and Monitoring Systems	Deploying digital twin versions of honeypots to attract, study, and collect data on potential cyber attackers.	Provides valuable threat intelligence, helping to identify and counter emerging threats while reducing the risk of undetected infiltration.
Article 10	Redundant System Architectures	DT Backup and Fallback Systems	Developing redundant systems that can take over during a failure of primary DT components or during cyber incidents.	Improves system resilience, reducing downtime and maintaining operations even in the face of attacks or technical failures.

3.3 Mapping between the threats, vulnerabilities and countermeasures

Table 4. Mapping between the threats, vulnerabilities and countermeasures

Type of threats	**Type of vulnerabilities**	**Type of countermeasures**
Software (SW) Attacks	Software Bugs and Weaknesses	Software Patching and Updates; ML-based Intrusion Detection Systems (IDS)
Rogue Devices	Authentication and Access Control	Robust Authentication Mechanisms; Role-Based Access Control (RBAC)
Denial of Service (DoS)	Resource Management Vulnerabilities	Energy-Efficient Resource Allocation; Redundant System Architectures
Reconnaissance Attacks	Vulnerable Network Architecture	Network Traffic Monitoring Tools; Simulation of Attack Scenarios
Lateral Movement	Vulnerable Network Architecture	Network Traffic Monitoring Tools; Role-Based Access Control (RBAC)
Exploitation of Digital Twins	Low Fidelity in Digital Twins	Simulation of Attack Scenarios; Gamification-Based Security Testing
Command Injection Attacks	Protocol Vulnerabilities	Encryption and Secure Protocols; Firmware Verification Mechanisms
Calculated Measurement Modification	Insufficient Data Validation	ML-based Intrusion Detection Systems (IDS); Real-Time Data Integrity Checks
Naive Measurement Modification	Insufficient Data Validation	Encryption and Secure Protocols; Incident Response Simulations
Person-In-The-Middle (PitM) Attacks	Interception-Prone Communication	Robust Authentication Mechanisms; Adaptive Communication Protocols

Data Tampering Attack	Data Quality and Integrity Issues	Provenance-Aware Blockchain Solutions; Real- Time Data Integrity Checks
Desynchronization of Digital Twins	Desynchronization Issues	Decentralized Consensus Mechanisms; Adaptive Communication Protocols
Resource Exhaustion Attacks	Resource Management Vulnerabilities	Energy-Efficient Resource Allocation; Redundant System Architectures
Synchronization Delay Exploits	Communication Latency Vulnerabilities	Adaptive Communication Protocols; Scalable Data Processing Frameworks
Bias Exploitation Attacks	Bias in AI Algorithms	Bias Detection and Mitigation Tools; Explainable AI (XAI) Implementation
Physical Threats to Infrastructure	Insufficient Monitoring of Digital-Physical Interactions	Incident Response Simulations; Redundant System Architectures
Firmware Manipulation Attacks	Firmware Integrity Vulnerabilities	Firmware Verification Mechanisms; ML-based Intrusion Detection Systems (IDS)
Honeypot Evasion Techniques	Reactive Defense Limitations	Honeypot Digital Twins; Gamification-Based Security Testing
Grid Data Spoofing	Data Quality and Integrity Issues	Real-Time Data Integrity Checks; Provenance-Aware Blockchain Solutions

5. Conclusion

Digital Twins have emerged as a transformative technology within Cyber-Physical Systems (CPS), offering substantial benefits across various industries, including manufacturing, healthcare, smart cities, and IoT. However, their integration into these interconnected environments also presents significant security challenges. Threats such as data breaches, unauthorized access, and cyber-attacks, including DDoS, malware, and insider sabotage, pose substantial risks to the integrity and reliability of Digital Twins. The complexity of these systems, coupled with real-time data exchange and sensor dependencies, further expands the attack surface, making security a critical concern. To mitigate these risks, a structured approach to risk management and assessment is essential. Identifying vulnerabilities, evaluating potential threats, and implementing robust security measures can enhance the resilience of Digital Twins against cyber threats. By ensuring the security of Digital Twins, organizations can maintain data integrity, protect critical infrastructure, and preserve the functionality of physical assets. Moving forward, continued research and the development of advanced security frameworks will be key to strengthening the protection of Digital Twins, ensuring their safe and effective deployment in CPS.

Conflicts Of Interest

The authors declare no conflicts of interest.

Funding

No funding.

Acknowledgment

References

[1] Alcaraz, C., & Lopez, J. (2022). Digital twin: A comprehensive survey of security threats. *IEEE Communications Surveys & Tutorials*, *24*(3), 1475-1503.

[2] Suhail, S., Jurdak, R., & Hussain, R. (2022). Security attacks and solutions for digital twins. *arXiv preprint arXiv:2202.12501*.

[3] Varghese, S. A., Ghadim, A. D., Balador, A., Alimadadi, Z., & Papadimitratos, P. (2022, March). Digital twin-based intrusion detection for industrial control systems. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)* (pp. 611-617). IEEE.

[4] Carr, C., Wang, S., Wang, P., & Han, L. (2022). Attacking digital twins of robotic systems to compromise security and safety. *arXiv preprint arXiv:2211.09507*.

[5] 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.

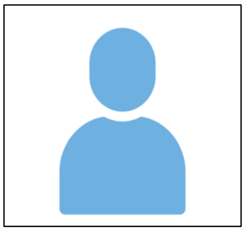
[6] Khan, L. U., Han, Z., Saad, W., Hossain, E., Guizani, M., & Hong, C. S. (2022). Digital twin of wireless systems: Overview, taxonomy, challenges, and opportunities. *IEEE Communications Surveys & Tutorials*, *24*(4), 2230-2254.

[7] Sarker, I. H., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. (2024). Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express*.

[8] Jeremiah, S. R., El Azzaoui, A., Xiong, N. N., & Park, J. H. (2024). A Comprehensive Survey of Digital Twins: Applications, Technologies and Security Challenges. *Journal of Systems Architecture*, 103120.

[9] Psaltikidis, T. (2024). Digital twins security, privacy and safety: threats, risks and measures.

[10] Sifat, M. M. H., Choudhury, S. M., Das, S. K., Ahamed, M. H., Muyeen, S. M., Hasan, M. M., ... & Das, P. (2023). Towards electric digital twin grid: Technology and framework review. *Energy and AI*, *11*, 100213.



Shahed Otoom in Cybersecurity program from the University of Jordan, Jordan. Her research interests include cybersecurity, cybersecurity risk assessment and cryptographic .